भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान मोहाली

शिक्षा मंत्रालय, भारत सरकार द्वारा स्थापित

सैक्टर 81,नॉलेज सिटी,प. ओ. मनोली, एस. ए. एस. नगर, मोहाली, पंजाब 140306

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH MOHALI

(Established by Ministry of Education, Govt. of India)

Sector-81, Knowledge city, PO-Manauli, SAS Nagar Mohali-140306, Punjab

PAN No. - AAAAI1781K GSTIN – 03AAAAI1781K2ZS

• Phone : +91-172- 2240121 • Fax : +91-172-2240124 • http://www.iisermohali.ac.in • Email: tenders@iisermohali.ac.in

CPPP/Institute Website

IISERM(1726)26/27-Pur Dated: 19th September 2026

ई - निविदा आमंत्रण सूचना

NOTICE INVITING E-TENDER

Online tenders are invited on behalf of the Director, IISER Mohali in **TWO BID SYSTEM** for **Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure for IISER Mohali** as per technical specification and details given below and BOQ list from the original manufacturer/supplier at CPPP i.e. **https://eprocure.gov.in/eprocure/app**. Tender documents may please be downloaded from the E-procurement portal website **https://eprocure.gov.in/eprocure/app** & Institute website **www.iisermohali.ac.in.**

Sd/-
सहायक कुलसचिव (क्रय तथा भंडार)
Assistant Registrar (Stores & Purchase)

NOTE: **This is a domestic Tender according to the DPIIT Order dated 15/07/2017, 04.06.2020 and subsequent amendments to the order for Public Procurement Preference & PROVISION FOR LOCAL SUPPLIERS TOWARDS PREFERENCE TO MAKE IN INDIA. The bidder required to declare on the letter head the percentage of Local content for the quoted instrument and submit with the Technical Bid. Bidder should also give details of the location(s) at which the local value addition is made.**

भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान मोहाली

शिक्षा मंत्रालय, भारत सरकार द्वारा स्थापित

सैक्टर 81,नॉलेज सिटी,प. ओ. मनोली, एस. ए. एस. नगर, मोहाली, पंजाब 140306

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH MOHALI

(Established by Ministry of Education, Govt. of India)

Sector-81, Knowledge city, PO-Manauli, SAS Nagar Mohali-140306, Punjab

PAN No. - AAAAI1781K GSTIN – 03AAAAI1781K2ZS

• **Phone : +91-172- 2240121** • **Fax : +91-172-2240124** • **http://www.iisermohali.ac.in** • **Email:** tenders@iisermohali.ac.in

CPPP/Institute Website

ई - निविदा आमंत्रण सूचना/NOTICE INVITING E-TENDER

Tender Ref.- IISERM(1726)26/27-Pur	19th September 2026

Critical Date Sections

Sr.	Description	Date	Time
1.	Tender Publishing Date and time	19th September 2026	6:00pm
2.	Tender Document download start Date & Time	19th September 2026	6:00pm
3.	Bid Submission start Date & Time	19th September 2026	6:00pm
4.	**Pre-Bid Meeting** Offline Mode (Admin Building)	**5th October 2026**	**11.00am**
5.	Bid Submission End date and Time	13th October 2026	Upto 2:30pm
6.	Tender opening Date and Time	14th October 2026	At 3:30pm

1. Online tenders are invited on behalf of the Director, IISER Mohali in **TWO BID SYSTEM** for following item(s) from the original manufacturer/supplier at CPPP i.e. **https://eprocure.gov.in/eprocure/app**. Tender documents may please be downloaded from the E-procurement portal website **https://eprocure.gov.in/eprocure/app** & Institute website **www.iisermohali.ac.in.**

2. Online Tender fee of Rs 590/- (Non-refundable) should be submitted by bidder favoring Registrar, IISER Mohali through NEFT/RTGS as per account details given below. UTR copy to be uploaded along with the technical bid.

3. EARNEST MONEY DEPOSIT (EMD): Tenderer must submit EMD of **Rs. 28,12,000/-** (Rupees Twenty Eight Lakhs and Twelve Thousand Only) in the format of e-payment / BG **irrespective of the items quoted i.e. schedule wise EMD amount as mentioned in the document will not be considered. Without EMD, the tender will be summarily rejected.**

A Bank Guarantee of equivalent amount from any Indian Nationalized bank/Scheduled Commercial Banks in a prescribed format **(Format enclosed below in Appendix-I)** favoring Registrar, IISER Mohali. BG should be valid for a period of 6 months. BG is also extendable depending on requirement. Original Scanned copy of Bank Guarantee needs to be uploaded along with tender which will be verified at the time of tender opening. **Original BG/FDR/DD/ISB copy needs to be send by Post/Courier immediately to Assistant Registrar (S&P), Sector-81, Knowledge city, PO-Manauli, SAS Nagar Mohali-140306, Punjab & it needs to be received within 05 days from the date of tender opening. Non receipt of the hard copy may lead to rejection of the bid. (OR)**

Online E-Payment shall be made through RTGS as per the details given below. However, online payment details i.e. UTR no and proof of current money transaction details are to be enclosed with our technical bid/tender:

Name: IISER Mohali
Account Number 4790101001912
Canara Bank, IISER Mohali Branch
IFSC : CNRB0004790

a) Request for adjustment of dues from the Corporation towards EMD will not be entertained.

b) **Refund of EMD :-** The EMD of the bidders whose bids are not qualified/not acceptable will be refunded after finalization of tender in the form of e-payment to those bidders who deposited EMD in the form of e payment, without any interest, upon receipt of a written request by the bidder after deducting bank charges, if any. Those who submitted EMD in the form of BGs, the same will be returned duly to the unsuccessful bidders. For successful bidders, EMD will be returned after submission of Security Deposit / PBG (if applicable).

c) **MSMEs in India registered with appropriate authority as per latest notification shall be exempted from EMD payment provided they are registered for the item being quoted. Micro & MSME/NSIC and Firms registered and the firms registered with concerned Ministries/ Departments, the bidders are exempted from payment of Tender Fee/EMD as per GOI notifications/GFR (2017) and Ministry of Finance OM No. F.9/4/2020-PPD dated 12 November 2020.**

d) IISER Mohali will not be responsible for any delayed receipt of Original EMD/BG etc. caused by postal authorities/courier services and loss in transit or delay.

ITEM WISE DETAILS

S.No.	Description	Qty.
1.	**Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure for IISER Mohali** **Technical specifications & Terms and Conditions: Refer to APPENDIX-VI**	**As per list and APPENDIX -VI**

A) IMPORTANT NOTES:-

I. **This is a domestic Tender according to the DPIIT Order dated 15/07/2017, 04.06.2020 and subsequent amendments thereof for Public Procurement Preference & PROVISION FOR LOCAL SUPPLIERS TOWARDS PREFERENCE TO MAKE IN INDIA. Bidders should also give details of Location(s); at which the local value addition is made. Bidders are requested to furnish the declaration regarding local content/locations in Appendix-II through CPPP portal.**

II. **Restriction under Rule 144 (xi) of the General Financial Rules (GFRs), 2017 under sub clause 3, in terms of DOE, MoF No. F.18/37/2020-PPD dated: 8th February, 2021 & further amendments thereon:**

(i) A bidder is permitted to procure raw material, components, sub-assemblies etc. from the vendors from countries which shares a land border with India. Such vendors will not be required to be registered with the Competent Authority, as it is not regarded as "sub-contracting".

(ii) However, in case a bidder has proposed to supply finished goods procured directly/indirectly form the vendors from the countries sharing land border with India, such vendor will be required to be registered with the Competent Authority. Kindly submit the declaration in Appendix IV.

III. The Online bids should be submitted directly by the original manufacturer/supplier/OEM, the OEM is required to furnish certificate to this effect. If quotation is submitted/filled by any representative/ agent/dealer then they must upload a Authorization certificate from the principal company/OEM.

IV. The online updated Price BOQ is in INR format. Bids are invited in INR only against domestic tender.

V. All MSME/NSIC/Startup Units shall be considered as per provisions/rules prescribed by Govt of India.

VI. Auto-extension of last date for E-Tenders has been activated by CPP Portal which has participation 2 bids or less.

B) SUBMISSION OF TENDER

I. All bid/tender documents are to be uploaded online at Central Public Procurement portal i.e. **https://eprocure.gov.in/eprocure/app** only and in the designated cover/ part on the website against tender ID. Tenders/ bids shall be accepted only through online mode and no manual submission of the same shall be entertained. Also upload **Appendix-I** (BG Format) if registered as **Micro & MSME/NSIC and Firms registered and the firms registered with concerned Ministries/ Departments.** Late tenders will not be accepted.

II. The online bids shall be opened at the office of the Assistant Registrar (S&P), IISER Mohali, on above given date and time. If the tender opening date happens to be on a holiday or non-working day due to any other valid reason, the tender opening process will be attended on the next working day at same time and place. IISER Mohali will not be responsible for any error like missing of schedule data while downloading by the

Bidder.

III. **The bidder shall upload the tender documents/NIT duly filled in and stamped by the authorized signatory on each and every page along with all necessary Appendixes as per NIT along with checklist. Tender not submitted/uploaded with the prescribed proforma/formats (Appendixes) as per the NIT, the bids will be rejected.**

Check List of Documents (signed & stamped) to be provided and uploaded by the bidder:

S. No.	Particulars of Documents	Yes/No	Page No. (As per technical bid)
1.	**Tender Notice Document Copy of NIT** **(duly signed and stamped in all pages)**		
2.	**EMD as per Appendix-I OR EMD remittance details (UTR/NEFT/RTGS)** **(issued by nationalized / schedule commercial bank in prescribed format)**		
3.	**Declaration of Local content/MII, with complete information (if applicable), Appendix-II (on letter head duly signed and stamped)**		
4.	**Technical Compliance Sheet** (product catalogue etc. with all technical specifications) **(on letter head duly signed and stamped)**		
5.	**Pre Bid Integrity Pact: In Appendix-III** **(duly signed in letter head with witnesses)**		
6.	**Land border sharing declaration in Appendix-IV**		
7.	**Non-blacklisting declaration, solvency certificates: In Appendix-V**		
8.	**Authorization/MAF Certificate** from OEM (principal)/Manufacturer certificate, if applicable **(signed and stamped copy)**		
9.	**Tender Fee**, if applicable or Exemption Certificate (NSIC/MSME Certificate) **(duly signed and stamped)**		
10.	**Attach Copy of PAN**		
11.	**Attach Copy of GST**		
12.	**Copy of pre-bid participation certified**		

**** If checklist is not provided by the bidder along with ABOVE DOCUMENTS (signed and stamped copy of NIT) the bid shall be summarily rejected.***

IV. The bidder shall upload scanned copy of the PAN Card, GST number duly signed and stamped. **Also bidders applying against "MSME/NSIC Certificate" issued by appropriate Authority, should ensure that the certificate attached is relevant to the area of service/supply. For example, If the tender is for "supply & installation of Desktop"** ***the certificate should be issued for activity/area of "Computer supply and services activities etc" otherwise bid will be REJECTED without notice.***

V. E-procurement system ensures locking on the scheduled date and time. The system will not accept any bid after the scheduled date and time of submission of bid.

C) INSTRUCTIONS

1. The Online bids should be submitted directly by the original manufacturer/supplier, If bid is submitted/filled by any representative/agent/dealer then they must upload a authority certificate from the principal company for quoting the price otherwise such bid will be rejected.

2. **The firms should be registered with GST Authorities. A valid PAN /GST Number of the tenderer has to be provided/enclosed/upload with a copy of proof with self attested. PAN and GST Number are required for both as below:**

    i) **Principal Company and**

    ii) **Authorised dealer/distributor/channel partner.**

3. The quantity mentioned in this enquiry is and shall be deemed to be only approximate and will not in any manner be binding on the Institute. Before the deadline for submission of the online bid, IISER Mohali reserves the right to modify the tender document terms and conditions. Such amendment/modification will be notified on website against said tender ID.
4. The rates offered should be FOR Chandigarh/Mohali in case of firms situated outside Chandigarh/Mohali, and free delivery at the Institute premises in case of local firms. Conditional tenders will be summarily rejected.
5. In case of Ex-godown terms the amount of packaging forwarding freight etc. should clearly be indicated by percentage or lump sum amount. Institute has policy not to make any advance payments towards any purchase, Letter of credit can be opened if required.
6. **Custom Duty as applicable, as per GOI Rules**.
7. **GST as applicable, as per GOI Rules**.
8. The work shall be carried out as per the specifications asked and as per the instructions of the Institute Authorities
9. The contractor shall deploy sufficient number of resources to complete the work within timeline mentioned.
10. The contractor has to clear and remove all contractor's equipment, surplus material, debris, waste material before issuance of completion certificate.
11. Non-responsive/Incomplete bids in any aspect shall become liable for rejection.
12. **EMD EXEMPTION:** The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this policy.
13. **The bidders are requested to provide/upload detailed description and specifications together with the detailed drawings, printed leaflets & literature of the article quoted** and also should enclose **Technical Compliance Sheet along with quoted product/material with make and model.** The name of the manufacturers and country of manufacture should also invariably be stated. In the absence of these particulars and documents, the quotation is liable for rejection. Tenders not accompanied by detailed information as required, are liable to be rejected.
14. **Preference to Make In India products (For bids < 200 Crore):** Preference shall be given to Class 1 local supplier as defined in public procurement (Preference to Make in India), Order 2017 as amended from time to time and its subsequent Orders/Notifications issued by concerned Nodal Ministry for specific Goods/Products. The minimum local content to qualify as a Class 1 local supplier is denoted in the bid document. If the bidder wants to avail the Purchase preference, the bidder must upload a certificate from the OEM regarding the percentage of the local content and the details of locations at which the local value addition is made along with their bid, failing which no purchase preference shall be granted. In case the bid value is more than Rs 10 Crore, the declaration relating to percentage of local content shall be certified by the statutory auditor or cost auditor, if the OEM is a company and by a practicing cost accountant or a chartered accountant for OEMs other than companies as per the Public Procurement (preference to Make-in -India) order 2017 dated 04.06.2020. Only Class-I and Class-II Local suppliers as per MII order dated 4.6.2020 will be eligible to bid. Non - Local suppliers as per MII order dated 04.06.2020 are not eligible to participate. However, eligible micro and small

enterprises will be allowed to participate. The buyers are advised to refer the OM No.F.1/4/2021-PPD dated 18.05.2023 OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017.

15. Purchase preference will be given to MSEs having valid Udyam Registration and whose credentials are validated online through Udyam Registration portal as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail themselves of the Purchase preference, the bidder must be the manufacturer / OEM of the offered product. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises and hence resellers offering products manufactured by some other OEM are not eligible for any purchase preference. In respect of bid for Services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service and Buyer will decide
eligibility for purchase preference based on documentary evidence submitted, while evaluating the bid. If L-1 is not an MSE and MSE Seller (s) has / have quoted price within L-1+ 15% (Selected by Buyer) of margin of purchase preference /price band defined in relevant policy, such MSE Seller shall be given opportunity to match L-1 price and contract will be awarded for 25% (selected by Buyer) percentage of total quantity. The buyers are advised to refer the OM No. F.1/4/2021-PPD dated 18.05.2023 OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017.

16. **Work Completion Certificate:** Wherever Bidders are insisting Work Completion Certificate from the Buyer, same shall be provided in Buyer's standard format only.

17. **Manufacturer Authorization:** Wherever Authorised Distributors/service providers are submitting the bid, Authorisation Form /Certificate with OEM/Original Service Provider details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid.

18. Bidder's offer is liable to be rejected if they fail to upload any of the certificates / documents sought in the Bid document and Corrigendum if any.

19. **Delivery, Unloading, Shifting and Safety:** The supplier shall be solely responsible for the safe and timely delivery of the material/equipment to the concerned Research/Teaching Laboratory or the Institute Works Department (IWD), as applicable, including unloading, handling, transportation within the Institute premises, and shifting to the designated location. The bidders are advised to inspect the installation site and transit routes prior to supply, the Institute shall not be responsible for any extra payment incurred OR any casualty happened due to site constraints viz. narrow passages, lift capacities, staircases, etc. The supplier shall remain fully and unconditionally liable for any accident, injury or fatality occurring to any personnel/ labour on the Institute premises and further, the Institute shall also bear no employer-employee relationship, statutory liability or financial obligation whatsoever with respect to any personnel/labour engaged by or on behalf of the supplier. The supplier shall provide and ensure the mandatory use of appropriate personal protective equipment (PPE), tools, tackles, lifting/handling equipment, and other safety arrangements commensurate with the nature of the work. All personnel engaged in such activities shall be adequately trained, competent, and medically fit, wherever required, and shall be supervised directly by the supplier or its authorised representative on-site. The supplier shall comply with all applicable Central/State Government laws, rules, regulations, labour laws, and occupational safety requirements including the Employees' Compensation Act and instructions/guidelines issued by the Government of India and other competent authorities from time to time, as well as the safety and security instructions of the Institute. The supplier shall be responsible for obtaining any required permissions and for ensuring that the work does not cause injury, damage to persons/property, or disruption to Institute activities. The supplier shall fully indemnify, defend and hold harmless the Institute, its officials and employees against all claims, liabilities, losses, damages, legal costs and expenses arising out of any injury, disability or fatality of personnel, damage to Institute property, or third-

party claims during the execution of this work. Any damage caused to the Institute's infrastructure, buildings, or equipment must be rectified by the supplier at their own cost within seven (7) days of notification. In the event that unloading and/or shifting is carried out using the Institute's resources, the actual charges incurred in this regard shall be borne by the Supplier. Such use of Institute resources shall be at the sole request of the supplier and acceptance by the Institute. The arrangement made by the Institute shall not relieve the supplier of its responsibility for ensuring compliance with applicable safety requirements, structural liability and Government/Institute instructions.

20. If any information furnished by the bidder is, at any stage found to be incorrect, false or fabricated, the Institute/purchaser shall have the absolute right to forfeit E.M.D. and PBG/security deposits, in addition to cancellation of contract, forfeiting the warranty/performance Guarantees and other action in accordance with law, such as black-listing, risk & cost etc.
21. Validity of offer: 180 days.
22. Security deposit/Performance Bank Guarantee @ 5% of the value of supply order as per norms may be sought from the firms, in terms of Ministry of Education, GOI, OM No. F. No. 29-1/2019-IFD dated 06th April, 2023 for compliance of Ministry of Finance, DoE, GOI, OM No.F.1/2/2023-PPD dated 03.04.2023.
23. **LIQUIDATED DAMAGES :** Being an Educational Institute, time is essence of the order. The date of delivery should be strictly adhered to. Otherwise this Institute reserves the right to not accept the delivery in part or full. The Liquidated damages @ 0.5% per week subject to a maximum of 10% of the value of the order can be imposed. In order to avoid double penalties, the penalties mentioned at Page No. 42-43 for delay as per Section-6 implementation timeline would be adjusted against the overall applicable LD.
24. **Pre-Bid Integrity Pact:-**
    - **a)** The Pre-Bid Integrity Pact as per Appendix-III is to be mandatorily submitted by the bidder on Rs. 100 stamp paper duly signed by the bidder and witnesses along with details like names and address of the witnesses. All bidder shall have to upload scanned copy of the Integrity Pact complete in all respects, duly signed & signed with of bid document.
    - **b)** Non-Submission of complete Integrity Pact as above may lead to disqualification and bid will not be evaluated further.
25. **Pre-Bid Meeting:** The Prospective Bidders shall attend pre-bid meeting as per schedule (date and time) mentioned in the critical date sections (page-2 of NIT). The pre-bid meeting will be held in offline mode. If bidder wishes to make a site visit, they may complete the site visit at least two (2) days prior to the pre-bid meeting. The site visit shall be conducted only after obtaining prior approval from the Institute by sending email to tenders@iisermohali.ac.in. Further, if any bidder wishes to make a site visit on day of pre-bid meeting, they may undertake the visit, however, no additional queries related to site visit would be entertained afterward.

    In person participation in the pre-bid meeting is mandatory for all intending bidders due to the technical and site-specific nature of the work. A Participation Certificate shall be issued to the participating bidder and the same shall be submitted along with the bid. **Failure to participate and/or submit the Participation Certificate shall render the bid liable to be treated as non-responsive and rejected**
26. The right to reject all or any of the quotation and to split up the requirements for itemized L-1 or relax any or all the above conditions without assigning any reason is reserved by the IISER Mohali. For any corrigendum and addendum please keep checking the website https://eprocure.gov.in/eprocure/app and http:/www.iisermohali.ac.in

27. The bidder should submit the Non-blacklisting declaration as per **Annexure V.**

28. For any queries kindly email : tenders@iisermohali.ac.in

29. Disputes, if any, shall be subject to jurisdiction of the Competent courts of SAS Nagar Mohali, Punjab subject to applicable laws and statutory provisions only.

-Sd/-
सहायक कुलसचिव (क्रय तथा भंडार)
Assistant Registrar (Stores & Purchase)

APPENDIX-I

PROFORMA FOR BANK GUARANTEE TOWARDS EMD
(TO BE USED BY ALL NATIONALISED BANKS/ SCHEDULED COMMERCIAL BANKS)

Ref. Bank Guarantee No.
Date:

To
The Registrar
Indian Institute of Science Education and Research Mohali
Sector – 81, Knowledge City,
PO – Manauli, SAS Nagar,
Mohali – 140 306, Punjab.

Dear Sir,

WHEREAS M/s. _____ having its registered office at _____ (hereinafter called "the supplier") has undertaken in pursuance of Tender No. _____ Dated _____ against Supply of _____ (hereinafter called "the order")

AND WHEREAS it has been stipulated by you in the said order that the Supplier shall furnish you with a bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the supplier's performance obligations in accordance with the order.

AND WHEREAS We, _____ Bank a body Corporate constituted under _____ having its Head Office at _____, having amongst others a branch office at _____ (hereinafter referred to as the "The Bank" which expression shall unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and assignees) have agreed to give the Supplier a Guarantee at the request of the supplier.

THEREFORE, WE _____ Bank hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of Rs. _____ [Rupees _____ Only] and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limits of _____ [Rupees _____Only] as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until _____.

Notwithstanding anything contained hereinabove.

i) Our liability under this Bank Guarantee shall not exceed Rs. _____ [Rupees _____only]
ii) This Bank Guarantee shall be valid upto _____.
iii) We are liable to pay the guaranteed amount or any part hereby under this bank guarantee only and only if you serve upon us a written claim or demand on or before _____.

Dated the _____ day of _____ 2026.

APPENDIX -II

SELF DECLARATION
[For Local Content of Products, Services or Works]

File/Tender No. ……..
Tender ID: …….. Dated: ……

To,

The Director
Indian Institute of Science Education and Research
(Established by Ministry of Education, Govt. of India)
Sector-81, Knowledge city, PO-Manauli,
SAS Nagar Mohali-140306, Punjab

1. With reference to Order no P.-45021/2/2017 PP (BE-II) dated 04.06.2020 and No. P-45021/2/2017-PP(BE-II) dated 16-09-2020 of DPIIT, Ministry of Commerce and Industry, Govt. of India, we fall under the following category of supplier (**please tick the correct category**) for the items for which this tender has been floated and being bided.

   - ☐ Class I local supplier – has local content equal to more than 50%. Local contents added at _____ (name of location).
   - ☐ Class II local supplier – has local content more than 20% but less than 50%. Local contents added at _____ (name of location).
   - ☐ Non-local supplier – has local content less than or equal to 20%. Local contents added at _____ (name of location).

2. We are solely responsible for the abovementioned declaration in respect of category of supplier. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules for which we may be debarred for up to 2 years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

Signature & seal of the company

Name and address of the organization
…….
…….
…….

Date: ……

Note: In cases of procurement for a value in excess of Rs. 10 crores, the 'Class-I local supplier' / 'Class-II local supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

* To be provided in company letter head duly signed and stamped.

APPENDIX -III

PRE BID INTEGRITY PACT

General

This pre-bid Agreement (hereinafter called the Integrity Pact) is made on _____ day of the month of _____ 2026, between, on one hand, the Director, IISER Mohali, Ministry of Education /Department, Government of India (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s _____ _____represented by Shri_____ Bidder or its authorized representative (hereinafter called the "BIDDER/Seller" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to procure (Name of the Stores/Equipment/Item) and the BIDDER/Seller is willing to offer/has offered the stores and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Ministry of Education/Department of the Government of India performing its functions on behalf of the President of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

Enabling the BUYER to obtain the desired said stores/equipment at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the bid/contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organisation or third party related to the bid/contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

Commitments of BIDDERs

3. The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.

3.3* BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4* BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5* The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator/authorised government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.

The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. <u>Previous Transgression</u>

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. <u>Earnest Money (Security Deposit)</u>

5.1 While submitting commercial bid, the BIDDER shall deposit an amount Rs. 28,12,000/- (Rupees Twenty-Eight Lakhs and Twelve Thousand Only as Earnest Money/Security Deposit, with the BUYER through any of the following instruments:

(i) Bank Draft or a Pay Order in favour of

(ii) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

(iii) Any other mode or through any other instrument (to be specified in the RFP).

5.2 The Earnest Money/Security Deposit shall be valid upto a period of one year or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions; wherever required:-

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

(iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilised to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.

(viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.

(x) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

7.1 The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry of Education/Department of the Government of India and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry of Education/Department of the Government of India at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given).

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 7 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful this Integrity Pact shall expire after six months from the date of the signing of the contract.

12.2 Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at _____ on _____

BUYER Name of the Officer. Designation IISER, MOHALI Deptt./MINISTRY of Education Govt. of India	BIDDER Bidder or its authorized representative
Witness 1. _____ 2. _____	Witness 1. _____ 2. _____

*Provisions of these clauses would need to be amended/deleted in line with the policy of the BUYER in regard to involvement of Indian agents of foreign suppliers.

APPENDIX -IV

(To be submitted on the letterhead of the company/firm)

CERTIFICATE BY THE BIDDER (FOR TENDERS)

I have read the clause regarding restrictions on procurement from bidder of as country which shares a land border with India.

- Kindly select the relevant field, whichever is applicable:-

  ☐ I certify that this bidder is not form such a company

  OR

  ☐ If from such a country, has been registered with the Competent Authority (copy of Registration Certificate enclosed).

I hereby certify that the bidder fulfills all requirements in this regard and is eligible to be considered. This is in terms of Restriction under Rule 144 (xi) of the General Financial Rules (GFRs) 2017 under sub clause 3, in terms of DOE, MoF No. F.18/37/2020-PPD dated: 8th February, 2021.

Date: Name of the company/firm/organization

Place: Signature with Date and stamp of the bidder

APPENDIX -V

CERTIFICATE FOR NON-BLACK LISTING

We. (Name of firm) do hereby certify that our company/firm/Manufacturers / Suppliers/ Dealers has not been black listed/banned /suspended/ debarred by any Government Department/Govt. Educational/Research Institute during the last three years.

Place:
Date:

Signature of Authorized Signatory
……
……Name of Signatory

APPENDIX -VI

Design, Supply, Installation, Testing, Commissioning, Integration and Support of Core Network Infrastructure for IISER Mohali

Contents

Section – 1: Introduction....20
Section – 2: Objective....20
Section – 3: Scope of Work....21
Section – 4: List of Materials....32
Section – 6: Implementation Timeline....42
Section – 7: Payment Terms....44
Section – 8: Evaluation Criteria....46
Section – 9: Project acceptance and completion criteria....47
Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI)....50
Annexure – 2: Eligibility Criteria of OEM (active components)....51
Annexure – 3: Eligibility criteria of OEM (Security System)....52
Annexure – 4: Eligibility criteria of OEM (Passive Components)....53
Annexure – 5: Check List to be submitted by Bidder/OEM....54
Annexure – 6: Past performance (to be submitted by letterhead)....56
Annexure – 7: Service Level Agreement (SLA)....57
Annexure – 8: Make and model number of all materials listed in section 4....60
Annexure – 9: Specifications as per the Section – 4 List of Materials....69
Annexure – 10: Building-wise Layout Schematics....156

Section – 1: Introduction

Indian Institute of Science Education and Research (IISER) Mohali invites online bids from eligible, reputed, and experienced bidders or system integrators (for the purposes of this document, the term *"Bidder"* shall hereinafter include the Bidder and/or System Integrator. Accordingly, any reference to *"Bidder"* throughout this document shall be deemed to refer to the Bidder or System Integrator, as applicable.) for the design, supply, installation, testing, commissioning, integration, and comprehensive maintenance of a modern, enterprise-grade Core Network Infrastructure for the institute campus.

The proposed network infrastructure is intended to provide high availability, redundancy, scalability, robust security, and simplified manageability, while effectively supporting the current and future expansion requirements of the institute.

The procurement shall be conducted under a Two-Bid System comprising:

- Technical Bid: Detailing technical compliance, proposed architecture, and qualifications.
- Financial Bid: Detailing itemized costs and commercial terms.

The complete solution shall be delivered on a turnkey basis.

IISER Mohali reserves the right to accept or reject any or all bids without assigning any reason thereof. Interested bidders are advised to regularly visit the institute's website for any corrigendum or updates.

Section – 2: Objective

To provide high availability, scalability, reliability, and security, through robust network architecture to the IIESR Mohali. The network infrastructure and the IT setup should offer minimal downtime due to link or device failure, breakdown, or planned outages. The network design to connect the buildings listed in the tender should integrate with any existing network infrastructure at least the last-mile connections and connect to each building. The backbone network architecture includes the ISP interfaces (at least three ISPs) and bandwidth management systems, security system including firewall deployment, core switching, distribution layer switching to last-mile connection including access switching, routing optimization, and implementation of redundancy protocols to ensure high-throughput, and stable connectivity. The network should be scalable and flexible to make future expansions and enhancements as and when the campus infrastructure expands.

1) The work is divided into four parts:
    a. Laying Optical Fiber Cable (OFC) from Computer Centre to Different Buildings: This component covers the supply, laying, termination, splicing, and testing of Optical Fiber Cable (OFC) from the Computer Centre (CC) to various campus buildings. The work includes installation of ducts, conduits, cable trays, and associated accessories wherever required, ensuring proper cable protection and management. Fiber links will be terminated in appropriate fiber distribution panels and tested using standard certification tools such as OTDR and power meters. The completed backbone shall provide high-bandwidth, low-latency connectivity between all buildings.
    b. Commissioning and Installation of Core Network Infrastructure: This work includes the design, installation, and configuration of the core network infrastructure, starting from the Internet Service Providers (ISP) connectivity to the security devices, followed by the Core Switch (CS), Distribution Switches (DS), and Access Switches (AS). The activity involves configuring routing, VLANs, trunking, redundancy, and inter-device communication to ensure a secure and resilient network backbone. All network components will be integrated to provide seamless connectivity, scalability, and high availability across the campus. The implementation will follow industry best practices for performance, security, and future expansion.
    c. Network Software Stack Configuration and Policy Implementation: This activity includes the configuration of the complete network software stack, encompassing switch operating

systems, routing protocols, VLAN management, DHCP, DNS, authentication services, monitoring tools, and network management platforms. Security policies such as access control lists (ACLs), port security, 802.1X authentication, Quality of Service (QoS), and network segmentation will be implemented to ensure secure and efficient operation. Continuous monitoring, logging, and performance optimization will be configured to maintain network reliability and simplify administration. The final deployment will be documented and validated to ensure compliance with the organization's networking and security requirements.

d. Last-Mile Connectivity from Access Switch to User I/O Port: This work involves providing structured cabling from the Access Switch (AS) to individual user I/O ports installed at workstations, laboratories, offices, and classrooms. The implementation includes laying Cat6/Cat6A cables, installing information outlets, patch panels, cable management systems, and labeling all network points. Each network outlet will be tested and certified to ensure compliance with structured cabling standards and reliable Gigabit (or higher) network performance. Proper documentation on cable routes, cable labeling and port mappings should also be provided.

2) The design and implementation of entire *Core Network Infrastructure* shall be as per ***Error! Reference source not found.***
3) The bidder is expected to physically visit the site (IISER Mohali) and plan for a turnkey solution to be provided to IISER Mohali. The vendor should plan all accessories and switches accordingly. In case, it is found at a later stage during installation some accessories/components are missing, it will be sole responsibility of the bidder to provide the missing components and make it operational.
4) Bidders are expected to submit bids with specified quantities, to maintain consistency across all participants. However, any adjustments to the quantities, either an increase or decrease, will be considered on a proportional basis. The number of items associated with that category mentioned defines the number for financial evaluation.

Section – 3: Scope of Work

The Institute intends to establish a state-of-the-art, high-speed, secure, scalable, resilient, and centrally managed campus-wide data network by deploying a comprehensive Active and Passive Network Infrastructure. The selected bidder shall be responsible for the design, engineering, supply, installation, integration, testing, commissioning, documentation, training, warranty support, and maintenance of the complete networking infrastructure on a turnkey basis.

The work shall include all hardware, software, licenses (if any), accessories, cables, racks, mounting hardware, tools, consumables, testing instruments, documentation, and all incidental items required for the successful completion of the project, irrespective of whether such items are explicitly mentioned either in the *Section – 4: List of Materials* or in the Bill of Quantities (BoQ). The Civil and Electrical works are within the scope of IISER Mohali.

The bidder is expected to thoroughly study the site conditions before submission of the bid and shall satisfy itself regarding all aspects of execution. No additional claim on account of lack of site knowledge shall be entertained after award of the contract.

The scope of work should include, but not be limited to, the following:

1) Site Survey, Planning and Design

The successful bidder shall conduct a comprehensive site survey covering all buildings, departments, laboratories, hostels, administrative blocks, academic blocks, library, conference halls, lecture halls, datacenters, and other locations identified by the Institute. Bidders are expected to make a site visit before pre-bid meeting as described elsewhere in the document.

a) Survey:

i. **Identification of Cable Pathways** – Identify the most suitable cable routing paths for optical fiber and copper cabling while minimizing disruption to existing infrastructure.

ii. **Survey for Installation of Fiber Backbone** – Conduct a detailed survey to determine the most suitable routes and installation methods for the campus optical fiber backbone.

iii. **Locations for Core, Distribution and Access Switches** – while the location for CS and DS are already finalized, vendor shall identify optimal locations for installation of Access Switches to ensure efficient network topology and coverage.

iv. **Last mile Connectivity:**

1. **Assessment of Existing Network Infrastructure** for last-mile connectivity – Assess the existing active and passive network infrastructure to determine its suitability for integration with the proposed network.
2. **Inspection of Existing Ducts, Conduits and Cable Trays** for last-mile connectivity – Inspect the condition, capacity, and usability of existing ducts, conduits, and cable trays for reuse or augmentation.
3. **Survey of Existing Racks for last-mile connectivity** – Survey existing racks to determine space availability, and environmental suitability.

v. **Identification of Electrical Power Requirements** – Assess the electrical power availability and additional power requirements for all active networking equipment.

vi. **Space Planning for Racks** – Plan adequate floor/wall/shaft space, clearances, and cable management provisions for installation of network racks and cabinets.

vii. **Future Expansion Planning** – Design the network infrastructure with sufficient scalability to accommodate future expansion without major modifications.

b) Engineering Drawings

i. **Campus Network Architecture** – Prepare a comprehensive architecture illustrating the overall design and hierarchical structure of the campus network based on site survey and as per document ***Error! Reference source not found.***

ii. **Physical Network Layout** – Develop detailed physical layouts showing the location of all networking equipment and interconnections.

iii. **Logical Network Topology** – Prepare logical topology diagrams depicting network segmentation, routing, VLANs, and connectivity between network devices.

iv. **Fiber Route Maps** – Prepare detailed route maps indicating the alignment, length, and termination points of all optical fiber cables.

v. **Floor-wise Network Layout** – Develop floor-wise layouts indicating the location of access switches, information outlets, and cable routing.

vi. **Rack Elevation Drawings** – Prepare rack elevation diagrams showing equipment placement, cable management, and power distribution within each rack.

vii. **Cable Routing Diagrams** – Develop detailed cable routing diagrams for both fiber and copper cabling throughout the campus.

viii. **Power Distribution Layout** – Prepare layouts indicating electrical power distribution, UPS connectivity, and power outlets for networking equipment.

ix. **Device Placement Drawings** – Identify the exact installation locations of all active and passive network components within each building.

x. **IP Addressing Plan** – Develop a structured IP addressing scheme for efficient network management, scalability, and future expansion.

xi. **VLAN Design** – Prepare a VLAN architecture defining logical segmentation, security boundaries, and inter-VLAN communication requirements.

xii. **Redundancy Architecture** – Design network redundancy mechanisms to eliminate single points of failure and ensure high availability.

c) Approval and Execution*:*

The bidder shall commence execution only after obtaining written approval of all engineering drawings and implementation plans from the Institute.

2) Core Network Infrastructure

a) The bidder shall supply, install, configure, integrate, test and commission the complete Active Network Infrastructure including:

i. **Internet Edge Connectivity** – Establish secure, high-speed Internet connectivity from the ISP handoff point to the Institute's network through redundant and resilient links.

ii. **Security Appliances** – Supply, install, configure, and commission enterprise-grade security appliances to provide perimeter security, threat prevention, VPN, and access control.

iii. **Core Switches (CS)** – Deploy Core Switches to provide high-speed switching, routing, and centralized connectivity for the campus network backbone.

iv. **Distribution Switches (DS)** – Install Distribution Switches to aggregate network traffic from Access Switches and provide resilient Layer-3 connectivity to the Core Switches.

v. **Access Switches (AS)** – Install and configure Access Switches to provide wired network connectivity to end-user devices and edge network equipment.

vi. **Management Network** – Configure a dedicated management network for centralized administration, monitoring, software updates, and maintenance of all network devices.

vii. **Redundant Backbone Links** – Establish redundant backbone connectivity between Core, Distribution, and Access layers to ensure uninterrupted network availability.

b) The bidder establishes seamless end-to-end connectivity beginning from the Internet Service Provider (ISP) handoff through the Security Appliances, Core Switches, Distribution Switches, and Access Switches. **The configuration shall include:**

i. **Layer-2 Switching** – Configure Layer-2 switching services including MAC learning, VLAN switching, trunking, and loop prevention mechanisms.

ii. **Layer-3 Routing** – Configure Layer-3 routing to enable secure and efficient communication between multiple VLANs and IP subnets.

iii. **IPv4 and IPv6** – Implement dual-stack IPv4 and IPv6 networking across all active network devices.

iv. **Dynamic Routing Protocols** – Configure dynamic routing protocols to enable automatic route learning, route optimization, and fast convergence.

v. **VLAN Creation** – Create and configure VLANs for logical segmentation of departments, users, and network services.

vi. **Inter-VLAN Routing** – Configure controlled routing between VLANs in accordance with the Institute's security and access policies.

vii. **Link Aggregation (LACP)** – Configure Link Aggregation Control Protocol (LACP) to increase bandwidth and provide link redundancy.

viii. **Spanning Tree Protocol (STP)** – Configure STP to eliminate switching loops and maintain a stable Layer-2 topology.

ix. **Multiple Spanning Tree (MSTP)** – Configure MSTP to optimize load balancing and loop prevention across multiple VLAN instances.

x. **Rapid Spanning Tree (RSTP)** – Enable RSTP to achieve rapid recovery from network topology changes and link failures.

xi. **VRRP/HSRP (where applicable)** – Configure gateway redundancy protocols to ensure uninterrupted default gateway availability during failures.

xii. **Quality of Service (QoS)** – Configure QoS policies to prioritize mission-critical, voice, video, and real-time application traffic.

xiii. **Multicast** – Configure multicast services for efficient distribution of multimedia and group communication traffic.

xiv. **Jumbo Frames** – Enable jumbo frame support on compatible devices to improve throughput for storage and high-performance applications.

xv. **Traffic Engineering** – Configure traffic engineering policies to optimize bandwidth utilization and network performance.

xvi. **Port Security** – Implement port security mechanisms to prevent unauthorized devices from accessing the network.

xvii. **DHCP Relay** – Configure DHCP relay services to support centralized IP address allocation across multiple VLANs.

xviii. **SNMP** – Configure SNMP for centralized monitoring, fault management, inventory, and performance reporting.

xix. **NTP** – Configure Network Time Protocol (NTP) to synchronize system clocks across all network devices.

xx. **Syslog** – Configure centralized Syslog services for logging, auditing, and troubleshooting of network events.

xxi. **Network Time Synchronization** – Ensure synchronized timestamps across all network devices for accurate event correlation and auditing.

xxii. **Device Authentication** – Configure secure administrator authentication using centralized AAA services such as RADIUS or TACACS+.

xxiii. **Network Monitoring** – Implement centralized monitoring of network devices, interfaces, bandwidth utilization, and system health.

xxiv. **High Availability Features** – Configure redundancy, failover, and resiliency mechanisms to ensure continuous operation of the network infrastructure.

The bidder shall ensure complete interoperability, seamless integration, and centralized management of all active network devices supplied under this project.

3) Laying of Optical Fiber Backbone in Campus

The bidder shall design and deploy a redundant campus-wide optical fiber backbone interconnecting the Computer Centre with all designated buildings to provide a high-speed, scalable, and reliable communication infrastructure.

a) The work shall include:

i. **Supply of OFC** – Supply ITU-T compliant single-mode optical fiber cables of the specified core count along with all associated accessories.

ii. **Laying of Underground** – Lay optical fiber cables through underground ducts and routes as per the approved network design and site conditions using non-trenching method in most of the cases. However, if some places the non-trenching is not possible, carry out excavation of trenches of the specified dimensions for laying optical fiber ducts and cables.

iii. **HDPE Ducts** – Supply and install HDPE ducts of appropriate size for the protection of underground optical fiber cables. Prove appropriate HDPE wherever required for safe route and mechanical protection of optical fiber cables on surface/wall.

iv. **Backfilling** – Restore all excavated Pits, holes, and trenches by proper backfilling, compaction, and surface restoration after cable installation.

v. **Accessories** for OFCs – Supply and install cable trays for structured routing and support of optical fiber cables inside buildings and communication rooms. Provide suitable clamps and fastening accessories to securely support and protect optical fiber cables along their routing paths. Install appropriate structural supports and brackets for cable trays, conduits, and overhead fiber routing.

vi. **Fiber Distribution Panels all weather junction box**– Supply and install Fiber Distribution Panels for organized fiber termination, management, and distribution. These will be placed open-sky areas.

vii. **LIUs** – Supply, install, and terminate optical fibers in rack-mounted Light Interface Units at designated locations for organized interconnection between backbone fibers and active network equipment.

viii. **Fiber Patch Cords** – Supply factory-terminated optical fiber patch cords of appropriate connector types and lengths for equipment connectivity.

ix. **Pigtails** – Supply and fusion-splice optical fiber pigtails for proper termination of all optical fiber cores.

x. **Splicing** – Perform fusion splicing of all optical fiber cores using calibrated splicing equipment to achieve minimum splice loss.

xi. **Termination** – Terminate all optical fiber cores using approved connectors and termination hardware in accordance with OEM recommendations.

xii. **Identification Labels** – Permanently label all fiber cables, cores, LIUs, ODFs, patch panels, and termination points using a standardized identification scheme.

b) The bidder shall perform:

i. **OTDR Testing** – Conduct Optical Time Domain Reflectometer (OTDR) testing on every fiber core to verify continuity, splice quality, attenuation, and cable integrity.

ii. **Power Meter Testing** – Measure the optical power loss of every fiber link using calibrated optical power meters and light sources.

iii. **Insertion Loss Measurement** – Measure and verify the insertion loss of each optical fiber link to ensure compliance with applicable standards and OEM specifications.

iv. It is expected to test the throughput to be 100G for each fibre link.

v. **End-to-End Fiber Certification** – Certify every installed optical fiber link through end-to-end testing and submit comprehensive test reports for approval by the Institute.

Every installed optical fiber core shall be individually tested, certified, documented, and approved by the Institute before the optical fiber backbone is accepted for commissioning.

4) Last-Mile Connectivity

The bidder shall establish reliable last-mile connectivity from the Access Switches to every user Information Outlet (IO) through a structured cabling system that complies with applicable industry standards.

a) The work shall include:

i. **Cable Laying** – Lay Cat-6/Cat-6A cables with appropriate conduits/pipes/channels from the Access Switches to each designated Information Outlet following the approved cable routing plan.

ii. **Cable Termination** – Terminate all copper cables at both patch panels and Information Outlets using OEM-recommended termination practices and standards.

iii. **Wall Outlets** – Supply and install Information Outlets (IOs) at designated user locations with proper mounting and labeling.

iv. **Faceplates** – Install modular faceplates compatible with the Information Outlets to provide a neat, secure, and user-friendly interface.

v. **Patch Cords** – Supply and connect factory-terminated Cat-6/Cat-6A patch cords between patch panels, switches, and user devices.

vi. **Patch Panel Connectivity** – Terminate and organize all horizontal cables on rack-mounted patch panels with proper cable management and labeling.

vii. **Switch Port Configuration** – Configure switch access ports with the appropriate VLAN assignments, security policies, and operational parameters for each user connection.

viii. **Cable Certification** – Certify every installed copper cable link using a calibrated cable certification tester to ensure compliance with applicable standards.

ix. **User Port Testing** – Test every Information Outlet for end-to-end connectivity, functionality, and compliance before commissioning.

b) Each node shall be individually tested for:

i. **Wire Mapping** – Verify correct pin-to-pin connectivity, conductor continuity, and the absence of wiring faults such as opens, shorts, reversals, or split pairs.

ii. **Return Loss** – Measure Return Loss to confirm that impedance mismatches are within acceptable limits and signal reflections are minimized.

iii. **Gigabit Performance** – Validate that every installed network node supports Gigabit Ethernet (respective throughput) communication or higher as specified in the tender.

The bidder shall submit complete cable certification reports for every installed Information Outlet, and only those nodes that successfully pass all specified performance tests shall be considered for final acceptance and commissioning.

5) Network Security Infrastructure

The bidder shall implement a comprehensive network security framework to ensure the confidentiality, integrity, availability, and secure management of the campus network.

The scope shall include:

i. **Firewall Configuration** – Configure enterprise firewall policies to secure the network perimeter and regulate inbound, outbound, and inter-zone traffic.

ii. **ACL Implementation** – Implement Access Control Lists (ACLs) to enforce granular access policies between network segments, users, and services.

iii. **VLAN Segmentation** – Configure VLAN-based network segmentation to isolate users, departments, servers, and critical services for enhanced security and performance.

iv. **Port Security** – Implement port security mechanisms to prevent unauthorized devices from accessing the network through switch access ports.

v. **MAC Authentication** – Configure MAC-based authentication to permit network access only to authorized endpoint devices.

vi. **IEEE 802.1X** – Implement IEEE 802.1X port-based network access control for secure user and device authentication.

vii. **DHCP Snooping** – Configure DHCP Snooping to prevent rogue DHCP servers and ensure trusted IP address allocation.

viii. **Dynamic ARP Inspection** – Implement Dynamic ARP Inspection (DAI) to protect the network against ARP spoofing and man-in-the-middle attacks.

ix. **IP Source Guard** – Configure IP Source Guard to prevent IP address spoofing and unauthorized network access.

x. **Storm Control** – Configure broadcast, multicast, and unknown unicast storm control to prevent network congestion and denial-of-service conditions.

xi. **Secure Management Access** – Secure administrative access to all network devices using encrypted management protocols such as SSH, HTTPS, and SNMPv3.

xii. **Role Based Administration** – Implement role-based administrative access with appropriate privileges for different categories of network administrators.

xiii. **Logging** – Configure centralized logging of security events, system activities, and configuration changes for audit and troubleshooting purposes.

xiv. **Event Monitoring** – Implement continuous monitoring of security events, alarms, and abnormal network behavior through centralized monitoring tools.

xv. **Security Auditing** – Conduct periodic security audits to verify compliance with the Institute's security policies and identify potential vulnerabilities.

6) Network Software Stack

The bidder shall install, configure, and commission the complete software stack required for centralized operation, management, monitoring, and maintenance of the campus network.

The scope shall include:

i. **Operating System Installation** – Install the latest OEM-supported operating system software on all active network devices.

ii. **Firmware Upgrades** – Upgrade all network devices to the latest stable and OEM-recommended firmware versions before commissioning.

iii. **Device Licensing** – Install, activate, and validate all software licenses required for the full functionality of the supplied network equipment.

iv. **Centralized Network Management** – Deploy and configure a centralized Network Management System (NMS) for administration, monitoring, and management of all network devices.

v. **Configuration Backup** – Configure automated backup and restoration of device configurations to facilitate disaster recovery and operational continuity.

vi. **Monitoring Tools** – Deploy network monitoring tools to continuously monitor device health, interface status, bandwidth utilization, and system performance.

vii. **Alerting System** – Configure automated alerts and notifications for network faults, security events, threshold violations, and device failures.

viii. **Inventory Management** – Implement an inventory management system for maintaining an up-to-date database of all active network assets and software licenses.

ix. **Performance Monitoring** – Configure continuous monitoring and reporting of network performance parameters, including latency, throughput, CPU, memory, and interface utilization.

x. **Dashboard Configuration** – Develop centralized dashboards providing real-time visualization of network health, alarms, utilization, and operational status.

xi. **Event Logging** – Configure centralized collection, storage, and analysis of system logs and operational events generated by all network devices.

xii. **Traffic Analysis** – Implement traffic analysis tools to monitor network utilization, application traffic, user behavior, and bandwidth consumption.

xiii. **Configuration Templates** – Develop standardized configuration templates to ensure uniform configuration, simplified deployment, and consistent policy enforcement across all network devices.

xiv. Captive Portal–Based Device Onboarding: Secure device registration, authentication, and network access through a captive portal. The appropriate Network Access Control must be implemented so that all devices shall be granted network access only after successful registration and approval by the network administrator.

xv. **Following software must be provided and integrated:**

1. **AAA Server:** Supply, installation, configuration, integration, testing, and commissioning of a centralized Authentication, Authorization, and Accounting (AAA) server supporting TACACS+ and/or RADIUS protocols for secure network access control, user management, policy enforcement, and accounting logs.
2. **Network Access Control (NAC):** Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network infrastructure.
3. **RADIUS Server:** Supply, installation, configuration, integration, testing, and commissioning of a standards-compliant RADIUS server supporting IEEE 802.1X/EAP authentication for centralized user authentication, authorization, and accounting across wired and wireless networks.
4. **LDAP Server:** Supply, installation, configuration, integration, testing, and commissioning of an LDAP directory service for centralized identity management, user authentication, role-based access control, and integration with AAA, NAC, network devices, and enterprise applications.
5. **Internal DNS Server:** Supply, installation, configuration, integration, testing, and commissioning of an Internal DNS server for secure name resolution, forward and reverse

lookup zones, dynamic DNS updates, and integration with internal directory and network services.

6. **External DNS Server:** Supply, installation, configuration, integration, testing, and commissioning of an External DNS server for authoritative public DNS hosting, secure zone management, redundancy, and integration with Internet-facing services.
7. **Network Management System (NMS):** Supply, installation, configuration, integration, testing, and commissioning of a centralized Network Management System for device discovery, inventory, topology visualization, configuration management, fault, performance, and availability monitoring using SNMP, Syslog, NetFlow/sFlow, and related protocols.
8. **Syslog Server:** Supply, installation, configuration, integration, testing, and commissioning of a centralized Syslog server for secure collection, storage, indexing, monitoring, correlation, alerting, and analysis of logs generated by network, security, and server infrastructure.
9. **Additional Network Services:** The successful bidder shall deploy and commission the above network services along with: DHCP, Internal and External DNS, Directory Services, including DC/ADC and LDAP, NTP, Syslog, User Access Logging

xvi. The bidder shall implement any additional features, functionalities, configurations, policies, or modifications reasonably required by the Institute during the execution of the project, as necessary for successful implementation and operation of the system at no additional cost.

7) Integration

The bidder shall ensure seamless integration of the newly deployed network infrastructure with the Institute's existing networking wherever required, computing, and security infrastructure without disrupting ongoing services along with aforementioned software stacks mentioned in Pt. (6).

The scope shall include:

i. **Existing Internet Links** – Integrate the new network infrastructure with the Institute's existing Internet connectivity while ensuring uninterrupted network services.

ii. **Existing Fiber Backbone** – Integrate the newly deployed optical fiber backbone with the existing fiber infrastructure wherever applicable.

iii. **Authentication Servers** – Integrate the network with existing authentication servers such as RADIUS, TACACS+, LDAP, or Active Directory for centralized user authentication.

iv. **DNS** – Configure seamless integration with the Institute's existing Domain Name System (DNS) infrastructure for reliable name resolution services.

v. **DHCP** – Integrate with the existing DHCP infrastructure to ensure centralized and efficient IP address allocation across the campus.

vi. **NTP** – Synchronize all network devices with the Institute's existing Network Time Protocol (NTP) servers for consistent system time across the network.

vii. **Directory Services** – Integrate the network management platform with existing directory services to enable centralized user and administrator management.

viii. **VLAN Architecture** – Extend and integrate the new network with the Institute's existing VLAN architecture while preserving existing segmentation and security policies during the deployment phase and replace it to new system slowly during deployment.

ix. **Existing Servers** – Ensure seamless connectivity and interoperability between the new network infrastructure and all existing application, database, storage, and utility servers.

x. **Data Centre Infrastructure** – Integrate all active and passive network components with the Institute's existing Data Centre infrastructure, including servers, storage systems, virtualization platforms, and management systems, to ensure seamless operation and centralized management.

xi. **Captive Portal & Device Onboarding:** Design, development, integration, testing, and commissioning of a secure captive portal for new device registration and onboarding, integrated with NAC, AAA/RADIUS, and LDAP/Active Directory, supporting user/device authentication, approval, policy enforcement, quarantine/onboarding VLAN, access logging, and **user-wise hardware inventory with a centralized database**.

8) General Testing and Validation.

