

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



**Stock Holding Corporation of India Limited
(StockHolding)**



RFP Reference Number: CPCM-47/2026-27

Date: 14-Oct-2026

GEM Reference No.: GEM/2026/B/8160662

**Request for Proposal for Implementation of Software Defined-Wide Area Network
(SDWAN) And Branch L2 Managed Switches**

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited (StockHolding), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by StockHolding to any parties other than the applicants who are qualified to submit the bids (“bidders”). The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. StockHolding makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. StockHolding may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP Document Details

Sr. No.	Description	Remarks
1	Name of Organization	Stock Holding Corporation of India Limited
2	RFP Reference Number	CPCM-47/2026-27
3	Requirement	RFP for Implementation of Software Defined-Wide Area Network (SDWAN) And Branch L2 Managed Switches
4	Interest free Earnest Money Deposit (EMD) [*]	₹34,00,000/- (Indian Rupees Thirty Four Lakhs only) by way of RTGS/NEFT/BG/FDR to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids on StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address. Bidders registered under Micro & Small Enterprises (MSE) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.
5	Email Id for correspondence	CPCM@stockholding.com
6	Date of Issue of RFP Document	14-Oct-2026
7	Date, Time and place for online Pre-bid meeting	23-Oct-2026 12:00 PM For participation in pre-bid meeting, please send mail for online meeting link to CPCM@stockholding.com before 22-Oct-2026 05:00 PM
8	Last Date for Submission of Pre bid queries	22-Oct-2026 05:00 PM
9	Last Date for Submission of Online Bid	04-Nov-2026 04:00 PM
10	Date of opening bid	05-Nov-2026 04:00 PM

This bid document is not transferable.

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Contents

RFP Document Details	3
SUBMISSION OF PROPOSAL	6
ELIGIBILITY CRITERIA (Documents to be Submitted Online)	8
Submission of Bids	10
Evaluation of Bids	10
REQUIREMENT	14
1. Introduction	14
2. Scope of Work	14
3. Current Architecture	14
4. Solution to be provided	16
5. Support	25
6. OEM / SI Support	25
7. FMS Support Activities	25
8. Documentation Deliverables	26
9. Buy-Back of Old Routers and Switches	26
10. Payment Milestones	26
11. Delivery Schedule and Timelines	27
12. Penalty Structure and Delivery Schedule	27
13. Service Level Agreement	28
14. Migration activities for change of location	30
15. Site Not Ready Clause	30
16. Contract Duration	31
17. Payment Terms	31
18. Other Terms	31
Refund of Earnest Money Deposit (EMD)	31
Performance Bank Guarantee (PBG)	31
Force Majeure	32
Dispute Resolution	32
Governing Law and Jurisdiction	32
Right to alter RFP	33
Integrity Pact	33
Sub-Contracting	33
Non-Disclosure Agreement (NDA)	33
Indemnify	33
Termination of contract for convenience	33
Termination Clause	33

Exit Management.....	34
Options Order Clause.....	34
Assignment.....	34
ANNEXURE - 1 - Details of Bidder's Profile	35
ANNEXURE - 2 – Eligibility Criteria	36
ANNEXURE - 3 – Technical Evaluation Criteria	38
ANNEXURE - 4 – Commercial Bid Format	40
ANNEXURE – 5 – Integrity Pact	43
ANNEXURE – 6 – Compliance Statement	49
ANNEXURE – 7– Format of