The bidder shall ensure seamless integration of the newly deployed network infrastructure with the Institute's existing networking wherever required, computing, and security infrastructure without disrupting ongoing services and shall perform following testing and validations:

a) Installation and Configuration

i) Complete installation, configuration, commissioning and integration of all network and security components, including switches, routers, firewalls/NGFW, ADC, CS, DS, structured cabling, optical fibre, racks and associated components, technical specifications.

ii) All equipment shall be operational, correctly configured and integrated with the existing campus network, wherever applicable.

b) Connectivity and Functional Testing

i) Verify end-to-end connectivity across all designated network segments, buildings, floors, racks, and user locations.

ii) Verify the functionality of LAN, WAN, routing, switching, VLANs, DHCP/DNS, Internet connectivity, firewall/NGFW, ADC, CS, DS and other applicable network services.

iii) Verify that all configured features, policies, services and protocols operate as specified in the technical requirements.

c) Performance and Capacity Testing

i) Conduct throughput, latency, packet-loss, concurrent-session and link-utilisation tests for critical network links and devices.

ii) Verify that switches, firewalls/NGFW, ADC, CS and DS meet the specified performance, capacity and throughput requirements under normal and representative load conditions.

d) Redundancy and Failover Testing

i) Test all applicable redundant links, switches, firewalls/NGFW, ADC, CS, DS, power supplies, gateways and network paths.

ii) Simulate failure of critical links or equipment and verify successful failover, service continuity and recovery as per the specified requirements.

e) Firewall and Security Functionality

i) Verify firewall policies, ACLs, NAT, VPN, routing, application control, security policies, logging, monitoring and administrative access.

ii) Verify that required security features are correctly configured and operational, and that unauthorized traffic is appropriately blocked.

f) CS and DS Functionality

i) Verify the complete functionality and integration of CS and DS, including their configured services, policies, management, connectivity and redundancy, as applicable to the proposed solution.

ii) All specified features and services shall be demonstrated and validated against the approved technical specifications.

g) Structured Cabling and Fibre Testing

i) Test and certify all copper and optical-fibre links using appropriate calibrated test equipment.

ii) Submit OTDR reports, fibre-loss measurements, copper certification reports and link-wise test records, wherever applicable.

h) Documentation and As-Built Records

i) Submit complete as-built network diagrams, security architecture, rack layouts, port mapping, IP addressing/VLAN details, cable schedules, device inventory, configurations and test reports.

ii) All equipment, ports, cables, fibre cores and patch panels shall be properly labelled and correspond to the submitted documentation.

i) Monitoring, Management and Backup

i) Verify integration of all applicable network, security and application infrastructure devices with the designated monitoring and management systems.

ii) Ensure configuration backup, logging, alerting, health monitoring and administrative access are operational.

j) UAT and Defect Rectification

i) The Institute shall conduct User/Operational Acceptance Testing (UAT/OAT) based on the approved test plan.

ii) All defects, deviations and deficiencies identified during testing shall be rectified by the Bidder/System Integrator at no additional cost before final acceptance.

k) Manpower Training

i) Provide necessary training to the Institute's designated technical personnel for operation, administration, monitoring and basic troubleshooting.

ii) Complete formal handover of all equipment, accessories, licenses (if any), credentials, configuration backups, manuals and technical documentation.

The project shall be completed through integrated testing and final verification of the implemented solution, including functional, performance, security, redundancy, failover and integration testing.

The scope shall include rectification of identified deficiencies, submission of test reports, configuration details and as-built documentation, and final handover of the complete system. Verification and final acceptance may be carried out by the Institute through the Execution Monitoring Committee, Internal Committee and/or an authorized Third Party.

Section – 4: List of Materials

Sl. No	Item No.	Item Description	Quantity	Units
1	1.1	Next Generation Firewall (NGWF): NGFW Firewall 4 x 100GE/40GE QSFP28 slots, 10 x 25GE/10GE SFP28 slots, 10 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing;HA support; SIEM integration; 7 Year Warranty	2	Number
2	1.2	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty	2	Number
3	2.1	Core Switch (CS): Core Switch Supply of Layer 3, 32 Port x 40/100 Gbps SFP port core switch; Switching capacity: at least 6Tbps; with field replaceable redundant power supplies and FANs; 7 Year Warranty;	2	Number
4	2.2	Distribution Switch (DS) Type - 1: DS Switch Type-1: Distribution Switch Supply of Layer 3, 48-port SFP28 10/25GbE, with 8x-port 40/100GbE; Switching capacity at least 4Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty;	10	Number
5	2.3	Distribution Switch (DS) Type - 2: DS Switch Type-2: Distribution Switch Supply of Layer 3, 24-port SFP28 10/25 G, with 4x-port 40/100GbE; Switching capacity: at least 2Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty,	10	Number
6	2.4	Access Switch (AS) Type - 1: AS Switch Type-1: Access Switch/Edge Switch: 24x1/10GbE Base-T RJ45 ports; 4 × 25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 680gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	12	Number
7	2.5	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	10	Number
8	2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	75	Number
9	2.7	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 ×	2	Number

		10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty		
10	2.8	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	4	Number
11	2.9	100G DAC Copper Cable - 1M: 100GbE QSFP28 to QSFP28 Direct Attached, Passive Copper Cable, 1m. Stacking	24	Number
12	2.10	100G DAC Cable - 1M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 1m, 1-pack	26	Number
13	2.11	100G DAC Cable - 5M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 5m, 1-pack	52	Number
14	2.12	100G DAC Cable - 10M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 10m, 1-pack	10	Number
15	2.13	40G DAC Cable - 5M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 5m, 1-pack	20	Number
16	2.14	40G DAC Cable - 10M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 10m, 1-pack	20	Number
17	2.15	40G QSFP+: 40GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack	16	Number
18	2.16	25G QSFP+: 25GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack	56	Number
19	2.17	10G SFPP: 10GBASE-LR, SFPP SMF LC CONNECTOR (No TAA)	364	Number
20	3.1	AAA Server: AAA Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Authentication, Authorization, and Accounting (AAA) server supporting TACACS+ and/or RADIUS protocols for secure network access control, user management, policy enforcement, and accounting logs.	1	Complete
21	3.2	Network Access Control (NAC): Network Access Control (NAC): Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network infrastructure.	1	Complete
22	3.3	RADIUS Server: RADIUS Server: Supply, installation, configuration, integration, testing, and commissioning of a standards-compliant RADIUS server supporting IEEE 802.1X/EAP authentication for centralized user authentication, authorization, and accounting across wired and wireless networks.	1	Complete
23	3.4	LDAP Server: LDAP Server: Supply, installation, configuration, integration, testing, and commissioning of an LDAP directory service for centralized identity management, user authentication, role-based access control, and integration with AAA, NAC, network devices, and enterprise applications.	1	Complete
24	3.5	Internal DNS Server: Internal DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an Internal DNS server for secure name resolution, forward and reverse lookup zones, dynamic DNS updates, and integration with internal directory and network services.	1	Complete
25	3.6	External DNS Server: External DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an External DNS server for authoritative	1	Complete

		public DNS hosting, secure zone management, redundancy, and integration with Internet-facing services.		
26	3.7	Network Management System (NMS): Network Management System (NMS): Supply, installation, configuration, integration, testing, and commissioning of a centralized Network Management System for device discovery, inventory, topology visualization, configuration management, fault, performance, and availability monitoring using SNMP, Syslog, NetFlow/sFlow, and related protocols.	1	Complete
27	3.8	Syslog Server: Syslog Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Syslog server for secure collection, storage, indexing, monitoring, correlation, alerting, and analysis of logs generated by network, security, and server infrastructure.	1	Complete
28	3.9	Software Stack Deployment: The successful bidder must deploy above network services along with DHCP, DNS (internal & external), Directory Server (DC/ ADC and LDAP), NTP, Syslog and User Access Log. All these servers must be configured preferably using Open Source.	1	Complete
29	4.1	96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket.	3500	Meter
30	4.2	48 Core OFC: Single Mode fiber 48 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket.	2500	Meter
31	4.3	24 Core OFC: Single Mode fiber 24: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable.	2200	Meter
32	4.4	12 Core OFC: Single Mode fiber 12: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable.	900	Meter
33	4.5	LIU-24P: 24 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails	8	Number
34	4.6	LIU-48P: 48 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails	75	Number
35	4.7	LC-LC Patch Cord-Type-1: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 0.5m	500	number
36	4.8	LC-LC Patch Cord-Type-2: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 1m	312	number
37	4.9	LC-LC Patch Cord-Type-3: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 2m	144	number
38	4.10	LC-LC Patch Cord-Type-4: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 5m	64	number
39	4.11	LC-LC Patch Cord-Type-5: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 10m	48	number
40	4.12	Custom Patch Cords-2c: 2-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord	500	meter
41	4.13	Custom Patch Cords-4c: 4-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord	200	meter
42	4.14	Custom Patch Cords-6c: 6-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord	100	meter
43	4.15	Custom Patch Cords-8c: 8-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord	100	meter
44	4.16	Compatible Pigtail: LC/UPC male type single-mode OS2 9/125 µm fiber pigtail, with locking latch, suitable for direct connection to LC female adapter of LIU with bare-fiber end for fusion splicing.	1600	number
45	4.17	Junction Box: Outdoor Junction Box for OFC termination IP67: all weather outdoor box, to be installed as a junction box for 96 fibres LIU	3	number

46	4.18	HDPE Duct-Type1: Duct for OFC HDPE Pipe 24 Core and 48 Core OFC	4550	meter
47	4.19	HDPE Duct-Type2: Duct for OFC HDPE Pipe for 96 Core OFC	3500	Meter
48	4.20	OFC Laying: OFC Laying by non-trenching method	7700	Meter
49	4.21	CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each	80	Boxes
50	4.22	CAT6 Cable type -2: Metallic armour CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each	5	Boxes
51	4.23	CAT6 Patch Panel 24P: 24 port CAT 6 Patch Panel	24	number
52	4.24	CAT6 Patch Panel 48P: 48 port CAT 6 Patch Panel	12	number
53	4.25	CAT6 Patch Cord - type - 1: Patch Cords 0.5M	1000	number
54	4.26	CAT6 Patch Cord - type - 2: Patch Cords 1M	1000	number
55	4.27	CAT6 Patch Cord - type - 3: Patch Cords 2M	500	number
56	4.28	CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each	20	Boxes
57	4.29	CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each	8	Boxes
58	4.30	CAT6A Patch Panel 24P: 24 port CAT 6A Patch Panel	4	number
59	4.31	CAT6A Patch Panel 48P: 48 port CAT 6A Patch Panel	4	number
60	4.32	CAT6A Patch Cord - type - 1: Patch Cords 0.5M	100	number
61	4.33	CAT6A Patch Cord - type - 2: Patch Cords 1M	100	number
62	4.34	CAT6A Patch Cord - type - 3: Patch Cords 2M	64	number
63	4.35	Conduit-Square: Conduit Square (24x24)	500	Meter
64	4.36	Conduit-Round: Conduit round (10mm)	500	meter
65	4.37	T-joints: Compatible with 10mm round conduit	100	number
66	4.38	L-joints: Compatible with 10mm round conduit	200	number
67	4.39	Flexi-pipe-a: Compatible with 10mm round conduit	100	Meter
68	4.40	Flexi-pipe-b: Compatible with 24mmx24mm conduits	100	meter
69	4.41	Racks-Type-1: 6 U Network racks	12	Number
70	4.42	Racks-Type-2: 9 U Network racks	12	Number
71	4.43	Racks-Type-3: 12 U Network racks	6	Number
72	4.44	Racks-Type-4: 15 U Network racks	12	Number
73	5.1	Work - 1: Work and commissioning of All switches, laying cables & installation of AS in every building, integrating to existing system, designing the entire network segment and implementing the policies etc.	1	Complete
74	6.1	Manpower: One (01) qualified and trained Network Engineer shall be deployed onsite for day-to-day network administration, monitoring, troubleshooting, configuration, preventive maintenance, and technical support of the networking infrastructure.	6	salary per month
75	7.1	Works - 2: Through Existing Concealed Conduits/Pipes: Pulling and routing CAT6/6A cable(s) through existing concealed conduits/pipes without providing any new conduit or channel. Includes cable pulling, routing, dressing, termination at both ends, testing, labeling, and commissioning.	1500	RM
76	7.2	Works - 3: Laying New PVC Conduit – Up to 2 CAT6/6A Cables: Fixing suitable PVC conduit with all necessary accessories for laying and routing up to 2 CAT6/6A cables,	1500	RM

		including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.		
77	7.3	Works - 4: New PVC Conduit – 3 to 10 CAT6/6A Cables: Fixing suitable PVC conduit of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	500	RM
78	7.4	Works - 5: New PVC Conduit – More than 10 CAT6/6A Cables: Fixing suitable PVC conduit(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
79	7.5	Works - 6: New PVC Trunking/Channel – Up to 2 CAT6/6A Cables: Fixing suitable PVC trunking/channel with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
80	7.6	Works - 7: New PVC Trunking/Channel – 3 to 10 CAT6/6A Cables: Providing and fixing suitable PVC trunking/channel of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
81	7.7	Works - 8: New PVC Trunking/Channel – More than 10 CAT6/6A Cables: Fixing suitable PVC trunking/channel(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
82	7.8	PVC Conduit 20MM: New 20 mm Heavy-Duty PVC Conduit: Fixing 20 mm HD PVC conduit with all accessories for laying and routing up to 2 CAT6/6A cables	100	RM
83	7.9	PVC Conduit 25MM: New 25 mm Heavy-Duty PVC Conduit: Fixing 25 mm HD PVC conduit with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
84	7.10	PVC Conduit 32MM: New 32 mm (Minimum) Heavy-Duty PVC Conduit: Fixing 32 mm HD PVC conduit (increasing to 40 mm or multiple conduits, as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
85	7.11	PVC Trunking/Channel 25 mm x16 mm: New 25 × 16 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing up to 2 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
86	7.12	PVC Trunking/Channel 40 mm x 25 mm: New 40 × 25 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
87	7.13	PVC Trunking/Channel 60 mm x 40 mm: New 60 × 40 mm (Minimum) PVC Trunking/Channel: Fixing PVC trunking/channel (increasing to larger sizes as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.	100	RM
88	7.14	Ferrule type - 1: Appropriate Ferrule for labelling Cat6 cable (100 x 10 Pieces) Each packet	100	Packet
89	7.15	Ferrule type - 2: Appropriate Ferrule for labelling Cat6A cable	100	Packet

		(100 x 10 Pieces) Each packet		
90	7.16	CAT6 IO Jacks: CAT6 IO jacks (RJ45 I/O modules)	500	Number
91	7.17	CAT6 Face Plates: CAT6 Face Plate (Single Port)	500	Number
92	7.18	CAT6 Mounting Box: Mounting Box / Backbox for Face Plate	500	Number
93	7.19	CAT6A IO Jacks: CAT6A IO jacks (RJ45 I/O modules)	100	Number
94	7.20	CAT6A Face Plates: CAT6A Face Plate (Single Port)	100	Number
95	7.21	CAT6A Mounting Box: Mounting Box / Backbox for Face Plate	40	Number
96	7.22	Flexi pipe - 1: to fit the size of conduit Size of 20 mm	100	Meter
97	7.23	Flexi pipe - 2: to fit the size of conduit Size of 25 mm	100	Meter
98	7.24	Flexi pipe - 3: to fit the size of conduit Size of 32 mm	100	Meter
99	7.25	T-Joints - 1: to fit the size of conduit Size of 20 mm	250	Number
100	7.26	T-Joints - 2: to fit the size of conduit Size of 25 mm	100	Number
101	7.27	T-Joints - 3: to fit the size of conduit Size of 32 mm	50	Number
102	7.28	L-joints - 1: to fit the size of conduit Size of 20 mm	250	Number
103	7.29	L-joints - 2: to fit the size of conduit Size of 25 mm	100	Number
104	7.30	L-joints - 3: to fit the size of conduit Size of 32 mm	50	Number

Section – 5: General Conditions

<table>
<tr><th>Sl. No</th><th>Conditions</th></tr>
<tr><td>1</td><td>Bidders or OEM must bid for all items.</td></tr>
<tr><td>2</td><td>Eligibility Criteria for the bidder, OEM, active and passive components could be found in Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI), Annexure – 2: Eligibility Criteria of OEM (active components), Annexure – 3: Eligibility criteria of OEM (Security System), and Annexure – 4: Eligibility criteria of OEM (Passive Components). The same shall be submitted along with the bid.</td></tr>
<tr><td>3</td><td>Past performance: the bidder shall have successfully completed during the last seven years one or more Campus Wide Network (LAN) projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions.

Bidder must satisfy both A & B
A. The bidder shall satisfy any one of the following:
a. One completed project involving at least 80% of the quantities listed below in table - 1; or
b. Two completed projects, each involving at least 60% of the quantities listed below in table - 1; or
c. Three completed projects, each involving at least 40% of the listed below in table - 1:
<table><tr><td colspan="2">Table - 1</td></tr><tr><td>Firewall/ADC</td><td>2 Nos</td></tr><tr><td>L3 Fibre Switches</td><td>30 Nos</td></tr><tr><td>L2 Switches</td><td>80 Nos</td></tr><tr><td>OFC Laying</td><td>8000m</td></tr><tr><td>Transceivers</td><td>430 Nos</td></tr><tr><td>I/O ports as Last-mile connection</td><td>1000 Nos</td></tr></table>
B. The bidder should have supplied and deployed software stack (Item numbers 3.1 to 3.9 in Section – 4: List of Materials.

Similar quantities shall be assessed based on the cumulative deployment of comparable campus-wide networking equipment such as managed switches, fibre backbone connectivity, structured cabling, and network commissioning.

Documentary evidence such as Purchase Orders, Completion Certificates, and Commissioning Certificates, shall be submitted as per

Annexure – 6: Past performance (to be submitted by <u>letterhead</u>).</td></tr>
<tr><td>4</td><td>Switches (Core Switches, Distribution Switches, and Access Switches) should be from a single OEM.</td></tr>
</table>

5	1. The pre-Bid meeting will be conducted on as date given elsewhere in the tender document. 2. Any query/queries must be sent through email to tenders@iisermohali. ac. in on or before two days of the pre-bid meeting. No new queries shall be entertained afterward. 3. If bidder wishes to make a site visit, they may complete the site visit at least two (2) days prior to the pre-bid meeting. The site visit shall be conducted only after obtaining prior approval from the Institute by sending email to tenders@iisermohali. ac. in. Further, if any bidder wishes to make a site visit on day of pre-bid meeting, they may undertake the visit, however, no additional queries related to site visit would be entertained afterward. 4. In person participation in the pre-bid meeting is mandatory for all intending bidders due to the technical and site-specific nature of the work. A Participation Certificate shall be issued to the participating bidder and the same shall be submitted along with the bid. **Failure to participate and/or submit the Participation Certificate shall render the bid liable to be treated as non-responsive and rejected.** 5. The bidders must adhere to the design provided in this tender, if there is any discrepancy shall be submitted as query for the discussion during pre-bid meeting. 6. The Bidder/OEM shall adhere to the network design specified in the tender. In case of any discrepancy or deviation identified in the prescribed design which may create serious issues, the same shall be clearly highlighted and submitted, along with appropriate justification, for discussion during the pre-bid meeting. 7. Bidders shall come prepared with a relevant network design plan and presentation for the pre-bid meeting. The committee may require the bidder to present and explain the proposed design during the meeting.
6	OEM should be registered in India & submit documentary proof.
7	Prices should NOT be given anywhere in the technical bid. Accidental/incidental mention of prices in technical bids may result in disqualification.
8	1. There must be clear documentation of each item and comparison tables if any; 2. The manual/brochures for each item must be included in the technical bid. 3. Bidder must provide a list of models proposed for each item. The data sheets must be available in public domain including URLs. a. A point-to-point compliance sheet and b. Make & models of each item as per Annexture - 8 must be submitted.
9	Bidder/OEM should have a direct local support office in Mohali-Chandigarh-Panchkula Tricity or in Delhi-NCR or within the radius of 250 kms.
10	1. A bid specific manufacturer authorization certificate (MAF) from the Original Equipment Manufacturer (OEM) is mandatory for bidders, who are not OEMs. 2. The document should state that firm is authorized by the manufacturer OEM to supply, install and maintain the system. 3. Where the quoted system comprises components from multiple OEMs, separate bid specific MAF from each OEM shall be submitted for all the active items such as NGFW, ADC, CS, DS, AS, CAT6, CAT6A, Optical fiber cable, Transceivers and compatible DAC Cables. 4. All these certificates must be on OEM letterhead

11	An undertaking (self-certificate) is to be submitted by the bidder that the organization has not been blacklisted by any Central/State Government Department/Organization and educational institutes in last one year.
12	The warranty period is to be counted from the date when the installation is completed, and the acceptance certificate has been issued by IISER Mohali.
13	Annexures 1 to 8 shall be duly completed, signed and stamped by the respective authorized party, as follows: *Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI), Annexure – 5: Check List to be submitted by Bidder/OEM,* *Annexure – 6: Past performance (to be submitted by* **letterhead**), *and Annexure – 7: Service Level Agreement (SLA)* by Bidder; *Annexure – 2: Eligibility Criteria of OEM (active components), Annexure – 3: Eligibility criteria of OEM (Security System), and Annexure – 4: Eligibility criteria of OEM (Passive Components)* by OEMs; *Annexure – 8: Make and model number of all materials listed in section 4,* along with compliance certificate from OEMs for all active items, including NGFW, ADC, CS, DS, AS, CAT6, CAT6A, Optical Fibre Cable, Transceivers, and compatible DAC Cables. The bidder/OEM must submit any other mandatory certification as pes the applicable guidelines of GoI. Failure to submit the required Annexures duly signed/stamped as applicable, may result in summary rejection of the bid.
14	Bidder/OEM warrants that all the goods are new, unused, and of the most recent or current supported models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.
15	The bidder/OEM should quote prices of each and every item separately as per prescribed format. IISER Mohali reserves the right to increase or decrease the quantity of items by up to 25%.
16	Bidder/OEM must submit the Service Level Agreement (SLA) mentioned in *Annexure – 7: Service Level Agreement (SLA)*
17	Bidder/OEM should ensure that the spare parts/components/items should be available for at least 7 years or at the updated version should be compatible with the offered hardware.
18	Canvassing in any form, including communication with institute officials other than what is provided here, would disqualify the OEM from further participation.
19	Bidder shall adhere to the implementation timeline as per *Section – 6: Implementation Timeline.*
20	Payment terms are mentioned in the *Section – 7: Payment Terms*
21	Evaluation Criteria will be followed as mentioned in *Section – 8: Evaluation Criteria*
22	• The base quantities of passive components specified in *Section – 4: List of Materials Item Nos.4.1 to 4.44* shall be deemed included in the quoted price. • Any additional requirement arising from actual site conditions, including

	additional cable length or other passive items beyond the specified quantities, shall require prior written intimation and approval of the Execution Committee before procurement or execution. • Additional quantities shall be jointly verified at site and, upon approval by the Execution Committee and upon approval of competent authority, shall be paid at the corresponding accepted BOQ unit rates on a pro-rata basis. • No payment shall be admissible for additional items/work executed without prior approval.
23	A separate work order will be issued for the Last-Mile connections (*Section – 4: List of Materials item no 7*). Bidder time shall adhere to the timeline as per *Section – 6: Implementation Timeline*
24	• The base quantity of Last-Mile I/O Ports, including installation of conduits and laying of cables, as specified under *Section – 4: List of Materials Item* Nos.7*.1 to 7.30* shall be deemed included in the quoted price. • Any additional I/O Ports required due to actual site conditions shall require prior written intimation and approval of the Execution Committee before execution. • Additional I/O Ports shall be jointly verified at site and, upon approval by the Execution Committee Authority and upon approval of competent authority, shall be paid at the corresponding accepted BOQ unit rates on a pro-rata basis. • No payment shall be admissible for additional I/O Ports or associated work executed without prior approval.

Section – 6: Implementation Timeline

Sl. No.	Name of Activity / Milestone	Timeline for Completion	Remarks / Conditions
1	Submission of Drawings (LLD and HLD and any other relevant drawings) and Implementation Plans: Submission of all drawings, network layouts and implementation plans as specified under *Section – 3: Scope of Work.* Shall execute and sign a Non-Disclosure Agreement (NDA) with the Institute	Within 30 days from the date of award of the Tender	Implementation work shall commence only after submission and approval of the required documents by the Execution Committee. Delays shall attract a penalty of ₹1000 per week or part thereof, subject to a maximum of 10% of the total contract value.
2	Delivery of Passive Components: Supply and delivery of all passive networking components/items (*Item 4.1 to 4.44* in the *Section – 4: List of Materials)* as specified in the tender.	Within 60 days from the date of award of the Tender	Materials shall be subject to inspection and acceptance by the Execution Committee. Delays shall attract a penalty of ₹2500 per week or part thereof, subject to a maximum of 10% of the total contract value.
3	Delivery of Active Components: Supply and delivery of active components including NGFW, ADC, CS, DS, AS, DAC Cables and Transceivers. (*Item 1.1, 1.2, 2.1 to 2.17 in the Section – 4: List of Materials*)	Within 90 days from the date of award of the Tender	Part payment may be allowed against actual delivery, inspection and acceptance by the Execution Committee. Delays shall attract a penalty of ₹5000 per week or part thereof, subject to a maximum of 10% of the total contract value.
4	OFC Infrastructure: Laying and commissioning OFC, including installation of LIUs and Junction Boxes and completion of LIU-to-LIU connectivity.	Within 90 days from the date of award of the Tender	Work shall be executed as per the approved network design and specifications and verified by the Execution Committee. Delays shall attract a penalty of ₹5000 per week or part thereof, subject to a maximum of 10% of the total contract value.
5	Installation of Active Components: Installation, configuration and commissioning of all active networking components at designated locations.	Within 120 days from the date of award of the Tender	Work shall be carried out as per the approved network architecture and technical specifications. Delays shall attract a penalty of ₹10000 per week or part thereof, subject to a maximum of 10% of the total contract value.

6	Software Stack: delivery, Installation, configuration, testing and deployment of the required software stack. (*Item 3.1 to 3.9* in the *Section – 4: List of Materials*)	Within 120 days from the date of award of the Tender	Implementation shall be carried out as per the approved implementation plan. Delays shall attract a penalty of ₹5000 per week or part thereof, subject to a maximum of 10% of the total contract value.
7	Testing: Completion of integrated system testing, performance verification and rectification of identified deficiencies.	Within 150 days from the date of award of the Tender	Testing shall be carried out to the satisfaction of the Execution Committee.
8	Last-Mile Connectivity: Completion of Last-Mile Connectivity from the Access Switch to the designated User I/O Port, delivery of related items (*Item 7.8 to 7.30* in the *Section – 4: List of Materials)* including installation, termination, patching, labelling and testing of the network connection.	Within 180 days from the date of award of the Tender	This activity shall be completed as part of the overall implementation. Updated connectivity records/as-built documentation shall be submitted.

The penalty shall be cumulative for every additional week of delay

Section – 7: Payment Terms

Payments shall be released against the successful completion of the milestones listed below. The bidder shall submit the required documents, delivery challans, installation reports, commissioning certificates, test reports, and acceptance certificates, as applicable for each milestone. Five percent (5%) of the payment against each milestone shall be retained as **Performance Bank Guarantee (PBG)** or released against submission of an equivalent Performance Bank Guarantee, as specified in the tender conditions.

The successful bidder shall furnish an irrevocable and unconditional Bank Guarantee, backed by Fixed Deposit (FD), for an amount equivalent to 100% of the value of the materials to be supplied, in favour of IISER Mohali, as security against the supply of materials. The Bank Guarantee shall remain valid until satisfactory installation is verified by the committee.

Part - A

Sl. No.	**Milestone**	**Milestone Payment (% of **Total Value of project)**
1	Delivery of Passive Components: Supply and delivery of all passive networking components/items as specified in the tender (*Item 4.1 to 4.44* in the *Section – 4: List of Materials*), subject to inspection and acceptance by the Execution Committee.	2.50%
2	Delivery of Active Components: Supply and delivery of active networking components including NGFW, ADC, Core Switches (CS), Distribution Switches (DS), Access Switches (AS), DAC Cables and Transceivers, as specified in the tender (*Item 1.1, 1.2, 2.1 to 2.17* in the *Section – 4: List of Materials)*. Part payment may be permitted against actual delivery, inspection and acceptance of the respective components by the Execution Committee.	45. 00%
3	OFC Infrastructure: Laying and commissioning of OFC, including installation of LIUs and Junction Boxes and completion of LIU-to-LIU connectivity, as per the approved network design and technical specifications, subject to verification by the Execution Committee.	2.50%
4	Installation of Active Components: Installation, configuration and commissioning of all active networking components at the designated locations, in accordance with the approved technical specifications and network architecture, subject to verification by the Execution Committee.	15. 00%
5	Software Stack (*Item 3.1 to 3.9* in the *Section – 4: List of Materials*): Delivery, Installation, configuration, testing and deployment of the required software stack in accordance with the technical specifications and approved implementation plan, subject to verification by the Execution Committee.	15. 00%

6	Testing: Completion of integrated system testing, performance verification and acceptance testing of the implemented solution, including rectification of deficiencies identified during testing, to the satisfaction of the Execution Committee.	15. 00%
7	Submission of PBG: Submission of equipment warranty agreement/document along with the submission of the Performance Bank Guarantee (PBG) in accordance with the terms and conditions of the tender and as approved by the Execution Committee.	5. 00%

**Total value of tender excluding manpower *Section – 4: List of Materials* item no 6.1 and last-mile connection *Item 7.1 to 7.30*.

Part – B: Payment towards the deployed manpower shall be released on a quarterly basis, against submission of the invoice by the bidder. The invoice shall be accompanied by the required supporting documents and duly certified/verified by the Execution Committee for the satisfactory deployment and performance of the manpower during the respective quarter.

Part – C

Sl. No.	**Milestone**	**Milestone Payment (% of Total Value of Last mile connection)**
1	Delivery of passive components/items required for Last Mile Connectivity. Release of payment only after delivery of all items mentioned in tender documents *(Item 7.8 to 7.30* in the *Section – 4: List of Materials*).	5%
2	Execution of Last Mile Connectivity from the Access Switch to the designated User I/O Port, including installation, termination, patching, labelling and testing of the required network connectivity. Payment shall be made on a monthly basis based on the actual work completed and duly certified by the competent authority.	Up to 90%
3	Successful completion and testing of all designated Last Mile Connections, along with submission of PBG.	5%

1. Payments shall be released only after certification by the Execution Monitoring Committee so that the corresponding milestone has been completed satisfactorily.
2. The **Testing & Deployment** payment shall be made only after successful acceptance testing and submission of all relevant test reports and as-built documentation.

Section – 8: Evaluation Criteria

The evaluation process for identifying the successful bidder shall be carried out in two stages:

(a) Technical Evaluation

1. The bids received from the bidders shall first undergo *Technical Evaluation*. The decision of the Institute shall be final and binding on all bidders.
2. The mandatory conditions and requirements specified elsewhere in the bidding document must be strictly complied with. Failure to meet any mandatory requirement or condition may result in the disqualification of the bid.
3. The Technical Evaluation shall be carried out based on the items, quantities, accessories etc. and their specifications along with other technical requirements specified in this bidding document.
4. Only those bidders who are found technically qualified and compliant with the requirements of the bidding document shall be considered for Commercial Evaluation.

(b) Commercial Evaluation

1. The Commercial Evaluation shall be carried out only for those bidders who qualify in the Technical Evaluation.
2. The financial evaluation shall be based on the quantities specified under each item and section – 4 list of material of this bidding document. Bidders shall appropriately quote the unit price for each applicable item.
3. Any missing value in the financial bid shall be treated as Nil (₹0. 00) solely for the purpose of determining the lowest bidder, unless otherwise specified in the bidding document.
4. For the determination of the Lowest Bidder (L1), the total evaluated cost of all items specified in the *Section – 4: List of Materials* shall be considered.

Note – 1: The successful bidder shall be identified based on the outcome of the Technical and Commercial Evaluations, subject to compliance with all applicable terms and conditions of the bidding document.

Note – 2: The quantities of items procured may vary, either higher or lower than the quantities specified in the bidding document, in accordance with the applicable variation/deviation provisions and permissible limits under the contract.

Section – 9: Project acceptance and completion criteria

The Project Acceptance and Completion Criteria shall be aligned with the respective Activity/Milestone stages. Completion of each milestone shall be subject to verification of the corresponding deliverables and acceptance criteria by the Institute or its authorized representatives.

1. Submission of Drawings and Implementation Plans

- Submit all drawings, network layouts and implementation plans specified under Section 3: Scope of Work.
- Implementation shall be carried out in accordance with the approved plans.

2. Delivery of Passive Components

[Corresponding to *Section – 7: Payment Terms,* Part – A, Milestone: 1]

- Supply and deliver all passive networking components/items specified under Items 4.1 to 4.44 of *Section – 4: List of Materials*.
- Items shall be verified against the approved BoQ and technical specifications.

3. Delivery of Active Components

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 2]

- Supply and deliver NGFW, ADC, CS, DS, AS, DAC Cables, Transceivers and other active components specified under Items 1.1, 1.2 and 2.1 to 2.17 of *Section – 4: List of Materials*.
- Verify the make, model, quantity, accessories and applicable licenses (if any) against the approved specifications.

4. OFC Infrastructure

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 3]

- Complete laying, termination and commissioning of OFC, including LIUs, Junction Boxes and LIU-to-LIU connectivity.
- Submit applicable OTDR reports, fibre-loss measurements and link-wise test records.
- Test: verify end-to-end connectivity across all designated network segments in each building with appropriate bandwidth measurements by connecting testing switches.

5. Installation, Configuration and Commissioning

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 4]

- Complete installation, configuration, commissioning and integration of all network and security components at designated locations.
- Verify that all equipment is operational and integrated with the existing campus network, wherever applicable.
- Test: Conduct throughput, latency, packet-loss, concurrent-session and link-utilization tests for critical network links and devices, redundancy establishment, and functionality of NGFW, CS, DS and AS.

6. Software Stack

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 5]

- Complete delivery, installation, configuration, testing and deployment of the required software stack specified under Items 3.1 to 3.9 of *Section – 4: List of Materials*.
- Verify that all applicable software, licenses (if any) and services are operational.
- Test: test and demonstrate the functionality and integration of AAA, NAC, RADIUS, LDAP, DHCP, Internal/External DNS, Directory Services, NTP, Syslog and User Access Logging, including authentication, authorization, connectivity, policy enforcement, monitoring, logging, backup and failover, wherever applicable.

7. Integrated System Testing and Defect Rectification

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 6]

Following completion of the installation, configuration, commissioning and software deployment activities, the complete solution shall undergo integrated system testing. The following shall be successfully completed:

a) **Connectivity and Functional Testing**
   - Verify end-to-end connectivity across all designated network segments, buildings, floors, racks and user locations.
   - Verify the functionality of LAN, WAN, routing, switching, VLANs, DHCP/DNS, Internet connectivity and other applicable network services.
   - Verify that all configured features, policies, services and protocols operate in accordance with the technical requirements.

b) Performance and Capacity Testing
   - Conduct throughput, latency, packet-loss, concurrent-session and link-utilisation tests for critical network links and devices.
   - Verify that NGFW, ADC, CS, DS and other applicable components meet the specified performance, capacity and throughput requirements under representative operating conditions.

c) Redundancy and Failover Testing
   - Test all applicable redundant links, devices, gateways and network paths.
   - Simulate failure of critical links or equipment, wherever applicable, and verify successful failover, service continuity and recovery.

d) Firewall and Security Functionality
   - Verify firewall policies, ACLs, NAT, VPN, routing, application control, security policies, logging, monitoring and administrative access.
   - Verify that all required security features are correctly configured and operational and that unauthorized traffic is appropriately blocked.

e) CS and DS Functionality
   - Verify the complete functionality and integration of CS and DS, including configured services, management, connectivity and redundancy, as applicable.
   - Demonstrate and validate all specified features against the approved technical specifications.

f) Structured Cabling and Fibre Testing
   - Test and certify all applicable copper and optical-fibre links using appropriate calibrated test equipment.
   - Submit copper certification reports, OTDR reports, fibre-loss measurements and link-wise test records, wherever applicable.

g) Monitoring, Management and Backup
   - Verify integration of applicable network, security and software infrastructure with the designated monitoring and management systems.

- Verify configuration backup, logging, alerting, health monitoring and administrative access.

h) Defect Rectification

- All defects, deviations and deficiencies identified during testing shall be documented and communicated to the Bidder/System Integrator.
- All such deficiencies shall be rectified by the Bidder/System Integrator at no additional cost before final acceptance.

Last-Mile Connectivity

[Corresponding to *Section – 7: Payment Terms*, Part – C, Milestone: 1 & 2]

- Complete Last-Mile Connectivity from the Access Switch to the designated User I/O Port.
- Supply the related items specified under Items 7.8 to 7.30 of *Section – 4: List of Materials*.
- Complete installation, termination, patching, labelling and testing of each network connection.

Final Acceptance and Completion

[Corresponding to *Section – 7: Payment Terms*, Part – A, Milestone: 7 and Part-C Milestone-3]

Before final acceptance, the Bidder/System Integrator shall:

- Submit complete as-built network diagrams, configurations, equipment details, test reports and other required documentation.
- Complete acceptance testing and rectify all identified defects and deficiencies.
- Provide required training and complete formal handover of equipment, licenses (if any), credentials, configuration backups, manuals and technical documentation.

The Completion/Acceptance Certificate shall be issued only after successful completion and verification of all applicable milestone requirements by the Institute. Verification may be carried out by the Execution Committee, Internal Committee and/or a Third Party authorized by the Institute.

Acceptance of an individual milestone shall not constitute final acceptance of the complete project. Final acceptance shall be granted only after completion and verification of all applicable milestones and final acceptance requirements.

Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI)

S. No.	Eligibility Criteria of Bidder	Complied (Y/N)	Remarks
1	Bidder should be ISO 9001:2015 certified.		
2	The Bidder must be a reputed manufacturer (OEM) or his authorized System Integrator of the type of products offered. In case of System Integrator, a Letter of Authorization from OEM, specific to the tender, should be enclosed. Signed Back-to-Back agreement is needed. The bids received without Letter of Authorization and Back-to-Back Agreement from OEM are liable to be rejected.		
3	The bidder shall have successfully completed during the last seven years one or more Campus Wide Network projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions. (Appropriate document should be provided)		
4	Bidder should be ISO 9001:2015, 27001:2013 and 20000-1:2011 certified and shall have a minimum CMMI Level 3 or above for Quality Management Systems. For providing Solutions and Services for Network, Router, Switches, Firewall, Cabling etc.		
5	The Bidder shall provide the Registration number GST/Sales Tax/Service Tax/PAN/TIN - Registration number and turnover certified by CA.		
6	The bidder has not been blacklisted by any Central/State Government Department/Organization or educational institutes in last three years.		

Annexure – 2: Eligibility Criteria of OEM (active components)

Sl. No	Eligibility Active Items OEM Active (Core, Distribution & Access Switches)	Complied (Y/N)	Remarks
1	The OEM of the equipment's quoted for should have multiple RMA centers (at least one RMA in Delhi-NCR or in Chandigarh Tricity) in India to support failure of equipment's and better resolution.		
2	The bidder must be a reputed manufacturer (OEM) or authorized System Integrator of the products offered. In the case of the System Integrator, a Letter of Authorization from OEM, specific to the tender, should be enclosed. Bid specific MAF and Back-to-Back support Agreement (bid specific) for the period of 07 years issued to the bidder by the OEM must be submitted for technical qualification of the bidder.		
3	The OEM should support next business day delivery against defective spares. OEM should have 24x7x365 support for India with a direct TAC support in the country.		
4	The OEM should have a registered office in India from last 10 years.		
5	OEM should be ISO 9001/ISO 27001 certified.		
6	OEM of LAN switching should operate a fully functional Design, development and research and development (R &D) center located in India. The center should staff more than 400+ qualified professionals who are actively engaged in product design, engineering, development and advanced R&D activities.		
7	OEM should not be blacklisted by any of the Government/PSU Institution in the last three years in India.		
8	Proposed OEM products should not be declared end of support life in the next 7 years.		
9	Core, Distribution, Access Switches must be from same OEM		
10	Escalation Matrix and Toll-Free Support Number		
11	1. Joint ventures are not accepted / allow in this bid 2. shall not sub-contract the Contract in whole or part to any entity.		

Annexure – 3: Eligibility criteria of OEM (Security System)

Sl. No.	Eligibility criteria for Active Items (Security System)	Complied (Y/N)	Remarks
1	The OEM of the equipment's quoted for should have multiple RMA centers (at least one RMA in Delhi-NCR or in Chandigarh Tricity) in India to support failure of equipment's and better resolution.		
2	The bidder must be a reputed manufacturer (OEM) or authorized bidder of the products offered. In the case of the bidder, a Letter of Authorization from OEM, specific to the tender, should be enclosed. Bid specific MAF and Back-to-Back support Agreement (bid specific) for the period of 07 years issued to the bidder by the OEM must be submitted for technical qualification of the bidder.		
3	The OEM should support next business day delivery against defective spares. OEM should have 24x7x365 support for India with a direct TAC support in the country.		
4	The OEM should have a registered office in India from last 10 years.		
5	OEM should be ISO 27001, ISO 27017, ISO 42001, Common Criteria/ISO-IEC 15408 & IPv6/ certification (IPv6 Logo & interoperability certification)		
6	OEM should not be blacklisted by any of the Government/PSU Institution in the last three years in India.		
7	Proposed OEM products should not be declared end of support life in the next 7 years.		
8	Escalation Matrix and Toll-Free Support Number		

Annexure – 4: Eligibility criteria of OEM (Passive Components)

Sl. No.	Eligibility Criteria for Passive Components	Complied (Y/N)	Remarks
1	The passive components' OEM must be ISO 9001 and ISO 14000 certified. The material must have been manufactured in the OEM's own manufacturing facilities and not outsourced.		
2	The OEM of passive components quoted by the bidder should have a presence in India for at least five years, ending on the previous day of the last day of submission of the tender. Supporting documents must be attached. The OEM should also have at least one manufacturing plant in India to comply with the Make in India initiative.		
3	Passive network components: All passive network components (IO Ports, cat cables, fibres, patch panel, patch cord etc.) preferably be from one OEM.		
4	All fiber cables should be bent compliant with ITU-T G.657. A1, OS2.		
5	For Cat 6 U/UTP cables, performance should be maintained even when termination is within 15 meters, thus ensuring the elimination of short resonance for 4-connector channels. UL/ETL reports for 4 Connectors need to be submitted.		
6	The Cat6/Cat6A U/UTP cable should be ETL verified, and all passive components should comply with the RoHS standard. The declaration of RoHS compliance should be mentioned on the datasheets of each Passive Component.		
7	The Cat 6/Cat6A U/UTP cable should comply with IEC60332-3-22, IEC 61034-1 and -2, IEC 60754-1 and -2, UL 94, EN 50575 features for environment safety.		
8	The Cat 6 U/UTP cable should be ETL verified, and all passive components should comply with the RoHS standard. The declaration of RoHS compliance should be mentioned on the datasheets of each Passive Component.		
9	Vendor/bidder should bring the sample of passive components and test reports (from any testing software/device) for evaluation by the technical evaluation committee.		
10	The Cat 6A U/UTP cable shall be ETL/UL verified and comply with ANSI/TIA-568.2-D, ISO/IEC 11801 and IEC 61156-5, supporting 10GBASE-T up to 100 meters.		

Annexure – 5: Check List to be submitted by Bidder/OEM

Sl. No	Particulars	Submitted (Yes/No)
1	Signed Integrity Pact	
2	EMD/valid exemption certificate (clearly mentioning that vendor is eligible for exemption).	
3	Land border sharing declaration certificates	
4	MII Content Certificates	
5	Bidder Turnover certificate certified by CA for last 5 years.	
6	Manufacturer's Authorization Form (MAF): Valid MAF for the products offered. 1. If products from multiple OEMs are quoted, a separate MAF from each such OEM shall be submitted. 2. In case the bidder is not the OEM, the MAF shall authorize the bidder to quote, supply, install, and support the offered products.	
7	The bidder shall provide its registration number, valid GSTIN, and PAN allotted by the competent authorities, along with any other applicable statutory registration details.	
8	A letter of commitment for seven years from the date of installation, with respect to hardware and firmware support from OEM should be enclosed in the cover for technical bid. Where the quoted system comprises components from multiple OEMs, separate seven-year commitment from each OEM shall be submitted.	
9	Undertaking (self-certificate) by bidder that the bidder or OEM has not been blacklisted by any Central/State Government Department/Organization or educational institutes in last three years.	
10	The OEM and the bidder shall provide a clearly defined escalation matrix (including Toll Free number), including designated contact persons and escalation levels, for timely resolution of issues.	
11	Undertaking that "No" EOL/EOS products have been quoted and the same should be stated on OEM letterhead that EOL/EOS would not be there for quoted products for at least 7 years. Where the quoted system comprises components from multiple OEMs, separate undertaking is required from each OEM and shall be submitted.	
12	Certificate for bidder has direct local sales and support office in Chandigarh-Mohali-Panchkula Tri-city or in Delhi NCR.	
13	Point by point compliance of all components *Annexure – 8: Make and model number of all materials listed in section 4 and* ***Error! Reference source not found.***	
14	All ISO certificates for bidders as SI and OEM	
15	Document proof that bidders have experience of executing similar orders in last 7 financial years as per *Annexure – 6: Past performance (to be submitted by letterhead*)	

16	Filled and submitted Annexture – 1-9; *Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI)* *Annexure – 2: Eligibility Criteria of OEM (active components)* *Annexure – 3: Eligibility criteria of OEM (Security System)* *Annexure – 4: Eligibility criteria of OEM (Passive Components)* *Annexure – 5: Check List to be submitted by Bidder/OEM* *Annexure – 6: Past performance (to be submitted by* **letterhead**) *Annexure – 7: Service Level Agreement (SLA)* *Annexure – 8: Make and model number of all materials listed in section 4*	
17	Non-Malicious code certificate to be submitted on the OEM letterhead.	

Annexure – 6: Past performance (to be submitted by letterhead)

List of the organizations for whom the bidder has undertaken such work during the last seven years. The documentary evidence of Purchase Orders and Completion Certificates must be submitted for each entry.

S. No	Name of Organization	Name of the Contact person and Contact details with Phone no	OEM	Purchase Order No	Purchase Order Date	Completion Date	Purchase Order Value	Value in Rupees
1								
2								
3								
…								
…								

Note: Without submission of the relevant Purchase orders, the experience will not be considered.

Annexure – 7: Service Level Agreement (SLA)

Sl. No	Conditions	Compliance (Yes/No)	Remarks if Any
1	The entire solution including each software, firmware and hardware component should have at least 7 years on-site NBD warranty. The vendor will be required to attend the complaint if any within two business-days.		
2	Bidder/OEM should ensure that the spare parts/components/items should be available for at least 7 years or at the updated version should be compatible with the offered hardware.		
3	The Bidder warrants that all the goods are new, unused, and of the most recent or current supported models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.		
4	The warranty period is to be counted from the date when the installation is completed, and the acceptance/completion certificate has been issued by IISER Mohali		
5	Requests for remote access for installation/fine-tuning will not be entertained during the installation period. No remote access should be asked for rectification or service-related issues during the warranty period.		
6	Acceptance certificate will be issued only after all the acceptance tests as outlined earlier have been satisfactorily passed.		
7	The Bidder shall deploy one (01) Network Engineer onsite with minimum 3 years' relevant enterprise networking experience for network administration, monitoring, configuration, troubleshooting and support. The engineer shall be available during Institute working hours and respond to critical incidents within 30 minutes. Deployment shall initially be for 6 months, extendable up to 1 year or more based on the requirement; Manpower will be deployed after issuing of completion certification; however, bidder agrees to involve the same engineer during testing phase to understand proposed network.		
8	Any newer version available of the firmware proposed in the respective devices such as NGFW, CS, DS, AS etc. should be provided and implemented at no extra cost for the entire contract period.		
9	All the components should have at least 7 years of End-of-life.		

10	The Bidder shall provide 24×7×365 days online support as and when required by the Institute. In the event that an issue is not resolved within 2 hours of being reported, including on public holidays, the Bidder shall depute a qualified engineer to the Institute's site within 24 hours of the issue being reported. In case of failure to provide the required support within the stipulated timeframe, the Institute shall be entitled to levy a penalty of ₹10,000 per day of delay. Any such penalty shall be recoverable from payments due or becoming due to the Bidder under the contract and, where applicable, may be recovered from the Performance Security, in accordance with the terms and conditions of the contract.		
11	The Bidder shall replace any faulty or defective material/part within 48 hours of the complaint being reported by the Institute. In case of failure to replace the faulty material/part within the stipulated timeframe, the Institute shall be entitled to levy a penalty of ₹5,000 per day of delay. The penalty shall be recoverable from any payments due or becoming due to the Bidder under the contract and, where applicable, may be recovered from the Performance Security, in accordance with the terms and conditions of the contract.		
12	The equipment warranty agreement/document must be submitted to IISER Mohali. The final payment will be released only upon receipt of warranty agreement/document.		
13	The defects, if any, during the guarantee/warranty period are to be rectified free of charge by arranging free replacement within 2 NBD.		
14	During the warranty period, the OEM/bidder must undertake comprehensive maintenance of the entire hardware components, equipment, and software support supplied by the vendor at the place of installation of the equipment.		
15	Technical support shall be provided for system administration and maintenance of all devices for the entire warranty period.		
16	The bidder must submit a list of service engineers employed by them who are competent to serve installation during commissioning time along with their contact details.		
17	The bidder should provide hands-on training to the IISER Mohali Network Team. It shall be on premises without charge.		
18	Active network components: Switches (CS, DS, AS, compatible transceivers etc.) should be from one OEM.		
19	All equipment must be installed following best practices recommended by the OEM (Original Equipment Manufacturer).		
20	The Bidder may submit all site-specific requirements identified during the site survey and clearly specify the existing network information/infrastructure required for		

	integration. IISER Mohali reserves the right to withhold any sensitive or security-critical information; the Bidder shall provide justification for any such information requested.		
21	Confidentiality and Non-Disclosure: The Bidder shall maintain strict confidentiality of all information, documents, data, and technical details relating to the Institute's network and IT infrastructure. This shall include, but not be limited to, network architecture and design, network topology/layout, IP addressing scheme, VLAN details, configurations, security policies and rules, firewall configurations, access controls, credentials, system diagrams, vulnerabilities, logs, and other security-related information. The Bidder shall not disclose, share, reproduce, publish, or make such information available to any third party without the prior written authorization of the Institute. The confidentiality obligations shall remain applicable throughout the contract period and after its completion or termination.		
22	Non-Disclosure Agreement (NDA): The successful bidder shall be required to execute and sign a Non-Disclosure Agreement (NDA) with the Institute prior to commencement of the work. The Bidder shall comply with all confidentiality and information-security requirements stipulated in the NDA throughout the contract period and thereafter, as applicable.		

Annexure – 8: Make and model number of all materials listed in section 4

List to be given for all items except the items related to *jobs, works and manpower*.

Sl. No	Item No.	Item Description	Make	Model Number	Country of origin	Compliance (Yes/No)	URL of the Product Datasheet
1	1.1	Next Generation Firewall (NGWF): NGFW Firewall 4 x 100GE/40GE QSFP28 slots, 10 x 25GE/10GE SFP28 slots, 10 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing;HA support; SIEM integration; 7 Year Warranty					
2	1.2	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty					
3	2.1	Core Switch (CS): Core Switch Supply of Layer 3, 32 Port x 40/100 Gbps SFP port core switch; Switching capacity: at least 6Tbps; with field replaceable redundant power supplies and FANs; 7 Year Warranty;					
4	2.2	Distribution Switch (DS) Type - 1: DS Switch Type-1: Distribution Switch Supply of Layer 3, 48-port SFP28 10/25GbE, with 8x-port					

		40/100GbE; Switching capacity at least 4Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty;					
5	2.3	Distribution Switch (DS) Type - 2: DS Switch Type-2: Distribution Switch Supply of Layer 3, 24-port SFP28 10/25 G, with 4x-port 40/100GbE; Switching capacity: at least 2Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty,					
6	2.4	Access Switch (AS) Type - 1: AS Switch Type-1: Access Switch/Edge Switch: 24x1/10GbE Base-T RJ45 ports; 4 × 25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 680gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty					
7	2.5	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty					
8	2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty					
9	2.7	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty					
10	2.8	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty					
11	2.9	100G DAC Copper Cable - 1M: 100GbE QSFP28 to QSFP28 Direct Attached, Passive Copper Cable, 1m. Stacking					

12	2.10	100G DAC Cable - 1M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 1m, 1-pack					
13	2.11	100G DAC Cable - 5M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 5m, 1-pack					
14	2.12	100G DAC Cable - 10M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 10m, 1-pack					
15	2.13	40G DAC Cable - 5M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 5m, 1-pack					
16	2.14	40G DAC Cable - 10M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 10m, 1-pack					
17	2.15	40G QSFP+: 40GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack					
18	2.16	25G QSFP+: 25GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack					
19	2.17	10G SFPP: 10GBASE-LR, SFPP SMF LC CONNECTOR (No TAA)					
20	3.1	AAA Server: AAA Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Authentication, Authorization, and Accounting (AAA) server supporting TACACS+ and/or RADIUS protocols for secure network access control, user management, policy enforcement, and accounting logs.					
21	3.2	Network Access Control (NAC): Network Access Control (NAC): Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network infrastructure.					
22	3.3	RADIUS Server: RADIUS Server: Supply, installation, configuration, integration, testing, and commissioning of a standards-compliant RADIUS server supporting IEEE 802.1X/EAP authentication for centralized user authentication, authorization, and accounting across wired and wireless networks.					

23	3.4	LDAP Server: LDAP Server: Supply, installation, configuration, integration, testing, and commissioning of an LDAP directory service for centralized identity management, user authentication, role-based access control, and integration with AAA, NAC, network devices, and enterprise applications.					
24	3.5	Internal DNS Server: Internal DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an Internal DNS server for secure name resolution, forward and reverse lookup zones, dynamic DNS updates, and integration with internal directory and network services.					
25	3.6	External DNS Server: External DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an External DNS server for authoritative public DNS hosting, secure zone management, redundancy, and integration with Internet-facing services.					
26	3.7	Network Management System (NMS): Network Management System (NMS): Supply, installation, configuration, integration, testing, and commissioning of a centralized Network Management System for device discovery, inventory, topology visualization, configuration management, fault, performance, and availability monitoring using SNMP, Syslog, NetFlow/sFlow, and related protocols.					
27	3.8	Syslog Server: Syslog Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Syslog server for secure collection, storage, indexing, monitoring, correlation, alerting, and analysis of logs generated by network, security, and server infrastructure.					
28	3.9	Software Stack Deployment: The successful bidder must deploy above network services along with DHCP, DNS (internal & external), Directory Server (DC/ ADC and LDAP), NTP, Syslog and User Access Log. All these servers must be configured preferably using Open Source.					
29	4.1	96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket.					

30	4.2	48 Core OFC: Single Mode fiber 48 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket.					
31	4.3	24 Core OFC: Single Mode fiber 24: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable.					
32	4.4	12 Core OFC: Single Mode fiber 12: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable.					
33	4.5	LIU-24P: 24 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails					
34	4.6	LIU-48P: 48 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails					
35	4.7	LC-LC Patch Cord-Type-1: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 0.5m					
36	4.8	LC-LC Patch Cord-Type-2: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 1m					
37	4.9	LC-LC Patch Cord-Type-3: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 2m					
38	4.10	LC-LC Patch Cord-Type-4: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 5m					
39	4.11	LC-LC Patch Cord-Type-5: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 10m					
40	4.12	Custom Patch Cords-2c: 2-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord					
41	4.13	Custom Patch Cords-4c: 4-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord					
42	4.14	Custom Patch Cords-6c: 6-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord					
43	4.15	Custom Patch Cords-8c: 8-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord					
44	4.16	Compatible Pigtail: LC/UPC male type single-mode OS2 9/125 µm fiber pigtail, with locking latch, suitable for direct connection to LC female adapter of LIU with bare-fiber end for fusion splicing.					
45	4.17	Junction Box: Outdoor Junction Box for OFC termination IP67: all weather outdoor box, to be installed as a junction box for 96 fibres					

		LIU					
46	4.18	HDPE Duct-Type1: Duct for OFC HDPE Pipe 24 Core and 48 Core OFC					
47	4.19	HDPE Duct-Type2: Duct for OFC HDPE Pipe for 96 Core OFC					
48	4.20	OFC Laying: OFC Laying by non-trenching method					
49	4.21	CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each					
50	4.22	CAT6 Cable type -2: Metallic armour CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each					
51	4.23	CAT6 Patch Panel 24P: 24 port CAT 6 Patch Panel					
52	4.24	CAT6 Patch Panel 48P: 48 port CAT 6 Patch Panel					
53	4.25	CAT6 Patch Cord - type - 1: Patch Cords 0.5M					
54	4.26	CAT6 Patch Cord - type - 2: Patch Cords 1M					
55	4.27	CAT6 Patch Cord - type - 3: Patch Cords 2M					
56	4.28	CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each					
57	4.29	CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each					
58	4.30	CAT6A Patch Panel 24P: 24 port CAT 6A Patch Panel					
59	4.31	CAT6A Patch Panel 48P: 48 port CAT 6A Patch Panel					
60	4.32	CAT6A Patch Cord - type - 1: Patch Cords 0.5M					
61	4.33	CAT6A Patch Cord - type - 2: Patch Cords 1M					
62	4.34	CAT6A Patch Cord - type - 3: Patch Cords 2M					
63	4.35	Conduit-Square: Conduit Square (24x24)					
64	4.36	Conduit-Round: Conduit round (10mm)					
65	4.37	T-joints: Compatible with 10mm round conduit					
66	4.38	L-joints: Compatible with 10mm round conduit					
67	4.39	Flexi-pipe-a: Compatible with 10mm round conduit					
68	4.40	Flexi-pipe-b: Compatible with 24mmx24mm conduits					

69	4.41	Racks-Type-1: 6 U Network racks					
70	4.42	Racks-Type-2: 9 U Network racks					
71	4.43	Racks-Type-3: 12 U Network racks					
72	4.44	Racks-Type-4: 15 U Network racks					
73	5.1	Work - 1: Work and commissioning of All switches, laying cables & installation of AS in every building, integrating to existing system, designing the entire network segment and implementing the policies etc.					
74	6.1	Manpower: One (01) qualified and trained Network Engineer shall be deployed onsite for day-to-day network administration, monitoring, troubleshooting, configuration, preventive maintenance, and technical support of the networking infrastructure. The minimum qualification of the engineer should be at least BE/ B.Tech /equivalent degree in network and information technology.					
75	7.1	Works - 2: Through Existing Concealed Conduits/Pipes: Pulling and routing CAT6/6A cable(s) through existing concealed conduits/pipes without providing any new conduit or channel. Includes cable pulling, routing, dressing, termination at both ends, testing, labeling, and commissioning.					
76	7.2	Works - 3: Laying New PVC Conduit – Up to 2 CAT6/6A Cables: Fixing suitable PVC conduit with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
77	7.3	Works - 4: New PVC Conduit – 3 to 10 CAT6/6A Cables: Fixing suitable PVC conduit of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
78	7.4	Works - 5: New PVC Conduit – More than 10 CAT6/6A Cables: Fixing suitable PVC conduit(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
79	7.5	Works - 6: New PVC Trunking/Channel – Up to 2 CAT6/6A Cables:					

		Fixing suitable PVC trunking/channel with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
80	7.6	Works - 7: New PVC Trunking/Channel – 3 to 10 CAT6/6A Cables: Providing and fixing suitable PVC trunking/channel of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
81	7.7	Works - 8: New PVC Trunking/Channel – More than 10 CAT6/6A Cables: Fixing suitable PVC trunking/channel(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.					
82	7.8	PVC Conduit 20MM: New 20 mm Heavy-Duty PVC Conduit: Fixing 20 mm HD PVC conduit with all accessories for laying and routing up to 2 CAT6/6A cables					
83	7.9	PVC Conduit 25MM: New 25 mm Heavy-Duty PVC Conduit: Fixing 25 mm HD PVC conduit with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.					
84	7.10	PVC Conduit 32MM: New 32 mm (Minimum) Heavy-Duty PVC Conduit: Fixing 32 mm HD PVC conduit (increasing to 40 mm or multiple conduits, as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.					
85	7.11	PVC Trunking/Channel 25 mm x16 mm: New 25 × 16 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing up to 2 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.					
86	7.12	PVC Trunking/Channel 40 mm x 25 mm: New 40 × 25 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.					

87	7.13	PVC Trunking/Channel 60 mm x 40 mm: New 60 × 40 mm (Minimum) PVC Trunking/Channel: Fixing PVC trunking/channel (increasing to larger sizes as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning.					
88	7.14	Ferrule type - 1: Appropriate Ferrule for labelling Cat6 cable (100 x 10 Pieces) Each packet					
89	7.15	Ferrule type - 2: Appropriate Ferrule for labelling Cat6A cable (100 x 10 Pieces) Each packet					
90	7.16	CAT6 IO Jacks: CAT6 IO jacks (RJ45 I/O modules)					
91	7.17	CAT6 Face Plates: CAT6 Face Plate (Single Port)					
92	7.18	CAT6 Mounting Box: Mounting Box / Backbox for Face Plate					
93	7.19	CAT6A IO Jacks: CAT6A IO jacks (RJ45 I/O modules)					
94	7.20	CAT6A Face Plates: CAT6A Face Plate (Single Port)					
95	7.21	CAT6A Mounting Box: Mounting Box / Backbox for Face Plate					
96	7.22	Flexi pipe - 1: to fit the size of conduit Size of 20 mm					
97	7.23	Flexi pipe - 2: to fit the size of conduit Size of 25 mm					
98	7.24	Flexi pipe - 3: to fit the size of conduit Size of 32 mm					
99	7.25	T-Joints - 1: to fit the size of conduit Size of 20 mm					
100	7.26	T-Joints - 2: to fit the size of conduit Size of 25 mm					
101	7.27	T-Joints - 3: to fit the size of conduit Size of 32 mm					
102	7.28	L-joints - 1: to fit the size of conduit Size of 20 mm					
103	7.29	L-joints - 2: to fit the size of conduit Size of 25 mm					
104	7.30	L-joints - 3: to fit the size of conduit Size of 32 mm					

Annexure – 9: Specifications as per the Section – 4 List of Materials

1.1	Next Generation Firewall (NGWF): NGFW Firewall 4 x 100GE/40GE QSFP28 slots, 10 x 25GE/10GE SFP28 slots, 10 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing; HA support; SIEM integration; 7 Year Warranty (Quantity: 2 Number)			
Spec. No	Parameters	Sub Items No	Technical Specifications	Compliance (Yes/No)
1.1.1	Hardware features and throughputs	1.1.1.1	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall appliance should have minimum 20 core processing and management purposes along with minimum 48 GB RAM	
		1.1.1.2	Next Gen Firewall throughput measured with Application Control/Identification and logging enabled, utilizing L7 transactions should be 25 Gbps or higher |OR| 32 Gbps or higher standard NGFW performance as measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.	
		1.1.1.3	Threat Prevention throughput measured with Application Control/Identification, IPS, antivirus, antispyware, sandboxing, file blocking, and logging enabled, utilizing L7 transactions should be 15 Gbps or higher |OR| 30 Gbps or higher standard Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic	
		1.1.1.4	support a minimum of 250 concurrent VPN connections with centralized user authentication and access control should be extendable to future upgradation.	
		1.1.1.5	Max concurrent sessions are measured utilizing L7 transactions should be 2 million or higher |OR| Concurrent Sessions (TCP) should	

			be minimum 40 million	
		1.1.1.6	New sessions per second utilizing L7 transactions should be 200K or higher |OR| New Sessions/Second (TCP) should be minimum 600K	
		1.1.1.7	Minimum I/O Ports required from Day 1: Min.1G/2.5G/5G/10G (12 Nos.), 1G/10G SFP/SFP+ (10 Nos.), 25G SFP28 (4 Nos.), 40G/100G QSFP/QSFP28 (2 Nos.) For each NGFW: SFP+ I/O ports to be loaded with atleast 2 Nos. SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant. QSFP28 I/O ports to be loaded with atleast 2 Nos. QSFP+ form factor, 40Gb SR4 optical transceiver, short reach 100m OM3, 8/12 strand MPO connector, IEEE 802.3ba 40GBASE-SR4 compliant	
		1.1.1.8	Minimum Dedicated Management Ports required from Day 1: Management port (1 No.), High availability (2), Console port (1 No.)	
		1.1.1.9	VDOM/virtual contexts/virtual systems within a single physical appliance should be available as a feature if required to be added.	
		1.1.1.10	Power Supply: Redundant 100–240 VAC (50–60Hz) Operating temperature: 0°C to 50°C Humidity tolerance: 10% to 90%	
		1.1.1.11	All throughputs should be on single hardware not to be calculated on clustering.	
1.1.2	Software/OS/Platform features:	1.1.2.1	Supported modes from day 1: active/active, active/passive	
		1.1.2.2	NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation)	
		1.1.2.3	NAT64, NPTv6	
		1.1.2.4	NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription	
		1.1.2.5	Aggregate interfaces (802.3ad), LACP.	
		1.1.2.6	802.1Q VLAN tags per device/per interface: 4, 094/4, 094	

		1.1.2.7	IPsec and SSL VPN: Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3des, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Secure access over IPsec or SSL VPN tunnels using VPN Gateway and portals	
		1.1.2.8	The proposed solution should support remote user based VPN clients for Windows. Module should be Common Criteria certified for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	
		1.1.2.9	Routing: OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD)	
		1.1.2.10	Interface Modes: L2, L3, tap, transparent	
		1.1.2.11	Should be able to stop known and unknown exploits, malware, spyware, and command-and-control (C2) threats	
		1.1.2.12	Should be able to inspect and apply policy to SSL/TLS-encrypted traffic, both inbound and outbound, including for traffic that uses TLSv1.3 and HTTP/2.	
		1.1.2.13	Should provide visibility into TLS traffic, such as the amount of encrypted traffic, SSL/TLS versions, cipher suites, and more, without decrypting.	
		1.1.2.14	Should provide an option to enable or disable decryption—based on, for example, URL category, source and destination zone, address, user, user group, device, and port—for privacy and regulatory compliance purposes.	

		1.1.2.15	Should enable visibility, security policies, reporting, and forensics based on users and group, and IP addresses.	
		1.1.2.16	Should have the provision to integrate with repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies.	
		1.1.2.17	Should prevent corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.	
		1.1.2.18	Should be able to identify the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (SSL/TLS)	
		1.1.2.19	Should have the ability to create custom application tags/signatures for proprietary applications	
		1.1.2.20	Should be able to identify all payload data within the application (e. g. , files and data patterns) to block malicious files and thwart data exfiltration attempts	
		1.1.2.21	Should embed machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.	
		1.1.2.22	Should leverage cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW. The sandboxing environment for analysis should support Windows, Mac OS X, Linux.	
		1.1.2.23	The solution should support or leverages artificial intelligence with machine learning (AIops) for enhanced network operations with features like: (a) assess the firewall's configuration and identify areas for improvement (b) provide easy access to runtime and historical telemetry data from firewalls (c) detect system issues (independent of the detection method) (d) reduce time to resolution through alert/notification workflows	

			(e) provide dynamic dashboards and visualizations	
		1.1.2.24	Should support IOT and OT Device Detection, IOT and OT vulnerability correlation; OT Application Control and IPS.	
		1.1.2.25	Should support predictable performance with all security services enabled, include centralized administration and configuration management of firewalls. In case centralized management is not available, the administrator should be able to configure the firewall directly from GUI with complete feature parity.	
1.1.3	Subscription, Support and Warranty	1.1.3.1	NGFW should have a 7 year subscription of Advanced Threat Prevention, Application Control/Identification, URL Filtering, Sandbox, DNS Security, IoT, SD-WAN, Client-based-VPN for Windows and Mac (If applicable). All updates, upgrades, and hotfixes should be applicable to a period of 7 years.	
		1.1.3.2	NGFW platform should have 24/7 OEM support via online/chat/telephone for a period of 7 years.	
		1.1.3.3	NGFW hardware should have 7 years RMA warranty	
1.1.4	Certifications	1.1.4.1	ISO 27001, ISO 27017, ISO 42001	
		1.1.4.2	Common Criteria/ISO-IEC 15408	
		1.1.4.3	IPv6/USGv6	
		1.1.4.4	TELECOMMUNICATION ENGINEERING CENTRE - CERTIFICATE OF MANDATORY CONFORMANCE	
		1.1.4.5	Make In India self declaration by OEM for NGFW	
		1.1.4.6	Following OEM certificates to be uploaded: a. Land Border Declaration b. Manufacturer Authorization Form for bidder c. Escalation Matrix and Toll Free Support Number d. SELF-CERTIFICATION for MII e. Non-Malicious Code Certificate f. Non-Blacklisting Declaration g. End of Life/Support of the Hardware h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625	

			Functional Package for SSH Version 1. 0 PP-Module for Intrusion Prevention Systems (IPS), Version 1. 0 PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 collaborative Protection Profile for Network Devices Version 3. 0e i. Common Criteria for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	
1.2	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty (Quantity: 2 Number)			
Spec. No	Parameters	Sub Items No	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
1.2.1	GENERAL	1.2.1.1	The proposed hardware platform should be of high performance and purpose-built next Generation platform for application delivery and security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF); Web Application solution should not be a white labeled WAF running on third party hardware.	
		1.2.1.2	The solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the solution and integration with automation and CI/CD tools including Ansible, Jenkins, and Terraform. The solution shall support overlay network like VxLAN/Geneve for integration with kubernetes services	
		1.2.1.3	The solution shall have integration with Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from the same make as WAF. It should not be third party or open source.	
		1.2.1.4	The Controller/Container Plugin shall support both Nodeport and	

			ClusterIP mode of deployment and also as an Ingress service capable of forwarding traffic to container clusters via NodePort and ClusterIP.	
		1.2.1.5	The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects and shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	
		1.2.1.6	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should register to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource Queue maintained by the controller.	
		1.2.1.7	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on global public domain like product datasheets, product guides etc. and the proposed solution must support all technical features specified in the RFP from the date of issue of this RFP.	
		1.2.1.8	Bidder/OEM may be asked to demonstrate all the technical features asked in the RFP through a POC and any non-compliance in the technical functionality/feature may lead to rejection of the bid.	
1.2.2	HARDWARE	1.2.2.1	The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 1.2 million 2) Network interfaces: 4x10G/1G RJ45 and 4x1G SFP+/SFP28/SFP from day 1. The 1G SFP interface should be upgradable to 10G and 25G by changing the transceivers. 3) SSL Throughput: at least 20 Gbps with 30K SSL TPS with 2K keys and 14K with ECC 4) Storage: at least 480 GB SSD 5) Memory: at least 64GB	
		1.2.2.2	The appliance must use its own Hypervisor which should be a specialized purpose-built hypervisor and NOT a commercially available hypervisor like XEN, KVM etc. The Appliance should not support deployment of any third-party software on its hardware. The	

			appliance must support at least 8 virtual instances from day 1 scalable up to 24 instances in future with license upgrade.	
1.2.3	Load Balancing Features	1.2.3.1	The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys	
		1.2.3.2	The proposed solution must offer out of band programming for control planes along with data plane scripting for functions like content inspection and traffic management. The proposed LB should be capable to trigger a script based on an event	
		1.2.3.3	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2	
		1.2.3.4	The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance	
		1.2.3.5	The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching, caching & compression, hardware based SSL offload and server side compression.	
		1.2.3.6	The Proposed solution should be able to monitor the applications using intelligent application monitors which can be either using system defined executable scripts. It should also provide mechanism to bind multiple health checks, support for application specific VIP health check and next gateway health checks	
1.2.4	WAF FEATURES	1.2.4.1	The solution should provide OWASP Compliance Dashboard which provides a holistic and interactive interface that clearly measures	

			app's compliance against the Application Security Top 10 attacks and also provide suggestions/shortcuts to address the compliances and configure policies for it	
		1.2.4.2	The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system. 1. Different WAF policy and signature set based on URI 2. Should redirect traffic to different pool members based on URI 3. Should be able to rate limit based on each URI	
		1.2.4.3	A given user must be enforced to follow a sequence of pages while accessing without any script and should have provision to apply the restriction to the application or part of the application based on Geo Location	
		1.2.4.4	The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.	
		1.2.4.5	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode. The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	
		1.2.4.6	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	
		1.2.4.7	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema	

			validation, common attacks mitigation, and XML parser denial-of-service prevention.	
		1.2.4.8	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)	
		1.2.4.9	System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.	
		1.2.4.10	The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance (without accessing the internet/cloud service) to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCI DSS compliance requirements for web application servers. Necessary logs to be generated for audit and compliance.	
		1.2.4.11	Solution should support the following Security Protections:	
			* BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats	
			* POSITIVE and NEGATIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic. The administrators should be able to see all the signatures and not just the signature categories. Admins can apply Specific signatures to specific policies	
		1.2.4.12	The solution must be able to block transactions with content matching known attack signatures while allowing everything else. The solution should also have an option to put a signature in staging mode. Meaning that the system applies the attack signatures to the web application traffic, but does not apply the blocking policy action	

			to requests that trigger those attack signatures.	
		1.2.4.13	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. - Ability to drop requests and responses, b. - Block the TCP session, c. - Block the application user, or IP address d. Should be able to generate unique identifier to track attack event	
		1.2.4.14	Proposed WAF Solution should have capability to automatically learn should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc. Solution should support different profiling like different values like Directories, URLs, Form Field Values, Metacharacters etc. for different applications.	
		1.2.4.15	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic	
		1.2.4.16	The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.	
		1.2.4.17	The WAF must provide BOT mitigation functionality (including CAPTCHA) without having to go on internet for some cloud based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc.	
		1.2.4.18	Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.	
		1.2.4.19	The solution should be able to perform profiling of JSON with a dedicated JSON parser to inspect all JSON messages and apply security policies to embedded object pairs and binary payloads. Solution should enforce JSON security policy parameters, such as restricting URL wildcards and parameters, malformed data, and	

			JSON payloads, methods and objects.	
		1.2.4.20	The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • Backend application parser protection against XML DOS • XML Encryption and XML Signatures • Granular WSDL methods selection	
		1.2.4.21	The proposed solution must support SSL VPN and Single Sign On functionality on the same hardware solution running on the same OS version from the same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and the same should be configurable. * Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken	
		1.2.4.22	The Web Application Firewall Solution shall have the Geo-location based IPv4 & IPv6 database. So, Geo-location based traffic filtering shall be done on the Web Application Firewall.	
1.2.5	API SECURITY	1.2.5.1	WAF must provide inbuilt capability of API security including support for uploading swagger file and protect leakage of user credentials accessing the web applications using HTML field Obfuscation to protect against malware-based attacks and the solution should have capability to protect Credential Attacks that can steal credentials from the user's browser to avoid cyber exploits. It should be able to authenticate users based on browser type and version, operating system type and version. Necessary logs to be	

			generated for audit and compliance.	
		1.2.5.2	Solution should be able to Imported OpenAPI file automatically and configure policy with all API specific parameters as a list of allowed URLs, parameters, methods, and so on. Solution should have an API security template which pre-configures WAF policy with all necessary violations and signatures to protect API backend.	
		1.2.5.3	Solution should support reverse engineering for API Schema via Learning mode, should be able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	
1.2.6	HIGH AVAILABILITY	1.2.6.1	The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to achieve horizontal scaling	
1.2.7	MONITORING, LOGGING AND REPORTING	1.2.7.1	The proposed solution should have the capability to create a granular logging policy per application. The system shall have the ability to customize logging. The proposed solution should have the capability to define a customized log format for each application.	
		1.2.7.2	The proposed solution should have the capability to define multiple log destinations for each application	
1.2.8	ADMINISTRATION	1.2.8.1	Proposed Solution should have Role-based management & Access Control with user authentication. There should be web application security administrator who has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(similar) who configure or view most parts of the web security policy object in specific controlled partitions holding the policy and profile objects. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor	

			d. Operator e. SSL Certificate Manager f. Guest	
		1.2.8.2	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)	
		1.2.8.3	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a. Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b. Number of failed login attempts which result in an account to be locked c. Lock duration in minutes	
		1.2.8.4	Should have diagnostics capability support (e. g. logs, core dumps, Syslogs, configurations etc.) which can be used to share with technical support team in case of any malfunctioning by the devices. Should have an online vulnerability and configuration diagnosing tool.	
1.2.9	Product / OEM Evaluation Criteria	1.2.9.1	WAF / WAF's Operating System should be tested and certified for NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	
		1.2.9.2	The WAF solution should be in the Gartner's/Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.	

2.1	Core Switch (CS): Core Switch Supply of Layer 3, 32 Port x 40/100 Gbps SFP port core switch; Switching capacity: at least 6Tbps; with field replaceable redundant power supplies and FANs; 7 Year Warranty; (Quantity: 2 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance (Yes/No)
2.1.1	Product details	2.1.1.1	Make, Model No. /OEM Part Code. (Please specify)	
2.1.2	Architecture & Port Density	2.1.2.1	The Switch shall have 32x 40G/100G QSFP+ Port from Day 1.100G DAC Passive cable 1m to be supplied with each switch, Transceivers should be supplied as per the solution. All the 40/100G ports should support 4x 10G SFP+ or 4x 25 G SFP28 by using split cable as required.	
		2.1.2.2	The Switch shall support Virtual Chassis (VC) or equivalent Switch Clustering/Stacking feature of 8 Switches or More, where the Switch Clustering feature shall combine multiple switches into a single network element. Stacking bandwidth of 400 Gbps should be supported.	
2.1.3	Performance	2.1.3.1	Switching Bandwidth: The Switch shall provide Switch Fabric Bandwidth Capacity of 6.4Tbps or more.	
2.1.4	Layer 2 features: it shall support from day 1	2.1.4.1	Should support 4K vlan Id	
		2.1.4.2	Should support 100K MAC addresses or more	
		2.1.4.3	IP multicast snooping IGMP v1, v2, v3	
		2.1.4.4	Jumbo Frames (up to 9216 bytes)	
2.1.5	Layer 3 features: it shall support from day 1	2.1.5.1	Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1	
		2.1.5.2	IPv4 & IPv6 Routing protocols & multicast routing available from day 1.	
		2.1.5.3	RIP v1 or v2, RIPng, OSPFv2, OSPFv3, BGP4, BGP4+, Multi-VRF, VRRP for both IPV4 and IPV6 protocol, VRRPv2 & VRRPv3, Vxlan	
		2.1.5.4	PIM-SSM, PIM Sparse, PIM Dense, PIM Anycast RP, and PIM passive IPv4 multicast routing.	
		2.1.5.5	PIM-SSM, PIM Sparse, PIM Anycast RP, MSDP and PIM6-SM Snooping IPv6 multicast routing	

		2.1.5.6	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.1.6	Security features	2.1.6.1	RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords	
		2.1.6.2	Secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.1.6.3	IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection	
		2.1.6.4	IPv4 and IPv6 ACLs: with up to 8000 rules / ACL per system	
		2.1.6.5	Flexible Authentication with 802.1x Authentication and MAC Authentication	
2.1.7	Manageability	2.1.7.1	Should support manageability using on prem Centralized Management platform using Web based Graphical User Interface (GUI) and also should be remotely manageable from the Cloud.	
		2.1.7.2	It shall support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP, access to switch for management/monitoring. NTP (Network Timing Protocol) should be supported.	
		2.1.7.3	It should also support NetFlow or sFlow or equivalent	
		2.1.7.4	It should support Hitless Failover/ISSU	
2.1.8	Physical Attributes	2.1.8.1	The Switch shall be configured with hot swappable, redundant AC power supplies/fans to provide 1:1 or N+1 power supply redundancy or better	
2.1.9	Mandatory Compliance	2.1.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	
		2.1.9.2	Switch should be TEC certified	
		2.1.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same	
2.1.10	Warranty	2.1.10.1	7 year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number	

			reflected on the official web site.	
2.2	Distribution Switch (DS) Type - 1: DS Switch Type-1: Distribution Switch Supply of Layer 3, 48-port SFP28 10/25GbE, with 8x-port 40/100GbE; Switching capacity at least 4Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty; (Quantity: 10 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance (Yes/No)
2.2.1	Product details	2.2.1.1	Make, Model No. /OEM Part Code. (Please specify)	
2.2.2	Architecture & Port Density	2.2.2.1	The Switch (referred after as It) should have a non-blocking architecture.	
		2.2.2.2	It should have at least 48 x 10G/25G SFP28 Ports and 8 x 40G/100G (QSFP+/QSFP28) ports for uplink/stacking. All the 40/100G ports should support 4x 10G SFP+ or 4x 25 G SFP28 by using split cable as required	
		2.2.2.3	The Switch shall support Virtual Chassis (VC) or equivalent Switch Clustering /Stacking feature of 8 Switches or More, where the Switch Clustering feature shall combine multiple switches into a single network element. Stacking bandwidth of 400 Gbps should be supported.	
2.2.3	Performance	2.2.3.1	It should provide Switch Fabric Bandwidth Capacity of 4 Tbps or more.	
2.2.4	Layer 2 features: it shall support from day 1	2.2.4.1	Should support 4K VLAN Id	
		2.2.4.2	Should support 96K MAC addresses or more	
		2.2.4.3	IP multicast snooping IGMP v1, v2, v3	
		2.2.4.4	Jumbo Frames (up to 9216 bytes)	
2.2.5	Layer 3 features: it shall support from day 1	2.2.5.1	Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1	
		2.2.5.2	IPv4 & IPv6 Routing protocols & multicast routing available from day 1.	
		2.2.5.3	RIP v1 or v2, RIPng, OSPFv2, OSPFv3, BGP4, BGP4+, Multi-VRF,	

			VRRP for both IPV4 and IPV6 protocol, VRRPv2 & VRRPv3, Vxlan	
		2.2.5.4	PIM-SSM, PIM Sparse, PIM Dense, PIM Anycast RP, and PIM passive IPv4 multicast routing.	
		2.2.5.5	PIM-SSM, PIM Sparse, PIM Anycast RP, MSDP and PIM6-SM Snooping IPv6 multicast routing	
		2.2.5.6	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.2.6	Security features	2.2.6.1	RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords	
		2.2.6.2	Secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.2.6.3	IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection	
		2.2.6.4	IPv4 and IPv6 ACLs: with up to 8000 rules / ACL per system	
		2.2.6.5	Flexible Authentication with 802.1x Authentication and MAC Authentication	
2.2.7	Manageability	2.2.7.1	Should support manageability using on prem Centralized Management platform using Web based Graphical User Interface (GUI) and also should be remotely manageable from the Cloud.	
		2.2.7.2	It shall support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch for management/monitoring. NTP (Network Timing Protocol) should be supported.	
		2.2.7.3	It should also support NetFlow or sFlow or equivalent	
		2.2.7.4	It should support Hitless Failover/ISSU	
2.2.8	Physical Attributes	2.2.8.1	The Switch shall be configured with hot swappable, redundant AC power supplies/Fans to provide 1:1 or N+1 power supply redundancy or better	
2.2.9	Mandatory Compliance:	2.2.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	

		2.2.9.2	Switch should be TEC certified	
		2.2.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same	
2.2.10	Warranty	2.2.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	
2.3	Distribution Switch (DS) Type - 2: DS Switch Type-2: Distribution Switch Supply of Layer 3, 24-port SFP28 10/25 G, with 4x-port 40/100GbE; Switching capacity: at least 2Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty, (Quantity: 10 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance (Yes/No)
2.3.1	Product details	2.3.1.1	Make, Model No. /OEM Part Code. (Please specify)	
2.3.2	Architecture & Port Density	2.3.2.1	The Switch shall have 24x 1G/10G SFP+ Ports and 2x 40G from day one / 2x 100 G from Day one. It should support 400Gbps Stacking bandwidth (Full duplex) and 40 G uplinks to the two Core Switches. All the 40/100G ports should support 4x 10G SFP+ or 4x 25 G SFP28 by using split cable as required.	
		2.3.2.2	The Switch shall support Virtual Chassis (VC) or equivalent Switch Clustering/Stacking feature of 8 Switches or More, where the Switch Clustering feature shall combine multiple switches into a single network element. Stacking bandwidth of 400 Gbps should be supported.	
2.3.3	Performance	2.3.3.1	Switching Bandwidth: The Switch shall provide Switch Fabric Bandwidth Capacity of 1 Tbps or more.	
2.3.4	Layer 2 features: it shall support from day 1	2.3.4.1	Should support 4K vlan Id with Minimum 1000 active VLANs	
		2.3.4.2	Should support 96K MAC addresses or more	
		2.3.4.3	IP multicast snooping IGMP v1, v2, v3	
		2.3.4.4	Jumbo Frames (up to 9216 bytes)	
2.3.5	Layer 3 features: it	2.3.5.1	Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual	

	shall support from day 1		Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1	
		2.3.5.2	IPv4 & IPv6 Routing protocols & multicast routing available from day 1.	
		2.3.5.3	RIP v1 or v2, RIPng, OSPFv2, OSPFv3, BGP4, BGP4+, Multi-VRF, VRRP for both IPV4 and IPV6 protocol, VRRPv2 & VRRPv3 from Day one	
		2.3.5.4	PIM-SSM, PIM Sparse, PIM Dense, PIM Anycast RP, and PIM passive IPv4 multicast routing.	
		2.3.5.5	PIM-SSM, PIM Sparse, PIM Anycast RP, MSDP and PIM6-SM Snooping IPv6 multicast routing	
		2.3.5.6	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.3.6	Security features	2.3.6.1	RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords	
		2.3.6.2	Secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.3.6.3	IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection	
		2.3.6.4	IPv4 and IPv6 ACLs: with up to 8000 rules / ACL per system	
		2.3.6.5	Flexible Authentication with 802.1x Authentication and MAC Authentication	
2.3.7	Manageability	2.3.7.1	Should support manageability using on prem Centralized Management platform using Web based Graphical User Interface (GUI) and also should be remotely manageable from the Cloud.	
		2.3.7.2	It shall support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch for management/monitoring. NTP (Network Timing Protocol) should be supported.	
		2.3.7.3	It should also support NetFlow or sFlow or equivalent	
		2.3.7.4	It should support Hitless Failover/ISSU	
2.3.8	Physical Attributes	2.3.8.1	The Switch shall be configured with hot swappable, redundant load	

			sharing AC power supplies to provide 1:1 or N+1 power supply redundancy or better	
2.3.9	Mandatory Compliance:	2.3.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	
		2.3.9.2	Switch should be TEC certified	
		2.3.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same.	
2.3.10	Warranty	2.3.10.1	7 year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	
2.4	Access Switch (AS) Type - 1: AS Switch Type-1: Access Switch/Edge Switch: 24x1/10GbE Base-T RJ45 ports; 4 × 25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 680gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 12 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance Yes / No
2.4.1	Product details- Please specify	2.4.1.1	Please mention Make, Model No. and Part Code	
2.4.2	Architecture & Port Density	2.4.2.1	The Switch (referred after as It) should have a non-blocking architecture.	
		2.4.2.2	It should have at least 24 x 10G Base T and 4 x 10/25 G SFP28 ports for uplink/stacking. required	
		2.4.2.3	The Switch shall support Virtual Chassis (VC) or equivalent Switch Clustering /Stacking feature of 8 Switches or More, where the Switch Clustering feature shall combine multiple switches into a single network element. Stacking bandwidth of 400 Gbps should be supported.	
2.4.3	Performance	2.4.3.1	It should provide Switch Fabric Bandwidth Capacity of 680 Gbps or more	
2.4.4	Layer 2 features: it	2.4.4.1	Should support 4K vlan Id	

	shall support from day 1	2.4.4.2	Should support 96K MAC addresses or more	
		2.4.4.3	IP multicast snooping IGMP v1, v2, v3	
		2.4.4.4	Jumbo Frames (up to 9216 bytes)	
2.4.5	Layer 3 features	2.4.5.1	Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1	
		2.4.5.2	IPv4 & IPv6 Routing protocols & multicast routing available from day 1.	
		2.4.5.3	RIP v1 or v2, RIPng, OSPFv2, OSPFv3, BGP4, BGP4+, Multi-VRF, VRRP for both IPV4 and IPV6 protocol, VRRPv2 & VRRPv3, Vxlan	
		2.4.5.4	PIM-SSM, PIM Sparse, PIM Dense, PIM Anycast RP, and PIM passive IPv4 multicast routing.	
		2.4.5.5	PIM-SSM, PIM Sparse, PIM Anycast RP, MSDP and PIM6-SM Snooping IPv6 multicast routing	
		2.4.5.6	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.4.6	Security features	2.4.6.1	RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords	
		2.4.6.2	Secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.4.6.3	IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection	
		2.4.6.4	IPv4 and IPv6 ACLs: with up to 8000 rules / ACL per system	
		2.4.6.5	Flexible Authentication with 802.1x Authentication and MAC Authentication	
2.4.7	Manageability	2.4.7.1	Should support manageability using on prem Centralized Management platform using Web based Graphical User Interface (GUI) and also should be remotely manageable from the Cloud.	
		2.4.7.2	It shall support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch for management/monitoring. NTP (Network Timing Protocol) should be	

			supported.	
		2.4.7.3	It should also support NetFlow or sFlow or equivalent	
		2.4.7.4	It should support Hitless Failover/ISSU	
2.4.8	Physical Attributes	2.4.8.1	The Switch shall be configured with hot swappable, redundant AC power supplies/Fans to provide 1:1 or N+1 power supply redundancy or better	
2.4.9	Mandatory Compliance	2.4.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	
		2.4.9.2	Switch should be TEC certified	
		2.4.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same.	
2.4.10	Warranty	2.4.10.1	7 years OEM TAC support & 7 years warranty shall be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item.	
2.5	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 10 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance Yes / No
2.5.1	Product details- Please specify	2.5.1.1	Please mention Make, Model No. and Part Code	
2.5.2	Architecture & Port Density	2.5.2.1	The Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 & Layer 3.	
		2.5.2.2	The Switch should have a minimum 48 Port 100/1000 G + 4 10/25 SFP28 Port from Day 1. Each switch should be supplied with 25G DAC cable. Each Switch should be supplied with Stacking and Transceivers as required mention in Bill of material	
		2.5.2.3	The Switch should support Stacking up to 8 Switches with more than 100Gbps stacking bandwidth per Switch. All Access Switches PoE	

			and Non PoE should be inter-stackable with each other.	
		2.5.2.4	The Switch should be able to stack with different models of same switch series of access switch for scalability	
		2.5.2.5	The Switch should provide USB-C serial Port, RJ45 Serial port and RJ45 OOB access for management, it should also provide USB-A Port for remote updates and backup	
2.5.3	Performance	2.5.3.1	Switching Bandwidth: Should provide non-blocking switch fabric capacity of 296 Gbps Gbps or more.	
		2.5.3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 220 Mpps or more.	
2.5.4	Layer 2 features	2.5.4.1	Should support for VXLAN for advanced network segmentation and data confidentiality	
		2.5.4.2	Should support 32K MAC addresses or more.	
		2.5.4.3	Shall support IP multicast snooping with support for IGMP v1, v2, v3 and MLD v1 & v2	
		2.5.4.4	Should support Jumbo Frames (up to 9K bytes)	
2.5.5	Layer 3 features	2.5.5.1	Should support minimum 12K IPv4 & 2K IPv6 routes	
		2.5.5.2	Should support Basic IPv4 and IPv6 Static Routing, RIPv1/V2, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from day one	
		2.5.5.3	Should support Dynamic IPv4 & IPv6 Routing protocols (OSPFv2 and OSPFv3) and Multicast Routing Protocol PIM SN, PIM -DM, POM-SSM, VRRP, PBR, VRF in future.	
		2.5.5.4	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.5.6	Security	2.5.6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)	
		2.5.6.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.5.6.3	Should support IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection.	

		2.5.6.4	Should support IPv4 and IPv6 ACLs	
		2.5.6.5	Should support Byte and packet-based broadcast, multicast, and unknown-unicast limits with suppression port dampening.	
		2.5.6.6	Should support IPv6 Router Advertisement (RA) Guard.	
		2.5.6.7	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.	
2.5.7	Manageability	2.5.7.1	Should support manageability using Centralized Management platform using Web based Graphical User Interface (GUI)	
		2.5.7.2	Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring	
		2.5.7.3	Should support SDN features in native as well as hybrid modes	
		2.5.7.4	Should support Digital Optical Monitoring and Virtual Cable Tester (VCT) or equivalent	
2.5.8	Mandatory Compliance	2.5.8.1	All categories of Switches, Transceivers & Switch OS should be from same OEM	
		2.5.8.2	Switch should be certified by NDcPP and TEC Certified	
2.5.9	OEM authorization	2.5.9.1	The bidder shall be OEM of the switch or an authorized distributor/reseller partner of the OEM. In case of the bidder being a distributor/reseller partner, authorization certificate from the OEM to quote against the tender shall be submitted by the bidder.	
		2.5.9.2	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
		2.5.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same.	
2.5.10	Warranty	2.5.10.1	7 years OEM TAC support & 7 years warranty shall be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item.	
2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 75 Number)			

Spec. No	Parameters	Sub Items No	Specifications	Compliance Yes / No
2.6.1	Product details- Please specify	2.6.1.1	Please mention Make, Model No. and Part Code	
2.6.2	Architecture & Port Density	2.6.2.1	The Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 & Layer 3.	
		2.6.2.2	The Switch should have a minimum 24 Port 100/1000 Mbps + 4 10/25 SFP28 Port from Day 1. Each switch should be supplied with 25G DAC cable. Each Switch should be supplied with Stacking and Transceivers as required mention in Bill of material	
		2.6.2.3	The Switch should support Stacking up to 8 Switches with more than 100Gbps stacking bandwidth per Switch. All Access Switches POE and Non Poe should be inter-stackable with each other.	
		2.6.2.4	The Switch should be able to stack with different models of same switch series of access switch for scalability	
		2.6.2.5	The Switch should provide USB-C serial Port, RJ45 Serial port and RJ45 OOB access for management, it should also provide USB-A Port for remote updates and backup	
		2.6.2.6	Switching Bandwidth: Should provide Non-Blocking switch fabric capacity of 248 Gbps Gbps or more.	
2.6.3	Performance	2.6.3.1	Forwarding Capacity: Should provide wire-speed packet forwarding of 184 Mpps or more.	
2.6.4	Layer 2 features	2.6.4.1	Should support for VXLAN for advanced network segmentation and data confidentiality	
		2.6.4.2	Should support 32K MAC addresses or more.	
		2.6.4.3	Shall support IP multicast snooping with support for IGMP v1, v2, v3 and MLD v1 & v2	
		2.6.4.4	Should support Jumbo Frames (up to 9K bytes)	
2.6.5	Layer 3 features	2.6.5.1	Should support minimum 12K IPv4 & 2K IPv6 routes	
		2.6.5.2	Should support Basic IPv4 and IPv6 Static Routing, RIPv1/V2, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from day one	
		2.6.5.3	Should support Dynamic IPv4 & IPv6 Routing protocols (OSPFv2	

			and OSPFv3) and Multicast Routing Protocol PIM SN, PIM -DM, POM-SSM, VRRP, PBR, VRF in future.	
		2.6.5.4	Switch should support Software Defined Video over Ethernet (SDVoE)	
2.6.6	Security	2.6.6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)	
		2.6.6.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.6.6.3	Should support IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection.	
		2.6.6.4	Should support IPv4 and IPv6 ACLs	
		2.6.6.5	Should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.	
		2.6.6.6	Should support IPv6 Router Advertisement (RA) Guard.	
		2.6.6.7	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.	
2.6.7	Manageability	2.6.7.1	Should support manageability using Centralized Management platform using Web based Graphical User Interface (GUI)	
		2.6.7.2	Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring	
		2.6.7.3	Should support SDN features in native as well as hybrid modes	
		2.6.7.4	Should support Digital Optical Monitoring and Virtual Cable Tester (VCT) or equivalent	
2.6.8	Mandatory Compliance	2.6.8.1	All categories of Switches, Transceivers & Switch OS should be from same OEM	
		2.6.8.2	Switch should be certified by NDcPP and TEC Certified	
2.6.9	OEM authorization	2.6.9.1	The bidder shall be OEM of the switch or an authorized distributor/reseller partner of the OEM. In case of the bidder being a distributor/reseller partner, authorization certificate from the OEM to quote against the tender shall be submitted by the bidder.	
		2.6.9.2	OEM End-of-sale declaration shall not have been released for the	

			quoted model at the time of the bid submission.	
		2.6.9.3	OEMs should not share land borders with India. Declaration on the OEM letter head to be submitted for the same.	
2.6.10	Warranty	2.6.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site	
2.7	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 2 Number)			
Spec. No	Parameters	Sub Items No	Specifications	Compliance Yes / No
2.7.1	Product details- Please specify	2.7.1.1	Please mention Make, Model No. and Part Code	
2.7.2	Architecture & Port Density	2.7.2.1	The Switch should have minimum 16 x 100/1000 Base T POE+ports and should have 2x 1G/10G SFP+ ports from Day 1.	
		2.7.2.2	The Switch should provide one USB Type-C port for console management for management/ Equivalent	
2.7.3	Performance	2.7.3.1	Switching Bandwidth: Should provide Switching fabric capacity of 72 Gbps or more.	
		2.7.3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 54 Mpps or more.	
2.7.4	Layer 2 features	2.7.4.1	Should support 16 K MAC addresses or more.	
		2.7.4.2	Shall support multicast snooping with support for IGMP snooping v1, v2, v3	
		2.7.4.3	Should support Jumbo Frames (up to 9K bytes)	
		2.7.4.4	Maximum Link aggregation group 64 with 8 ports in one Lag group	
2.7.5	Mirroring: Port-based, ACL-based, MAC Filter-based	2.7.5.1	Port Loop Detection, Uni-Directional Link Detection (UDLD), Q-in-Q and selective Q-in-Q, GVRP,	

2.7.6	Security	2.7.6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)	
		2.7.6.2	Should support secure communications to the management interface and system through, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.7.6.3	Should support DHCP snooping and Dynamic ARP Inspection. Dhcp server and dhcp relay	
		2.7.6.4	Should ACL mapping to priority queue, and TOS/DSCP	
		2.7.6.5	Should support Broadcast, multicast, and unknown unicast rate limiting	
		2.7.6.6	Should support Flexible Authentication with 802.1x Authentication, web authentication and MAC Authentication.	
2.7.7	Manageability	2.7.7.1	Should support manageability using Centralized Management platform using Web based Graphical User Interface (GUI)	
		2.7.7.2	Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch, . It should support NTP.	
2.7.8	Mandatory Compliance	2.7.8.1	All categories of Switches, Transceivers & Switch OS should be from same OEM	
		2.7.8.2	All Switch should be certified by Common Criteria NDcPP and TEC Certified	
2.7.9	OEM authorization	2.7.9.1	Manufacturing authorization certificate from the OEM to quote against the tender shall be submitted by the bidder.	
		2.7.9.2	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
2.7.10	Warranty	2.7.10.1	7 years OEM TAC s warranty shall be provided by the OEM and Product should be covered under LLW. The warranty certificate/declaration shall be from the OEM of the item.	
2.8	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 4 Number)			

Spec. No	Parameters	Sub Items No	Specifications	Compliance Yes / No
2.8.1	Product details- Please specify	2.8.1.1	Please mention Make, Model No. and Part Code	
2.8.2	Architecture & Port Density	2.8.2.1	The Switch should have minimum 8x 100/1000 Base T POE+ports and should have 2x 1G/10G SFP+ ports from Day 1. .	
		2.8.2.2	The Switch should provide one USB Type-C port for console management for management/ Equivalent	
2.8.3	Performance	2.8.3.1	Switching Bandwidth: Should provide Switching fabric capacity of 72 Gbps or more.	
		2.8.3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 54 Mpps or more.	
2.8.4	Layer 2 features	2.8.4.1	Should support 16 K MAC addresses or more.	
		2.8.4.2	Shall support multicast snooping with support for IGMP snooping v1, v2, v3	
		2.8.4.3	Should support Jumbo Frames (up to 9K bytes)	
		2.8.4.4	Maximum Link aggregation group 64 with 8 ports in one Lag group	
2.8.5	Mirroring: Port-based, ACL-based, MAC Filter-based	2.8.5.1	Port Loop Detection, Uni-Directional Link Detection (UDLD), Q-in-Q and selective Q-in-Q, GVRP,	
2.8.6	Security	2.8.6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)	
		2.8.6.2	Should support secure communications to the management interface and system through, Secure Shell (SSHv2), Secure Copy and SNMPv3	
		2.8.6.3	Should support DHCP snooping and Dynamic ARP Inspection. Dhcp server and dhcp relay	
		2.8.6.4	Should ACL mapping to priority queue, and TOS/DSCP	
		2.8.6.5	Should support Broadcast, multicast, and unknown unicast rate limiting	
		2.8.6.6	Should support Flexible Authentication with 802.1x Authentication, web authentication and MAC Authentication.	

2.8.7	Manageability	2.8.7.1	Should support manageability using Centralized Management platform using Web based Graphical User Interface (GUI)	
		2.8.7.2	Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch, . It should support NTP.	
2.8.8	Mandatory Compliance	2.8.8.1	All categories of Switches, Transceivers & Switch OS should be from same OEM	
		2.8.8.2	All Switch should be certified by Common Criteria NDcPP and TEC Certified	
2.8.9	OEM authorization	2.8.9.1	Manufacturing authorization certificate from the OEM to quote against the tender shall be submitted by the bidder.	
		2.8.9.2	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
2.8.10	Warranty	2.8.10.1	7 years OEM TAC s warranty shall be provided by the OEM and Product should be covered under LLW. The warranty certificate/declaration shall be from the OEM of the item.	

2.9	100G DAC Copper Cable - 1M: 100GbE QSFP28 to QSFP28 Direct Attached, Passive Copper Cable, 1m. Stacking (Quantity: 24 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.9.1	Type of Interface	QSFP28	
2.9.2	Length	1M	
2.9.3	Active/Passive	Passive	
2.9.4	Optical /Copper	Copper	
2.10	100G DAC Cable - 1M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 1m, 1-pack (Quantity: 26 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.10.1	Type of Interface	QSFP28	
2.10.2	Length	1M	
2.10.3	Active/Passive	Active	
2.10.4	Optical /Copper	Optical	

2.11	100G DAC Cable - 5M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 5m, 1-pack (Quantity: 52 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.11.1	Type of Interface	QSFP28	
2.11.2	Length	5M	
2.11.3	Active/Passive	Active	
2.11.4	Optical /Copper	Optical	
2.12	100G DAC Cable - 10M: 100GE QSFP28 to QSFP28 Direct Attached, Active Optical Cable, 10m, 1-pack (Quantity: 10 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.12.1	Type of Interface	QSFP28	
2.12.2	Length	10M	
2.12.3	Active/Passive	Active	
2.12.4	Optical /Copper	Optical	
2.13	40G DAC Cable - 5M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 5m, 1-pack (Quantity: 20 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.13.1	Type of Interface	QSFP+	
2.13.2	Length	5M	
2.13.3	Active/Passive	Active	
2.13.4	Optical /Copper	Optical	
2.14	40G DAC Cable - 10M: 40GE Direct Attach QSFP+ to QSFP+ Active Optical Cable, 10m, 1-pack (Quantity: 20 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.14.1	Type of Interface	QSFP+	

2.14.2	Length	10M	
2.14.3	Active/Passive	Active	
2.14.4	Optical /Copper	Optical	
2.15	40G QSFP+: 40GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack (Quantity: 16 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.15.1	Type of Transceiver	QSFP+40G LR	
2.15.2	SFP Mode	Single	
2.15.3	IEEE STD	802.3ba	
2.15.4	Wavelength(nm)	1264.5 to 1337.5	
2.15.5	Distance	10KM	
2.15.6	Digital Optical Monitoring and Hot- Pluggable/Swappable		
2.15.7	Safety Standard	EN 60825-1	
2.15.8	Onsite OEM Warranty (Year)	7	
2.16	25G QSFP+: 25GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack (Quantity: 56 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.16.1	Type of Transceiver	SFP28	
2.16.2	SFP Mode	Single	
2.16.3	IEEE STD	802.3bm	
2.16.4	Wavelength (nm)	1310	
2.16.5	Distance	10KM	
2.16.6	Digital Optical Monitoring and Hot-Pluggable/Swappable		
2.16.7	Safety Standard	EN 60825-1	
2.16.8	OnSite OEM Warranty (Year)	7	

2.17	10G SFPP: 10GBASE-LR, SFPP SMF LC CONNECTOR (No TAA) (Quantity: 364 Number)		
Sln	SPECIFICATIONS		Compliance (Yes/No)
2.17.1	Type of Transceiver	SFP+ 10G	
2.17.2	SFP Mode	Single	
2.17.3	IEEE STD	802.3ae	
2.17.4	Wavelength(nm)	1310	
2.17.5	Distance	10KM	
2.17.6	Digital Optical Monitoring and Hot-Pluggable/Swappable		
2.17.7	Safety Standard	EN 60825-1	
2.17.8	Onsite OEM Warranty (Year)	7	

3.1	AAA Server: AAA Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Authentication, Authorization, and Accounting (AAA) server supporting TACACS+ and/or RADIUS protocols for secure network access control, user management, policy enforcement, and accounting logs. (Quantity: Job Complete)			
Spec. No	Parameters	Sub Items No	Features	Compliance (Yes/No)
3.1.1	Make	3.1.1.1	Please specify the make and model	
		3.1.1.2	The offered solution shall be ON Premises Virtual appliance to be provided in High Availability with all the necessary Operating system, required RAM, CPUs to cater the required number of devices mentioned in the subsequent clause. Licenses/subscriptions should be provided to 5000 users with 3 devices each from day 1.	
3.1.2	Functionality	3.1.2.1	Solution should support Authorisation, Authentication & Accounting (AAA), and secure on boarding for IT owned, BYOD and Guest Access by incorporating identity, physical/device information and conditional elements on a single platform.	
		3.1.2.2	Should support a variety of authentication methods (802.1 X, MAC auth and web auth) for Wired and wireless networking equipment.	
		3.1.2.3	Solution should support up to 5000 users with 3 devices each from day 1. Licenses/Subscription to be considered accordingly. The solution should be scalable to support 20000 users or more in future.	

		3.1.2.4	Solution should support RBAC (Role based access control)	
		3.1.2.5	Solution should support RADIUS server for client device authentication and TACACS+ for network device authentication with logging.	
		3.1.2.6	Solution should have device profiling functionality	
		3.1.2.7	Solution should have integrated support for iOS, Android, Mac OS, ChromeOS, windows, Linux end points.	
		3.1.2.8	Authentication or authorization support for LDAP, AD, SAML 2. 0 & O Auth	
		3.1.2.9	The solution should have the following features · Built-in guest management and device/user on boarding. · Web based management interface with dashboard. · Reporting and analysis with custom data filters. · Data repository for user, device, transaction information · Rich policies using identity and device	
3.1.3	BYOD	3.1.3.1	Support for popular smart devices and traditional computing platforms.	
		3.1.3.2	Ability to support iOS, Android, Mac OS, ChromeOS, windows	
		3.1.3.3	The system should correlate user, device, and authentication information for troubleshooting and tracking purposes.	
		3.1.3.4	The system should support automated device onboarding, allowing for secure access through a self-service portal.	
		3.1.3.5	The system should be able to integrate with Active Directory, LDAP, SAML, Oauth allowing authentication of BYOD users based on their identity and device attributes.	
3.1.4	Guest Access	3.1.4.1	Built-in guest management and device/user on boarding.	
		3.1.4.2	Self provisioned Guest access users should be available from day one.	
		3.1.4.3	Ability to send automated SMS or email credentials to the guest users.	
		3.1.4.4	The solution should offer fully customizable self-registration pages for guest account creation.	
3.1.5	Licenses/Subscription	3.1.5.1	Perperual license with 7 Year OEM TAC and OS support for all	

	& support		licenses and Software. All software and Hardware should be included in the solution for 20000 users.	
3.1.6	Mandatory compliance	3.1.6.1	All switches, NMS, Transceivers, AAA should be from the same OEM for better interoperatability, management and support.	
3.2	Network Access Control (NAC): Network Access Control (NAC): Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network infrastructure. (Quantity: Job Complete)			
Spec. No	Specifications			Compliance (Yes/No)
3.2.1	Product details -			
	Make, Model No. /OEM Part Code. (Please specify)			
	Network Access Control (NAC) solution shall provide centralized, secure and policy-based control over wired and wireless network access. The solution shall support 802.1X authentication, RADIUS, MAC Authentication Bypass (MAB), Active Directory/LDAP integration, certificate-based authentication, device profiling and identification, user/device-based policy enforcement, dynamic VLAN/role assignment, guest and BYOD access, posture assessment and quarantine/remediation of non-compliant devices. The NAC solution shall provide real-time visibility of connected users and endpoints, including managed, unmanaged, unknown and IoT devices, and shall support centralized monitoring, logging, reporting and audit trails. It shall integrate with existing network switches and wireless infrastructure using standard protocols such as 802.1X, RADIUS, SNMP and RADIUS Change of Authorization (CoA) or equivalent standards-based mechanisms. The solution shall support role-based access control, API/SIEM integration, IPv4/IPv6, high availability and scalability to accommodate future expansion of the network. The proposed solution shall be capable of enforcing access policies based on user identity, device type, authentication status, device compliance, location and security posture, thereby ensuring that only authorized and compliant users/devices are permitted appropriate access to network resources.			
3.3	RADIUS Server: RADIUS Server: Supply, installation, configuration, integration, testing, and commissioning of a standards-			

	compliant RADIUS server supporting IEEE 802.1X/EAP authentication for centralized user authentication, authorization, and accounting across wired and wireless networks. (Quantity: Job Complete)			
Spec. No	Parameters	Sub Items No	Features	Compliance (Yes/No)
3.3.1	RADIUS Authentication	3.3.1.1	The proposed solution shall support integration with an Enterprise-grade RADIUS server for centralized Authentication, Authorization, and Accounting (AAA). The solution shall meet the following minimum requirements:	
		3.3.1.2	Support standard RADIUS protocol (RFC 2865 and RFC 2866).	
		3.3.1.3	Support centralized Authentication, Authorization, and Accounting (AAA).	
		3.3.1.4	Support integration with LDAP v3 and Microsoft Active Directory.	
		3.3.1.5	Support authentication for Wired (IEEE 802.1X), Wireless (WPA2/WPA3-Enterprise), and VPN users.	
		3.3.1.6	Support Role-Based Access Control (RBAC) and user/group-based policies.	
		3.3.1.7	Support MAC Authentication Bypass (MAB) for devices that do not support 802.1X.	
		3.3.1.8	Support secure communication between network devices and the RADIUS server.	
		3.3.1.9	Maintain authentication and accounting logs for monitoring and auditing.	
		3.3.1.10	Support High Availability (HA) and redundant RADIUS servers.	
		3.3.1.11	The bidder shall provide complete installation, configuration, integration, testing, and commissioning of the RADIUS authentication solution.	
3.4	LDAP Server: LDAP Server: Supply, installation, configuration, integration, testing, and commissioning of an LDAP directory service for centralized identity management, user authentication, role-based access control, and integration with AAA, NAC, network devices, and enterprise applications. (Quantity: Job Complete)			
Spec. No	Description of Requirement			Compliance (Yes/No)

3.4.1	The proposed solution shall support integration with the Institute's existing directory services through LDAP v3 and/or Microsoft Active Directory for centralized authentication and authorization. The solution shall support secure LDAP (LDAPS), user and group-based access control, Role-Based Access Control (RBAC), and shall allow seamless integration with the existing identity management infrastructure without requiring any modification to the current environment. The bidder shall carry out complete installation, configuration, integration, testing, and commissioning of the LDAP authentication services as part of the project scope.			
3.5	Internal DNS Server: Internal DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an Internal DNS server for secure name resolution, forward and reverse lookup zones, dynamic DNS updates, and integration with internal directory and network services. (Quantity: Job Complete)			
Spec. No	Description of Requirement			Compliance Yes/No
3.5.1	The bidder shall provide and configure an Enterprise-grade DNS solution for the campus network. The DNS solution shall:			
3.5.2	Support IPv4 and IPv6.			
3.5.3	Support Authoritative and Recursive DNS services.			
3.5.4	Support DNSSEC.			
3.5.5	Support Forward and Reverse DNS.			
3.5.6	Support High Availability with redundant DNS servers.			
3.5.7	Support centralized management and monitoring.			
3.5.8	Maintain DNS logs and audit trails.			
3.5.9	Integrate with the existing network infrastructure, DHCP, and Active Directory/LDAP (where applicable).			
3.5.10	Be scalable to support future expansion of the campus network.			
3.6	External DNS Server: External DNS Server: Supply, installation, configuration, integration, testing, and commissioning of an External DNS server for authoritative public DNS hosting, secure zone management, redundancy, and integration with Internet-facing services. (Quantity: Job Complete)			
Spec.	Description of Requirement			Compliance Yes/No

No				
3.6.1	The bidder shall provide and configure an Enterprise-grade DNS solution for the campus network. The DNS solution shall:			
3.6.2	Support IPv4 and IPv6.			
3.6.3	Support Authoritative and Recursive DNS services.			
3.6.4	Support DNSSEC.			
3.6.5	Support Forward and Reverse DNS.			
3.6.6	Support High Availability with redundant DNS servers.			
3.6.7	Support centralized management and monitoring.			
3.6.8	Maintain DNS logs and audit trails.			
3.6.9	Integrate with the existing network infrastructure, DHCP, and Active Directory/LDAP (where applicable).			
3.6.10	Be scalable to support future expansion of the campus network.			
3.7	Network Management System (NMS): Network Management System (NMS): Supply, installation, configuration, integration, testing, and commissioning of a centralized Network Management System for device discovery, inventory, topology visualization, configuration management, fault, performance, and availability monitoring using SNMP, Syslog, NetFlow/sFlow, and related protocols. (Quantity: Job Complete)			
Spec. No	Parameters	Sub Items No	Features	Compliance (Yes/No)
3.7.1		3.7.1.1	The NMS shall be a multi-user system and based on Graphical User Interface.	
3.7.2		3.7.2.1	The NMS shall be able to diagnose its own faults by running diagnostic software	
3.7.3		3.7.3.1	The NMS shall provide the complete view of the network elements and the interconnecting links.	
3.7.4		3.7.4.1	The NMS shall provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.	
3.7.5		3.7.5.1	It shall provide the graphical layout of the network element with modules drawn using different colours to indicate their status	
3.7.6		3.7.6.1	Messaging system – The NMS shall have a messaging system	

			which will generate and send alerts via email or SMS to the designated personnel depending upon the location ofNE, on generation of alarms.	
3.7.7		3.7.7.1	lt shall be possible to produce pre-defined reports.	
3.7.8	NMS Licensing should be Device based.	3.7.8.1	Network mapping and discovery software using Layer 2/ Layer 3 protocols for devices.	
3.7.9	Discovery Features:-	3.7.9.1	Support for SNMP v1-3, IPv4/IPv6 address range, SNMP Smartscan, hosts file	
		3.7.9.2	Scheduled discovery scans	
		3.7.9.3	Web-based discovery	
3.7.10	Mapping Features:-	3.7.10.1	Automated map creation	
		3.7.10.2	Customizable topology maps	
		3.7.10.3	Display of Device dependencies	
		3.7.10.4	Multi-level topology views	
3.7.11	Monitoring Features:-	3.7.11.1	SNMP v1-3, SSH and WMI support	
		3.7.11.2	Real-time monitoring	
		3.7.11.3	MIB Walker, MIB Explorer and MIB Manager	
		3.7.11.4	WMI application monitoring	
		3.7.11.5	Wireless Infrastructure Monitoring, Popup and audio-visual Alerting and Reporting	
		3.7.11.6	Custom monitoring with Jscript or VBScript	
		3.7.11.7	Threshold monitoring (Performance, Passive and Flow)	
		3.7.11.8	Blackout period to suspend specific actions during the scheduled period of time	
		3.7.11.9	Management Console, Alerts Notification and ReportingFeatures:-	
3.7.12	Management Console, Alerts Notification and Reporting Features:-	3.7.12.1	Web and Windows based management console	
		3.7.12.2	Alert Center for centralized alerts/notifications/escalation management.	
		3.7.12.3	It should have support Web Alarm and should support & SMS & Email Notification so thatit can be augmented in future.	

		3.7.12.4	Configurable Alert with Popup and audio-visual mode and Notification escalation policies	
		3.7.12.5	Mobile Interface with one-click log-in	
		3.7.12.6	Configurable role-based management	
		3.7.12.7	Dashboard manager	
		3.7.12.8	Real-time split second and historical graphs	
		3.7.12.9	Scheduling of recurring reports	
		3.7.12.10	Report export to: email, Excel®, and PDF formats	
		3.7.12.11	Pre-defined and customizable reports	
		3.7.12.12	Configurable alert thresholds	
		3.7.12.13	Inventory or other device specific information	
3.7.13	Visual Mapping features:-	3.7.13.1	Based upon discovery, should be able to automatically generate integrated network topology maps showing both Layer 3 addressing and Layer 2 connectivity.	
3.7.14	Inventory features:-	3.7.14.1	Agentless scans for inventory.	
3.7.15	Single point Console features for:-	3.7.15.1	Managing network discovery, creation and administration of maps, to access detailed device inventory and configuration information.	
3.7.16	User Defined Device Categories	3.7.16.1	Should provide the users to have the ability to define, edit, add or delete device categories from auto discovered connected devices.	
3.7.17	Layer 2 Trace	3.7.17.1	Should support both LAN or WAN connectivity	
		3.7.17.2	Should display in-bound and out-bound interfaces for each network device in the path	
		3.7.17.3	Should provide Layer 2 trace feature to help network managers to rapidly pinpoint physical layer connectivity issues from the console.	
3.7.18	IP/Mac Finder features:-	3.7.18.1	Should provide an IP/Mac finder tool to locate an IP or Mac address on a network from the console.	
3.7.19	Cloud Monitoring	3.7.19.1	Should automatically discovers, maps and monitors cloud environments including Amazon Web Services and Azure servers	
		3.7.19.2	Solution should monitor, report and alert on the status and performance of every metric your cloud service collects via its own native API	

		3.7.19.3	Solution should track cloud billing and show this report on a simple dashboard	
3.7.20	Configuration Management	3.7.20.1	Automate configuration and change management for routers, switches and firewalls on your network.	
		3.7.20.2	Archive and Restore Network Configurations	
		3.7.20.3	Alert on Configuration Changes	
		3.7.20.4	Audit and Report on Network Configurations	
3.7.21	Network Traffic Analysis	3.7.21.1	Get Detailed Visibility to Bandwidth Usage Patterns	
		3.7.21.2	Monitor and set threshold-based alerts on network traffic and bandwidth usage. Collect and view data for Cisco CBQoS and NBAR.	
		3.7.21.3	Receive Alerts about Your Network Traffic	
		3.7.21.4	Report on Your Network Traffic	
3.7.22	Application Monitoring	3.7.22.1	Component Monitoring of Pre Defined Applications, Reports and Alerts	
3.7.23	Virtual Monitoring	3.7.23.1	Virtualization Monitoring needs to discovers, maps, monitors, alerts and reports on VMware and Hyper-V performance for hosts and guests and clusters on the network	
3.7.24	Log Management	3.7.24.1	Visualize and analyze Syslogs and Window Event Logs from NMS	
		3.7.24.2	Ingest and filter Windows Event Logs & Syslogs	
		3.7.24.3	Quickly search collected logs	
		3.7.24.4	Configure log searches and export search results	
		3.7.24.5	Export logs to various formats automatically or on-demand	
		3.7.24.6	Archive logs for regulatory compliance	
		3.7.24.7	View log status and events on customizable dashboards	
		3.7.24.8	Trigger alerts on customizable conditions	
3.8	Syslog Server: Syslog Server: Supply, installation, configuration, integration, testing, and commissioning of a centralized Syslog server for secure collection, storage, indexing, monitoring, correlation, alerting, and analysis of logs generated by network, security, and server infrastructure. (Quantity: Job Complete)			

Spec. No	Parameters	Sub Items No	Features	Compliance (Yes/No)
3.8.1	Chassis	3.8.1.1	2U Rack Mountable	
3.8.2	CPU	3.8.2.1	2 x Intel 5th Gen processor with minimum 2.2 GHz, 24Cores or Higher.	
3.8.3	Chipset	3.8.3.1	Intel® C741 Chipset	
3.8.4	Memory	3.8.4.1	32DIMM slots.	
		3.8.4.2	The server should be populated with 256 GB (8 x 32 GB) RAM expandable up to 256 GB	
3.8.5	Controller	3.8.5.1	PCIe based x16 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60, 1T, 10T supporting up to 16 direct- connected storage devices (SAS/SATA/NVMe).	
		3.8.5.2	Controller must support SSD, NVMe SSD & SATA/NL-SAS Drives	
		3.8.5.3	The controller must support 6G SATA, 12G SAS, 16G NVMe.	
		3.8.5.4	Controller must support following: 1. Expand Logical Drive 2. Instant Secure Erase 3. Migrate RAID/Stripe Size 4. Modifying Cache Write Policy 5. Move Logical Drive 6. Re-enable Failed Logical Drive	
3.8.6	Bus Slots	3.8.6.1	The server should support up to Six PCI-Express 5. 0 x16 slots (Bus width)	
3.8.7	HDD Bays	3.8.7.1	8 SFF/LFF HDD/SSD	
3.8.8	Storage	3.8.8.1	2 x 1.92TB SSD + 4 x 4TB NL-SAS HDD's	
3.8.9	Networking Port	3.8.9.1	Server should support and offered below networking cards: • 1Gb 4-port network adapter • 2-port 10G SFP+ adapter	
3.8.10	Interfaces	3.8.10.1	Serial - (Optional)	
		3.8.10.2	VGA – 1	
		3.8.10.3	USB 2. 0 or higher, support With Up to 4 totals: 1 front, 2 rear, 1	

			internal.	
		3.8.10.4	1GbE Dedicated management port	
3.8.11	Power Supply	3.8.11.1	Should support hot plug redundant platinum power supplies with minimum 94% efficiency	
3.8.12	Fans	3.8.12.1	Redundant hot-plug system fans	
3.8.13	Industry Standard	3.8.13.1	ACPI 6.3 Compliant or Equivalent Industry Standard Compliance.	
		3.8.13.2	PCIe 5. 0 Compliant	
		3.8.13.3	WOL Support	
		3.8.13.4	Microsoft® Logo certifications	
		3.8.13.5	PXE Support	
		3.8.13.6	USB 3. 0 Compliant	
		3.8.13.7	Energy Star	
		3.8.13.8	SMBIOS 3.2 Compliant or Equivalent Industry Standard Compliance.	
		3.8.13.9	Redfish API	
		3.8.13.10	IPMI 2. 0	
		3.8.13.11	Secure Digital 4. 0	
		3.8.13.12	Advanced Encryption Standard (AES)	
		3.8.13.13	Triple Data Encryption Standard (3DES)	
		3.8.13.14	SNMP v3	
		3.8.13.15	TLS 1.2	
		3.8.13.16	DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP)	
		3.8.13.17	Active Directory v1. 0	
		3.8.13.18	ASHRAE A3/A4	
		3.8.13.19	UEFI (Unified Extensible Firmware Interface Forum) 2.7	
3.8.14	System Security	3.8.14.1	UEFI Secure Boot and Secure Start support	
		3.8.14.2	Tamper-free updates - components digitally signed and verified	
		3.8.14.3	Immutable Silicon Root of Trust	
		3.8.14.4	Ability to rollback firmware	

		3.8.14.5	FIPS 140-2 validation	
		3.8.14.6	Secure erase of NAND/User data	
		3.8.14.7	TPM (Trusted Platform Module) 1.2	
		3.8.14.8	Configurable for PCI DSS compliance	
		3.8.14.9	TPM (Trusted Platform Module) 2. 0	
		3.8.14.10	Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser	
		3.8.14.11	Bezel Locking Kit option	
		3.8.14.12	Support for Commercial National Security Algorithms (CNSA)	
		3.8.14.13	Chassis Intrusion detection option	
		3.8.14.14	Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
3.8.15	Latest Operating Systems and Virtualization Software Support	3.8.15.1	Microsoft Windows Server	
		3.8.15.2	Red Hat Enterprise Linux (RHEL)	
		3.8.15.3	SUSE Linux Enterprise Server (SLES) Vmware	
3.8.16	Secure encryption	3.8.16.1	The system should support encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys.	
		3.8.16.2	Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
3.8.17	Provisioning	3.8.17.1	Should support tool to provision server using RESTful API to discover and deploy servers at scale	
3.8.18	Firmware security	3.8.18.1	For firmware security, the system should provide Silicon root of trust or equivalent. The feature should be immutable.	
		3.8.18.2	Should maintain a repository for firmware and driver recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory-tested secured firmware	
3.8.19	Remote Management and firmware security	3.8.19.1	System remote management should support browser based graphical remote console along with Virtual Power button, remote	

			boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication	
		3.8.19.2	Server should have dedicated 1Gbps remote management port	
		3.8.19.3	The server should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware	
		3.8.19.4	Server should support agentless management using the out-of-band remote management port	
		3.8.19.5	The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur.	
		3.8.19.6	Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browsers. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. [Equivalent Feature]	
		3.8.19.7	Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation	
		3.8.19.8	Should support RESTful API integration	

		3.8.19.9	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
		3.8.19.10	The server should have a security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features	
		3.8.19.11	One-button Secure Erase designed to decommission/repurpose servers	
		3.8.19.12	NVMe wear level display [Optional Feature]	
		3.8.19.13	Workload Performance Advisor - Provides server tuning recommendations to improve server performance.	
3.8.20	Server Management & Benchmarking	3.8.20.1	Software should support dashboard views to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resource's user is authorized to view.	
		3.8.20.2	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts	
		3.8.20.3	Server Profiles	
		3.8.20.4	Server Hardware	
		3.8.20.5	Appliance alerts	
		3.8.20.6	The Systems Management software should provide Role-based access control	
		3.8.20.7	Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations and Microsoft System Center & Admin Center	
		3.8.20.8	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	

		3.8.20.9	Solution should provide online access to the product, support information and provide information to track warranties, support contracts and status.	
		3.8.20.10	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		3.8.20.11	Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline	
		3.8.20.12	The Server Management Software should be of the same brand as the server supplier.	
		3.8.20.13	SPEC INT_rate_base 2017 > 429 SPEC FP_rate_base 2017 > 565 for the product (must be available on SPEC dot ORG before evaluation)	
		3.8.20.14	The OEM / Brand must have presence in India as a manufacturer of similar items and support establishment for more than 10 years, the documentary proof should also be submitted.	
		3.8.20.15	Server should be provided with 7 Years 24x7x365 Support Directly from OEM. The 7-years support Undertaking should be submitted along with the Bid specific to this tender and the support warranty document at the time of supply of material is required.	
3.9	Software Stack Deployment: The successful bidder must deploy above network services along with DHCP, DNS (internal & external), Directory Server (DC/ ADC and LDAP), NTP, Syslog and User Access Log. All these servers must be configured preferably using Open Source. (Quantity: Job Complete)			
Spec. No	Parameters	Sub Items No	Features	Compliance (Yes/No)
3.9.1	Software Stack Deployment	3.9.1.1	The successful bidder must deploy above network services along with DHCP, DNS (internal & external), Directory Server (DC/ ADC and LDAP), NTP, Syslog and User Access Log. All these servers must be configured preferably using Open Source. (Job)	

4.1	96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 3500 Meter)		
Sln	Parameters	Specifications	Compliance (Yes/No)
4.1.1	Fiber Type	Single Mode, 9/125-micron primary coated buffers, OS2.	
4.1.2	Construction type	Multi-tube construction,	
4.1.3	Tube:	6 Nos Polybutylene, Terephthalate (PBT)	
4.1.4	No of fibers:	96 core (6/8 Fiber per tube)	
4.1.5	Water Blocking	Water Jell	
4.1.6	Armoring:	Corrugated Steel Tape Armor (ECCS Tape)	
4.1.7	Strength Member	Fibre Reinforced Plastic(FRP)	
4.1.8	Ripcord:	2 Nos	
4.1.9	Outer Sheath	HDPE	
4.1.10	Sheath thickness	1.8 mm nominal	
4.1.11	Sheath color	Black	
4.1.12	Standards	ISO. IEC 11801 - 2nd Edition, type OS2; AS/ACIF S008; AS/NZS 3080, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor ducts, direct burial and backbone cabling, RoHS Complaint	
4.1.13	Dimensions and Mass Overall, Cable (Nominal):	11. 0 ± 1. 0 MM	
4.1.14	Mass (Nominal)	Max 120Kg/Km	
4.1.15	Cable length	2 km ± 10%	
4.1.16	Bending Radius (During installation)	20 X Overall diameters	
4.1.17	Bending Radius (During full load):	10 X Overall diameters	
4.1.18	Tensile Strength-Short Term	3500N	
4.1.19	Crush Resistance-	6000N/10 cm	

	Short Term:		
4.1.20	Operating Temperature range	-20°C ±70°C	
4.1.21	Attenuation	Max. Attenuation (dB/Km) @ 1310 nm <= 0.34 @ 1550 nm <= 0.22 dB/km	
4.1.22	Warranty	25 years of System Performance and application Assurance warranty Site certificate must be issued by OEM.	
4.1.23	MAF	Bidder Must produce the manufacturer Authorization certificate from the OEM	
4.2	48 Core OFC: Single Mode fiber 48 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 2500 Meter)		
Sln	Parameters	Specifications	Compliance (Yes/No)
4.2.1	Fiber Type	Single Mode, 9/125-micron primary coated buffers, OS2.	
4.2.2	Construction type	Multi-tube construction,	
4.2.3	Tube:	6 Nos Polybutylene, Terephthalate (PBT)	
4.2.4	No of fibers:	48 core (6/8 Fiber per tube)	
4.2.5	Water Blocking	Water Jell	
4.2.6	Armoring:	Corrugated Steel Tape Armor (ECCS Tape)	
4.2.7	Strength Member	Fibre Reinforced Plastic(FRP)	
4.2.8	Ripcord:	2 Nos	
4.2.9	Outer Sheath	HDPE	
4.2.10	Sheath thickness	1.8 mm nominal	
4.2.11	Sheath color	Black	
4.2.12	Standards	ISO. IEC 11801 - 2nd Edition, type OS2; AS/ACIF S008; AS/NZS 3080, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor ducts, direct burial and backbone cabling, RoHS Complaint	
4.2.13	Dimensions and Mass Overall, Cable (Nominal):	11. 0 ± 1. 0 MM	

4.2.14	Mass (Nominal)	Max 120Kg/Km	
4.2.15	Cable length	2 km ± 10%	
4.2.16	Bending Radius (During installation)	20 X Overall diameters	
4.2.17	Bending Radius (During full load):	10 X Overall diameters	
4.2.18	Tensile Strength-Short Term	3500N	
4.2.19	Crush Resistance-Short Term:	6000N/10 cm	
4.2.20	Operating Temperature range	-20°C ±70°C	
4.2.21	Attenuation	Max. Attenuation (dB/Km) @ 1310 nm <= 0.34 @ 1550 nm <= 0.22 dB/km	
4.2.22	Warranty	25 years of System Performance and application Assurance warranty Site certificate must be issued by OEM.	
4.2.23	MAF	Bidder Must produce the manufacturer Authorization certificate from the OEM	
4.3	24 Core OFC: Single Mode fiber 24: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable. (Quantity: 2200 Meter)		
Sln	Parameters	Specifications	Compliance (Yes/No)
4.3.1		Should be ISO/IEC 11801:2002; Multi-tube Armoured with ECCS tape	
4.3.2		Type: Single Mode.9/125 micron, OS2	
4.3.3		Cable Jacket material: 1.8 mm HDPE sheath	
4.3.4		Minimum Cores 24	
4.3.5		Cable overall diameter 10.8 mm or more	
4.3.6		Tensile Strength 3500N short term and crush resistance 4400N	
4.3.7		Central Strength Member: Fibre Reinforced Plastic (FRP)	
4.3.8	Mechanical characteristics	Required Value	
	Core Diameter	9.2 ± 0.4 µm	

	Cladding Diameter	125 ± 1. 0 μm	
	Coating Diameter	242 + 5 μm	
	Primary Coating Cladding Concentricity error	≤ 12. 0 μm	
	Max. Attenuation	At 1310 nm: 0.35 dB/km At 1550 nm: 0.22 dB/km	
	Chromatic Dispersion	1285-1330nm: ≤3.5 ps/nm. km 1550nm: ≤18. 0 ps/nm. km	
	Zero Dispersion Wavelength	1302 to 1322nm	
	Zero Dispersion Slope	≤0. 091 ps/nm2. km	
	Cable cut-off wavelength	≤1260 nm	
	Mode Field Diameter at 1310nm	9.2 ±0.5 μm	
	Core clad Concentricity Error	≤0.8 μm	
	Cladding Non-Circularity	≤1 %	
	Polarisation mode dispersion	≤ 0.2ps/km	
		End to End Structured Cabling Products from Single Brand and Single OEM. OEMs should have once RCDD / CDCP in India.	
	Warranty	25 years of System Performance and application Assurance warranty Site certificate must be issued by OEM.	
	MAF	Bidder Must produce the manufacturer Authorization certificate from the OEM	
4.4	12 Core OFC: Single Mode fiber 12: -Armored Multi-Tube, 9/125μm, OS 2 Type Optical Fiber Cable. (Quantity: 900 Meter)		
Sln	Parameters	Specifications	Compliance

			(Yes/No)
4.4.1		Should be ISO/IEC 11801:2002; Multi-tube Armoured with ECCS tape	
4.4.2		Type: Single Mode.9/125 micron, OS2	
4.4.3		Cable Jacket material: 1.8 mm HDPE sheath	
4.4.4		Minimum Cores 12	
4.4.5		Cable overall diameter 10.8 mm or more	
4.4.6		Tensile Strength 3500N short term and crush resistance 4400N	
4.4.7		Central Strength Member: Fibre Reinforced Plastic (FRP)	
4.4.8	Mechanical characteristics	Required Value	
	Core Diameter	9.2 ± 0.4 µm	
	Cladding Diameter	125 ± 1. 0 µm	
	Coating Diameter	242 + 5 µm	
	Primary Coating Cladding Concentricity error	≤ 12. 0 µm	
	Max. Attenuation	At 1310 nm: 0.35 dB/km At 1550 nm: 0.22 dB/km	
	Chromatic Dispersion	1285-1330nm: ≤3.5 ps/nm. km 1550nm: ≤18. 0 ps/nm. km	
	Zero Dispersion Wavelength	1302 to 1322nm	
	Zero Dispersion Slope	≤0. 091 ps/nm2. km	
	Cable cut-off wavelength	≤1260 nm	
	Mode Field Diameter at 1310nm	9.2 ±0.5 µm	
	Core clad Concentricity Error	≤0.8 µm	
	Cladding Non-Circularity	≤1 %	

	Polarisation mode dispersion	≤ 0.2ps/km	
		End to End Structured Cabling Products from Single Brand and Single OEM. OEMs should have once RCDD / CDCP in India.	
	Warranty	25 years of System Performance and application Assurance warranty Site certificate must be issued by OEM.	
	MAF	Bidder Must produce the manufacturer Authorization certificate from the OEM	
4.5	LIU-24P: 24 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails (Quantity: 8 Number)		
Spec. No	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.5.1	Connector Type	LC-Style	
4.5.2	Operating temperature	-20 Degree C to +70 Degree C or better	
4.5.3	MM connectors	500 cycles, Beige	
4.5.4	SM connectors	200 cycles, Blue	
4.5.5	Ferrules	Pre-radiused Ceramic Ferrules	
4.5.6	Attenuation	Not more than 0.75 dB per mated pair	
4.5.7	Fiber Optic Patch panels	24 Ports Loaded	
4.5.8	FMS- Front Patching / Splicing Shelf	1U 19” / ETSI versions available	
4.5.9		The FMS fiber management shelf series is ideal for high density front patching applications.	
4.5.10		Its compact design and high density capacity allows it to deliver carrier class fiber management to central offices, Pops, FTTx, mobile systems and LANs.	
4.5.11	High Density	1U: 12/24 Fiber terminations Upgradable Upto 96 LC port in 1 U	
4.5.12		Should be supplied loaded with secondary coated LC pigtails, Splice Tray & Splice Protector	

4.5.13		Mounting brackets can be placed in different positions	
4.5.14	Sliding Drawer concept allows for	Easy access to splicing tray	
4.5.15		Easy access to back side of connector	
4.5.16		Labeling strip for adhesive labels and better cable management	
4.5.17		Fiber guides, radius controls & secure tie downs provided	
4.5.18	Buffer Diameter	900µ tight buffer	
4.5.19	Strength Member	Aramid Yarn	
4.5.20	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.5.21	Connector Loss	0.30dB(max)	
4.5.22	Operating Temperature	-40°C to +85°C	
4.5.23	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	
4.6	LIU-48P: 48 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails (Quantity: 75 Number)		
Spec. No	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.6.1	Connector Type	LC-Style	
4.6.2	Operating temperature	-20 Degree C to +70 Degree C	
4.6.3	SM connectors	200 cycles, Blue	
4.6.4	Ferrules	Pre-radiused Ceramic Ferrules	
4.6.5	Attenuation	Not more than 0.75 dB per mated pair	
4.6.6	Fiber Optic Patch panels	48 Ports Loaded	
4.6.7	FMS- Front Patching / Splicing Shelf	1U 19” / ETSI versions available	

4.6.8		The FMS fiber management shelf series is ideal for high density front patching applications.	
4.6.9	High Density	1U: 12/24 Fiber terminations Upgradable Upto 96 LC port in 1 U	
4.6.10		Should be supplied loaded with secondary coated LC pigtails, Splice Tray & Splice Protector. Mounting brackets can be placed in different positions	
4.6.11	Sliding Drawer concept allows for	Easy access to splicing tray	
4.6.12		Easy access to back side of connector	
4.6.13		Labeling strip for adhesive labels and better cable management	
4.6.14		Fiber guides, radius controls & secure tie downs provided	
4.7	LC-LC Patch Cord-Type-1: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 0.5m (Quantity: 500 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.7.1		9/125 µm, OS2, Duplex Zipcord.	
4.7.2	Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with 2XLC type fiber connectors terminated at one end and 2X LC type fiber connectors at other end of the patch cord.	
4.7.3	Cordage O. D	(Duplex): 2. 0mm ± 0.1mm x 4.1± 0.2mm	
4.7.4	Buffer Diameter	900µ tight buffer	
4.7.5	Strength Member	Aramid Yarn	
4.7.6	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.7.7	Connector Loss	0.30dB(max)	
4.7.8	Operating Temperature	-40°C to +85°C	
4.7.9	Certificate	ETL Tested	
4.7.10	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	

4.8	LC-LC Patch Cord-Type-2: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 1m (Quantity: 312 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.8.1		9/125 µm, OS2, Duplex Zipcord.	
4.8.2	Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with 2XLC type fiber connectors terminated at one end and 2X LC type fiber connectors at other end of the patch cord.	
4.8.3	Cordage O. D	(Duplex): 2. 0mm ± 0.1mm x 4.1± 0.2mm	
4.8.4	Buffer Diameter	900µ tight buffer	
4.8.5	Strength Member	Aramid Yarn	
4.8.6	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.8.7	Connector Loss	0.30dB(max)	
4.8.8	Operating Temperature	-40°C to +85°C	
4.8.9	Certificate	ETL Tested	
4.8.10	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	
4.9	LC-LC Patch Cord-Type-3: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 2m (Quantity: 144 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.9.1		9/125 µm, OS2, Duplex Zipcord.	
4.9.2	Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with 2XLC type fiber connectors terminated at one end and 2X LC type fiber connectors at other end of the patch cord.	
4.9.3	Cordage O. D	(Duplex): 2. 0mm ± 0.1mm x 4.1± 0.2mm	
4.9.4	Buffer Diameter	900µ tight buffer	
4.9.5	Strength Member	Aramid Yarn	
4.9.6	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.9.7	Connector Loss	0.30dB(max)	

4.9.8	Operating Temperature	-40°C to +85°C	
4.9.9	Certificate	ETL Tested	
4.9.10	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	
4.10	LC-LC Patch Cord-Type-4: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 5m (Quantity: 64 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.10.1		9/125 µm, OS2, Duplex Zipcord.	
4.10.2	Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with 2XLC type fiber connectors terminated at one end and 2X LC type fiber connectors at other end of the patch cord.	
4.10.3	Cordage O. D	(Duplex): 2. 0mm ± 0.1mm x 4.1± 0.2mm	
4.10.4	Buffer Diameter	900µ tight buffer	
4.10.5	Strength Member	Aramid Yarn	
4.10.6	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.10.7	Connector Loss	0.30dB(max)	
4.10.8	Operating Temperature	-40°C to +85°C	
4.10.9	Certificate	ETL Tested	
4.10.10	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	
4.11	LC-LC Patch Cord-Type-5: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 10m (Quantity: 48 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.11.1		9/125 µm, OS2, Duplex Zipcord.	
4.11.2	Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with	

		2XLC type fiber connectors terminated at one end and 2X LC type fiber connectors at other end of the patch cord.	
4.11.3	Cordage O. D	(Duplex): 2. 0mm ± 0.1mm x 4.1± 0.2mm	
4.11.4	Buffer Diameter	900µ tight buffer	
4.11.5	Strength Member	Aramid Yarn	
4.11.6	Jacket Material	LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
4.11.7	Connector Loss	0.30dB(max)	
4.11.8	Operating Temperature	-40°C to +85°C	
4.11.9	Certificate	ETL Tested	
4.11.10	Standards	ISO/IEC 1108:2008, ANSI/TIA/ EIA 568. C.3, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596	
4.12	Custom Patch Cords-2c: 2-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord (Quantity: 500 meter)		
Sln	Specifications		Compliance (Yes/No)
4.12.1	2-Core OS2 Single-Mode, 9/125 µm fibre, LC–LC duplex connectors, suitable for 10/25/40/100 GbE applications.		
4.12.2	Flexible metallic armoured fibre construction with aramid yarn reinforcement and rugged LSZH/TPU outer jacket for enhanced mechanical protection.		
4.12.3	Provides high crush, compression and rodent resistance, with increased protection against accidental mechanical damage.		
4.12.4	Suitable for indoor/outdoor, industrial and harsh environments, including data centres and high-traffic areas.		
4.12.5	Custom-built to match site-specific requirements, with cable length and connector configuration tailored for LIU-to-rack and rack-to-switch connections at different locations.		
4.13	Custom Patch Cords-4c: 4-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord (Quantity: 200 meter)		
Sln	Specifications		Compliance (Yes/No)

4.13.1	4-Core OS2 Single-Mode, 9/125 µm fibre, LC–LC duplex connectors, suitable for 10/25/40/100 GbE transmission.	
4.13.2	Flexible metallic armoured fibre construction with aramid yarn reinforcement and durable LSZH/TPU outer jacket.	
4.13.3	Provides enhanced crush, compression, tensile and rodent resistance for demanding installations.	
4.13.4	Suitable for data centres, industrial areas and harsh outdoor environments, including mechanically exposed locations.	
4.13.5	Custom-built to match site-specific requirements, with cable length and connector configuration tailored for LIU-to-rack and rack-to-switch connections at different locations.	
4.14	Custom Patch Cords-6c: 6-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord (Quantity: 100 meter)	
Sln	Specifications	Compliance (Yes/No)
4.14.1	6-Core OS2 Single-Mode, 9/125 µm fibre, LC–LC duplex connectors, suitable for high-speed optical networking.	
4.14.2	Flexible metallic armoured fibre construction with aramid yarn reinforcement and rugged LSZH/TPU outer jacket.	
4.14.3	Provides high crush, compression, tensile and rodent resistance with enhanced physical protection.	
4.14.4	Suitable for industrial, outdoor and harsh-environment applications, including high-traffic areas.	
4.14.5	Custom-built to match site-specific requirements, with cable length and connector configuration tailored for LIU-to-rack and rack-to-switch connections at different locations.	
4.15	Custom Patch Cords-8c: 8-Strand Flexible Armoured 9/125 µm Singlemode OS2 Optical Fibre Patch Cord (Quantity: 100 meter)	
Sln	Specifications	Compliance (Yes/No)
4.15.1	8-Core OS2 Single-Mode, 9/125 µm fibre, LC–LC duplex connectors, suitable for 10/25/40/100 GbE applications.	
4.15.2	Flexible metallic armoured fibre construction with aramid yarn reinforcement and rugged LSZH/TPU outer jacket.	
4.15.3	Designed for superior crush, compression, tensile and rodent resistance, providing increased cable protection.	

4.15.4	Suitable for data centres, industrial installations and harsh outdoor environments, where enhanced durability and mechanical protection are required.		
4.15.5	Custom-built to match site-specific requirements, with cable length and connector configuration tailored for LIU-to-rack and rack-to-switch connections at different locations.		
4.16	Compatible Pigtail: LC/UPC male type single-mode OS2 9/125 µm fiber pigtail, with locking latch, suitable for direct connection to LC female adapter of LIU with bare-fiber end for fusion splicing. (Quantity: 1600 number)		
Sln	Specifications		Compliance (Yes/No)
4.16.1	Product details -		
	Make, Model No. /OEM Part Code. (Please specify)		
	Optical Fiber Pigtail: Single Mode OS2, 9/125 µm, G.657A2 fiber pigtail, 1 metre length, LS0H jacket, suitable for fusion splicing and installation in ODF/LIU/Fiber Patch Panel. It shall be factory terminated with LC/SC/ST connectors		
4.17	Junction Box: Outdoor Junction Box for OFC termination IP67: all weather outdoor box, to be installed as a junction box for 96 fibres LIU (Quantity: 3 number)		
Sln	Specifications		Compliance (Yes/No)
4.17.1	Outdoor Street Cabinet/Fiber Distribution Cabinet (IP 65 Rated):		
4.17.2	Street Cabinet/ Fiber Distribution Cabinet 144F, SC/APC or LC/APC the Street cabinet shall be used for Fiber Cable distribution at field side and is a plinth mountable outdoor unit, IP 65 Rated Weatherproof. It should at least have the following features:		
4.17.3	Should be loaded with an adequate number of SCAPC/LCAPC Adapters and pigtails so that all the Distribution fiber ports can be patched to the incoming and outgoing main cables. The numbers of Ports shall exceed 12 numbers at the maximum.		
4.17.4	Should have provision for loading up to 12 X 12F splice trays, the product should be loaded with an adequate number of splice trays for splicing the conventional fibers.		
4.17.5	Capacity can be flexibly customized as required		
4.17.6	Built-in direct splice unit is capable for providing direct connection function		

4.17.7	Perfect design of fiber wiring routing could facilitate management and maintenance of fibers	
4.17.8	The box should have the provision to terminate Armoured drop cable and & fiber tube of 12F	
4.17.9	The adapter panel should have the following features.	
4.17.10	The panel should be Door type for easy access.	
4.17.11	The 12F, Main Fiber Cable & Distribution fiber Cable inputs and outputs should be patched to the front of the adapter panel.	
4.17.12	The Panel should have Fiber Splitter slots,	
4.17.13	The pigtails should be patched to the rear of the adapter panel.	
4.17.14	The adapter panel should be pre-loaded with anadequate number of SCAPC/LCAPC adapters and pigtails so that all the splitter ports can be patched to the incoming and outgoing main and distribution cables.	
4.17.15	The cabinet should have the parking lot available for splitters unused ports. There should be a provision for fixing 144F simplex adapters.	
4.17.16	The adapters should be fixed using screws to the adapter panel.	
4.17.17	Should be loaded with adequate number of splice trays for splicing the GPON as well as the conventional fibers.	
4.17.18	The blank adapter ports should be closed with plastic blanking plugs.	
4.17.19	Baskets should be provided for looping the uncut loose tubes The Cabinet should have a locking System.	
4.17.20	The cabinet should have a document holder.	
4.17.21	The Cabinet should have hole for easy cable entry	
4.17.22	The cabinet should be supplied with all the required accessories for installation viz. Fusion splice protectors (40mm), cable ties, IPA, tissue paper, hose clamps, red adhesive tape, grounding accessories, route card, transport tube.	
4.18	HDPE Duct-Type1: Duct for OFC HDPE Pipe 24 Core and 48 Core OFC (Quantity: 4550 meter)	
Sln	Specifications	Compliance (Yes/No)
4.18.1	HDPE Duct for 24-Core & 48-Core OFC: Supply and installation of PLB HDPE Duct, minimum 40/33 mm (OD/ID), manufactured from high-quality HDPE material with a permanently lubricated low-friction inner layer, suitable for underground laying and pulling/blowing of 24-Core and 48-Core OFC cables. The duct shall be UV/moisture resistant, mechanically strong and suitable for underground installation	

4.19	HDPE Duct-Type2: Duct for OFC HDPE Pipe for 96 Core OFC (Quantity: 3500 Meter)		
Sln	Specifications		Compliance (Yes/No)
4.19.1	HDPE Duct for 96 Core OFC: Supply and installation of PLB HDPE Duct, minimum 40/33 mm (OD/ID), manufactured from high-quality HDPE material with a permanently lubricated low-friction inner layer, suitable for underground laying and pulling/blowing of 96 Core OFC cables. The duct shall be UV/moisture resistant, mechanically strong and suitable for underground installation		
4.20	OFC Laying: OFC Laying by non-trenching method (Quantity: 7700 Meter)		
Sln	Specifications		Compliance (Yes/No)
4.20.1	Supply, installation and laying of HDPE/PLB-HDPE duct for OFC through Horizontal Directional Drilling (HDD) / non-trenching method, including route survey, marking, pilot drilling, reaming, drilling fluid, pulling of HDPE duct, jointing, testing and commissioning. The duct shall be laid at the required depth with minimum disturbance to existing roads, pavements, utilities and structures. The work shall include all necessary HDD machinery, manpower, tools, equipment, couplers and accessories, complete in all respects as per approved route, site conditions and applicable standards.		
4.21	CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 80 Boxes)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.21.1	Type	Unshielded twisted pair cabling system, TIA 568.2-D Category 6	
4.21.2	Network support	Supports ultrahigh speed data networks such as Gigabit Ethernet (1000 Base-T and 1000 Base-TX) or more.	
4.21.3	TIA 568.2-D	ETL Verified & UL Listed & ETL 4 Connector Channel report (Certificates are mandatory)	
4.21.4	IEEE 802.3ab	Zero-bit Error	
4.21.5	POE	Suitable for PoE applications: IEEE 802.3bt from Type 1 to Type 4,	

4.21.6	Fire Rating	IEC 60332-1, Acid gas IEC 60754-2 Smoke density IEC 61034-2	
4.21.7	Conductors	23 AWG solid bare copper	
4.21.8	Insulation	Polyethylene	
4.21.9	Sheath Type	LSZH Complies to IEC 60332-1	
4.21.10	Pulling Force	100N or 11 KG Minimum	
4.21.11	NVP	69%	
4.21.12	Packing	Box of 305 meters	
4.21.13	Instant Volt rated	300V	
4.21.14	Impedance	100 Ohms + / - 15 ohms	
4.21.15	Delay Skew:	45ns Max	
4.21.16	Mutual Capacitance:	5.6nF/100m Nominal	
4.21.17	Approved	RoHS Compliant	
4.22	CAT6 Cable type -2: Metallic armour CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 5 Boxes)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.22.1	Type	Unshielded twisted pair cabling system Category 6 ANSI/TIA 568.2-D ISO/IEC 11801 IEC 61156-5	
4.22.2	Network support	Supports ultrahigh speed data networks such as Gigabit Ethernet (1000 Base-T and 1000 Base-TX) or more.	
4.22.3	Sheath Type(Inner & Outer)	Inner LSZH Outer UV Resistant PVC.	
4.22.4	External OD	7. 0 ± 1. 0 mm	
4.22.5	Conductors	23 AWG solid bare copper	
4.22.6	Insulation	Solid Polyolefin	
4.22.7	Pulling Force	100N or 11 KG Minimum	
4.22.8	NVP	69%	
4.22.9	Packing	Box of 305 meters	

4.22.10	Outdoor Use	Yes	
4.22.11	Operating Temp	, -20 °C to +70 °C	
4.22.12	Approved	RoHS Compliant	
4.23	CAT6 Patch Panel 24P: 24 port CAT 6 Patch Panel (Quantity: 24 number)		
Sln	Specifications		Compliance (Yes/No)
4.23.1	Should be supplied with individually replaceable 24 numbers Category-6A I/O Jacks complying as per the ANSI/TIA-568.2 D.		
4.23.2	Should be 19” rack mountable and of 1U height & complete with all mounting accessories		
4.23.3	Should have label holder/cover for identification of ports		
4.23.4	IDC Connector plastic housing should be polycarbonate and UL94V-0 rated.		
4.23.5	Operating Life should be Minimum 20 determinations and contact material should be copper alloy.		
4.23.6	Material should be CRS (cold rolled steel)		
4.23.7	Should be supplied with metallic integrated rear cable management shelf as for cable strain relief & for better cable dressing at the rear		
4.23.8	Jack (I/O) operating Life should be minimum 750 insertion cycles and contact material should be copper alloy.		
4.23.9	Jack (I/O) contact plating should be 50µ Gold/ 50µ Nickel minimum		
4.23.10	Jack (I/O) on the panel must have protection from dust and contaminants.		
4.23.11	Should be RoHS Compliant		
4.23.12	Should be certified by ETL/UL		
4.24	CAT6 Patch Panel 48P: 48 port CAT 6 Patch Panel (Quantity: 12 number)		
Sln	Specifications		Compliance (Yes/No)
4.24.1	Should be supplied with individually replaceable 48 numbers Category-6 I/O Jacks complying as per the ISO/IEC 11801-1:2017, ANSI/TIA-568.2 D or latest		
4.24.2	Should be 19” rack mountable and of 2U height & complete with all mounting accessories		

4.24.3	Material should be CRS (cold rolled steel)		
4.24.4	Jack (I/O) should have protection from dust and contaminants.		
4.24.5	Jack (I/O) operating Life should be minimum 750 insertion cycles and contact material should be copper alloy.		
4.24.6	Jack (I/O) contact plating should be 50µ Gold/ 50µ Nickel minimum		
4.24.7	Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, with optional color labels / icons.		
4.24.8	Operating Life should be Minimum 20 determinations and contact material should be copper alloy.		
4.24.9	Should be supplied with metallic integrated rear cable management shelf as for cable strain relief & for better cable dressing at the rear		
4.24.10	Port numbering is provided on the front and rear of the panel		
4.24.11	Should be RoHS Compliant		
4.24.12	Jack panels should be certified by ETL/UL.		
4.25	CAT6 Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 1000 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.25.1	Type	Cat 6 U/UTP supports data networks for 10/100BASE-T and 1000BASE-T applications.	
4.25.2	Conductor size:	24 AWG stranded copper wire	
4.25.3	Nom. O. D.:	6 mm ± 0.5 mm	
4.25.4	Sheath:	LS0H	
4.25.5	POE	Suitable for PoE applications: IEEE 802.3bt from Type 1 to Type 4,	
4.25.6	Boots	Transparent Plug with anti-snag slip on boots	
4.25.7	RJ45 Plug Standard	ISO/IEC 60606-7-4 and FCC 47 Part 68	
4.25.8	Sheath Standards	Fire Propagation compliant with CSA FTI, IEC 60332-1 & IEC 61034	
4.25.9	Operating temperature range:	-20°C to 60°C	
4.25.10	MIN operating life	: 750 insertion cycles	
4.25.11	RJ45 plug and boot	Clear polycarbonate	

	material:		
4.25.12	Contact material:	0.35mm thick copper alloy	
4.25.13	Contact plating:	Selective gold	
4.25.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	
4.25.15	Verified	UL Listed & ETL Verified	
4.25.16	Standard length available	0.5mt	
4.26	CAT6 Patch Cord - type - 2: Patch Cords 1M (Quantity: 1000 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.26.1	Type	Cat 6 U/UTP supports data networks for 10/100BASE-T and 1000BASE-T applications.	
4.26.2	Conductor size:	24 AWG stranded copper wire	
4.26.3	Nom. O. D.:	6 mm ± 0.5 mm	
4.26.4	Sheath:	LS0H	
4.26.5	POE	Suitable for PoE applications: IEEE 802.3bt from Type 1 to Type 4,	
4.26.6	Boots	Transparent Plug with anti-snag slip on boots	
4.26.7	RJ45 Plug Standard	ISO/IEC 60606-7-4 and FCC 47 Part 68	
4.26.8	Sheath Standards	Fire Propagation compliant with CSA FTI, IEC 60332-1 & IEC 61034	
4.26.9	Operating temperature range:	-20°C to 60°C	
4.26.10	MIN operating life	: 750 insertion cycles	
4.26.11	RJ45 plug and boot material:	Clear polycarbonate	
4.26.12	Contact material:	0.35mm thick copper alloy	
4.26.13	Contact plating:	Selective gold	
4.26.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	

4.26.15	Verified	UL Listed & ETL Verified	
4.26.16	Standard length available	1 mt	
4.27	CAT6 Patch Cord - type - 3: Patch Cords 2M (Quantity: 500 number)		
Sln	Parameters	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.27.1	Type	Cat 6 U/UTP supports data networks for 10/100BASE-T and 1000BASE-T applications.	
4.27.2	Conductor size:	24 AWG stranded copper wire	
4.27.3	Nom. O. D.:	6 mm ± 0.5 mm	
4.27.4	Sheath:	LS0H	
4.27.5	POE	Suitable for PoE applications: IEEE 802.3bt from Type 1 to Type 4,	
4.27.6	Boots	Transparent Plug with anti-snag slip on boots	
4.27.7	RJ45 Plug Standard	ISO/IEC 60606-7-4 and FCC 47 Part 68	
4.27.8	Sheath Standards	Fire Propagation compliant with CSA FTI, IEC 60332-1 & IEC 61034	
4.27.9	Operating temperature range:	-20°C to 60°C	
4.27.10	MIN operating life	: 750 insertion cycles	
4.27.11	RJ45 plug and boot material:	Clear polycarbonate	
4.27.12	Contact material:	0.35mm thick copper alloy	
4.27.13	Contact plating:	Selective gold	
4.27.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	
4.27.15	Verified	UL Listed & ETL Verified	
4.27.16	Standard length available	2 mt	

4.28	CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 20 Boxes)	
Sln	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)
4.28.1	Category 6A 4 pair LSZH cable should be compliant with TIA/EIA-568.2-D	
4.28.2	Should be of 4 twisted pairs of 23 AWG solid conductors	
4.28.3	Should support network line speed up to 10 Gigabits per second.	
4.28.4	Shall be 4-pair twisted pair with an isolator (+), i. e.4 pair cable should be individual screened pairs for electromagnetic interference (EMI) protection, meeting Category 6A tested to 500 MHz. (4 connector test report from ETL(Intertek) to be submitted with offer & must be available on Intertek site for verification).	
4.28.5	Should be ETL verified to TIA/EIA-568.2-D Category 6A standard for 500MHz (ETL certificate to be enclosed along with the bid)	
4.28.6	Must comply with ISO/IEC 11801, IEC 61156-5, IEEE 802.3bt	
4.28.7	Conductor should be solid Copper 23 AWG	
4.28.8	Pulling Force - Short Term - 400N	
4.28.9	Insulator should be Polyethylene/Polyolefin	
4.28.10	Jacket/ Sheath type should be LS0H (Low Smoke Zero Halogen) as per IEC60332-I & IEC 60332-3-22	
4.28.11	NVP should be 72% or better	
4.28.12	The screen should be each individual pair enclosed in laminated aluminium foil with drain wire	
4.28.13	Mean Impedance should be 100Ω ± 6 @ 1-500 MHz	
4.28.14	Coupling Attenuation should be 45dB min @30-100 MHz 40-20 Log (f/100) @ 100-500 MHz	
4.28.15	Operating Temperature should be: -20˚C to +60˚C	
4.28.16	Should be RoHS Compliant	
4.28.17	Should be certified by ETL/UL	
4.29	CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each (Quantity: 8 Boxes)	
Sln	TECHNICAL SPECIFICATIONS	Compliance (Yes/No)

4.29.1	Type	6A S/FTP 4-Pair Shielded- PVC+PE Sheath (Armored) Cable Category 6A ANSI/TIA 568.2-D ISO/IEC 11801 IEC 61156-5	
4.29.2	Network support	Supports ultrahigh speed data networks such as Gigabit Ethernet	
4.29.3	Sheath Type(Inner & Outer)	Inner PVC Outer UV Resistant HDPE.	
4.29.4	External OD	11. 0 ± 1 mm	
4.29.5	Conductors	23 AWG solid bare copper	
4.29.6	Insulation	Solid Polyolefin	
4.29.7	Pulling Force	100N or 11 KG Minimum	
4.29.8	Armour	Braided steel wires	
4.29.9	Packing	Box of 305 meters	
4.29.10	Outdoor Use	Yes	
4.29.11	Operating Temp	, -25 °C to +70 °C	
4.29.12	Approved	RoHS Compliant	
4.30	CAT6A Patch Panel 24P: 24 port CAT 6A Patch Panel (Quantity: 4 number)		
Sln	Specifications		Compliance (Yes/No)
4.30.1	Should be supplied with individually replaceable 24 numbers Category-6A I/O Jacks complying as per the ANSI/TIA-568.2 D.		
4.30.2	Should be 19” rack mountable and of 1U height & complete with all mounting accessories		
4.30.3	Should have label holder/cover for identification of ports		
4.30.4	IDC Connector plastic housing should be polycarbonate and UL94V-0 rated.		
4.30.5	Operating Life should be Minimum 20 reterminations and contact material should be copper alloy.		
4.30.6	Material should be CRS (cold rolled steel)		
4.30.7	Should be supplied with metallic integrated rear cable management shelf as for cable strain relief & for better cable dressing at the rear		
4.30.8	Jack (I/O) operating Life should be minimum 750 insertion cycles and contact material should be copper alloy.		
4.30.9	Jack (I/O) contact plating should be 50µ Gold/ 50µ Nickel minimum		

4.30.10	Jack (I/O) on the panel must have protection from dust and contaminants.		
4.30.11	Should be RoHS Compliant		
4.30.12	Should be certified by ETL/UL		
4.31	CAT6A Patch Panel 48P: 48 port CAT 6A Patch Panel (Quantity: 4 number)		
Sln	Specifications		Compliance (Yes/No)
4.31.1	Should be supplied with individually replaceable 48 numbers Category-6 I/O Jacks complying as per the ISO/IEC 11801-1:2017, ANSI/TIA-568.2 D or latest		
4.31.2	Should be 19” rack mountable and of 2U height & complete with all mounting accessories		
4.31.3	Material should be CRS (cold rolled steel)		
4.31.4	Jack (I/O) should have protection from dust and contaminants.		
4.31.5	Jack (I/O) operating Life should be minimum 750 insertion cycles and contact material should be copper alloy.		
4.31.6	Jack (I/O) contact plating should be 50µ Gold/ 50µ Nickel minimum		
4.31.7	Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, with optional color labels / icons.		
4.31.8	Operating Life should be Minimum 20 reterminations and contact material should be copper alloy.		
4.31.9	Should be supplied with metallic integrated rear cable management shelf as for cable strain relief & for better cable dressing at the rear		
4.31.10	Port numbering is provided on the front and rear of the panel		
4.31.11	Should be RoHS Compliant		
4.31.12	Jack panel should be certified by ETL/UL.		
4.32	CAT6A Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 100 number)		
Sln	Specifications		Compliance (Yes/No)
4.32.1	Category 6A Equipment cords (Length – 0.5 Mtr)		
4.32.2	Conductors Should be of 4 twisted pairs of 26 AWG stranded copper for better flexibility		

4.32.3	Patch cords should conform to ANSI/TIA-568.2-D for Cat 6A	
4.32.4	Should have RJ-45 jacks with boot at both the ends.	
4.32.5	All patch cords should be factory crimped and packed.	
4.32.6	Anti-snag slim strain relief slip on boots	
4.32.7	Should have LSZH jacket for safety complied to IEC 60332-1-1 & IEC 61034-2	
4.32.8	Operating Temperature should be -20°C to +60°C	
4.32.9	Screen material should be aluminum/polyester with tinned copper drain wire.	
4.32.10	Plug Insertion Life should be Minimum 750 times	
4.32.11	Contact Plating should be 1.27um gold or better	
4.32.12	Shall be RoHS Compliant	
4.32.13	Should be certified by ETL/UL.	
4.33	CAT6A Patch Cord - type - 2: Patch Cords 1M (Quantity: 100 number)	
Sln	Specifications	Compliance (Yes/No)
4.33.1	Category 6A Equipment cords (Length – 1 Mtr)	
4.33.2	Conductors Should be of 4 twisted pairs of 26 AWG stranded copper for better flexibility	
4.33.3	Patch cords should conform to ANSI/TIA-568.2-D for Cat 6A	
4.33.4	Should have RJ-45 jacks with boot at both the ends.	
4.33.5	All patch cords should be factory crimped and packed.	
4.33.6	Anti-snag slim strain relief slip on boots	
4.33.7	Should have LSZH jacket for safety complied to IEC 60332-1-1 & IEC 61034-2	
4.33.8	Operating Temperature should be -20°C to +60°C	
4.33.9	Screen material should be aluminum/polyester with tinned copper drain wire.	
4.33.10	Plug Insertion Life should be Minimum 750 times	
4.33.11	Contact Plating should be 1.27um gold or better	
4.33.12	Shall be RoHS Compliant	
4.33.13	Should be certified by ETL/UL.	

4.34	CAT6A Patch Cord - type - 3: Patch Cords 2M (Quantity: 64 number)		
Sln	Specifications		Compliance (Yes/No)
4.34.1	Category 6A Equipment cords (Length – 2 Mtr)		
4.34.2	Conductors Should be of 4 twisted pairs of 26 AWG stranded copper for better flexibility		
4.34.3	Patch cords should conform to ANSI/TIA-568.2-D for Cat 6A		
4.34.4	Should have RJ-45 jacks with boot at both the ends.		
4.34.5	All patch cords should be factory crimped and packed.		
4.34.6	Anti-snag slim strain relief slip on boots		
4.34.7	Should have LSZH jackket for safety complied to IEC 60332-1-1 & IEC 61034-2		
4.34.8	Operating Temperature should be -20°C to +60°C		
4.34.9	Screen material should be aluminum/polyester with tinned copper drain wire.		
4.34.10	Plug Insertion Life should be Minimum 750 times		
4.34.11	Contact Plating should be 1.27um gold or better		
4.34.12	Shall be RoHS Compliant		
4.34.13	Should be certified by ETL/UL.		
4.35	Conduit-Square: Conduit Square (24x24) (Quantity: 500 Meter)		
Sln	Specifications		Compliance (Yes/No)
4.35.1	Supply and installation of 24x24 mm square nominal rigid, heavy-duty, high-impact and flame-retardant PVC/uPVC square conduit, corrosion-resistant, moisture-resistant and non-conductive, suitable for concealed or surface installation for routing electrical, data, CCTV and other ELV cables		
4.36	Conduit-Round: Conduit round (10mm) (Quantity: 500 meter)		
Sln	Specifications		Compliance

		(Yes/No)
4.36.1	Supply and installation of 10 mm nominal diameter rigid, heavy-duty, high-impact and flame-retardant PVC/uPVC round conduit, corrosion-resistant, moisture-resistant and non-conductive, suitable for concealed or surface installation for routing electrical, data, CCTV and other ELV cables	

4.37	T-joints: Compatible with 10mm round conduit (Quantity: 100 number)		
Sln	Specifications		Compliance (Y/N)
4.37.1	Size	10 MM round conduit fix	
4.37.2	Color	White or any other compatible color as per the conduit	
4.38	L-joints: Compatible with 10mm round conduit (Quantity: 200 number)		
Sln	Specifications		Compliance (Y/N)
4.38.1	Size	10 MM round conduit fix	
4.38.2	Color	White or any other compatible color as per the conduit	
4.39	Flexi-pipe-a: Compatible with 10mm round conduit (Quantity: 100 Meter)		
Sln	Specifications		Compliance (Y/N)
4.39.1	Size	10 MM round conduit fix	
4.39.2	Color	White or any other compatible color as per the conduit	
4.40	Flexi-pipe-b: Compatible with 24mmx24mm conduits (Quantity: 100 meter)		
Sln	Specifications		Compliance (Y/N)
4.40.1	Size	compatible to fix with 24x24 mm conduit	
4.40.1	Color	White or any other compatible color as per the conduit	

4.41	Racks-Type-1: 6 U Network racks (Quantity: 12 Number)	
Sln	Specifications	Compliance (Yes/No)
4.41.1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.	
4.41.2	The racks should be conform to EIA-310 Standard, ISO 9001-2015, 14001-2015, 27001-2013, 45001-2018, IEC-	

	60297, DIN- 41494 & RoHS for Cabinets, Racks, standard 19” rack mount equipment.	
4.41.3	Wall Mount Rack with Front Glass door and welded structure should be CRCA sheet.	
4.41.4	Racks should have a provision for cable entry from the top and bottom.	
4.41.5	The racks should be available with vertical equipment mounting space of 6U	
4.41.6	The racks should have a minimum of IP 20 rating.	
4.41.7	Front and Rear mounting rails should be adjustable for depth.	
4.41.8	All racks should be 550 mm width and 500 mm deep. The height of the Racks should be 6U (usable)	
4.41.9	All Racks should be provided with cable manager Horizontal with MS loop, 1 Fan 230V AC 90 CFM, Hardware (pack of 10 nos), Fixed shelf/cantilever shelf,	
4.41.10	one number of PDU, 6 socket 5 AMP with switch & indicator, 2 mtr cable with 3 pin plug	
4.41.11	Load Bearing Capacity upto 35 kg	
4.42	Racks-Type-2: 9 U Network racks (Quantity: 12 Number)	
Sln	Specifications	Compliance (Yes/No)
4.42.1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.	
4.42.2	The racks should be conform to EIA-310 Standard, ISO 9001-2015, 14001-2015, 27001-2013, 45001-2018, IEC-60297, DIN- 41494 & RoHS for Cabinets, Racks, standard 19” rack mount equipment.	
4.42.3	Wall Mount Rack with Front Glass door and welded structure should be CRCA sheet.	
4.42.4	Racks should have a provision for cable entry from the top and bottom.	
4.42.5	The racks should be available with a vertical equipment mounting space of 9U	
4.42.6	The racks should have a minimum of IP 20 rating.	
4.42.7	Front and Rear mounting rails should be adjustable for depth.	
4.42.8	All racks should be 550 mm width and 500 mm deep. The height of the Racks should be 9U (usable)	
4.42.9	All Racks should be provided with cable manager Horizontal with MS loop, 1 Fan 230V AC 90 CFM, Hardware (pack of 10 nos), Fixed shelf/cantilever shelf,	
4.42.10	one number of PDU, 6 socket 5 AMP with switch & indicator, 2 mtr cable with 3 pin plug	
4.42.11	Load Bearing Capacity upto 35 kg	

4.43	Racks-Type-3: 12 U Network racks (Quantity: 6 Number)		
Sln	Specifications		Compliance (Yes/No)
4.43.1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.		
4.43.2	The racks should be conform to EIA-310 Standard, ISO 9001-2015, 14001-2015, 27001-2013, 45001-2018, IEC-60297, DIN- 41494 & RoHS for Cabinets, Racks, standard 19” rack mount equipment.		
4.43.3	Wall Mount Rack with Front Glass door and welded structure should be CRCA sheet.		
4.43.4	Racks should have a provision for cable entry from the top and bottom.		
4.43.5	The racks should be available with a vertical equipment mounting space of 12U		
4.43.6	The racks should have a minimum of IP 20 rating.		
4.43.7	Front and Rear mounting rails should be adjustable for depth.		
4.43.8	All racks should be 550 mm width and 500 mm deep. The height of the Racks should be 12U (usable)		
4.43.9	All Racks should be provided with cable manager Horizontal with MS loop, 1 Fan 230V AC 90 CFM, Hardware (pack of 10 nos), Fixed shelf/cantilever shelf,		
4.43.10	one number of PDU, 6 socket 5 AMP with switch & indicator, 2 mtr cable with 3 pin plug		
4.43.11	Load Bearing Capacity upto 45 kg		
4.44	Racks-Type-4: 15 U Network racks (Quantity: 12 Number)		
Sln	Specifications		Compliance (Yes/No)
4.44.1	The racks should be designed to provide a secure, managed environment for server and Networking equipment.		
4.44.2	The racks should be conform to EIA-310 Standard, ISO 9001-2015, 14001-2015, 27001-2013, 45001-2018, IEC-60297, DIN- 41494 & RoHS for Cabinets, Racks, standard 19” rack mount equipment.		
4.44.3	Wall Mount Rack with Front Glass door and welded structure should be CRCA sheet.		
4.44.4	Racks should have a provision for cable entry from the top and bottom.		
4.44.5	The racks should be available with a vertical equipment mounting space of 15U		
4.44.6	The racks should have a minimum of IP 20 rating.		
4.44.7	Front and Rear mounting rails should be adjustable for depth.		

4.44.8	All racks should be 550 mm width and 500 mm deep. The height of the Racks should be 15U (usable)		
4.44.9	All Racks should be provided with cable manager Horizontal with MS loop, 1 Fan 230V AC 90 CFM, Hardware (pack of 10 nos), Fixed shelf/cantilever shelf,		
4.44.10	one number of PDU, 6 socket 5 AMP with switch & indicator, 2 mtr cable with 3 pin plug		
4.44.11	Load Bearing Capacity upto 45 kg		
5.1	Work - 1: Work and commissioning of All switches, laying cables & installation of AS in every building, integrating to existing system, designing the entire network segment and implementing the policies etc. (Quantity: job Complete)		
Spec. No	Parameters	Specifications	Compliance (Yes/No)
5.1.1	Work	Work and commissioning of All switches, laying cables & installation of AS in every building, integrating to existing system, designing the entire network segment and implementing the policies etc	
6.1	Manpower: One (01) qualified and trained Network Engineer shall be deployed onsite for day-to-day network administration, monitoring, troubleshooting, configuration, preventive maintenance, and technical support of the networking infrastructure. (Quantity: 1 salary per month)		
Spec. No	Parameters	Specifications	Compliance (Yes/No)
6.1.1	Manpower	One (01) qualified and trained Network Engineer shall be deployed onsite for day-to-day network administration, monitoring, troubleshooting, configuration, preventive maintenance, and technical support of the networking infrastructure.	
6.1.2		The engineer shall have minimum 3 years of relevant experience in enterprise networking, with hands-on expertise in switches, routers, VLANs, routing, firewalls, wireless networks, network monitoring, and troubleshooting.	
6.1.3		The manpower deployment shall initially be for six (06) months, extendable up to one (01) year based on satisfactory performance and organizational requirement. The quoted total cost for six (06) months shall be considered for determining L1.	

7.1	Works - 2: Through Existing Concealed Conduits/Pipes: Pulling and routing CAT6/6A cable(s) through existing concealed conduits/pipes without providing any new conduit or channel. Includes cable pulling, routing, dressing, termination at both ends, testing, labeling, and commissioning. (Quantity: 1500 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.1.1	Running per meter	Through Existing Concealed Conduits/Pipes: Pulling and routing CAT6/6A cable(s) through existing concealed conduits/pipes without providing any new conduit or channel. Includes cable pulling, routing, dressing, termination at both ends, testing, labeling, and commissioning.	
7.2	Works - 3: Laying New PVC Conduit – Up to 2 CAT6/6A Cables: Fixing suitable PVC conduit with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 1500 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.2.1	Running per meter	Laying New PVC Conduit – Up to 2 CAT6/6A Cables: Fixing suitable PVC conduit with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	
7.3	Works - 4: New PVC Conduit – 3 to 10 CAT6/6A Cables: Fixing suitable PVC conduit of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 500 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.3.1	Running per meter	New PVC Conduit – 3 to 10 CAT6/6A Cables: Fixing suitable PVC conduit of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	
7.4	Works - 5: New PVC Conduit – More than 10 CAT6/6A Cables: Fixing suitable PVC conduit(s) of appropriate size and quantity		

	for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.4.1	Running per meter	New PVC Conduit – More than 10 CAT6/6A Cables: Fixing suitable PVC conduit(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	
7.5	Works - 6: New PVC Trunking/Channel – Up to 2 CAT6/6A Cables: Fixing suitable PVC trunking/channel with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.5.1	Running per meter	New PVC Trunking/Channel – Up to 2 CAT6/6A Cables: Fixing suitable PVC trunking/channel with all necessary accessories for laying and routing up to 2 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	
7.6	Works - 7: New PVC Trunking/Channel – 3 to 10 CAT6/6A Cables: Providing and fixing suitable PVC trunking/channel of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.6.1	Running per meter	New PVC Trunking/Channel – 3 to 10 CAT6/6A Cables: Providing and fixing suitable PVC trunking/channel of appropriate size for laying and routing 3 to 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	

7.7	Works - 8: New PVC Trunking/Channel – More than 10 CAT6/6A Cables: Fixing suitable PVC trunking/channel(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.7.1	Running per meter	New PVC Trunking/Channel – More than 10 CAT6/6A Cables: Fixing suitable PVC trunking/channel(s) of appropriate size and quantity for laying and routing more than 10 CAT6/6A cables, including cable pulling, routing, dressing, termination, testing, labeling, and commissioning.	
7.8	PVC Conduit 20MM: New 20 mm Heavy-Duty PVC Conduit: Fixing 20 mm HD PVC conduit with all accessories for laying and routing up to 2 CAT6/6A cables (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.8.1	Running per meter	Supply and installation of 20 mm Heavy-Duty PVC Conduit, rigid, high-impact and flame-retardant type, suitable for routing and protection of OFC/network/data cables. The conduit shall be manufactured from high-quality PVC, corrosion-resistant, moisture-resistant and suitable for concealed, surface or ceiling installation. All accessories such as screws, cable tie, clips, etc. must be including for laying this conduit. (preferably white color)	
7.9	PVC Conduit 25MM: New 25 mm Heavy-Duty PVC Conduit: Fixing 25 mm HD PVC conduit with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.9.1	Running per meter	Supply and installation of 25 mm Heavy-Duty PVC Conduit, rigid, high-impact and flame-retardant type, suitable for routing and protection of OFC/network/data cables. The conduit shall be manufactured from high-quality PVC, corrosion-resistant, moisture-resistant and suitable for concealed, surface or ceiling installation. All accessories such as screws, cable tie, clips, etc. must be including for laying this conduit. (preferably white	

		color)	
7.10	PVC Conduit 32MM: New 32 mm (Minimum) Heavy-Duty PVC Conduit: Fixing 32 mm HD PVC conduit (increasing to 40 mm or multiple conduits, as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.10.1	Running per meter	Supply and installation of 32 mm Heavy-Duty PVC Conduit, rigid, high-impact and flame-retardant type, suitable for routing and protection of OFC/network/data cables. The conduit shall be manufactured from high-quality PVC, corrosion-resistant, moisture-resistant and suitable for concealed, surface or ceiling installation. All accessories such as screws, cable tie, clips, etc. must be including for laying this conduit. (preferably white color)	
7.11	PVC Trunking/Channel 25 mm x16 mm: New 25 × 16 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing up to 2 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.11.1	Running per meter	Supply and installation of 25 × 16 mm PVC Trunking/Channel, made of high-quality rigid PVC, suitable for routing and protection of OFC, network, data and low-voltage cables. The trunking shall be flame-retardant, impact-resistant, corrosion-resistant and moisture-resistant, with a smooth internal surface and removable snap-fit cover for easy cable installation and maintenance. (preferably white color)	
7.12	PVC Trunking/Channel 40 mm x 25 mm: New 40 × 25 mm PVC Trunking/Channel: Fixing PVC trunking/channel with all accessories for laying and routing 3 to 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance

			Yes / No
7.12.1	Running per meter	Supply and installation of 40 × 25 mm PVC Trunking/Channel, made of high-quality rigid PVC, suitable for routing and protection of OFC, network, data and low-voltage cables. The trunking shall be flame-retardant, impact-resistant, corrosion-resistant and moisture-resistant, with a smooth internal surface and removable snap-fit cover for easy cable installation and maintenance. (preferably white color)	
7.13	PVC Trunking/Channel 60 mm x 40 mm: New 60 × 40 mm (Minimum) PVC Trunking/Channel: Fixing PVC trunking/channel (increasing to larger sizes as required) for laying and routing more than 10 CAT6/6A cables, including pulling, routing, dressing, termination, testing, labeling, and commissioning. (Quantity: 100 RM)		
Sln	Parameters	Specifications	Compliance Yes / No
7.13.1	Running per meter	Supply and installation of 60 × 40 mm PVC Trunking/Channel, made of high-quality rigid PVC, suitable for routing and protection of OFC, network, data and low-voltage cables. The trunking shall be flame-retardant, impact-resistant, corrosion-resistant and moisture-resistant, with a smooth internal surface and removable snap-fit cover for easy cable installation and maintenance. (preferably white color)	
7.14	Ferrule type - 1: Appropriate Ferrule for labelling Cat6 cable (100 x 10 Pieces) Each packet (Quantity: 100 Packet)		
Sln	Parameters	Specifications	Compliance Yes / No
7.14.1	Provide appropriate CAT6 ferrules with various numbering options to enable clear and complete cable labeling in a single line of Cat6 Cable.		
7.15	Ferrule type - 2: Appropriate Ferrule for labelling Cat6A cable (100 x 10 Pieces) Each packet (Quantity: 100 Packet)		
Sln	Parameters	Specifications	Compliance Yes / No
7.15.1	Provide appropriate CAT6A ferrules with various numbering options to enable clear and complete cable labeling in a single line of Cat6A Cable.		

7.16	CAT6 IO Jacks: CAT6 IO jacks (RJ45 I/O modules) (Quantity: 500 Number)		
Sln	Parameters	Specifications	Compliance Yes / No
7.16.1	Type	Should be confirmed to Category-6 as per ISO/IEC 11801: 2002 Class EA and ANSI/TIA-568.2-D	
7.16.2	Bandwidth support	Should be support network line speeds up to 1 Gbps	
7.16.3	POE	Suitable for PoE applications: IEEE 802.3bt from Type 1 to Type 4,	
7.16.4	Pattern support	Dual color-coding allows for 568 A/B wiring	
7.16.5	Compatibility	RJ-11 compatible	
7.16.6	Dust Proof	Jack (I/O) should have protection from dust and contaminants.	
7.16.7	RJ45 I/O Compatibility	Individual Compatible RJ45 Jack & Pointed IDC Tower on RJ45 Jack for easy termination	
7.16.8	Plastic Housing:	Thermoplastic UL94V-0 rated or equivalent	
7.16.9	Operating Life:	Minimum 750 insertion cycles	
7.16.10	Contact Material:	Copper Alloy	
7.16.11	Contact Plating:	50µ" Gold/100µ" Nickel	
7.16.12	Plug Retention Force:	11 lbf minimum	
7.16.13	Operating Life:	Minimum 20 re-terminations	
7.16.14	Wire Accommodation:	22-24 AWG solid	
7.16.15	Interface Resistance:	20 milliohms	
7.16.16	Insulation Resistance:	>100 Megaohms	
7.16.17	Approval	ROHS Complied	
7.16.18	Certification	Should be covered by UL/ETL certification.	
7.17	CAT6 Face Plates: CAT6 Face Plate (Single Port) (Quantity: 500 Number)		
Sln	Specifications		Compliance

			Yes / No
7.17.1	Single Gang square plate, 86mmx86mm,		
7.17.2	Write on labels in transparent plastic window – supplied with plate		
7.17.3	Screw hole covers – to be supplied with plate, Plug in Icons – Icon tree – to be supplied with plate		
7.17.4	Should be able to support variety of jacks – – Unshielded & Shielded		
7.17.5	Shall be RoHS Compliant		
7.18	CAT6 Mounting Box: Mounting Box / Backbox for Face Plate (Quantity: 500 Number)		
Sln	Specifications		Compliance Yes / No
7.18.1	Mounting Box of the same OEM if manufactured by OEM or equivalent good brand (Anchor & Havells or Equivalent Manufacture) if not manufactured by OEM or sample may be approved by Customer before Delivery.		
7.18.2	Size	3 X 3	
7.19	CAT6A IO Jacks: CAT6A IO jacks (RJ45 I/O modules) (Quantity: 100 Number)		
Sln	Specifications		Compliance Yes / No
7.19.1	Should be conform to Category-6A as per ANSI/TIA-568.2-D & ISO 11801		
7.19.2	Should be support network line speeds up to 10 Gbps		
7.19.3	Jack (I/O) Should support POE i. e IEEE 802.3bt from Type 1 to Type 4,		
7.19.4	Jack (I/O) operating Life should be minimum 750 insertion cycles and contact material should be copper alloy.		
7.19.5	Jack (I/O) contact plating should be 50µ Gold/ 50µ Nickel minimum		
7.19.6	Jack (I/O) must have protection from dust and contaminants.		
7.19.7	All information outlets for 22-24 AWG copper cable should be used insulation displacement connectors (IDC)		
7.19.8	Operating Life should Minimum 20 re-terminations.		
7.19.9	Interface Resistance: 20mΩ (milli Ohms)		
7.19.10	Insulation Resistance: >100MΩ (Mega Ohms)		

7.19.11	I/O should be terminated using industry standard punch-down tools.		
7.19.12	Should be RoHS Compliant		
7.19.13	Should be certified by ETL/UL		
7.20	CAT6A Face Plates: CAT6A Face Plate (Single Port) (Quantity: 100 Number)		
Sln	Specifications		Compliance Yes / No
7.20.1	Single square plate, 86x86mm,		
7.20.2	Write on labels in transparent plastic window – supplied with plate		
7.20.3	Screw hole covers – to be supplied with plate, Plug in Icons – Icon tree – to be supplied with plate		
7.20.4	Should be able to support variety of jacks – Unshielded & Shielded		
7.20.5	Shall be RoHS Compliant		

7.22	Flexi pipe - 1: to fit the size of conduit Size of 20 mm (Quantity: 100 Meter)		
Sln	Specifications		Compliance (Y/N)
7.22.1	Size	20 MM	
7.22.2	Color	White or any other compatible color as per the conduit	
7.23	Flexi pipe - 2: to fit the size of conduit Size of 25 mm (Quantity: 100 Meter)		
Sln	Specifications		Compliance (Y/N)
7.23.1	Size	25 MM	
7.23.2	Color	White or any other compatible color as per the conduit	
7.24	Flexi pipe - 3: to fit the size of conduit Size of 32 mm (Quantity: 100 Meter)		

Sln	Specifications		Compliance (Y/N)
7.24.1	Size	32 MM	
7.24.2	Color	White or any other compatible color as per the conduit	
7.25	T-Joints - 1: to fit the size of conduit Size of 20 mm (Quantity: 250 Number)		
Sln	Specifications		Compliance (Y/N)
7.25.1	Size	20 MM	
7.25.2	Color	White or any other compatible color as per the conduit	
7.26	T-Joints - 2: to fit the size of conduit Size of 25 mm (Quantity: 100 Number)		
Sln	Specifications		Compliance (Y/N)
7.26.1	Size	25 MM	
7.26.2	Color	White or any other colors	
7.27	T-Joints - 3: to fit the size of conduit Size of 32 mm (Quantity: 50 Number)		
Sln	Specifications		Compliance (Y/N)
7.27.1	Size	32 MM	
7.27.2	Color	White or any other compatible color as per the conduit	
7.28	L-joints - 1: to fit the size of conduit Size of 20 mm (Quantity: 250 Number)		
Sln	Specifications		Compliance (Y/N)

7.28.1	Size	20 MM	
7.28.2	Color	White or any other compatible color as per the conduit	
7.29	L-joints - 2: to fit the size of conduit Size of 25 mm (Quantity: 100 Number)		
Sln	Specifications		Compliance (Y/N)
7.29.1	Size	25 MM	
7.29.2	Color	White or any other compatible color as per the conduit	
7.30	L-joints - 3: to fit the size of conduit Size of 32 mm (Quantity: 50 Number)		
Sln	Specifications		Compliance (Y/N)
7.30.1	Size	32 MM	
7.30.2	Color	White or any other compatible color as per the conduit	

Annexure - 10

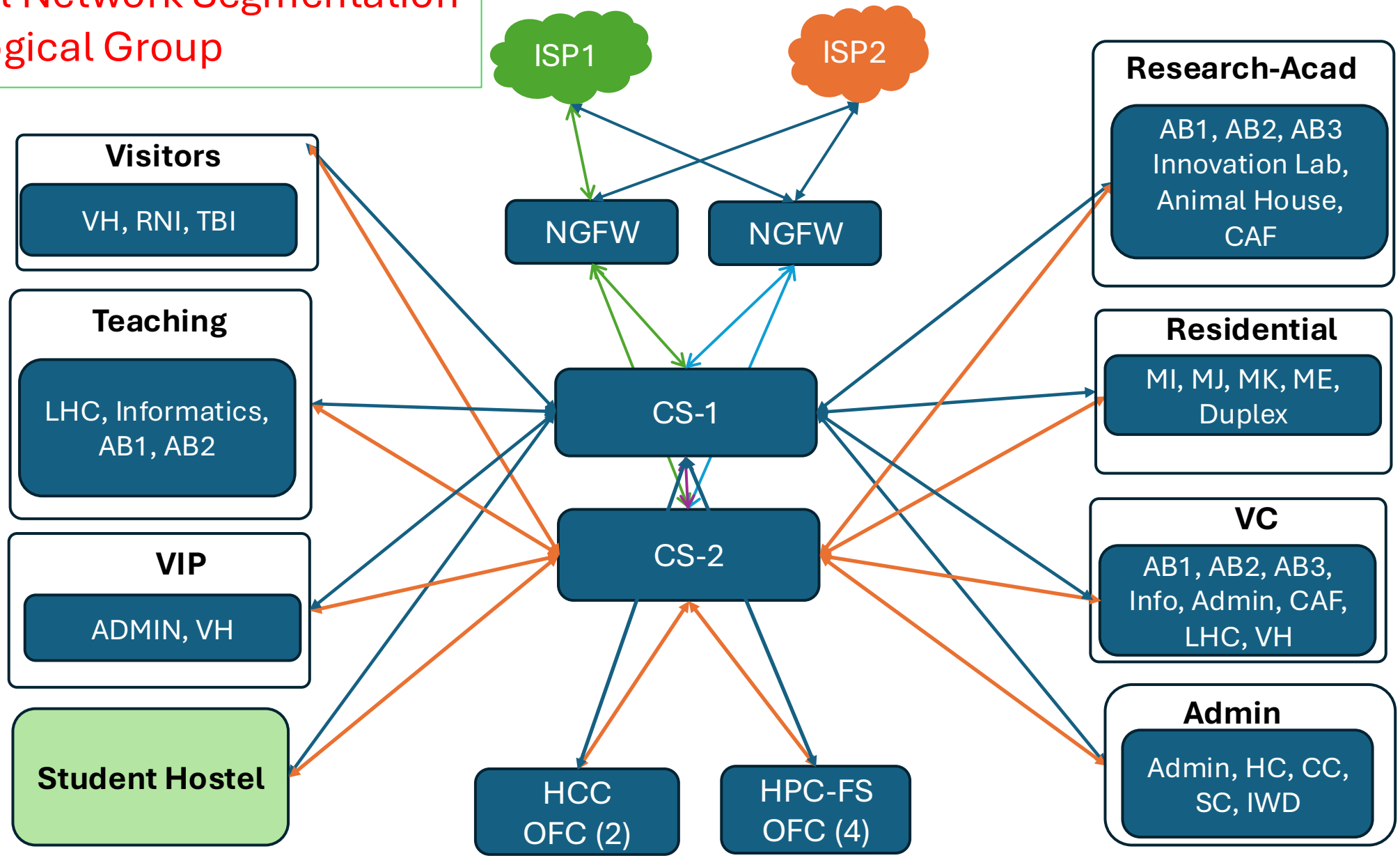
Schematics of Core network infrastructure along with LAN and OFC routing

Nomenclature

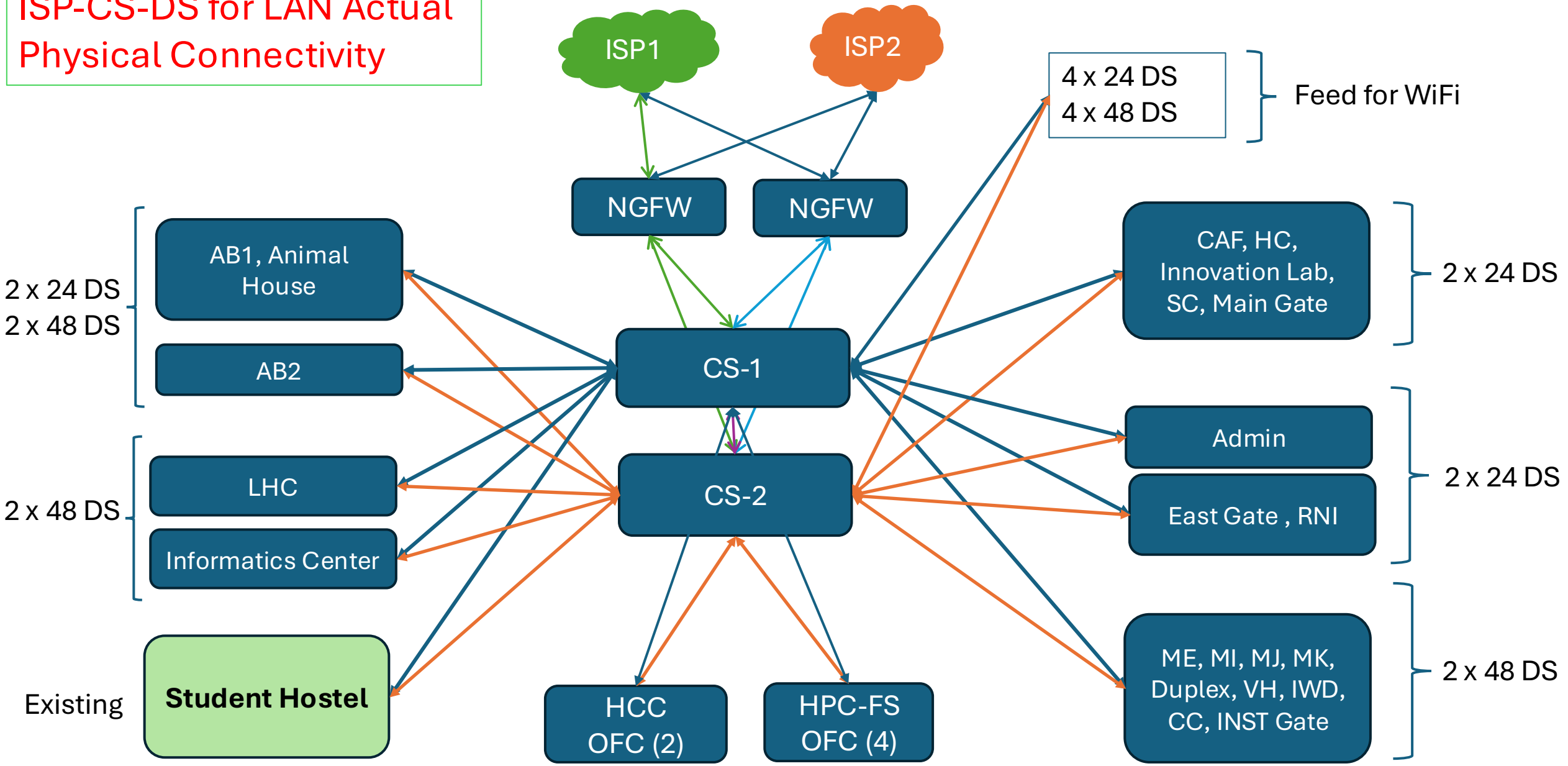
Name	Acronyms
AB1	Academic Block - 1
AB2	Academic Block - 2
CC	Community Center
LHC	Lecture Hall Complex
SC	Sports Complex
HC	Health Center
CAF	Central Analytical Facility
IWD	Institute Works Department
ME	Residential Building Name ME
MI	Residential Building Name MI
MJ	Residential Building Name MJ
MK	Residential Building Name MK
VH	Visitors Hostel
RNI	Research and Innovation Park
DC	Data Center (Informatics Center)

Name	Acronyms
AS	Access Switches
CS	Core Switch
DS	Distribution Switch
LIU	Light Interface Unit
JB	Junction Box
SFP	Small Form-Factor Pluggable
DAC	Direct Access Cable
LC	Lucent Connector
NGFW	Next Generation Firewall
OFC	Optical Fibre Cable

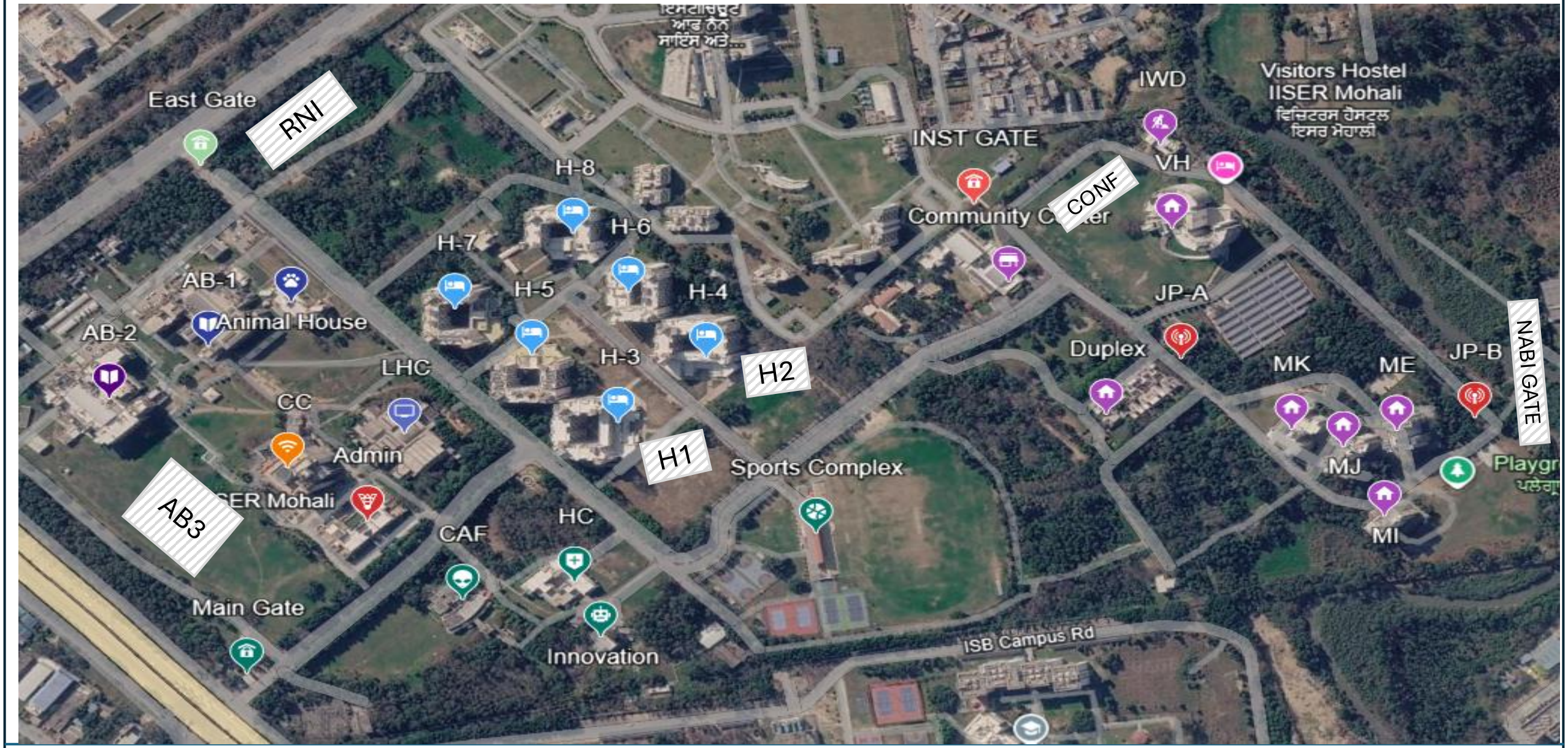
Logical Network Segmentation and Logical Group



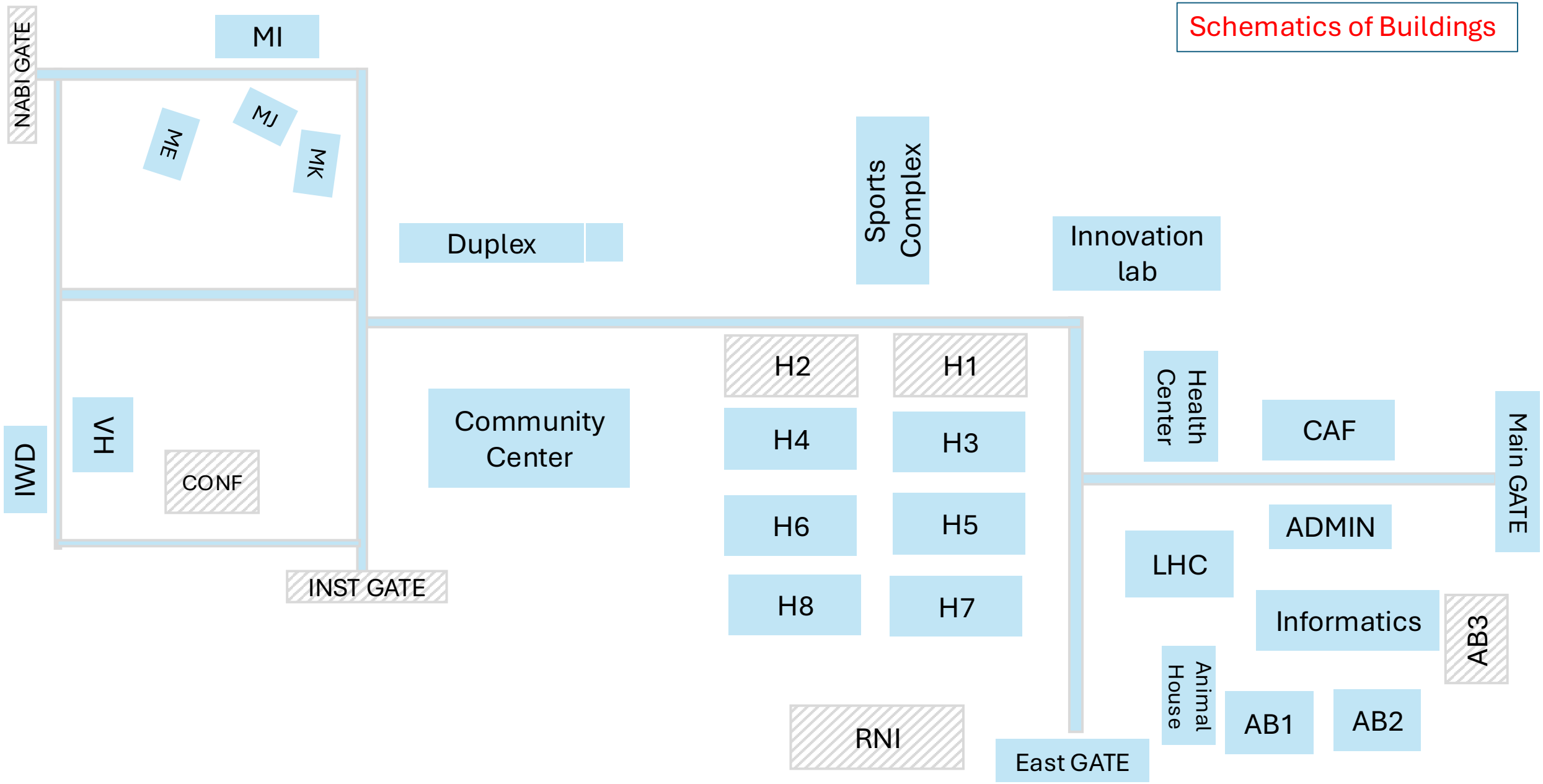
ISP-CS-DS for LAN Actual Physical Connectivity

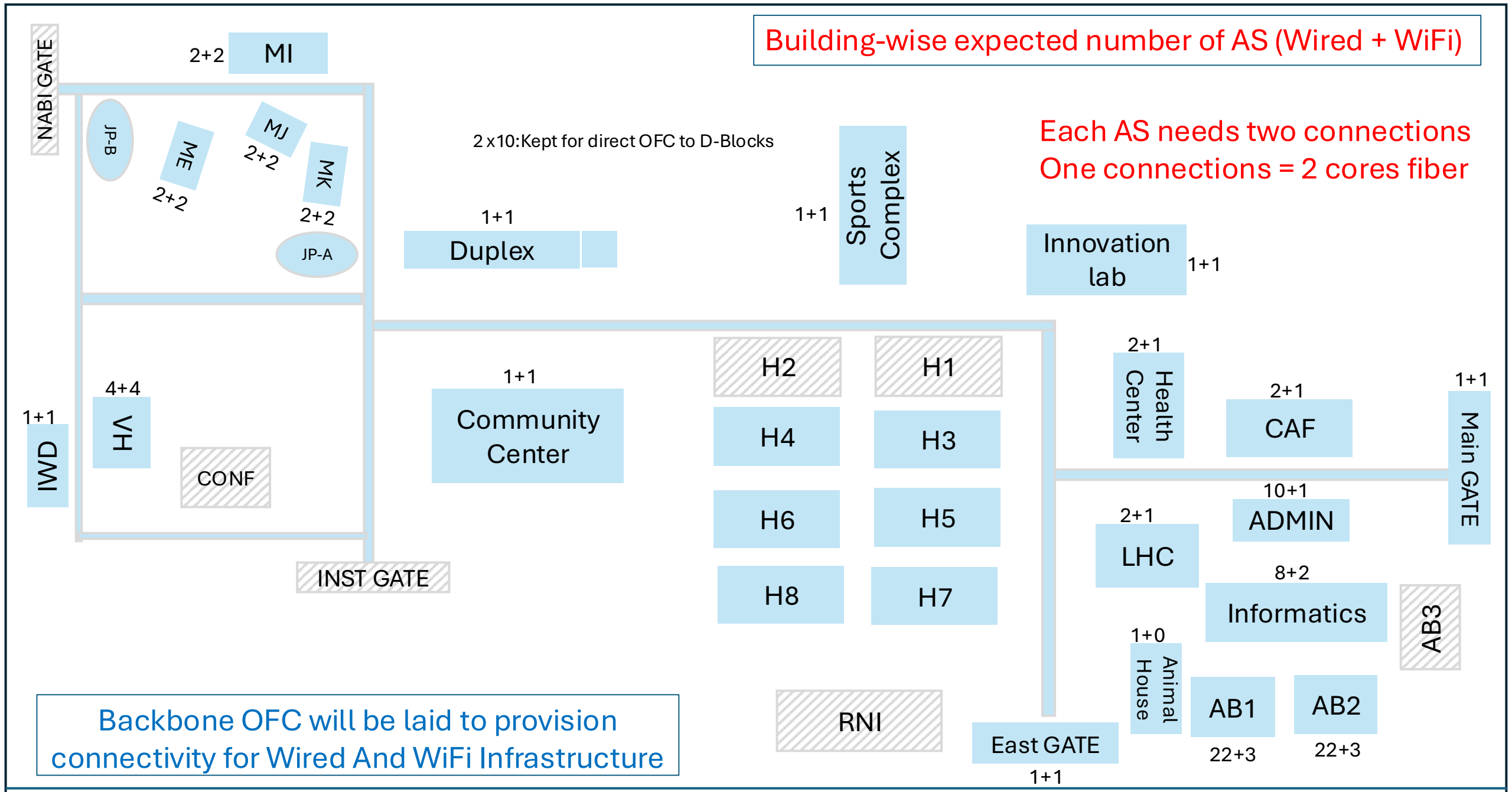


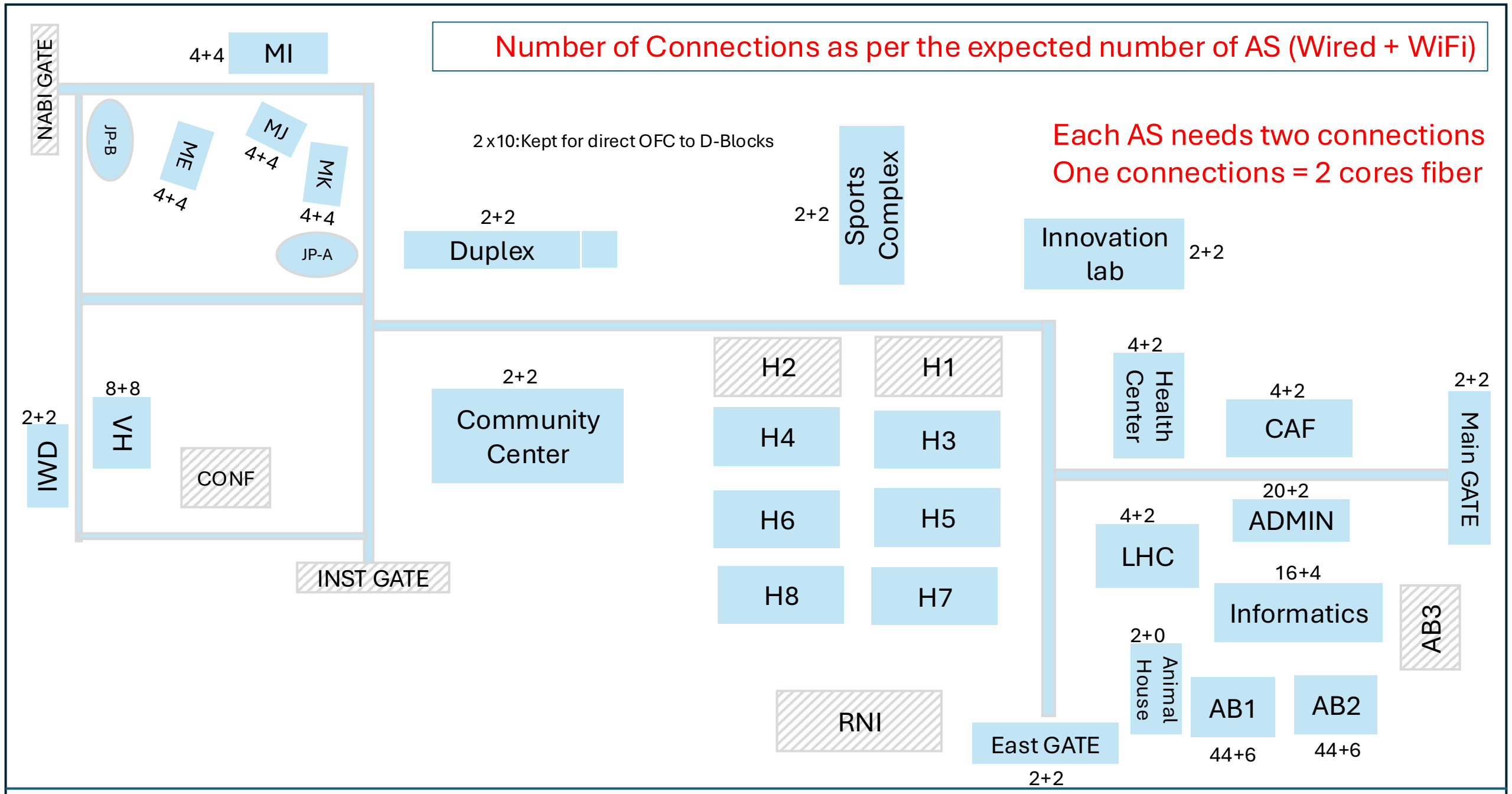
IISER Mohali Campus

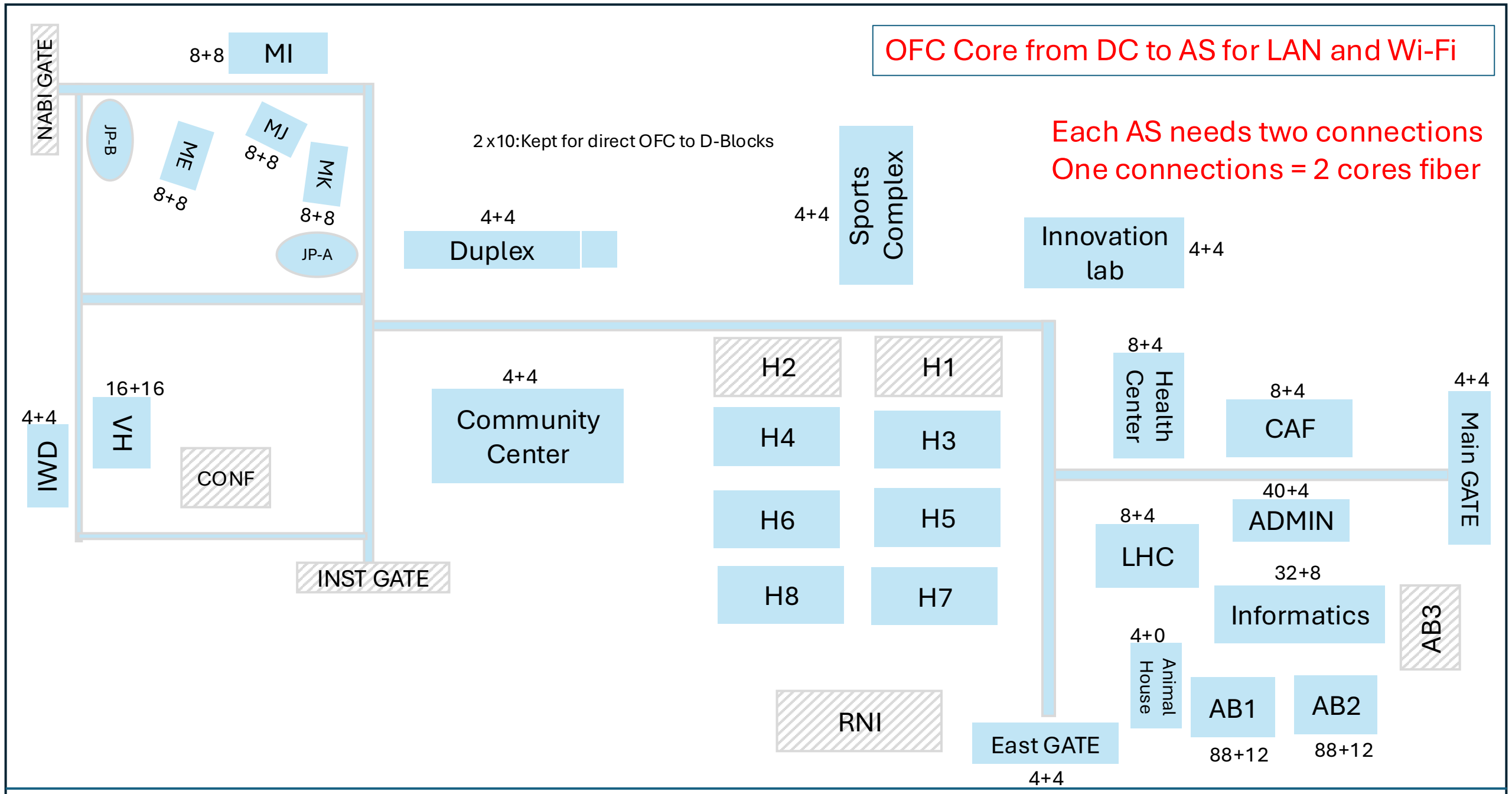


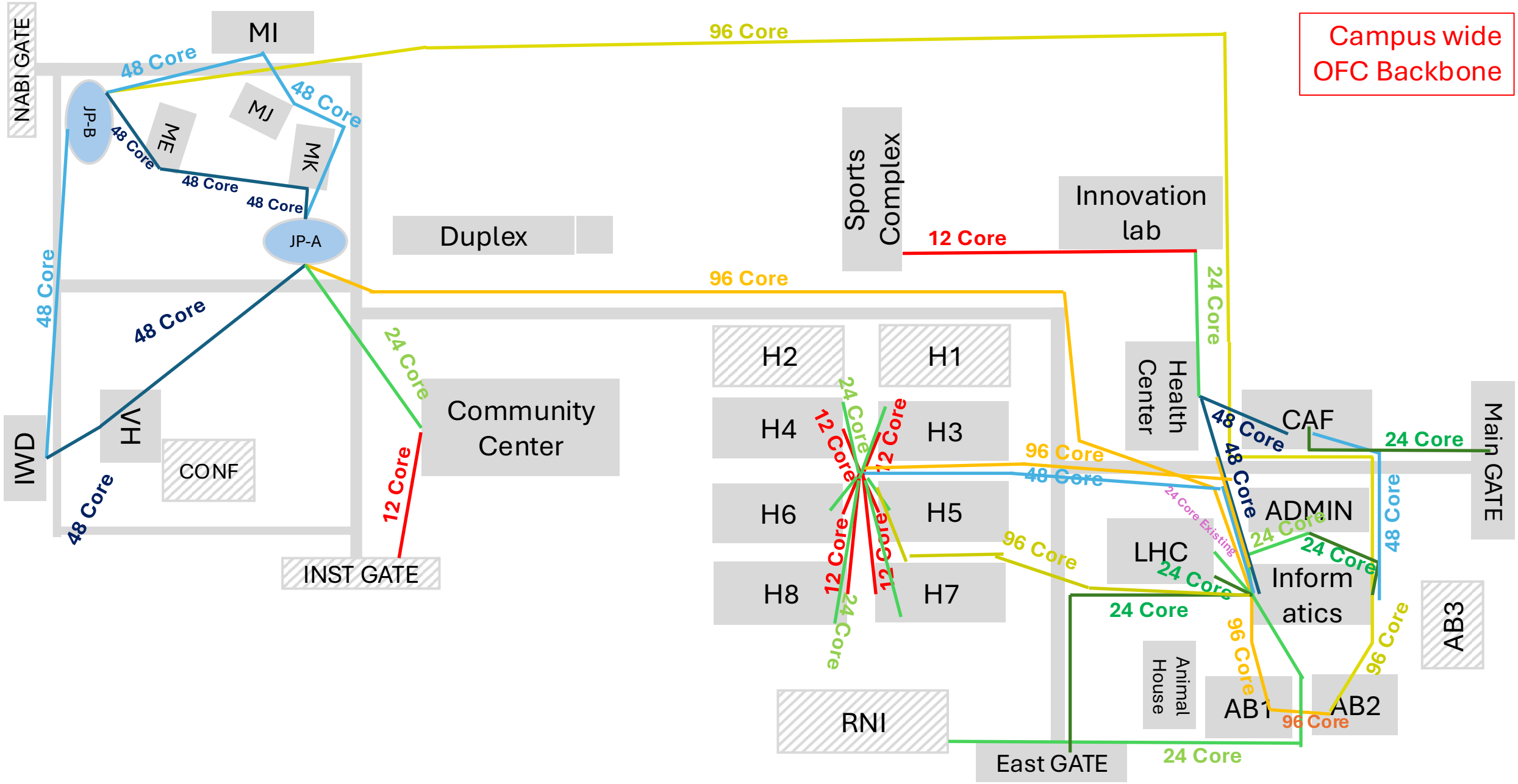
Schematics of Buildings



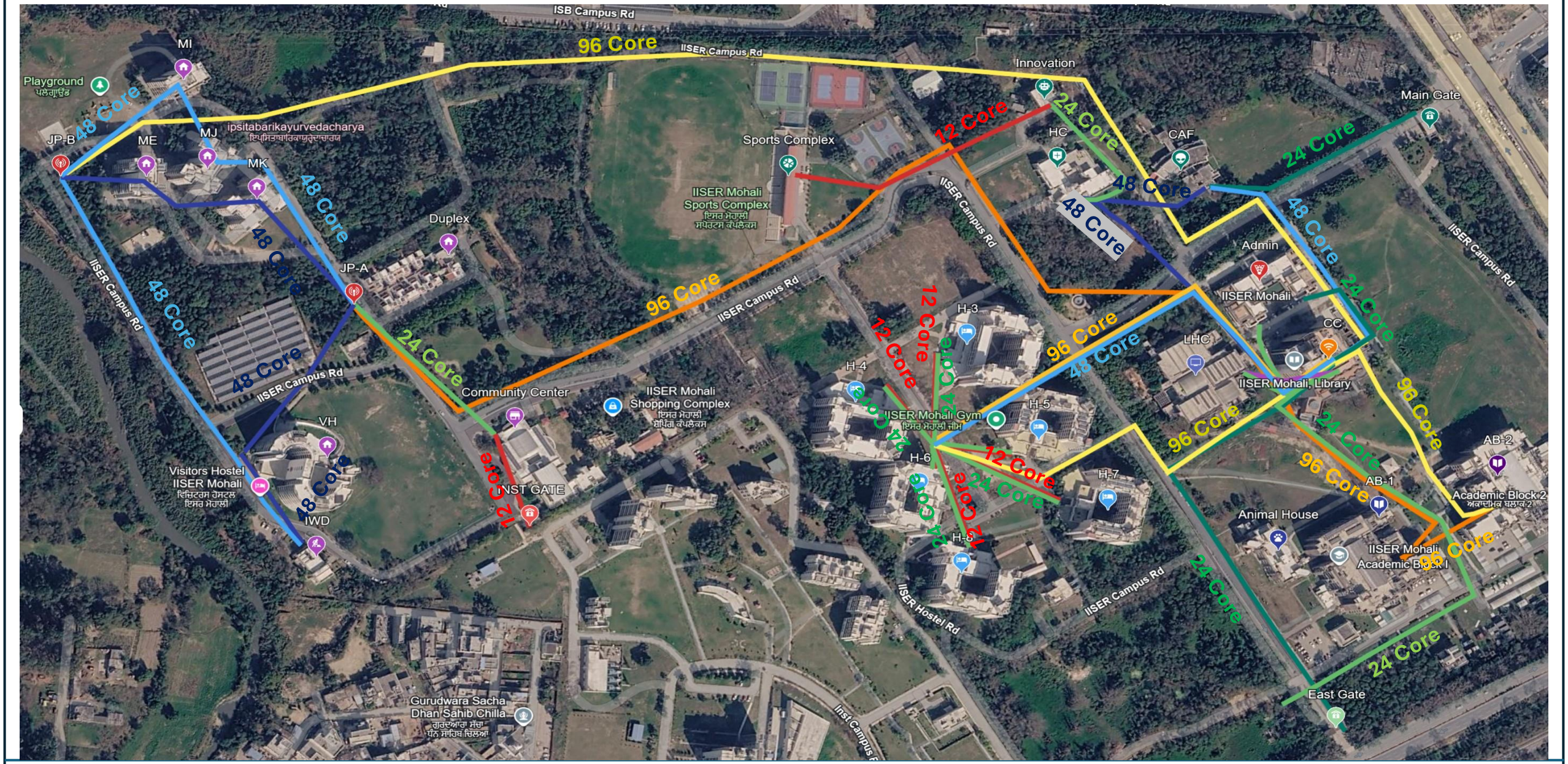

Building-wise expected number of AS (Wired + WiFi)
NABI GATE
2+2
MI
JP-B
ME
2+2
MJ
2+2
MK
2+2
JP-A
2 x10:Kept for direct OFC to D-Blocks
1+1
Duplex
1+1
Sports Complex
Each AS needs two connections
One connections = 2 cores fiber
Innovation lab
1+1
1+1
IWD
4+4
VH
CONF
1+1
Community Center
H2
H1
H4
H3
H6
H5
H8
H7
INST GATE
2+1
Health Center
2+1
CAF
1+1
Main GATE
10+1
ADMIN
2+1
LHC
8+2
Informatics
AB3
1+0
Animal House
AB1
22+3
AB2
22+3
RNI
East GATE
1+1
Backbone OFC will be laid to provision connectivity for Wired And WiFi Infrastructure


Number of Connections as per the expected number of AS (Wired + WiFi)
Each AS needs two connections
One connections = 2 cores fiber
NABI GATE
4+4
MI
JP-B
ME
4+4
MJ
4+4
MK
4+4
JP-A
2 x10:Kept for direct OFC to D-Blocks
2+2
Duplex
2+2
Sports Complex
Innovation lab
2+2
2+2
IWD
8+8
VH
CONF
INST GATE
2+2
Community Center
H2
H1
H4
H3
H6
H5
H8
H7
RNI
4+2
Health Center
4+2
CAF
2+2
Main GATE
20+2
ADMIN
4+2
LHC
16+4
Informatics
AB3
2+0
Animal House
AB1
44+6
AB2
44+6
East GATE
2+2


OFC Core from DC to AS for LAN and Wi-Fi
Each AS needs two connections
One connections = 2 cores fiber
NABI GATE
8+8
MI
JP-B
ME
8+8
MJ
8+8
MK
8+8
JP-A
2 x10:Kept for direct OFC to D-Blocks
4+4
Duplex
4+4
Sports Complex
Innovation lab
4+4
8+4
Health Center
8+4
CAF
4+4
Main GATE
16+16
VH
4+4
IWD
CONF
4+4
Community Center
H2
H1
H4
H3
H6
H5
H8
H7
INST GATE
RNI
East GATE
4+4
8+4
LHC
40+4
ADMIN
32+8
Informatics
AB3
4+0
Animal House
AB1
88+12
AB2
88+12


Campus wide
OFC Backbone
NABI GATE
MI
96 Core
48 Core
48 Core
JP-B
48 Core
ME
MJ
MK
48 Core
48 Core
JP-A
Duplex
Sports Complex
12 Core
Innovation lab
96 Core
24 Core
48 Core
48 Core
24 Core
Community Center
H2
H1
H4
H3
H6
H5
H8
H7
12 Core
12 Core
12 Core
12 Core
24 Core
24 Core
Health Center
CAF
24 Core
Main GATE
96 Core
48 Core
48 Core
24 Core Existing
ADMIN
24 Core
24 Core
48 Core
IWD
VH
CONF
48 Core
48 Core
12 Core
INST GATE
96 Core
LHC
24 Core
24 Core
Inform atics
AB3
96 Core
96 Core
Animal House
AB1
AB2
96 Core
RNI
East GATE
24 Core

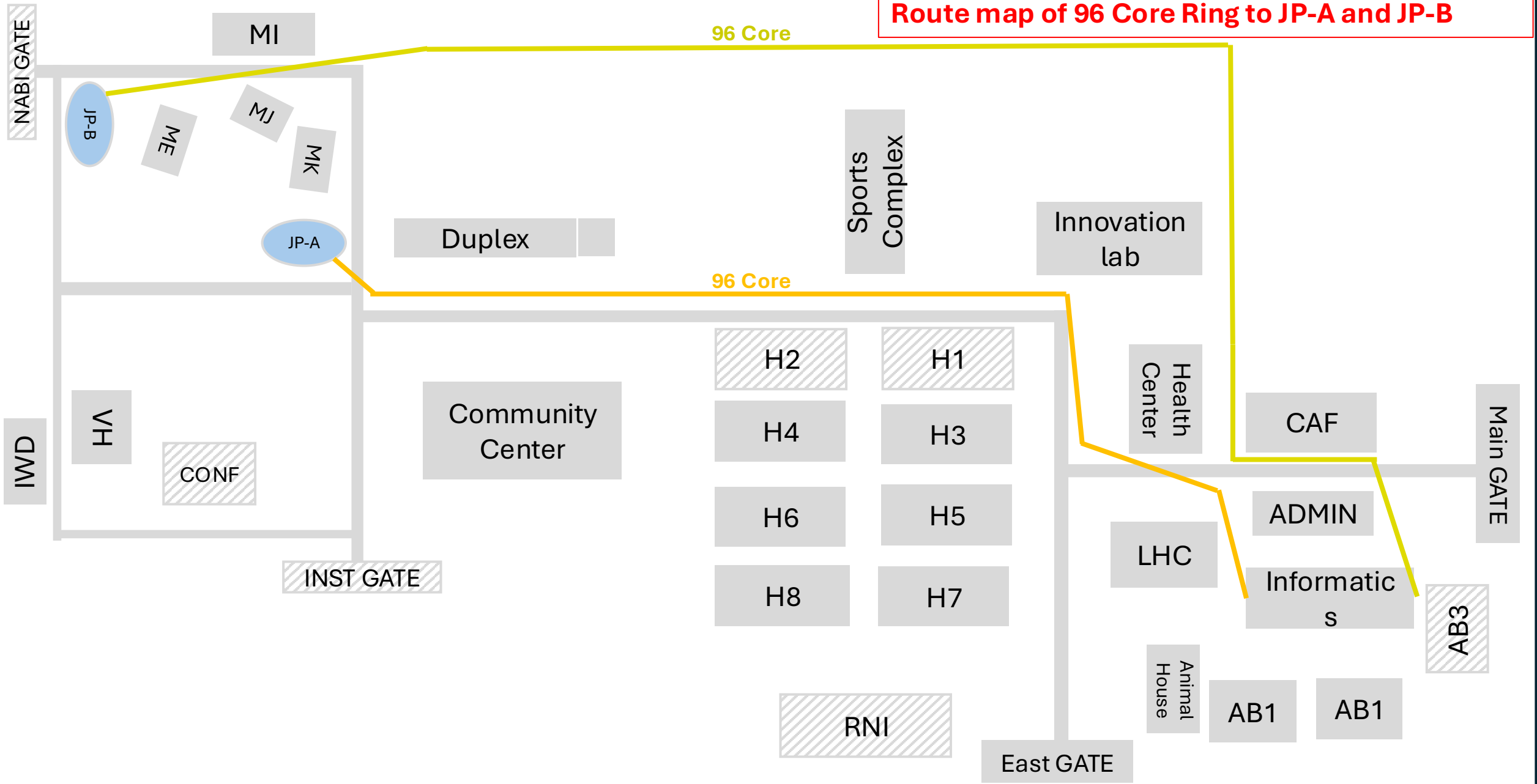
Key map of OFC route



Schematics of Residential Complex

Items	**Particulars**
Buildings	VH, IWD, Duplex, MI, ME, MJ, MK, DC
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc.)	Required for wired connections

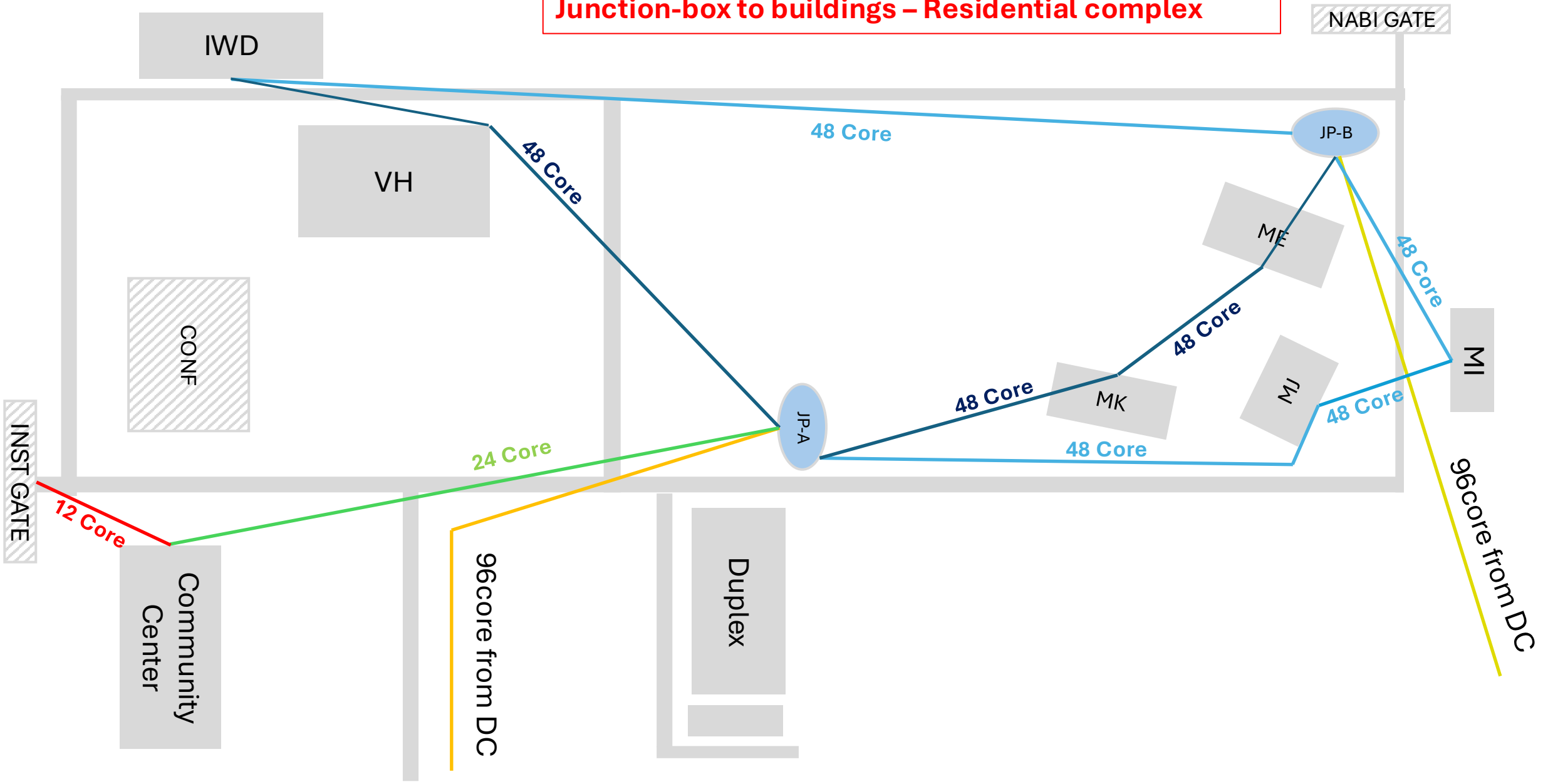
Route map of 96 Core Ring to JP-A and JP-B



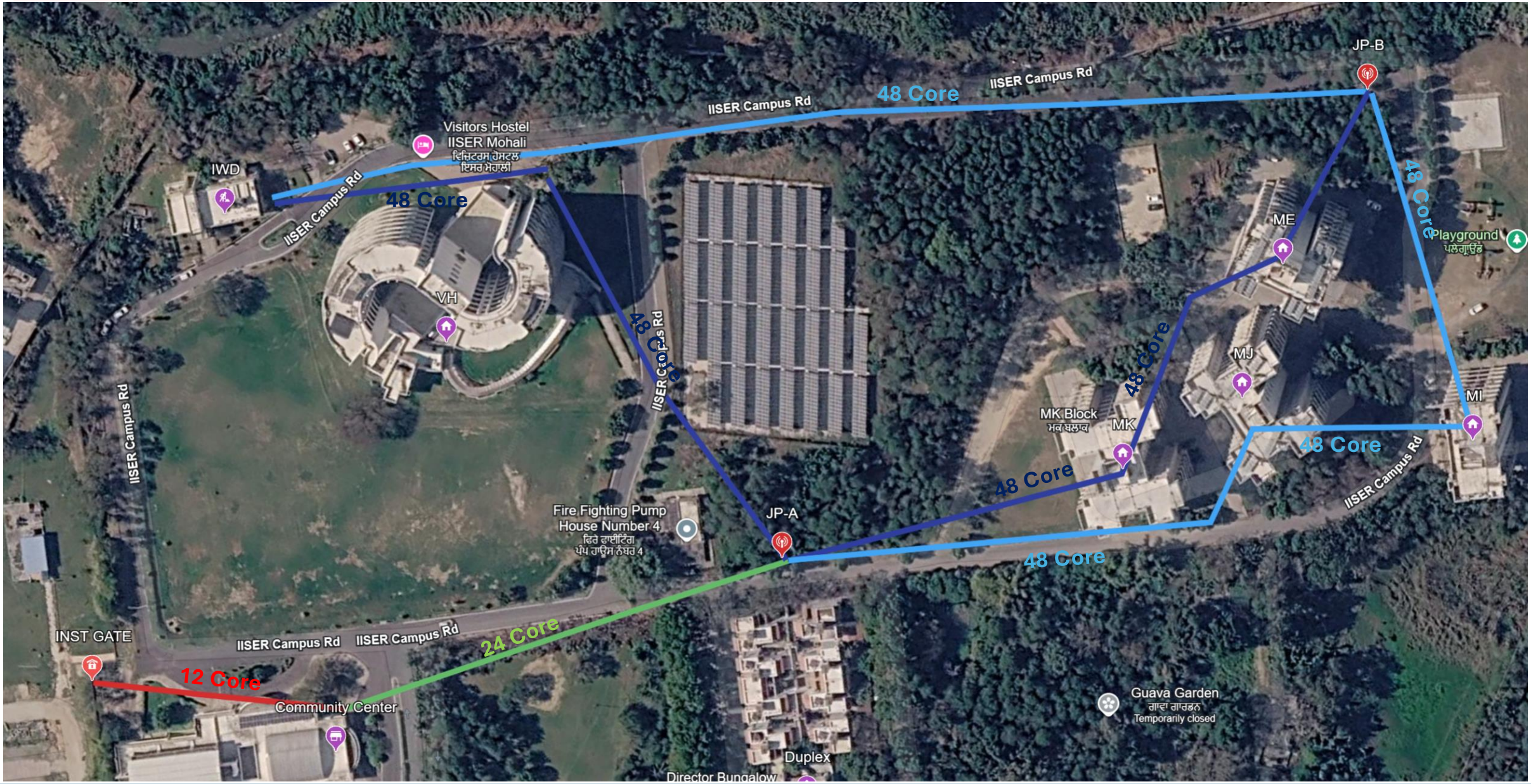
Route map of 96 Core Ring to JP-A and JP-B

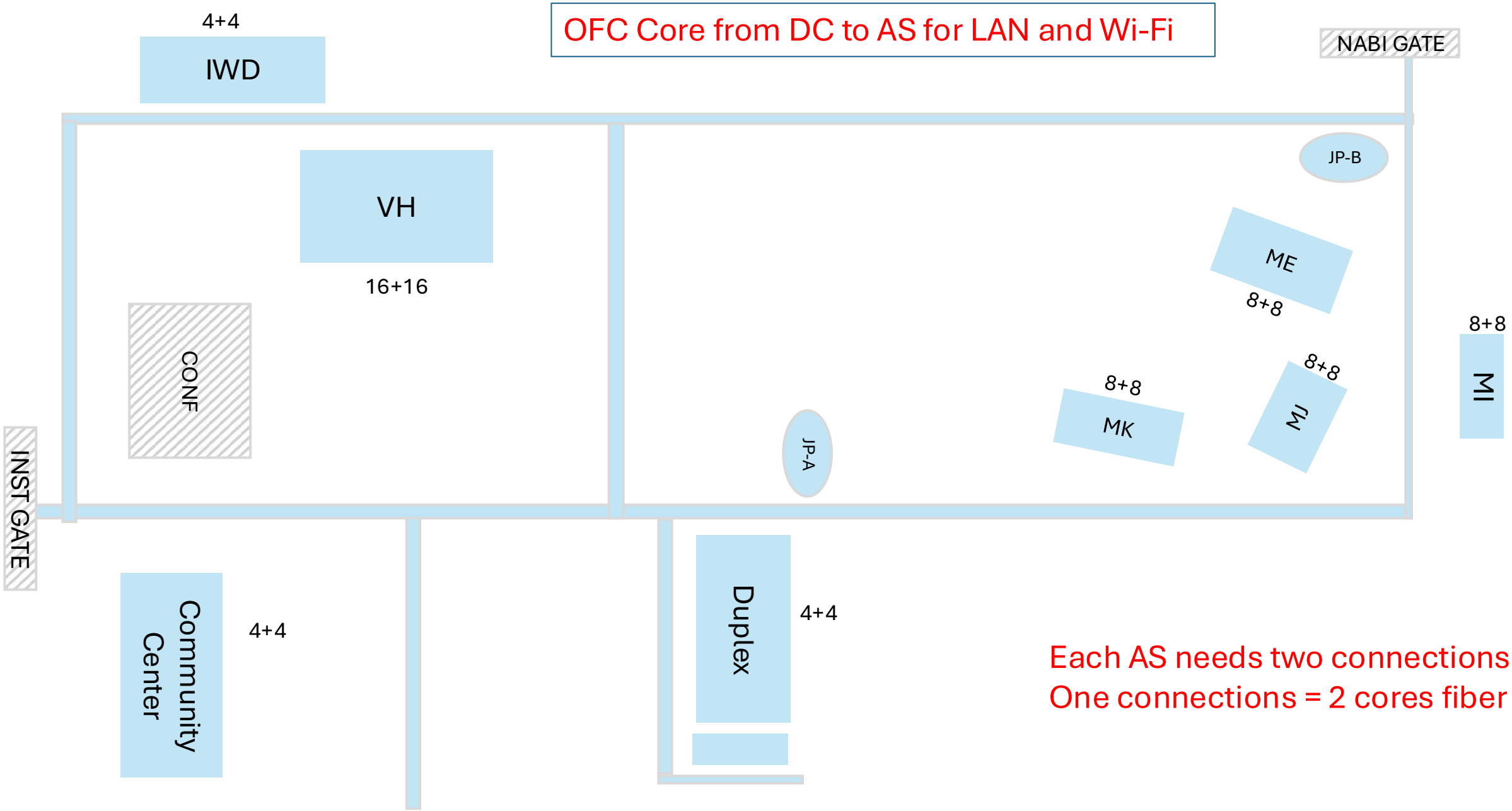


Junction-box to buildings – Residential complex

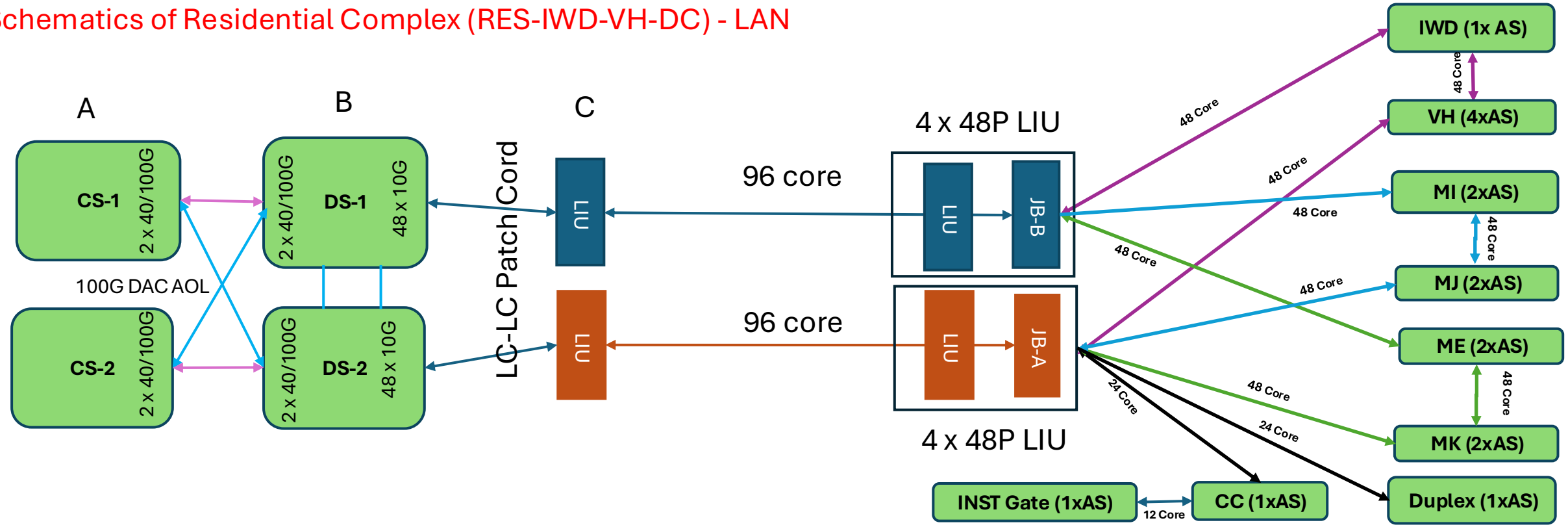


Junction-box to buildings – Residential complex




OFC Core from DC to AS for LAN and Wi-Fi
4+4
IWD
NABI GATE
VH
16+16
JP-B
ME
8+8
8+8
MI
CONF
8+8
MK
8+8
MJ
JP-A
INST GATE
Community Center
4+4
Duplex
4+4
Each AS needs two connections
One connections = 2 cores fiber

Schematics of Residential Complex (RES-IWD-VH-DC) - LAN

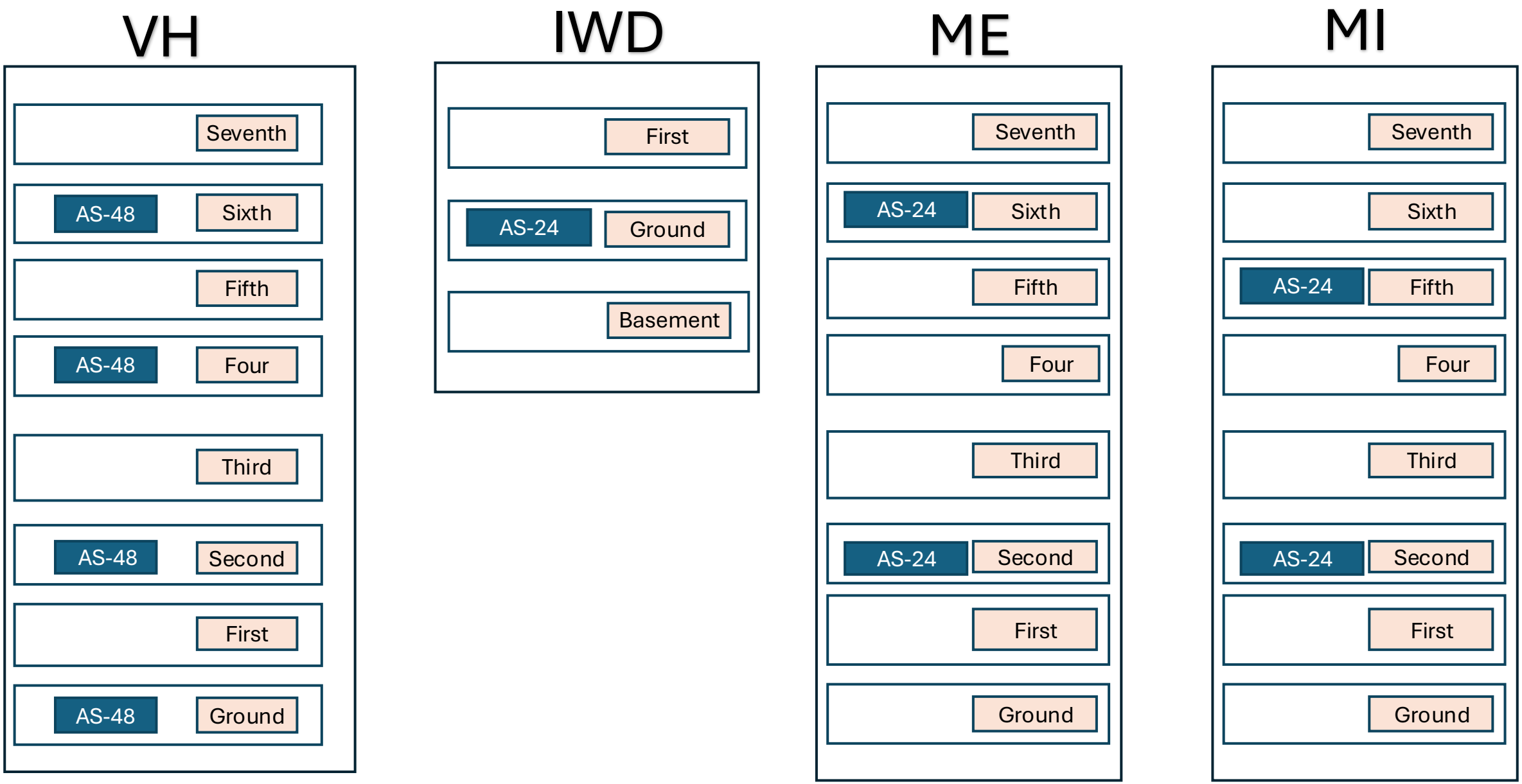


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48P)	LIU at RES JB-A + JB-B (48P) + Buildings	Core Required	Patch Cord LC-LC	SFP 10G	Connection on AS	AS
2	4	2	16 + 16	32	4	4 + 4 +12	32+32	32	16+16	16+16	16

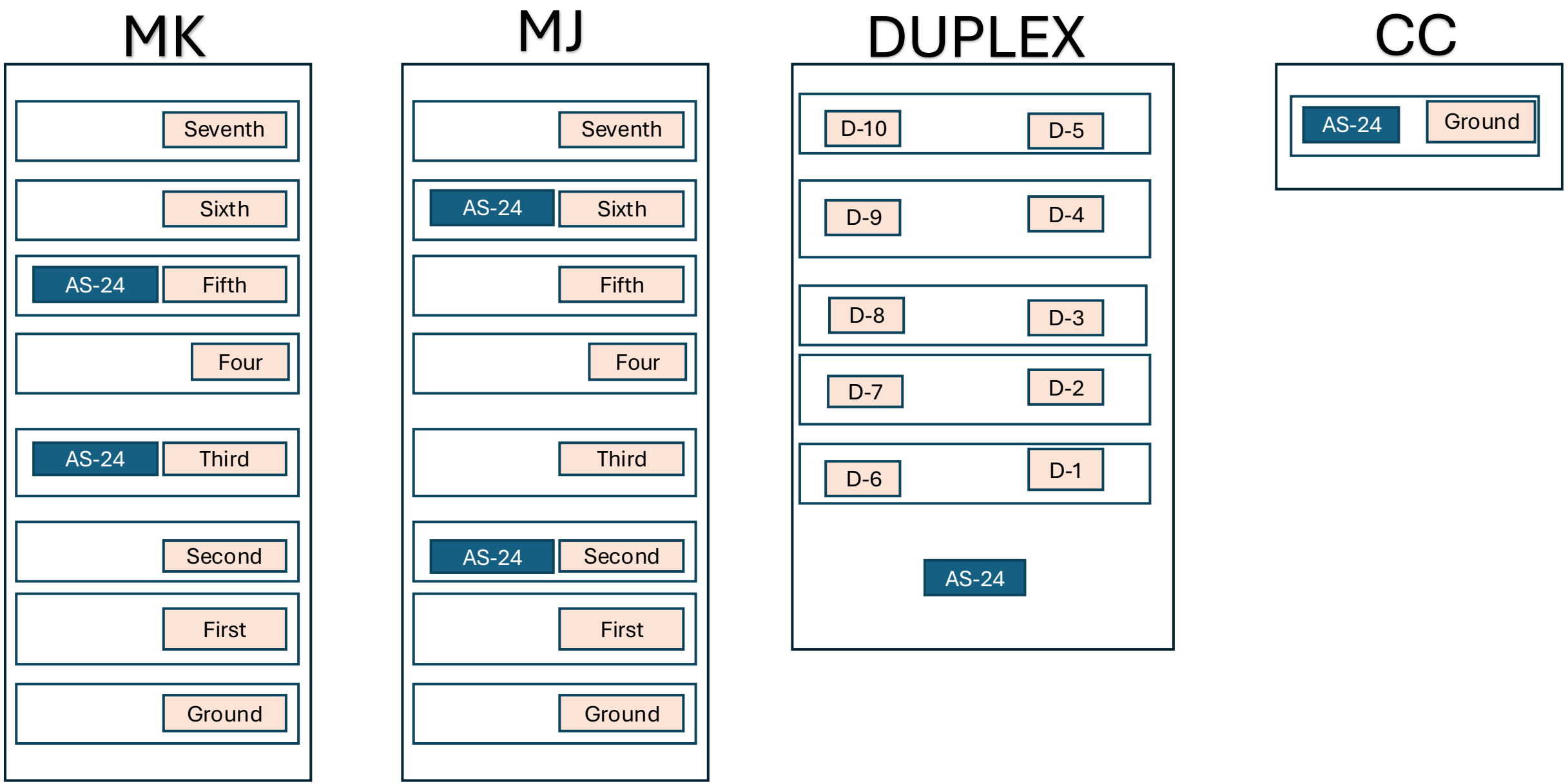
Total Core for LAN	Total Core for WiFi	Total Core for Duplex	Total Required	Cable Required	DAC Cable	Short Cable
32 + 32	32 + 32	20 + 20	84 + 84	96C + 96C	4	2

	Total 96	Total 48	Total 24 Core	Total 12 Core
Two redundant OFC	1 + 1	3 + 3 + 3	2	1
Length				

Residential Hostel Complex (RES-IWD-VH-DC) – Positioning of AS



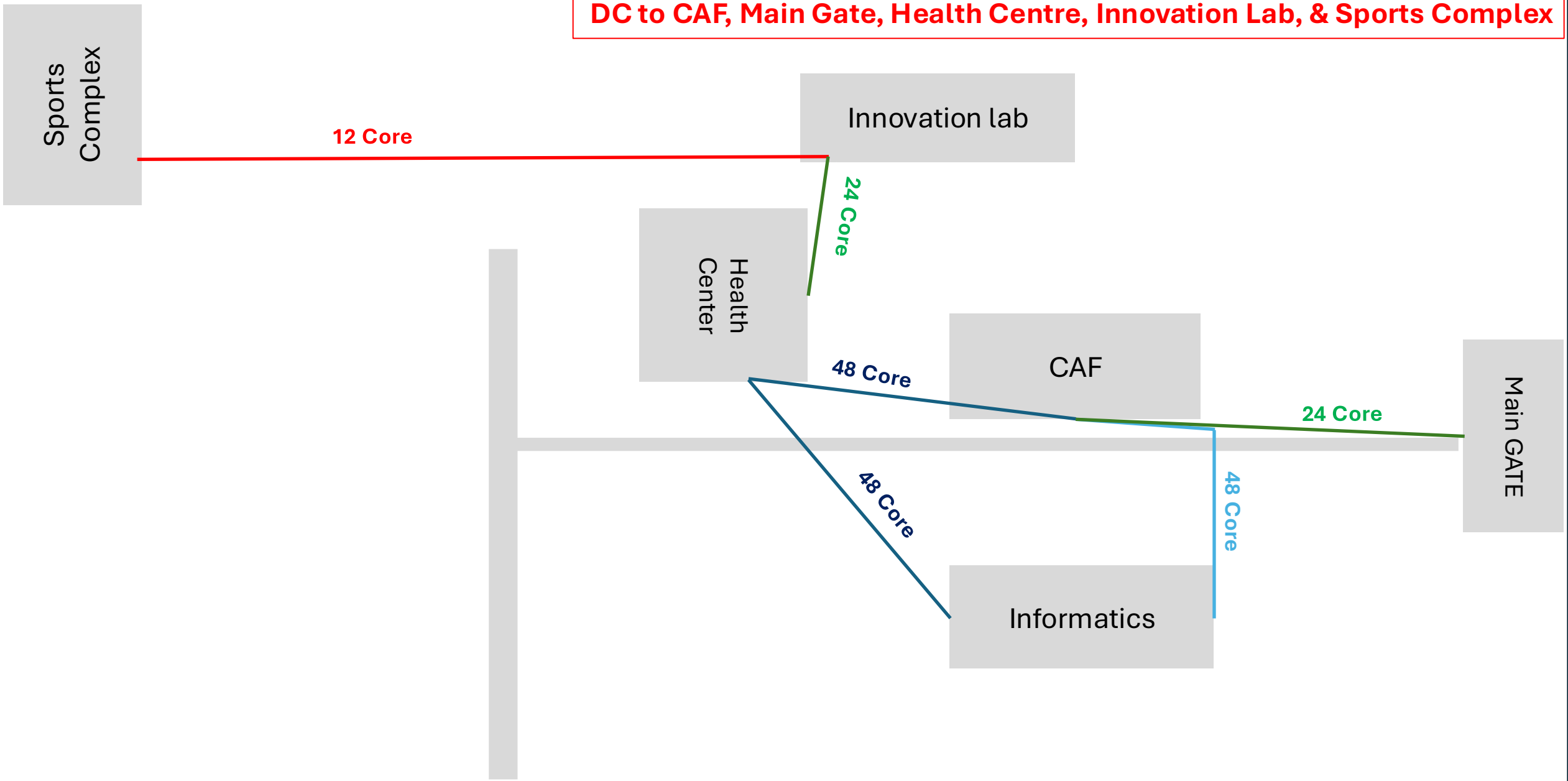
Residential Hostel Complex (RES-IWD-VH-DC) – Positioning of AS



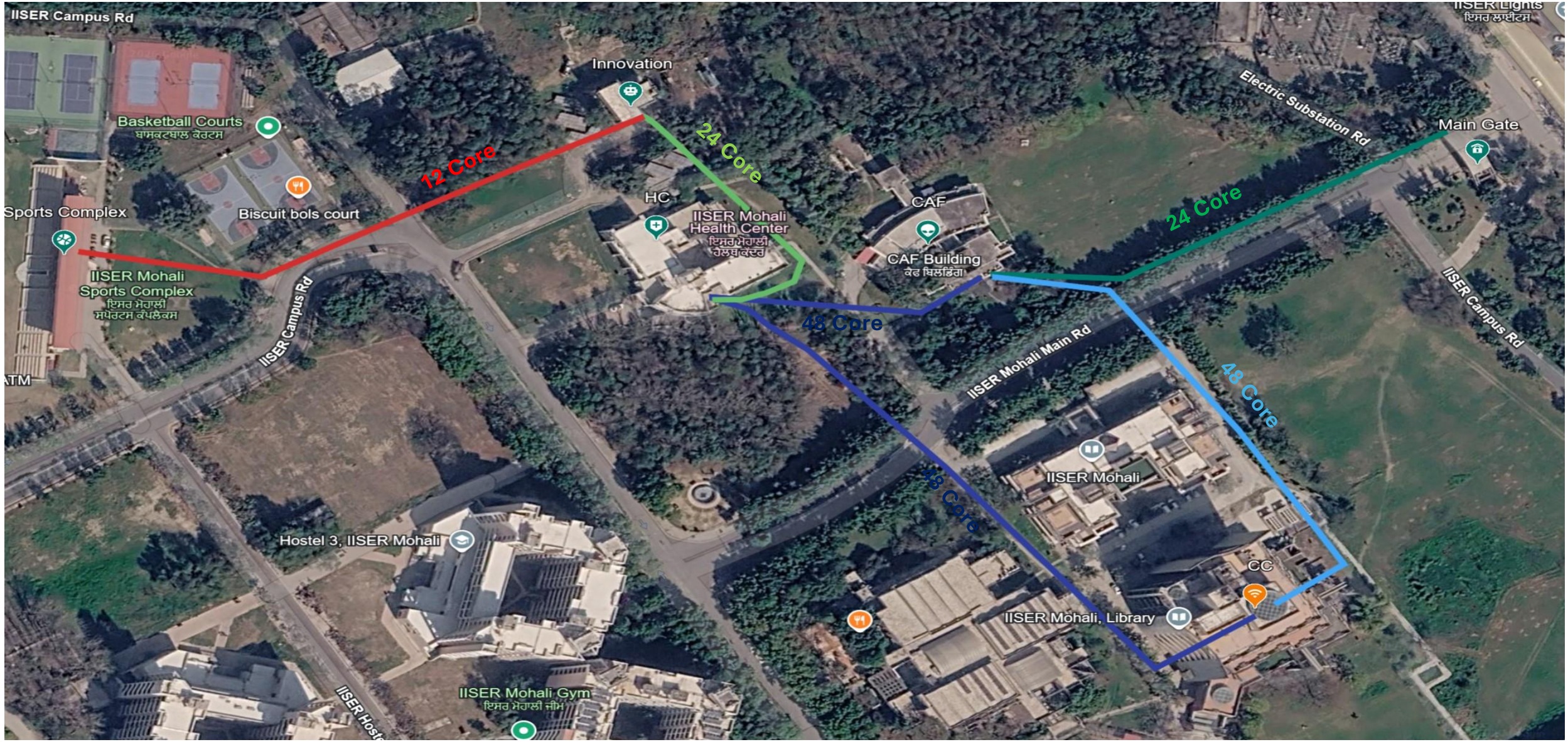
Schematics of CAF, HC, Main Gate, Innovation LAB, SC

Items	**Particulars**
Buildings	CAF, HC, Main Gate, Innovation LAB, SC
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

DC to CAF, Main Gate, Health Centre, Innovation Lab, & Sports Complex

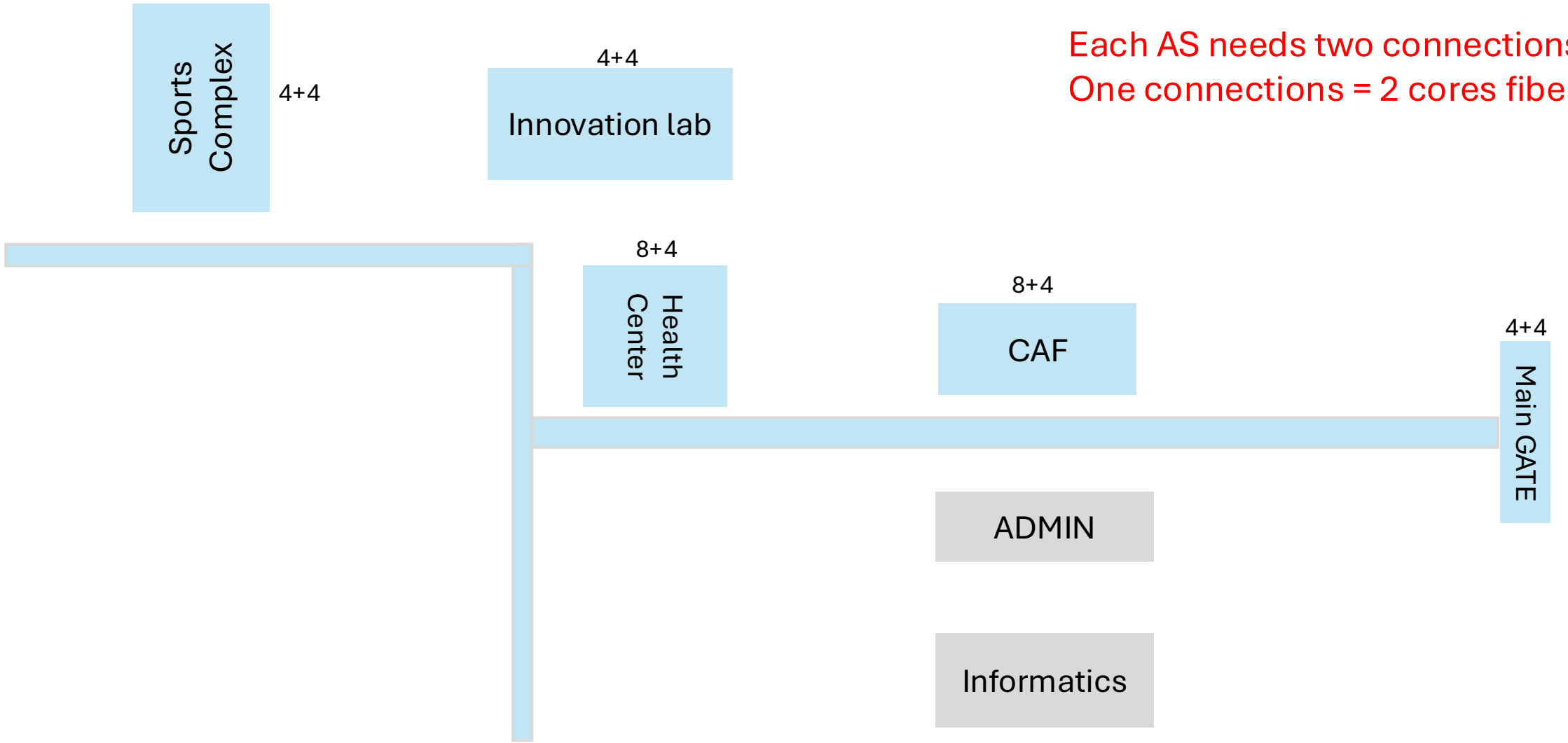


DC to CAF, Main Gate, Health Centre, Innovation Lab, & Sports Complex

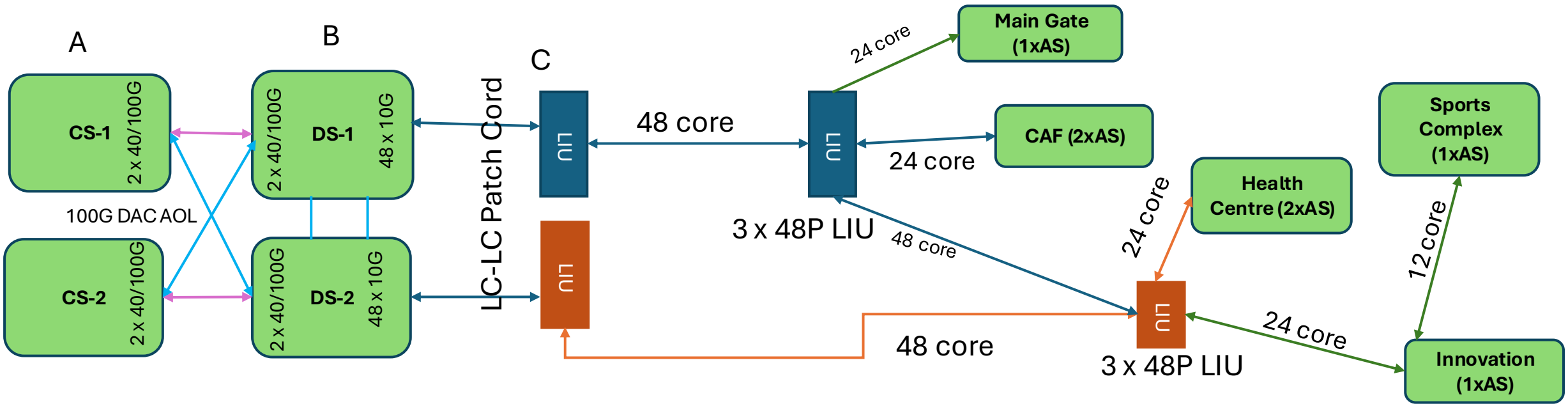


OFC Core from DC to AS for LAN and Wi-Fi

Each AS needs two connections
One connections = 2 cores fiber



CAF, HC, Main Gate, Innovation LAB, SC - LAN



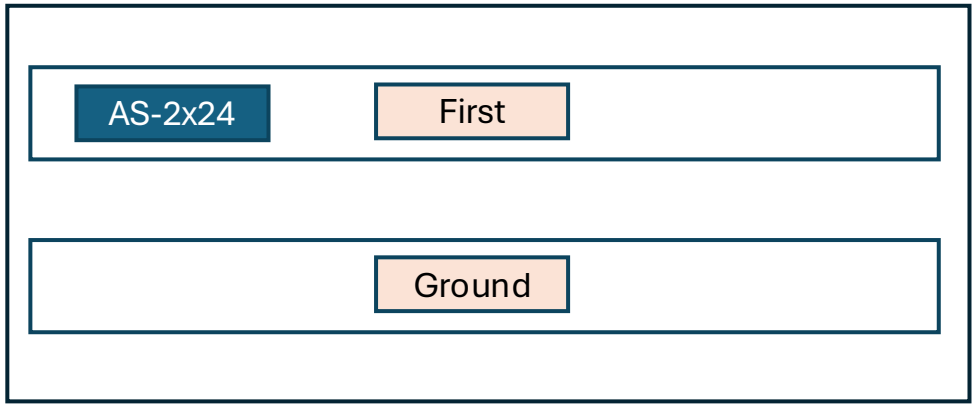
DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48P)	LIU at CAF + HC (48P)	Core Required	Patch Cord LC-LC	SFP 10G	Connection on AS	AS
2	4	2	7 + 7	14	2	3+3	14 + 14	14	7+7	7 + 7	7

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
14 + 14	10 + 10	24 + 24	24C + 24C	4	2

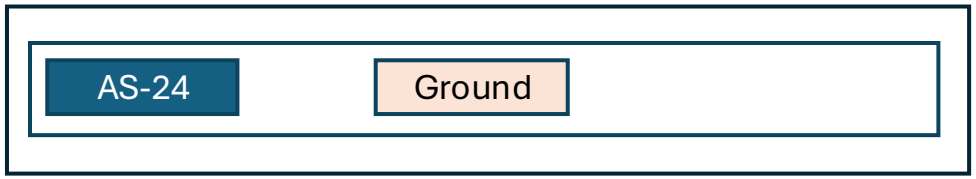
	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	0+0	1+1+1	2	1	2 x 4
Length					

CAF, HC, Main Gate, Innovation LAB, SC – Positioning of AS

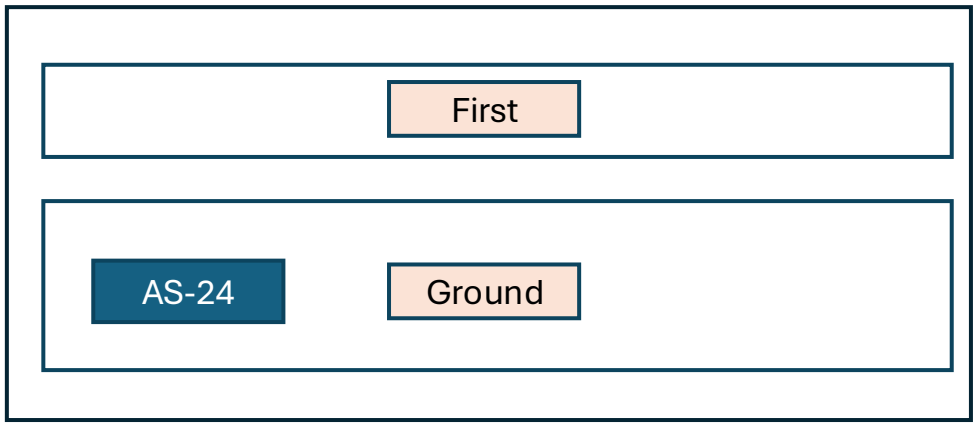
HC



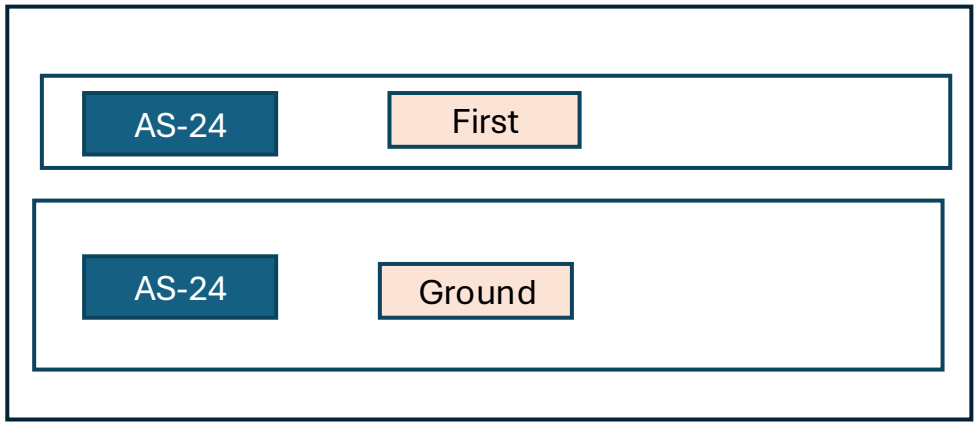
Sports Complex



Innovation



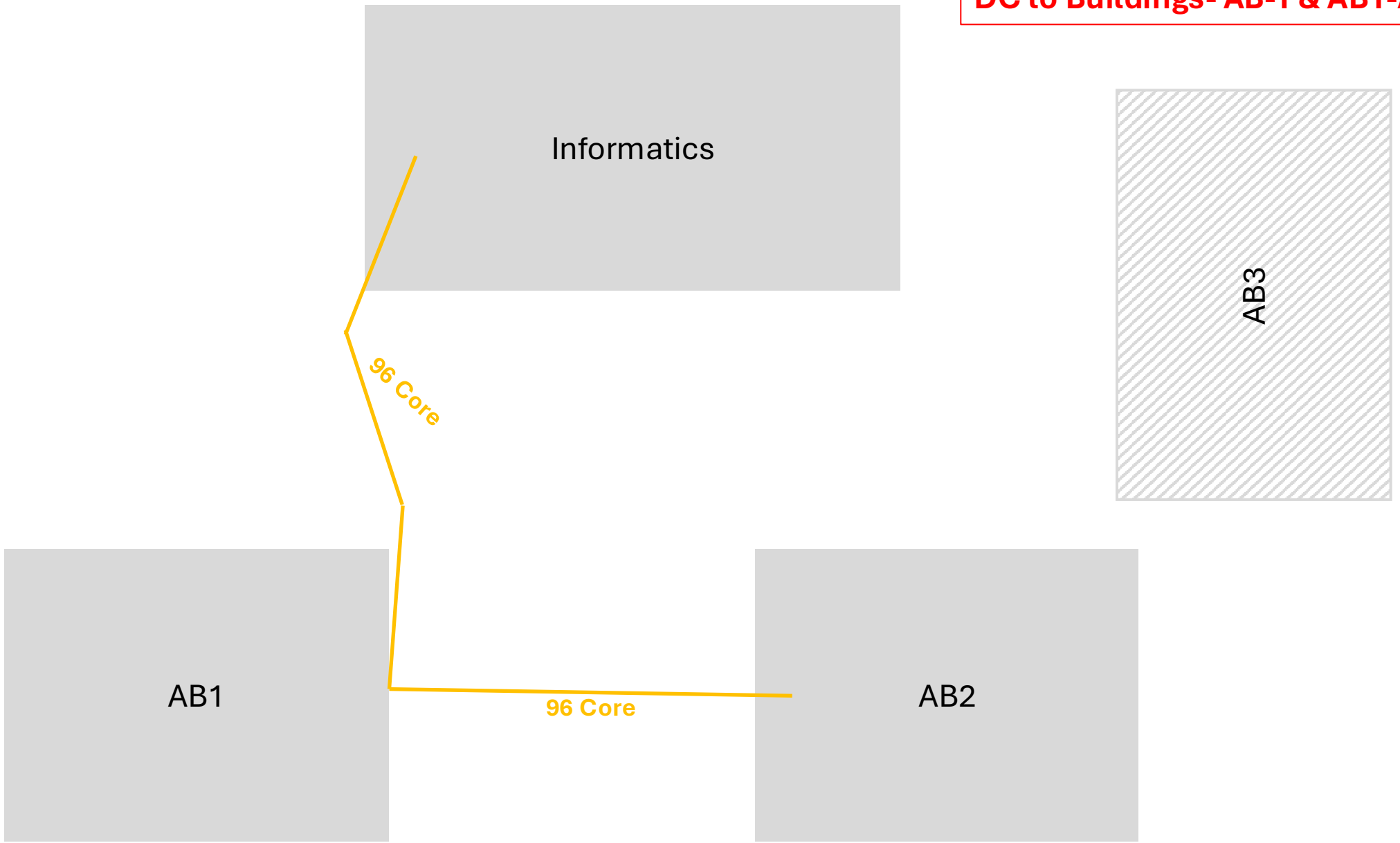
CAF



Schematics of Academic Block-1 and Animal House

Items	**Particulars**
Buildings	AB-1 and Animal House
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

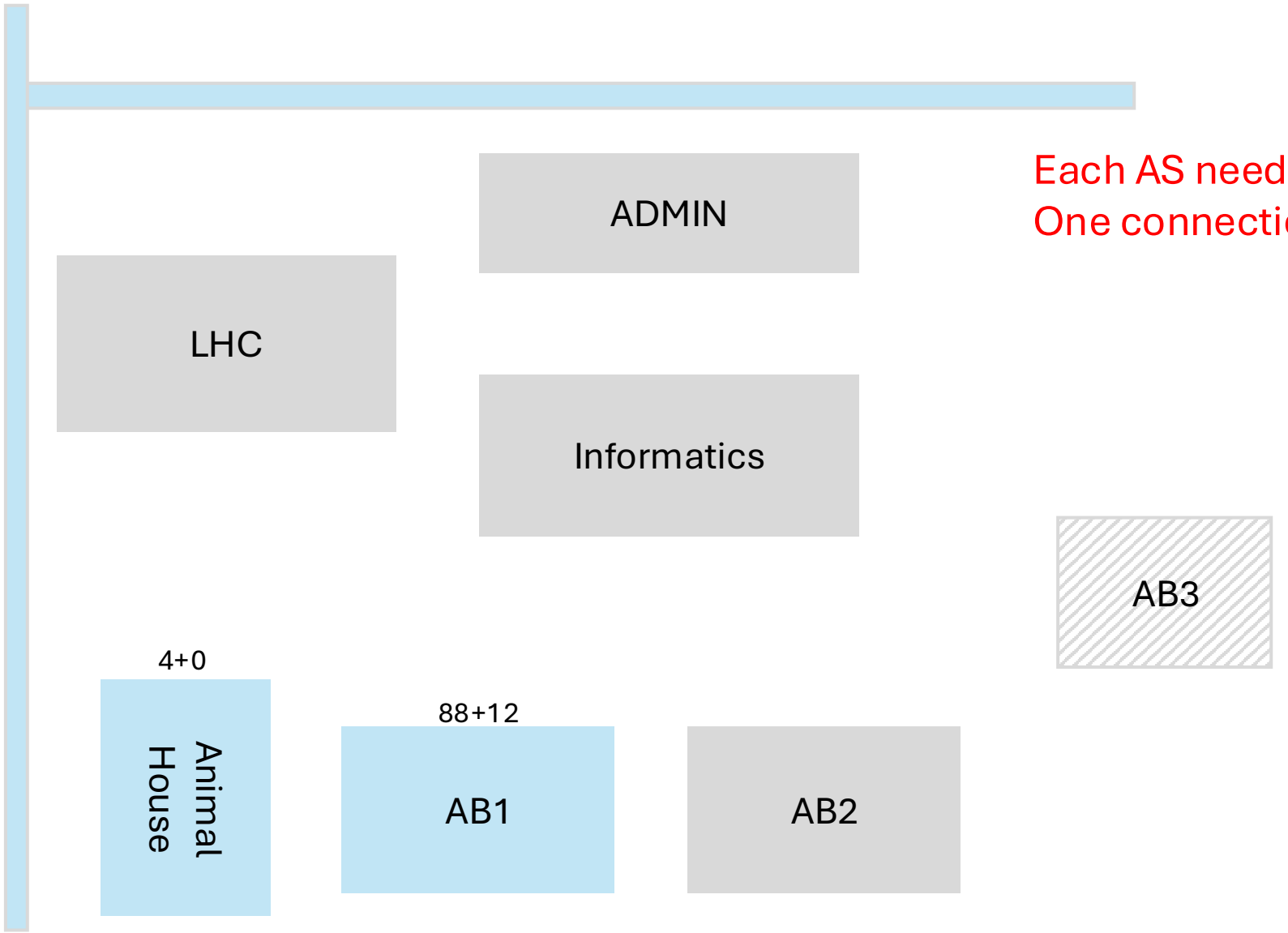
DC to Buildings- AB-1 & AB1-AB-2



DC to Buildings- AB-1 & AB-1 to AB-2

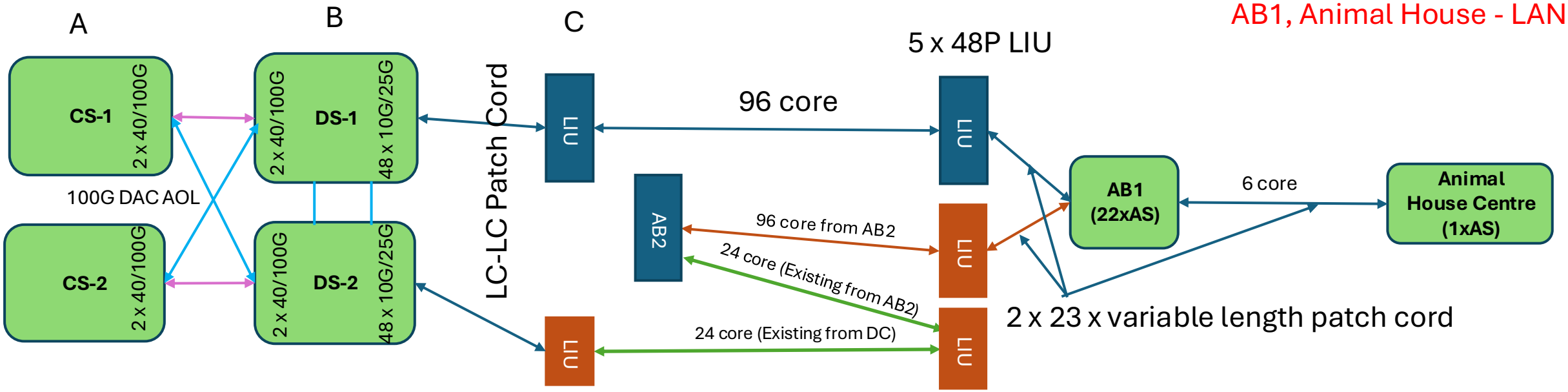


OFC Core from DC to AS for LAN and Wi-Fi



Each AS needs two connections
One connections = 2 cores fiber

AB1, Animal House - LAN

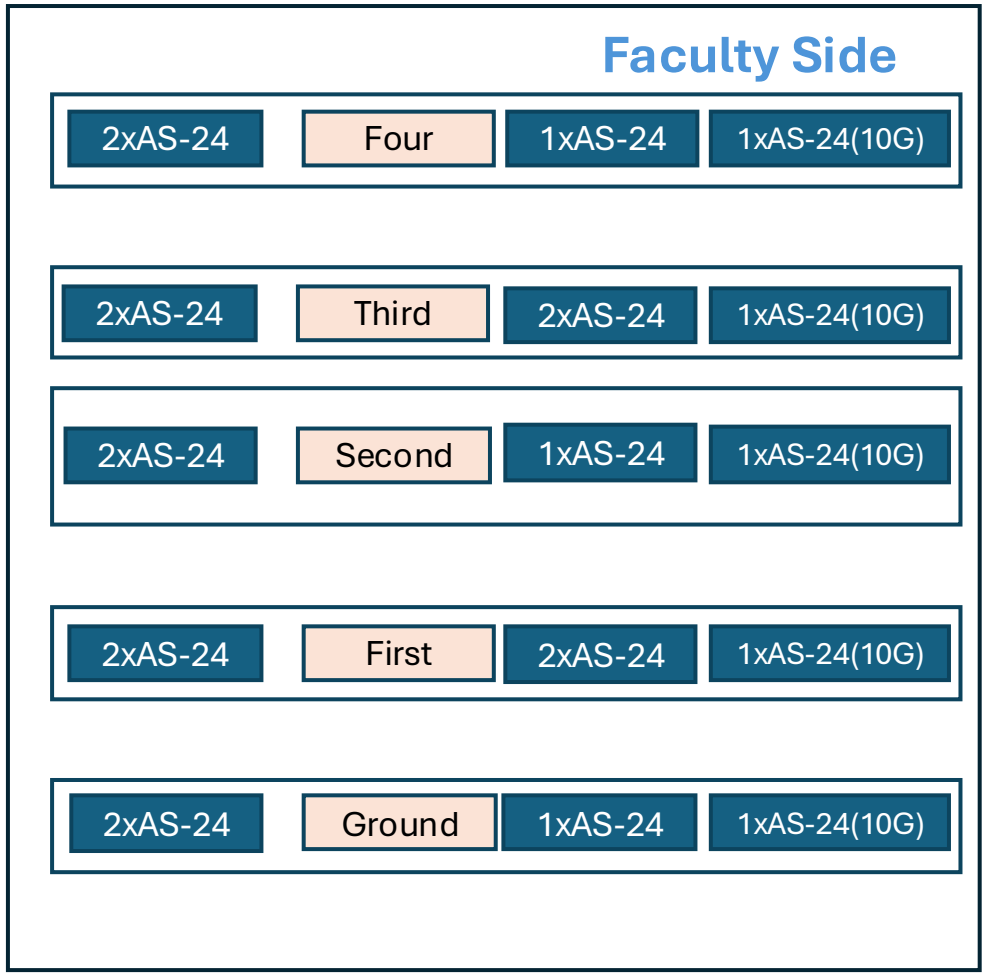


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G/25G	Patch-cord LC-LC	LIU at DC (48P)	LIU at AB1 (48P)	Core Required	Patch Cord LC-LC	SFP 10G/25G	Connection on AS	AS
2	4	2	18 + 18 5 + 5	46	3	5	46+46	46	18+18 5+5	23+23	23

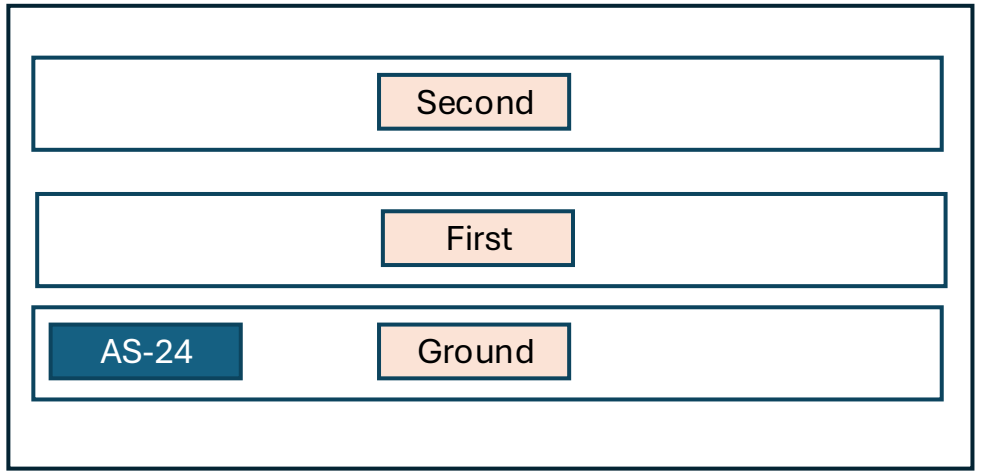
Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
46 + 46	6 + 6	52 + 52	96C + 96C	4	2

	Total 96 Core	Total 48 Core	Total 24 Core	Total 6 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	1 + 1	0+0	0 + 0	0 + 0	2 x 23
Length					

AB 1



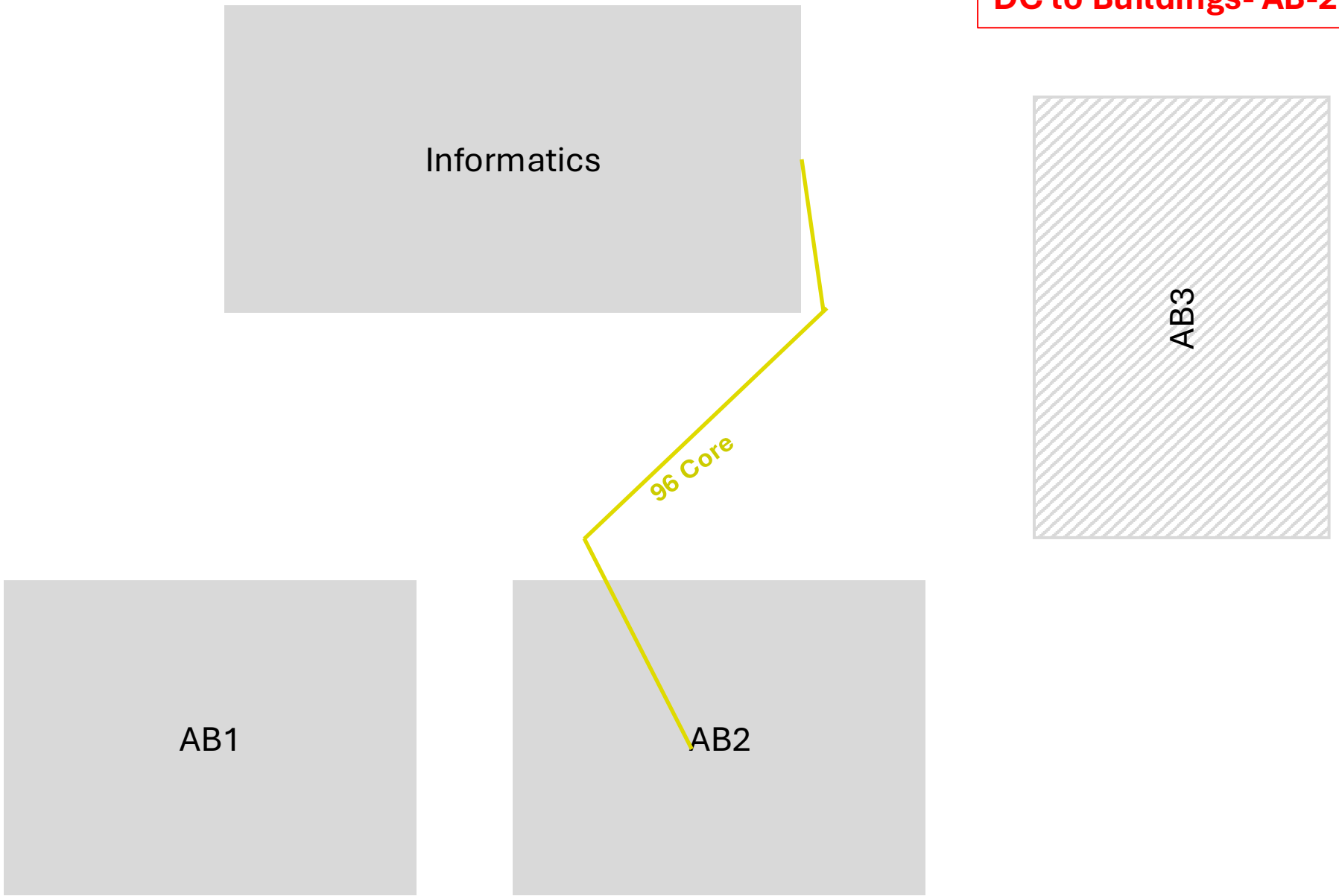
Animal House



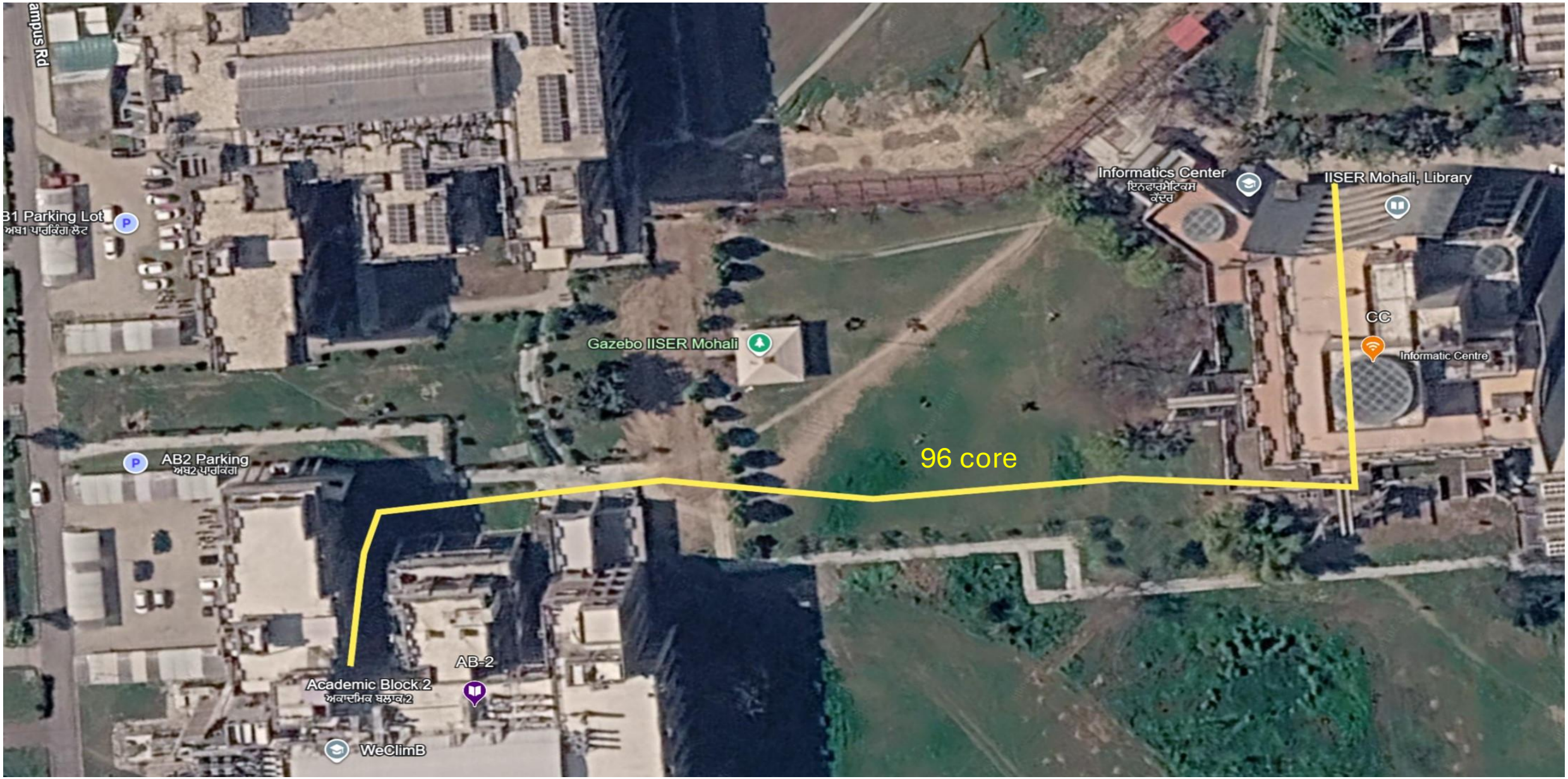
Schematics of Academic Block -2

Items	**Particulars**
Buildings	AB-2
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

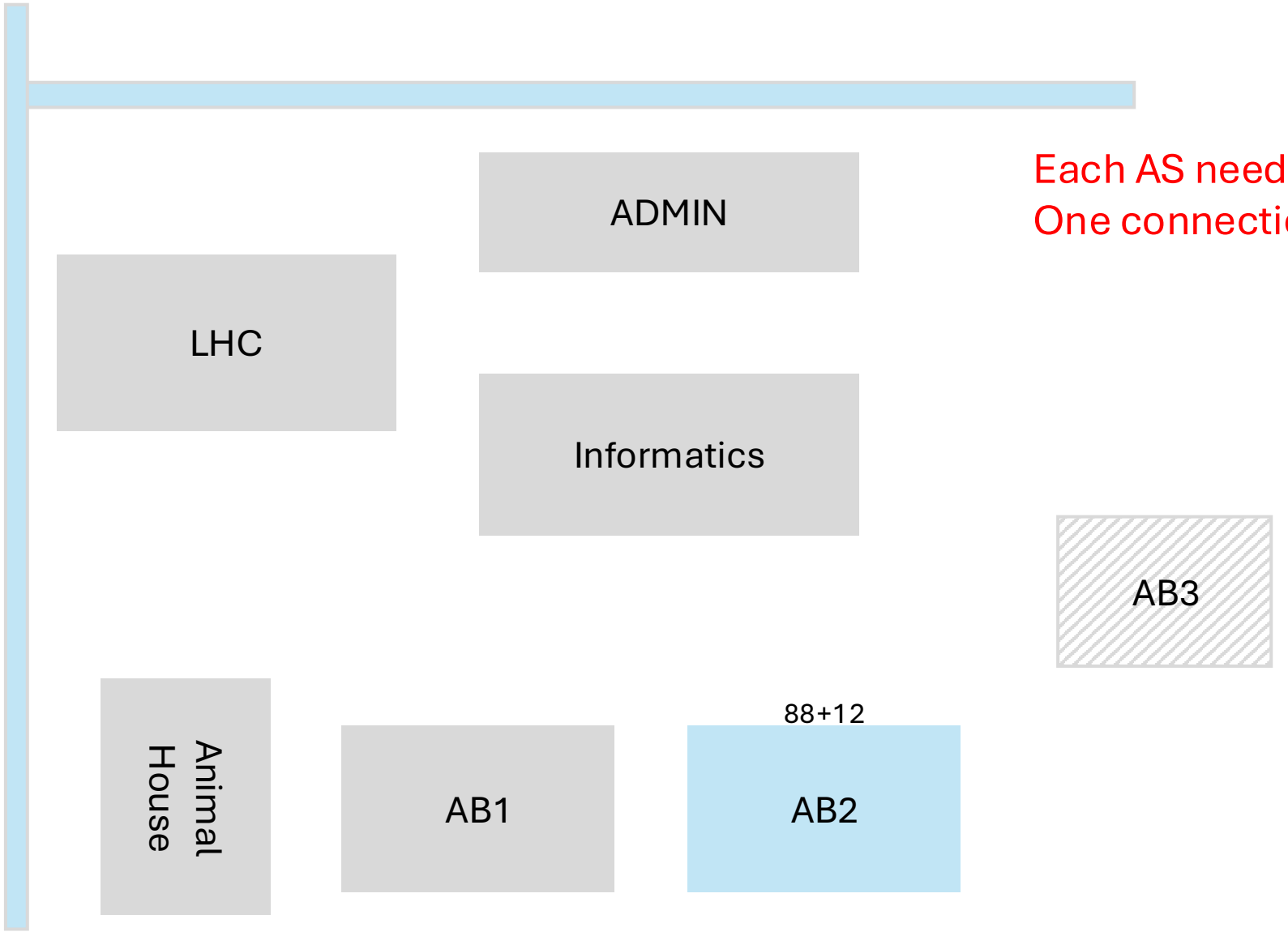
DC to Buildings- AB-2



DC to Buildings- AB-2

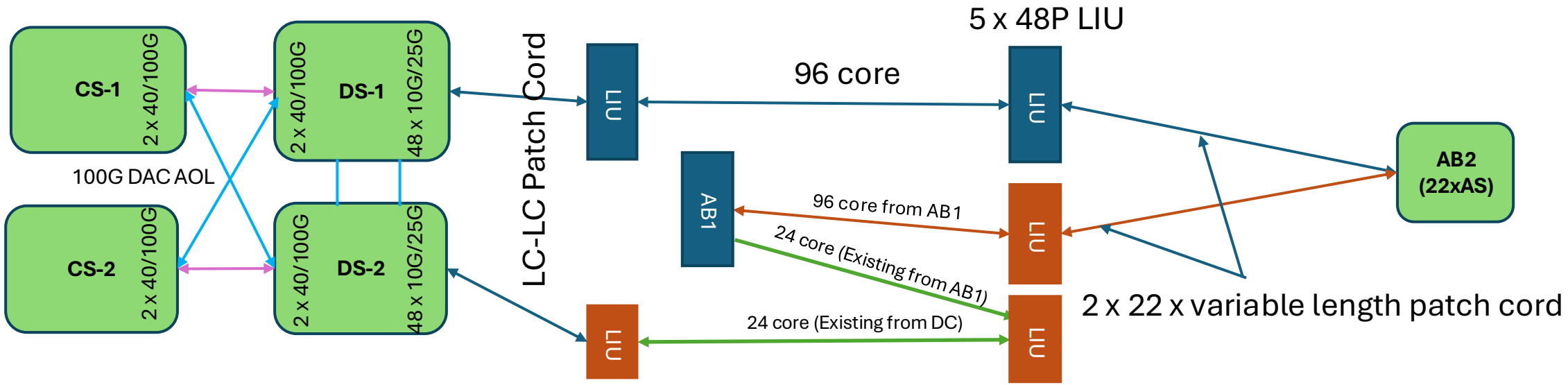


OFC Core from DC to AS for LAN and Wi-Fi



Each AS needs two connections
One connections = 2 cores fiber

AB 2 - LAN

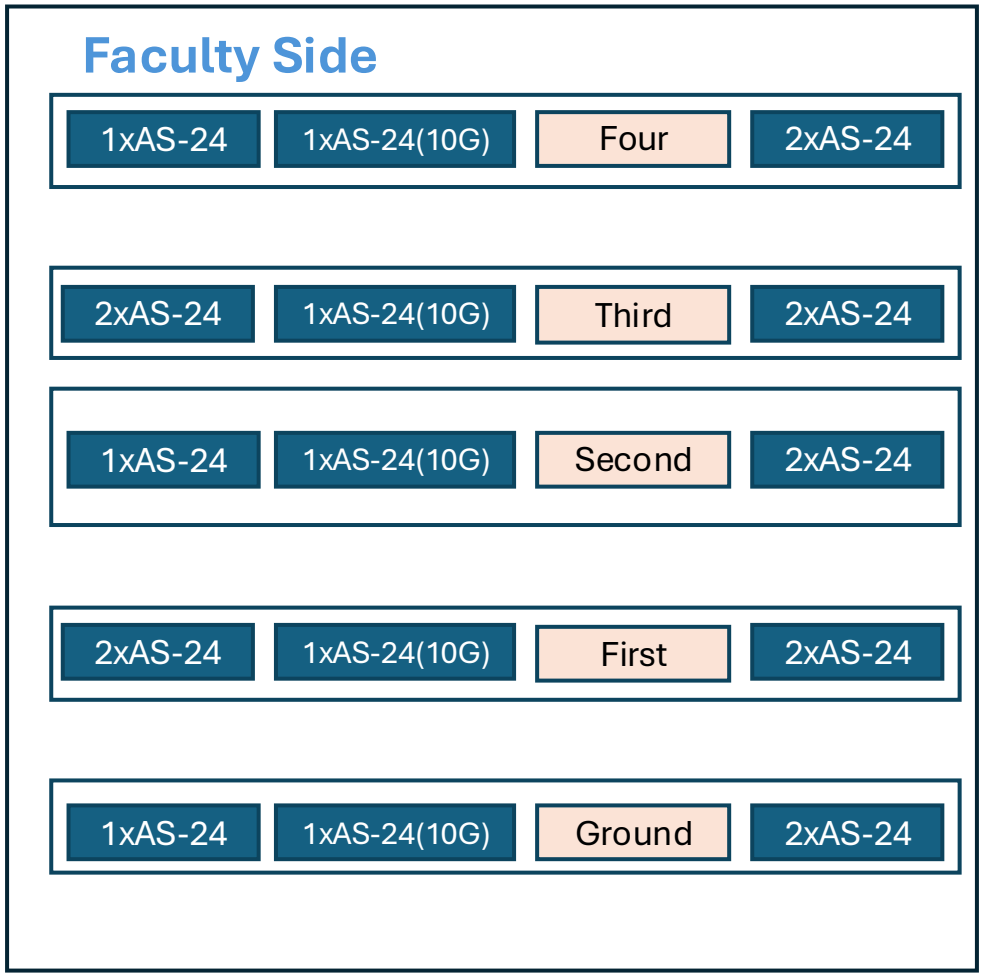


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G/25G	Patch-cord LC-LC	LIU at DC (48P)	LIU at AB2 (48P)	Core Required	Patch Cord LC-LC	SFP 10G/25G	Connection on AS	AS
2	4	2	17+17 5 + 5	44	3	5	44+44	44	17+17 5 + 5	22 + 22	22

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
44+44	6 + 6	50+50	96C	4	2

	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	1	0+0	0 + 0	0 + 0	2 x 22
Length					

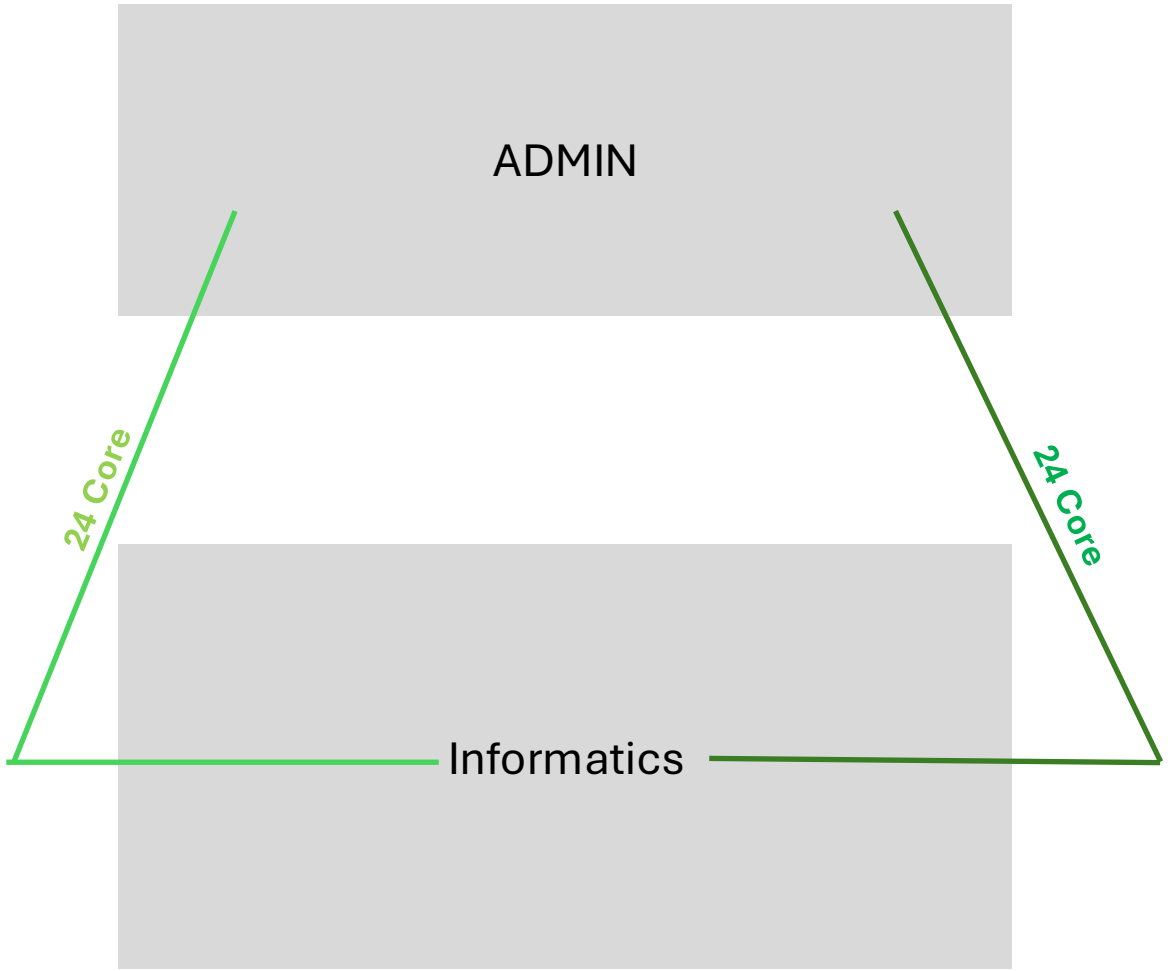
AB 2


Faculty Side
1xAS-24
1xAS-24(10G)
Four
2xAS-24
2xAS-24
1xAS-24(10G)
Third
2xAS-24
1xAS-24
1xAS-24(10G)
Second
2xAS-24
2xAS-24
1xAS-24(10G)
First
2xAS-24
1xAS-24
1xAS-24(10G)
Ground
2xAS-24

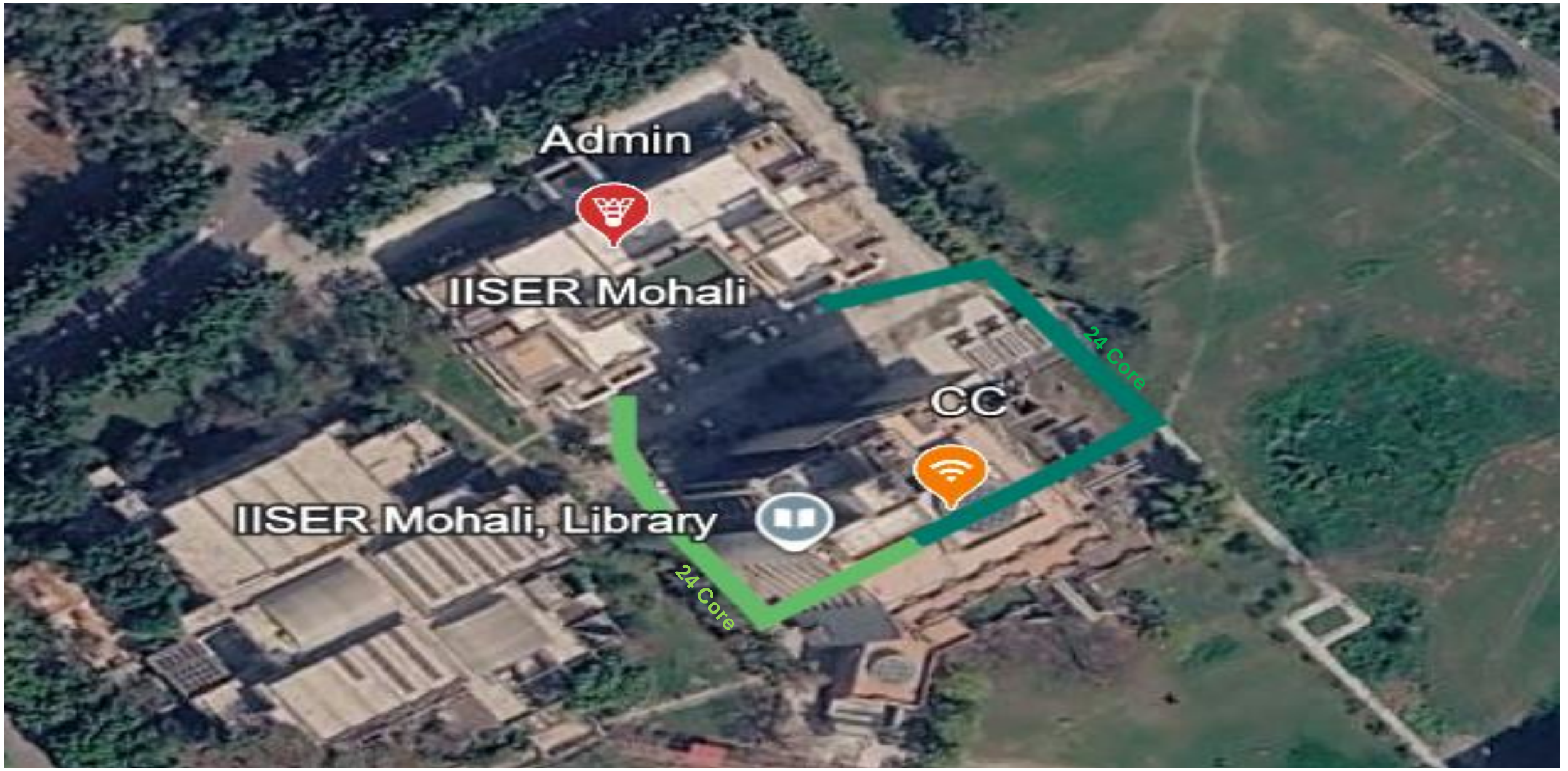
Schematics of Admin

Items	**Particulars**
Buildings	Admin
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

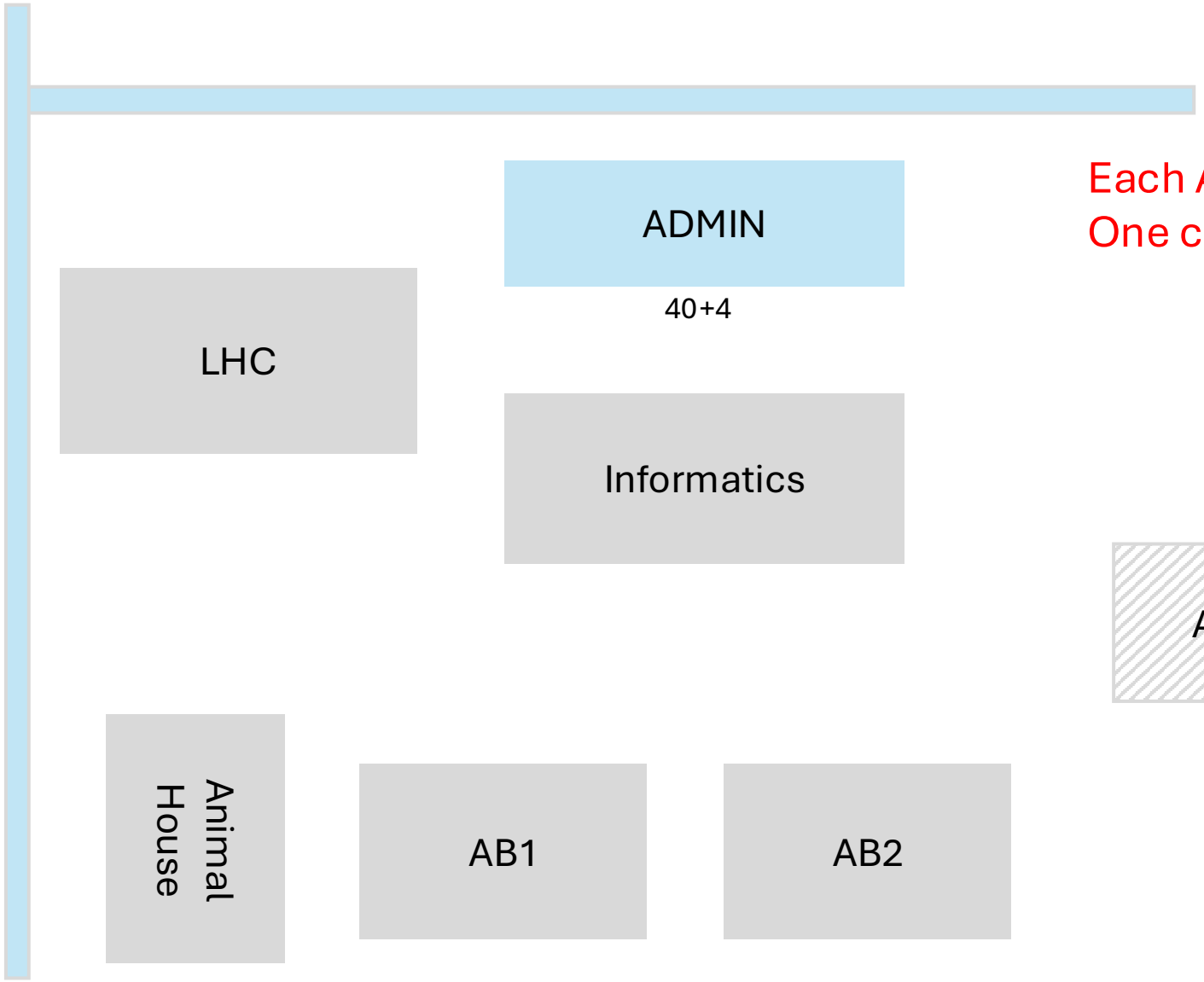
DC to Admin Building



DC to Admin Building

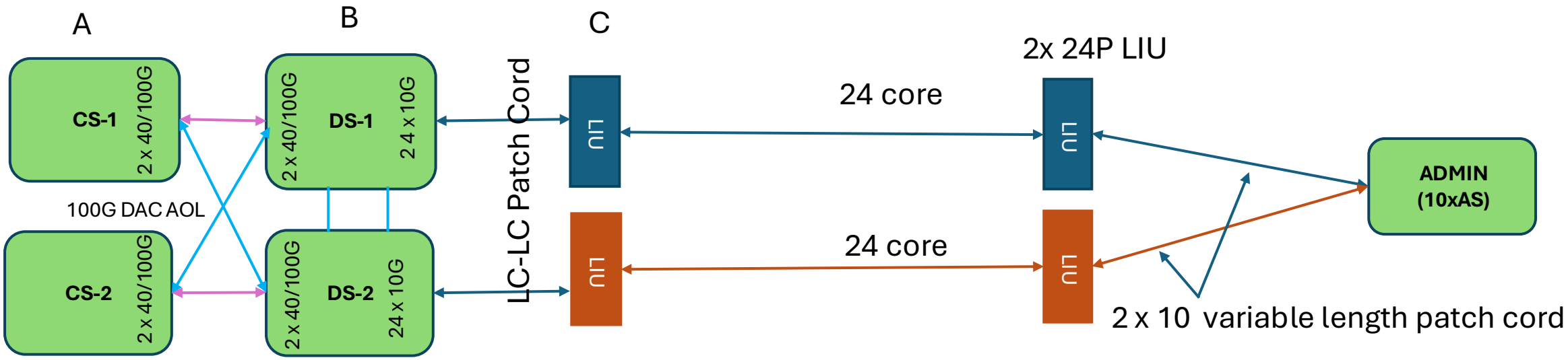


OFC Core from DC to AS for LAN and Wi-Fi



Each AS needs two connections
One connections = 2 cores fiber

ADMIN - LAN

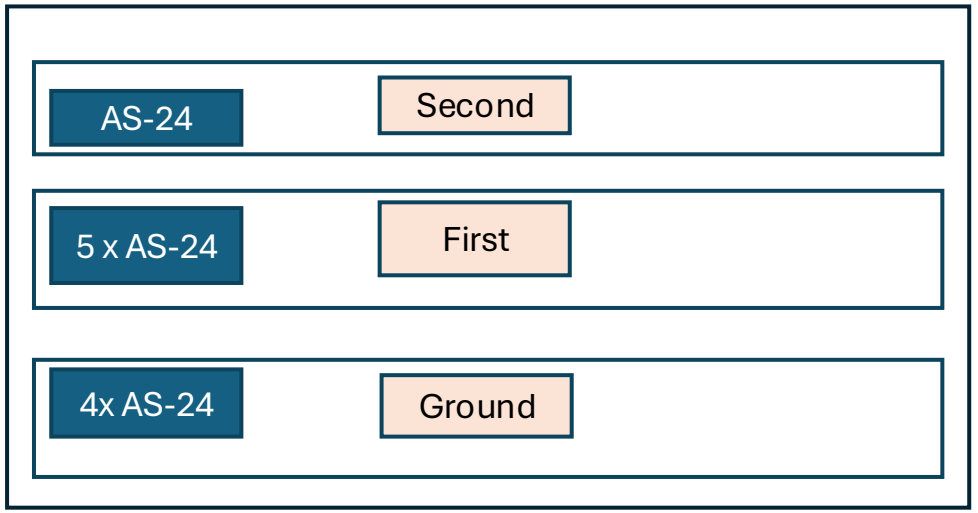


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48P)	LIU at ADMIN (24P)	Core Required	Patch Cord LC-LC	SFP 10G	Connection on AS	AS
2	4	2	10 + 10	20	2	2	20+20	20	10+10	10+10	10

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
20 + 20	2 + 2	22+22	24C + 24C	4	2

	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	0 + 0	0+0	1+1	0 + 0	2 x 10
Length					

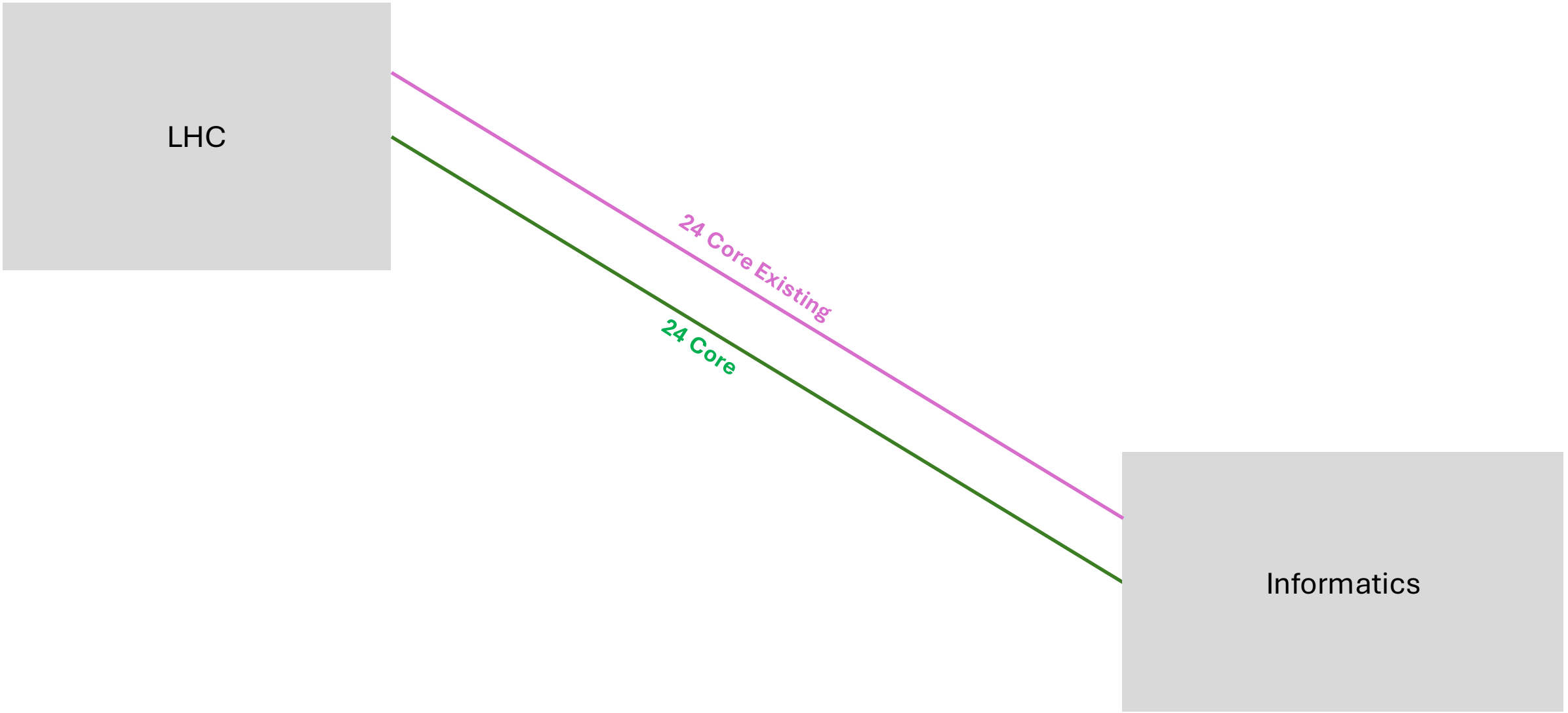
Admin



Schematics of Lecture Hall Complex

Items	**Particulars**
Buildings	LHC
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

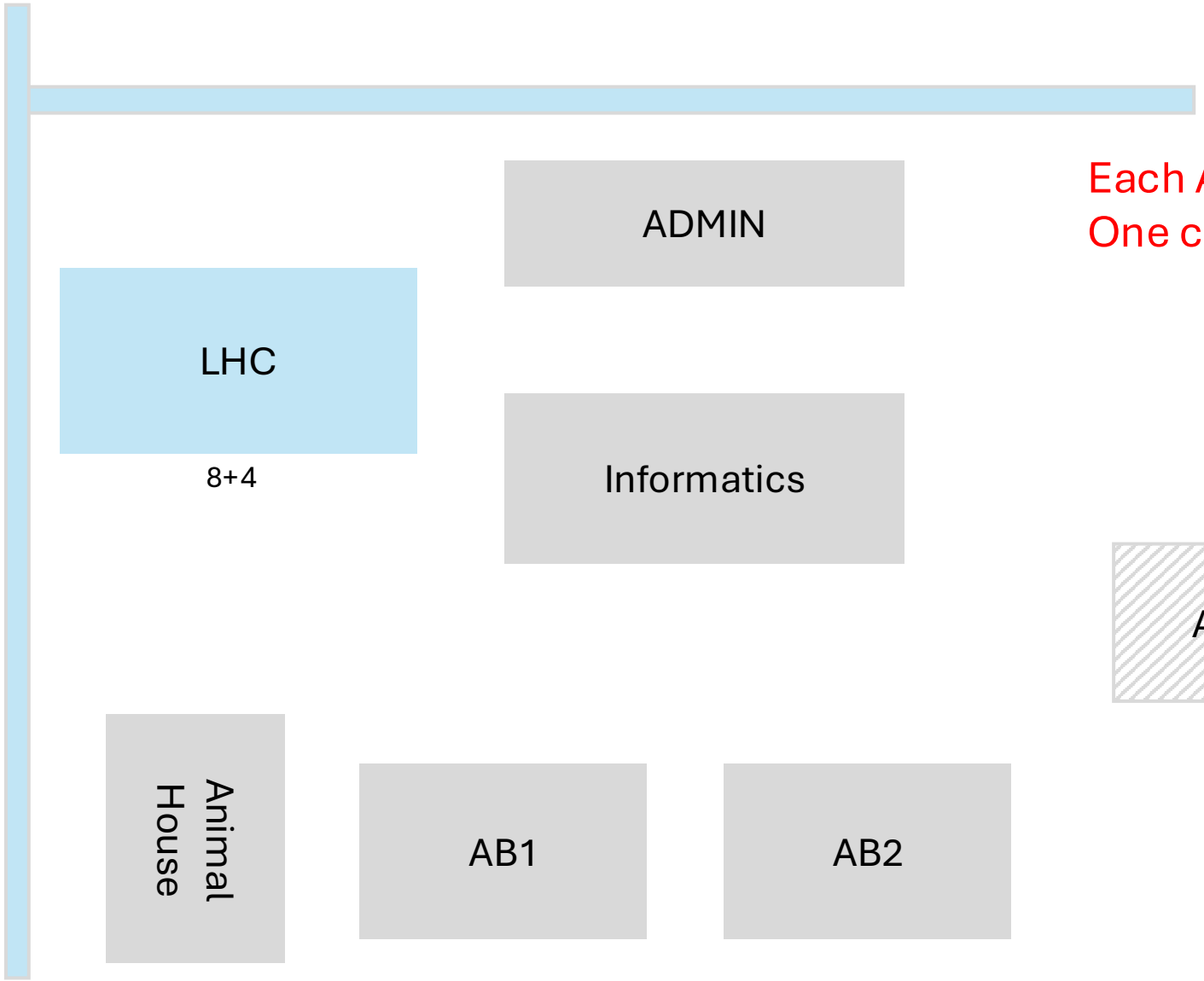
DC to LHC



DC to LHC

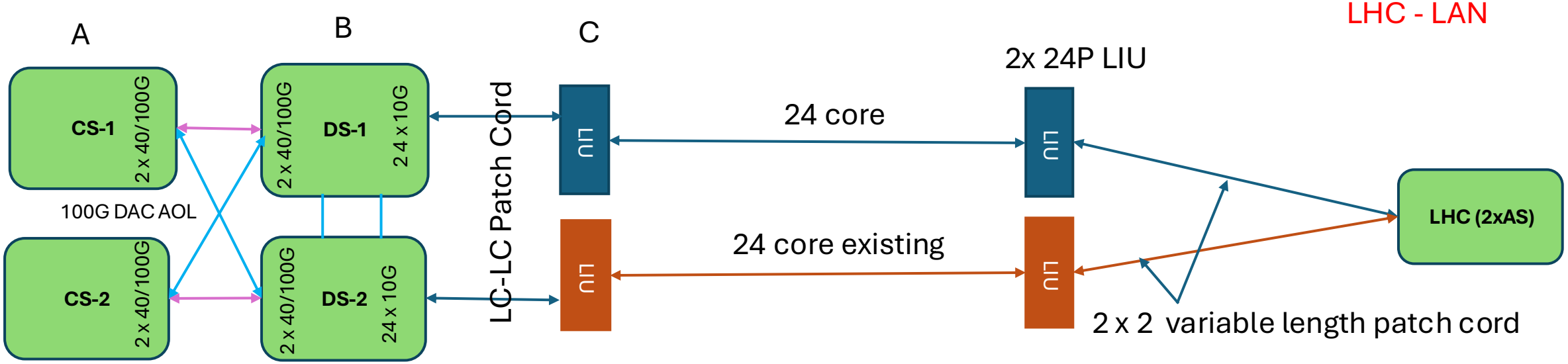

Eatery Outlet
ਐਟਰੀ ਆਉਟਲੇਟ
LHC
Lecture Hall Complex, IISER Mohali
ਲੈਕਚਰ ਹਾਲ ਕੰਪਲੈਕਸ, ਇਸਰ...
IISER Mohali, Library
Informatic Centre
CC
24 Core Existing
24 Core
Informatics Center
ਇਨਫਾਰਮੈਟਿਕਸ ਕੇਂਦਰ

OFC Core from DC to AS for LAN and Wi-Fi



Each AS needs two connections
One connections = 2 cores fiber

LHC - LAN

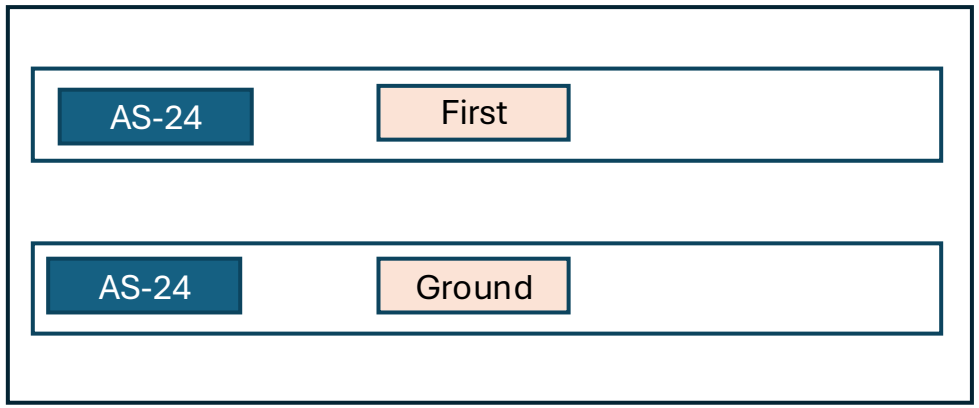


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48P)	LIU at LHC (24P)	Core Required	Patch Cord LC-LC	SFP 10G	Connection on AS	AS
2	4	2	2+2	4	2	2	4+4	4	2+2	2+2	2

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
4+4	2+2	6 + 6	24C + 24C	4	2

	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	0 + 0	0+0	1+1	0 + 0	2 x 2
Length					

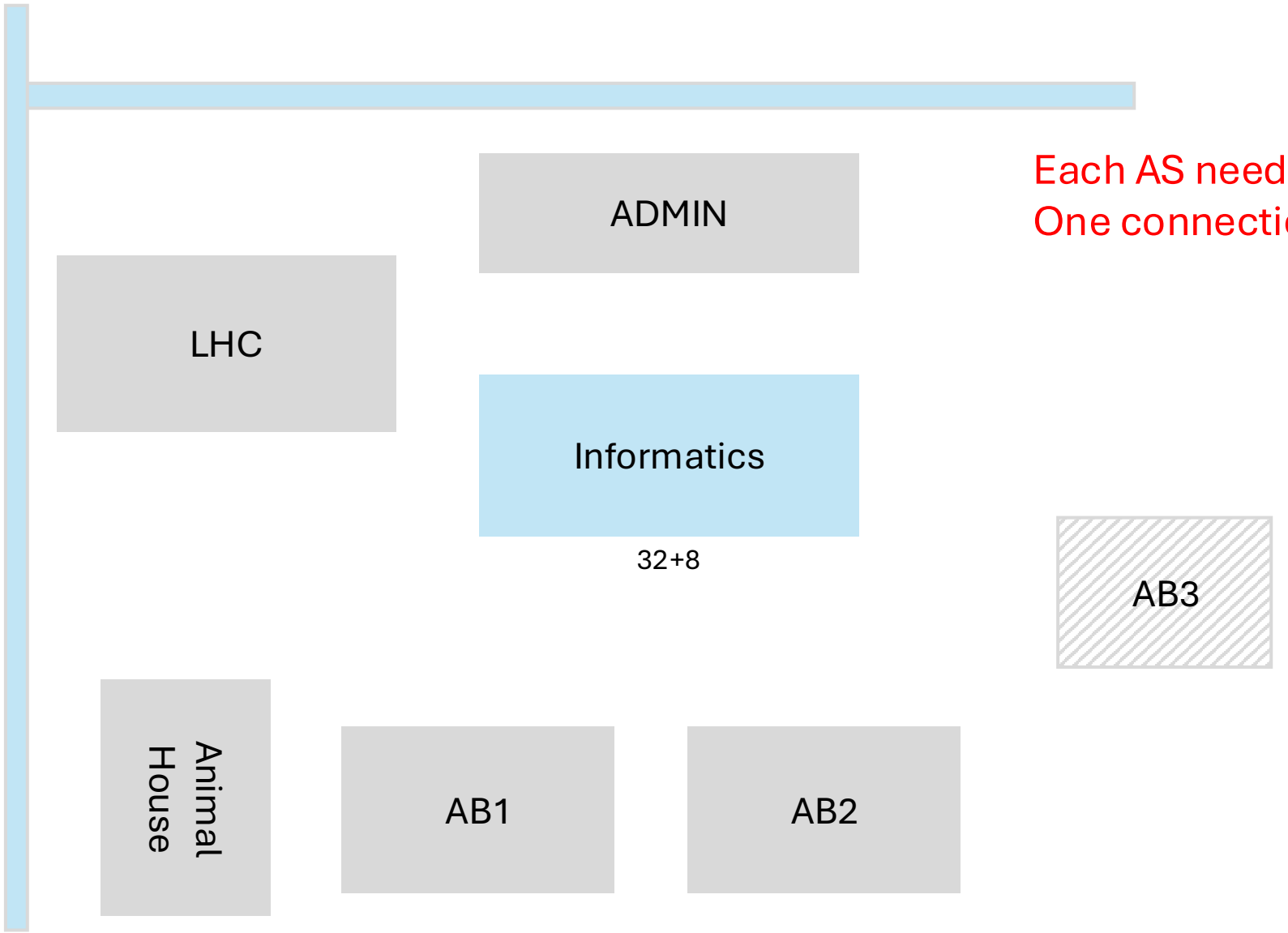
LHC



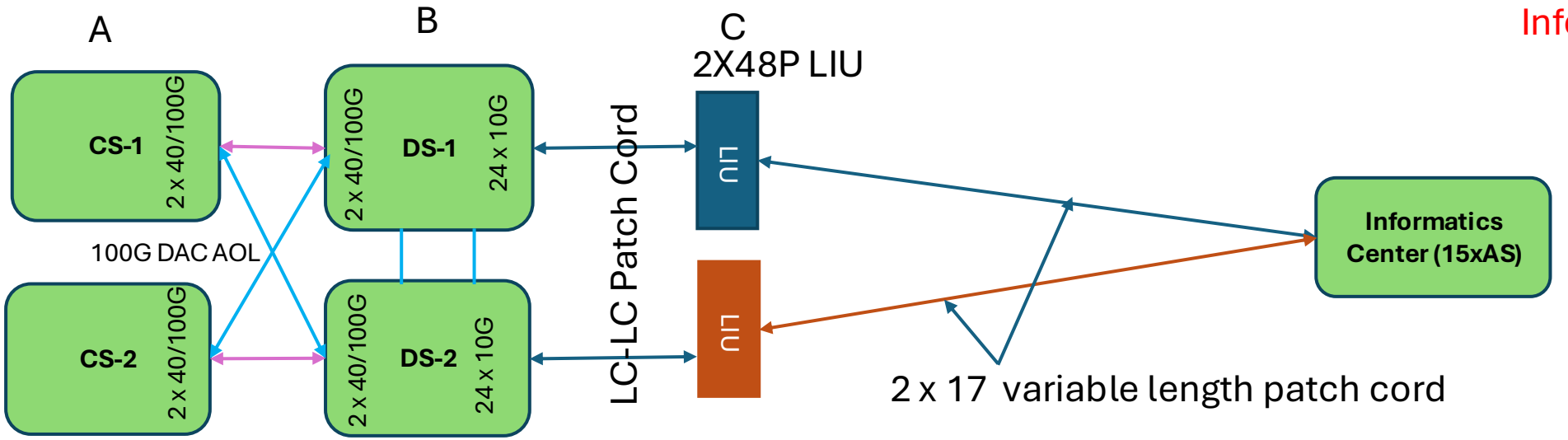
Schematics of Informatics Center

Items	**Particulars**
Buildings	Informatics Center
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

OFC Core from DC to AS for LAN and Wi-Fi



Each AS needs two connections
One connections = 2 cores fiber

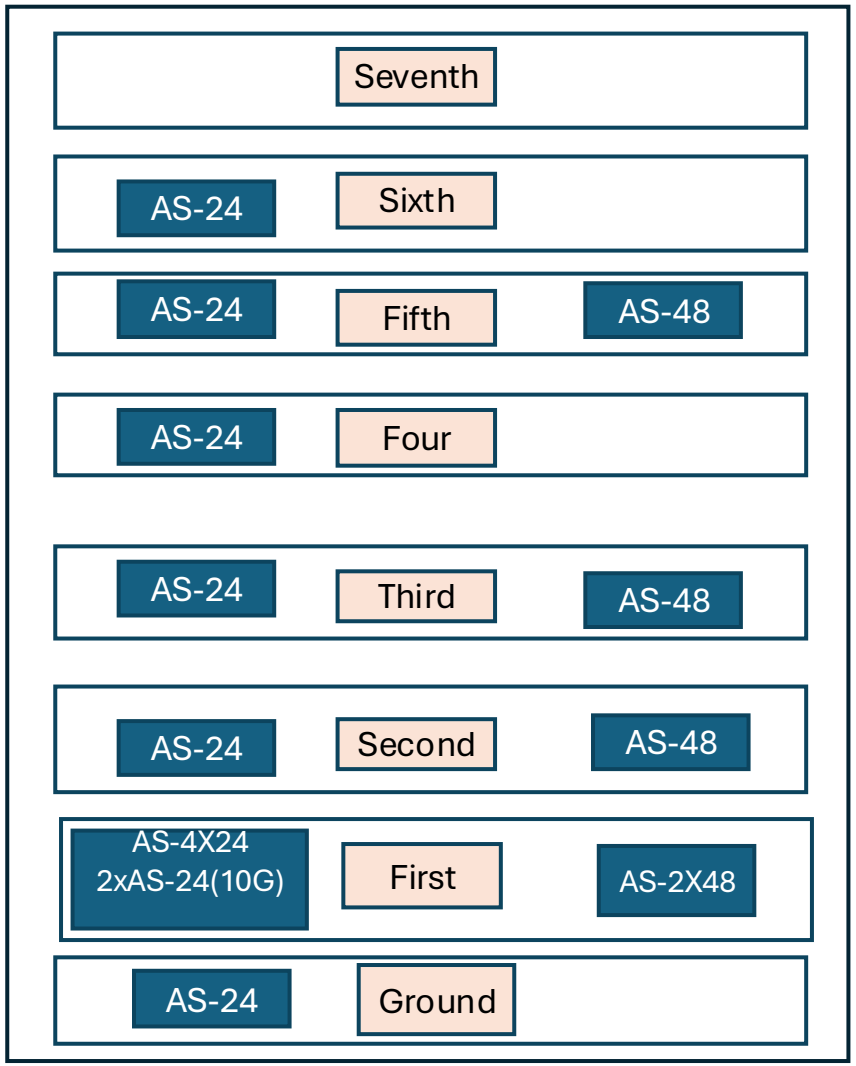


DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G/25G	Patch-cord LC-LC	LIU at DC (48P)	Core Required	Patch Cord LC-LC	SFP 10G/25G	Connection on AS	AS
2	4	2	15+15 2+2	34	2	34+34	34	15+15 2+2	17+17	17

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
34+34	4+4	38 + 38		4	2

	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	0 + 0	0+0	0+0	0 + 0	2 x 17
Length					

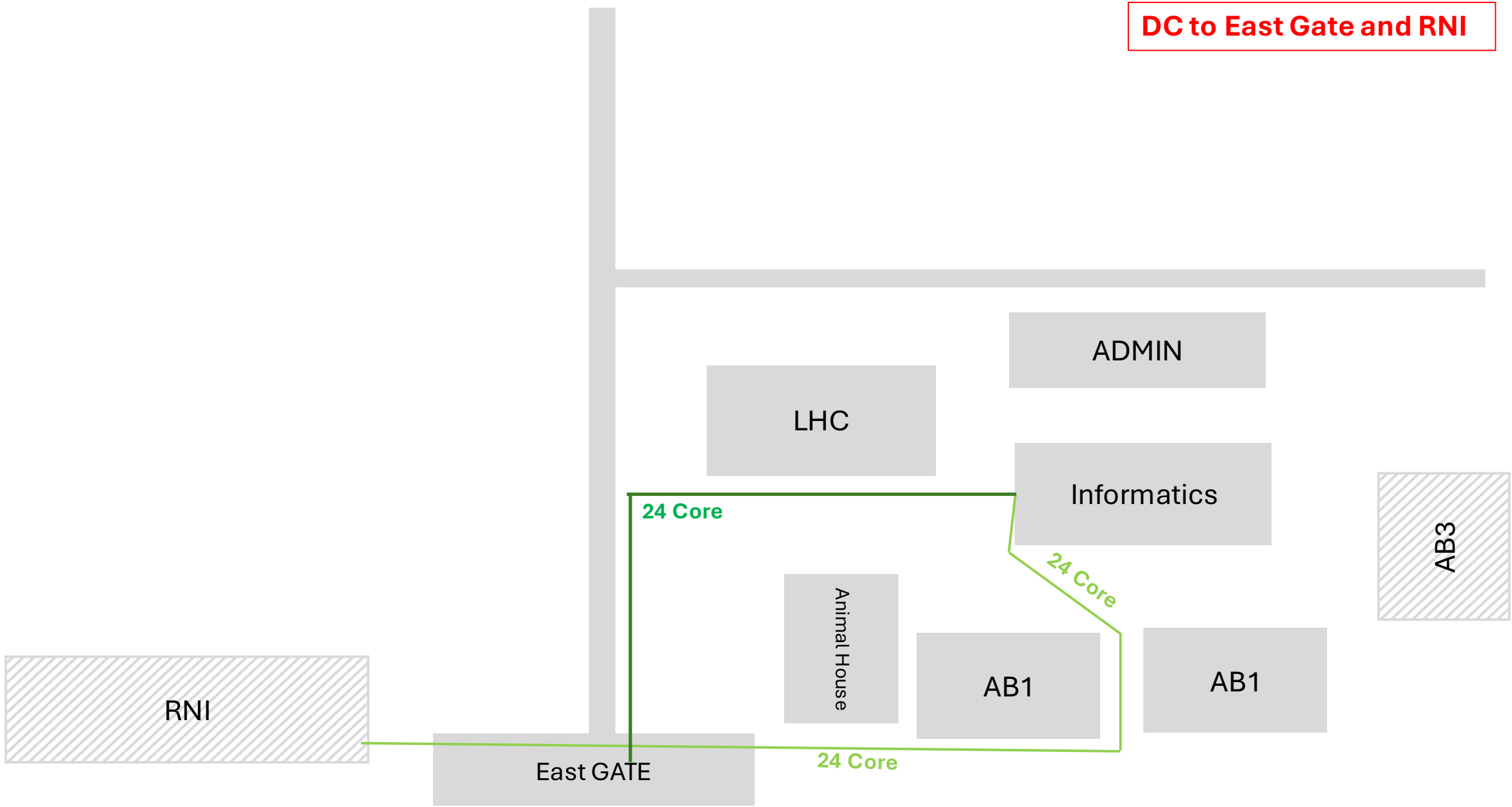
Informatics Center



Schematics of East Gate and RNI

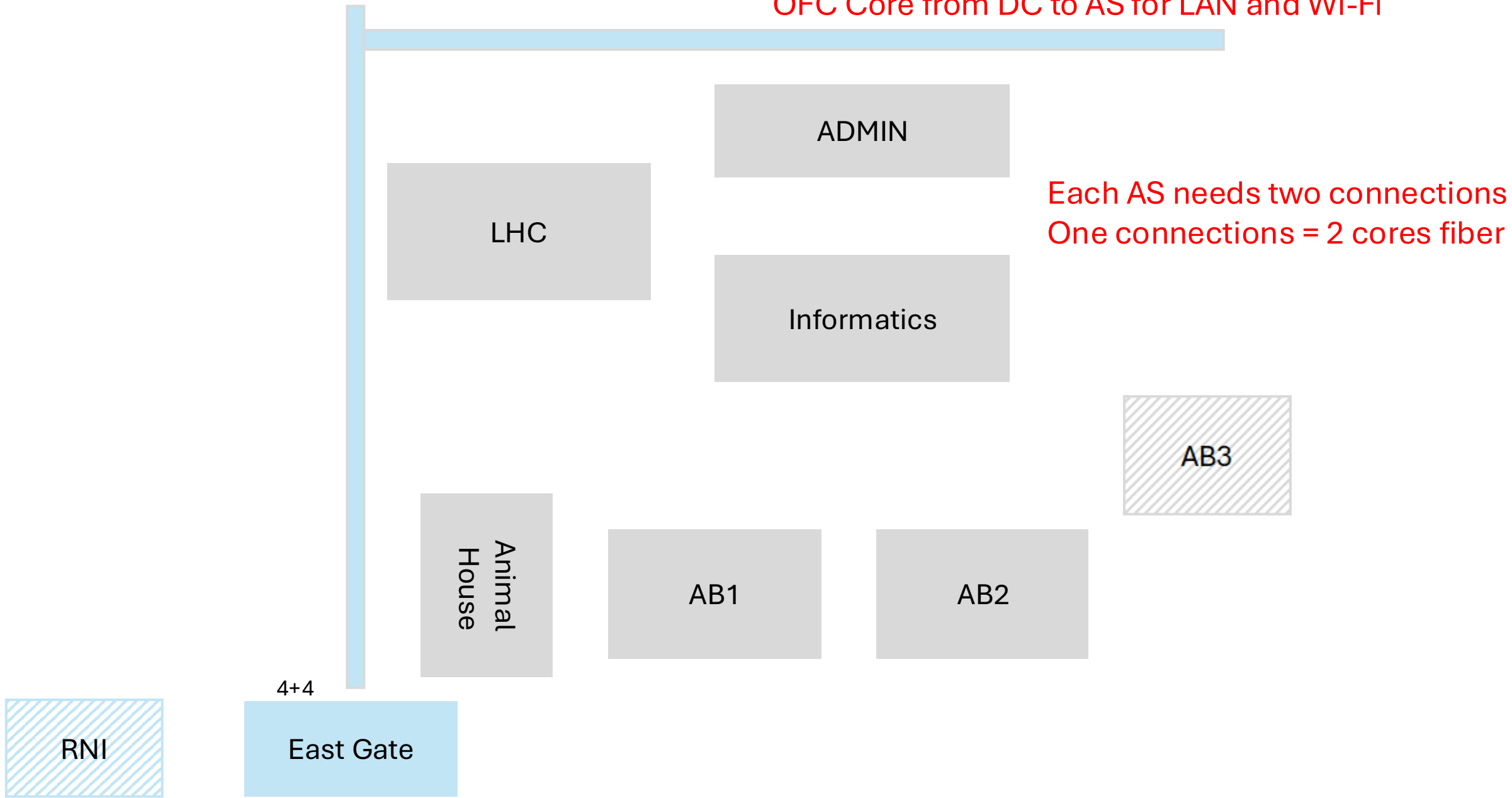
Items	**Particulars**
Buildings	East Gate and RNI
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Only Wired connection (LAN only)
Accessories (SFPs, Patch Cords, LIU, Junction boxes, conduits, cables etc)	Required for wired connections

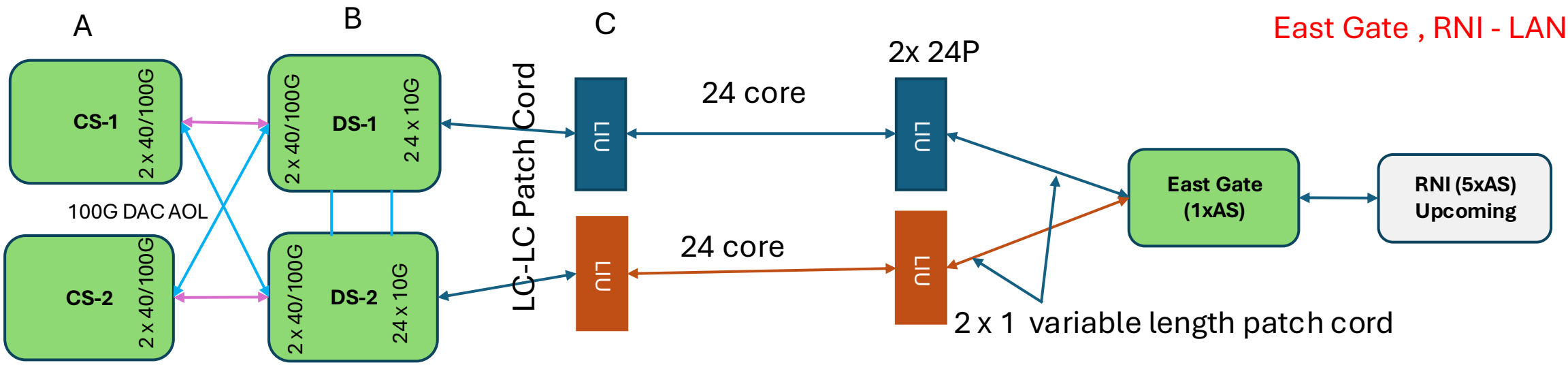
DC to East Gate and RNI



DC to East Gate and RNI




OFC Core from DC to AS for LAN and Wi-Fi
ADMIN
LHC
Informatics
Each AS needs two connections
One connections = 2 cores fiber
AB3
Animal House
AB1
AB2
4+4
RNI
East Gate



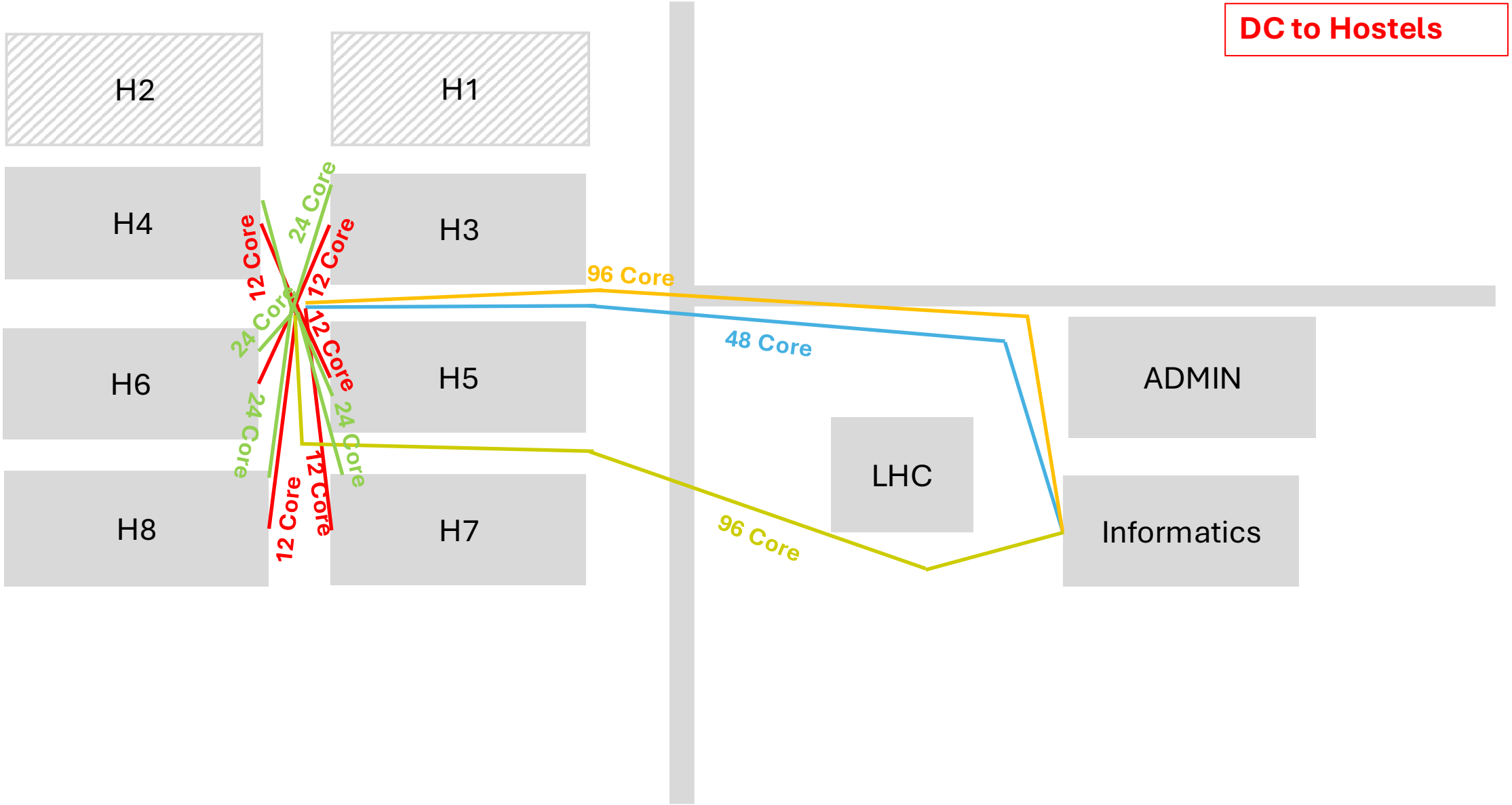
DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48)	LIU at East Gate(24)	Core Required	Patch Cord LC-LC	SFP 10G	Connection on AS	AS
2	4	2	1+1	2	2	2	2 + 2	2	1 + 1	1 + 1	1

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
2 + 2	2 + 2	4 + 4	24C + 24C	4	2

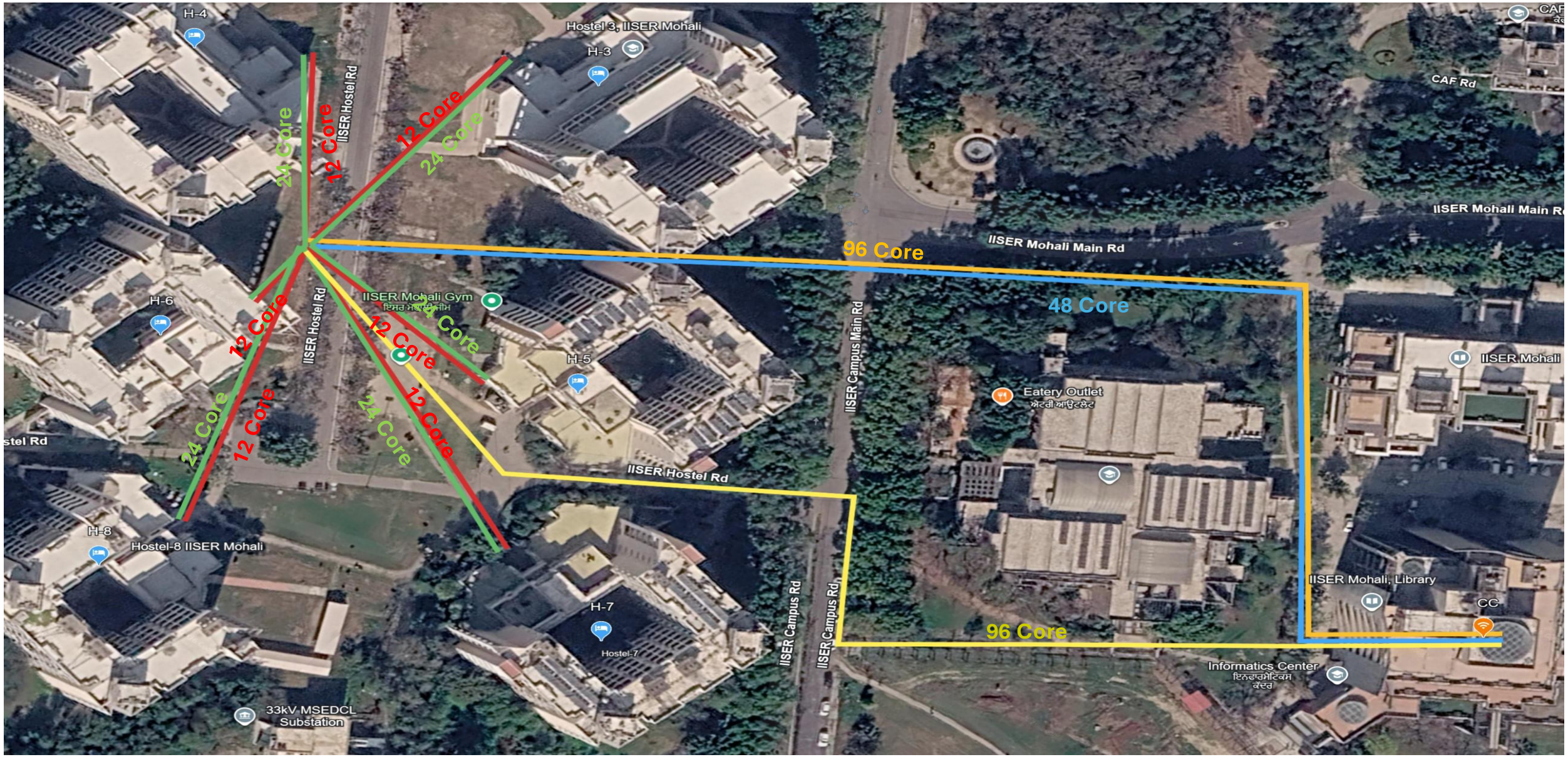
	Total 96 Core	Total 48 Core	Total 24 Core	Total 12 Core	Variable length Patch cords to be connected from the LIU to each AS Switch
Two redundant OFC	0 + 0	0+0	1+1	0 + 0	2 x 1
Length					

Schematics of Student Hostels

Items	**Particulars**
Buildings	H3,H4,H5,H6,H7,H8
Laying OFC:	Provisioning for Connections for both LAN and WiFi
Switching:	Not required
Accessories (LIU, Junction boxes, conduits, cables etc)	Required for wired connections

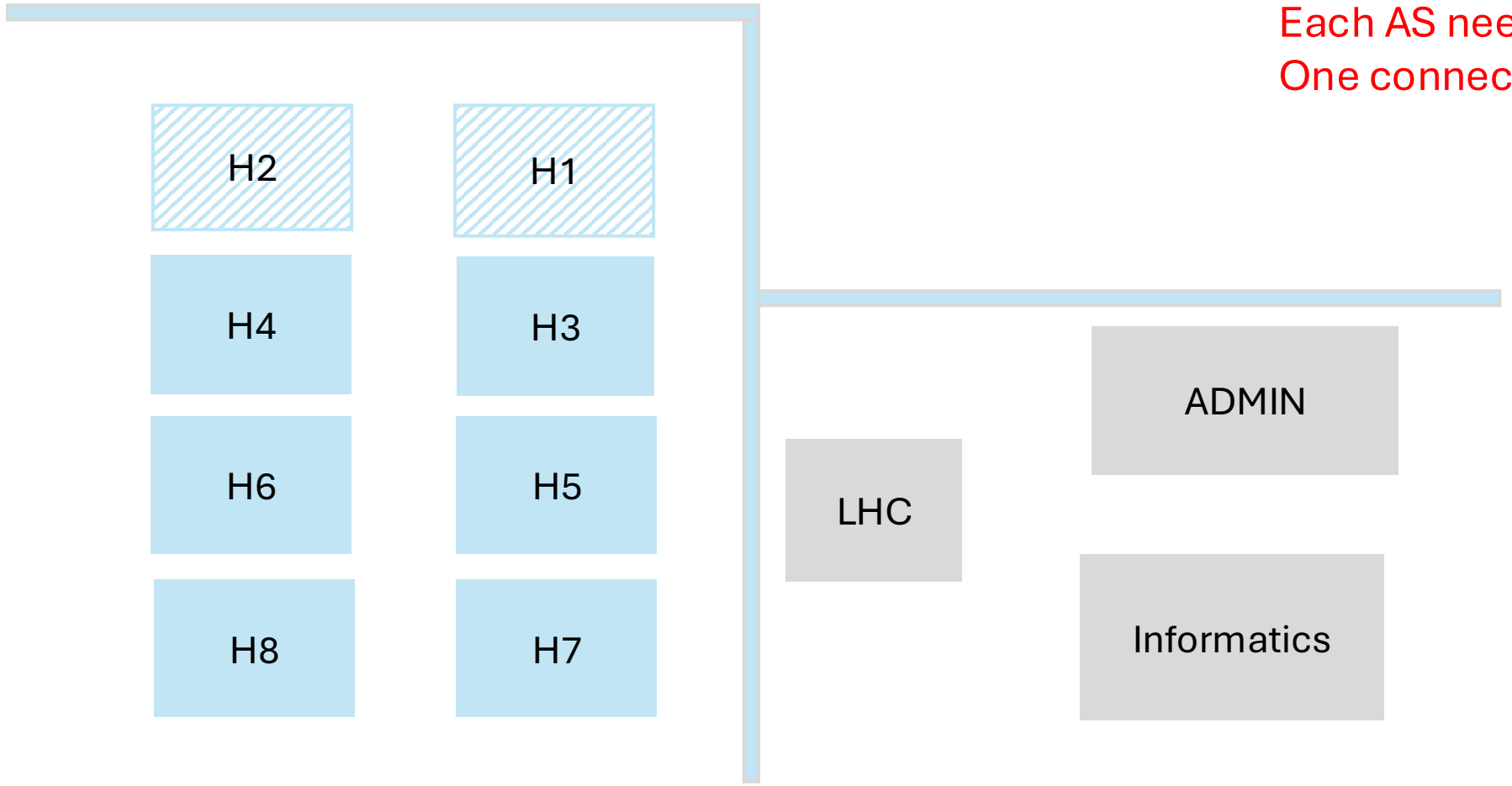

DC to Hostels
H2
H1
H4
H3
H6
H5
H8
H7
LHC
ADMIN
Informatics
24 Core
12 Core
12 Core
24 Core
12 Core
24 Core
24 Core
12 Core
12 Core
24 Core
12 Core
96 Core
48 Core
96 Core

DC to Hostels



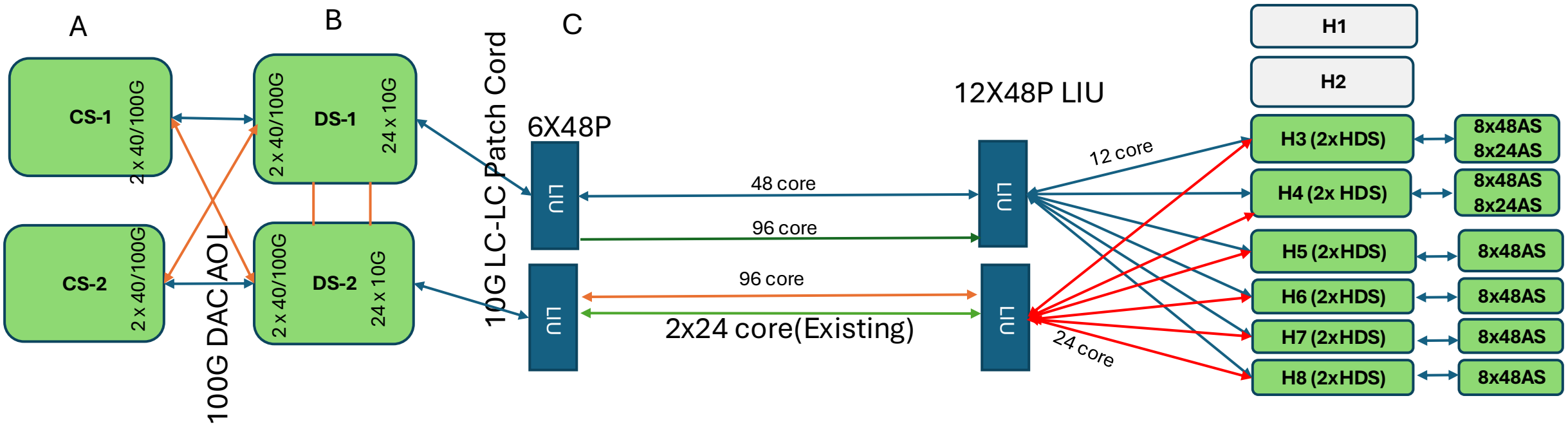
OFC Core from DC to AS for LAN and Wi-Fi

Each AS needs two connections
One connections = 2 cores fiber



Scope is to lay only the OFC cables 2 x 96C + 1 x 48C + 6x 12C + 6 x 24C, LIU & junction Boxes, and establish the LIU-to-LIU connectivity

Student Hostel Complex - LAN



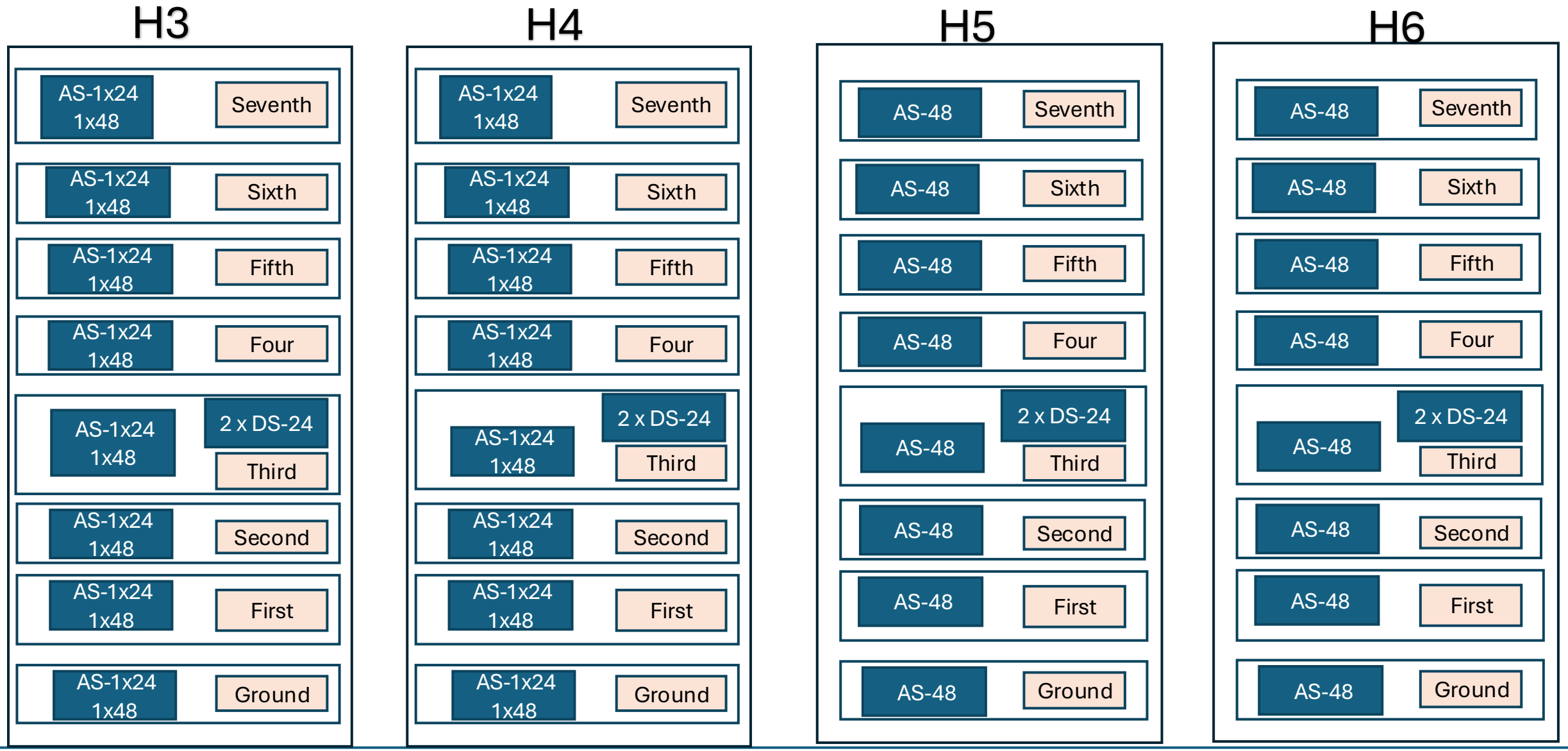
DS-CS 1M-DAC	DS-CS 5m DAC	DS 48 P	SFP 10G	Patch-cord LC-LC	LIU at DC (48)	LIU at Hostels (48P)	Core Required	Patch Cord LC-LC	SFP 10G	Connection on HDS	HDS & AS
				24	6	12	24+24	24		12+12	12 & 64

Total Core for LAN	Total Core for WiFi	Total Required	Cable Required	DAC Cable	Short Cable
			48C and 96C + 96C		

Total 96	Total 48	Total 24 Core	Total 12 Core
1 + 1	1+0	6	6

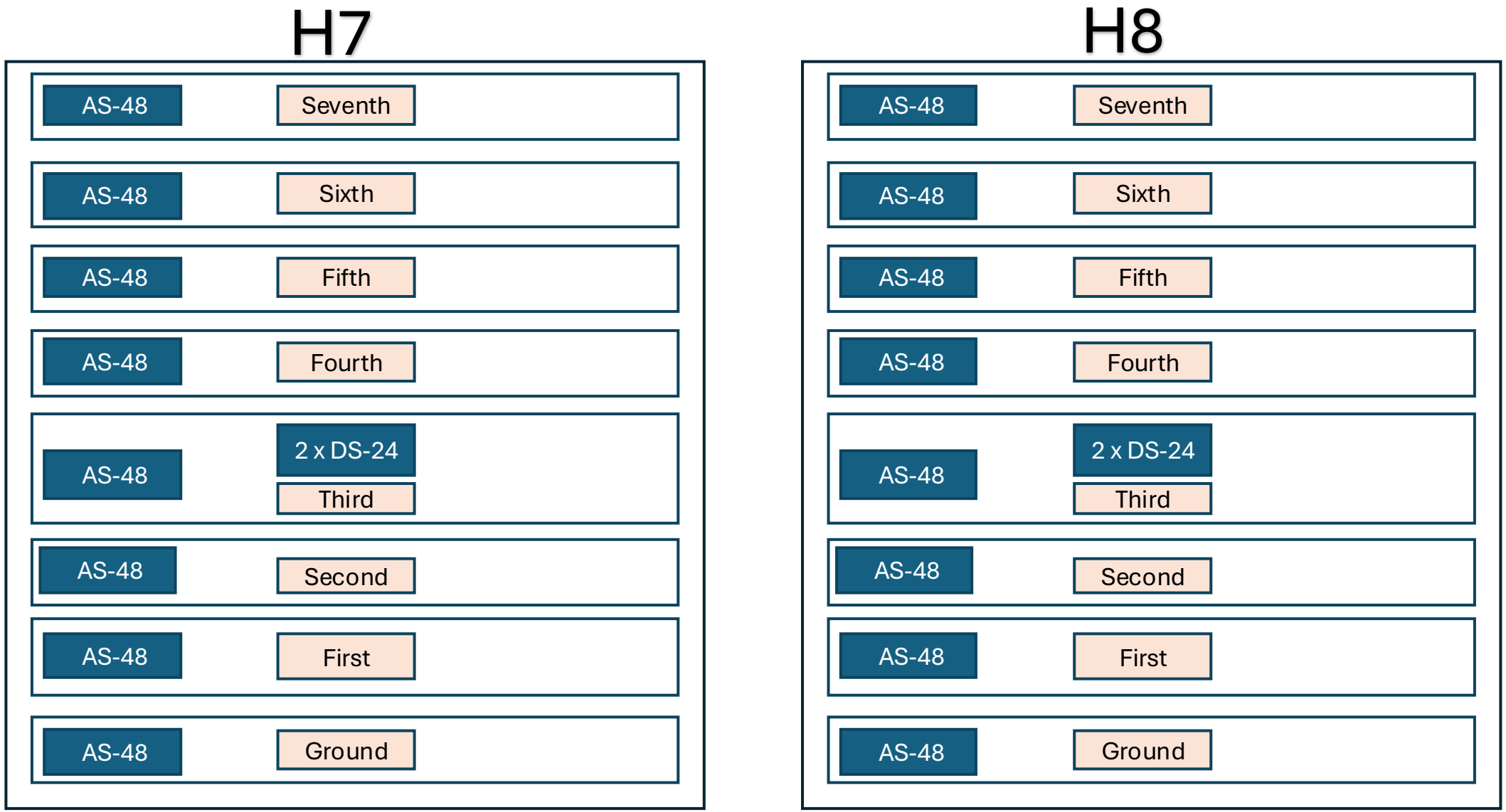
Student Hostels – Positioning of AS

Scope is to lay only the OFC cables 2 x 96C + 1 x 48C + 6x 12C + 6 x 24C, LIU & junction Boxes, and establish the LIU-to-LIU connectivity

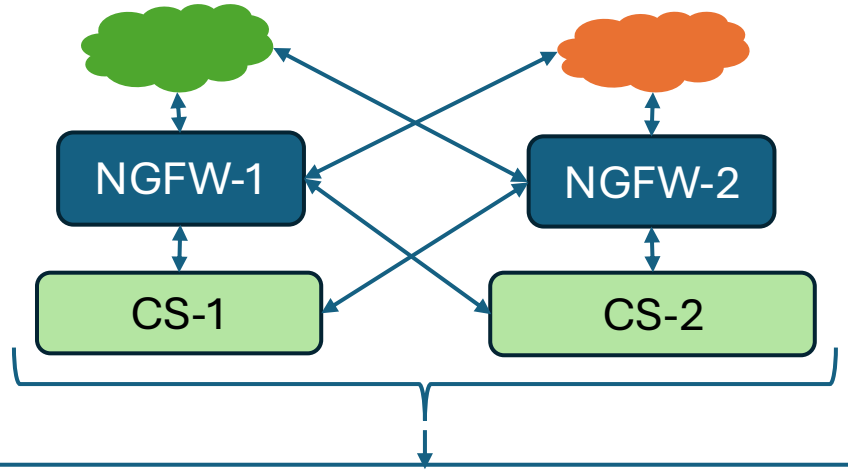


Student Hostels – Positioning of AS

Scope is to lay only the OFC cables 2 x 96C + 1 x 48C + 6x 12C + 6 x 24C, LIU & junction Boxes, and establish the LIU-to-LIU connectivity



Building wise - ISP-CS-DS-LAN



Total 2x6 DS for Wired
+
Total 2x4 DS for WiFi Feed

DS-1 (AB-1)	DS-1 (AB-2)	DS-1 (HSTL)	DS-1 (RES)	DS-1 (LHC)	DS-1 (ADMIN)	DS-1(RNI)	DS-1 (CAF-HC)	DS-1 (Informatics)
DS-2 (AB-1)	DS-2 (AB-2)	DS-2 (HSTL)	DS-2 (RES)	DS-2 (LHC)	DS-2 (ADMIN)	DS-2 (RNI)	DS-2 (CAF-HC)	DS-2 (Informatics)

AS	#
24 -10G	5
24-1G	18

CN	#
25G	10
10G	36

AS	#
24 -10G	5
24-1G	17

CN	#
25G	10
10G	34

HDS	#
24 -1G	0
24-10G	0

CN	#
25G	0
10G	0

AS	#
24 -1G	11
48-1G	4

CN	#
25G	0
10G	30

AS	#
24 -1G	2
24-1G	

CN	#
25G	0
10G	4

AS	#
24 -1G	10
24-10G	0

CN	#
25G	0
10G	20

AS	#
24 -1G	1
24-10G	0

CN	#
25G	0
10G	2

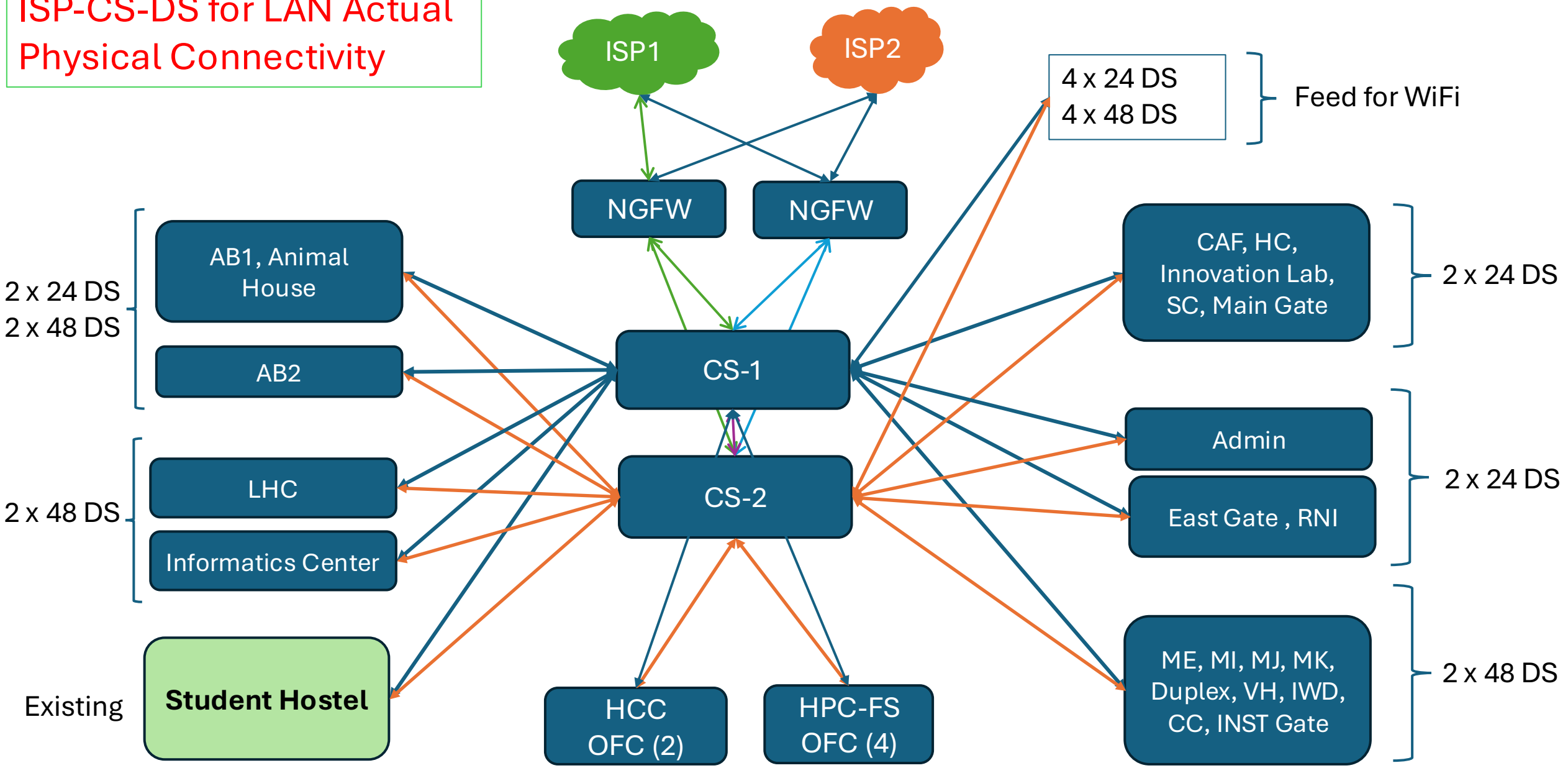
AS	#
24 -1G	7
24-10G	0

CN	#
25G	0
10G	14

AS	#
24 -1G	2
24-10G	2
48-1G	4

CN	#
25G	4
10G	12

ISP-CS-DS for LAN Actual Physical Connectivity



Building-wise Requirement

Building	#Floor	AS, Uplink fibre, downloading copper					Total AS	Patch Cord	Racks		
		8P-1G	16P-1G	24P-1G	48P-1G	24P-10G			6U	9U	12U
AB-1	5			17		5	22	88	5		11
AB-2	5			17		5	22	88	3		11
AB-3	Upcoming							0			
LHC	2			2			2	8	1		1
Informatics	8			10	5	2	17	68	2		12
CAF	2			2			2	8	1		3
Animal House	3		1				1	4	1	1	
ADMIN	3			10			10	40	2	1	7
IWD	2			1			1	4			3
VH	8				4		4	16		4	3

Building-wise Requirement

Building	#Floor	AS, Uplink fibre, downloading copper					Total AS	Patch Cord	Racks		
		8P-1G	16P-1G	24P-1G	48P-1G	24P-10G			6U	9U	12U
Duplex	10 Houses			1			1	4	1		1
MJ	7			2			2	8	1	1	3
MK	7			2			2	8	2	1	2
ME	7			2			2	8	2	1	2
MI	7			2			2	8	2	1	2

Building-wise Requirement

Building	#Floor	AS, Uplink fibre, downloading copper					Total AS	Patch Cord	Racks		
		8P-1G	16P-1G	24P-1G	48P-1G	24P-10G			6U	9U	12U
H1	Upcoming							0			
H2	Upcoming							0			
H3	8			8	8		16	64	4		8
H4	8			8	8		16	64	4		8
H5	8				8		8	32	2		8
H6	8				8		8	32	2		8
H7	8				8		8	32	2		8
H8	8				8		8	32	2		8

Building-wise Requirement

Building	#Floor	AS, Uplink fibre, downloading copper					Total AS	Patch Cord	Racks		
		8P-1G	16P-1G	24P-1G	48P-1G	24P-10G			6U	9U	12U
RNI								0			
HC	2			2			2	8			3
Innovation	2			1			1	4		1	
Sports Complex	1	1					1	4			2
Community Center	1	1					1	4			2
Main Gate	1		1				1	4	1		
East Gate	1	1					1	4	1		
INST-Gate	1	1					1	4	1		
NABI-Gate	1							0	1		
Total		**4**	**2**	**87**	**57**	**12**	**162**	**648**	**43**	**11**	**116**
Without Hostel		**4**	**2**	**71**	**9**	**12**	**98**	**392**	**27**	**11**	**68**

CS	DS		AS				
	24P	48P	8P-1G	16P-1G	24P-1G	48P-1G	24P-10G
2	10	10	4	2	71	9	12

AS, Uplink fibre, downloading copper				
8P-1G	16P-1G	24P-1G	48P-1G	24P-10G
4	2	71	9	12

Compatible DAC	Number
100G DAC Copper Cable - 1M	24
100G DAC Active Optical Cable - 1M	26
100G DAC Active Optical Cable - 5M	52
100G DAC Active Optical Cable - 10M	10
40G DAC Active Optical Cable - 5M	20
40G DAC Active Optical Cable - 10M	20

Compatible Transceiver		
10GBASE-LR SFPP SMF LC CONNECTOR (No TAA)	25GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF	40GBASE-LR4 QSFP+ optic (LC), for up to 10km over SMF
342	48	16

Group	Particulars	LIU24	LIU48
Group - 1	VH, IWD, Duplex, MI, ME, MJ, MK, DC		24
Group - 2	CAF, HC, Main Gate, Innovation LAB, SC		8
Group - 3	Admin	2	2
Group - 4	LHC	2	2
Group - 5	AB-1 and Animal House		8
Group - 6	AB-2		8
Group - 7	East Gate and RNI	2	2
Group -8	H3,H4,H5,H6,H7,H8		18
Group - 9	Informatics Center		2
	Total	6	74

Components for OFC Laying (In Meter)			
Type	Laying	Duct	Cable
96C	3254.8	3461.8	3470.8
48C	2062.03	2404.03	2437.03
24C	1871.95	2154.95	2165.95
12C	578.95	840.95	834.95
Total	7767.73	8861.73	8908.73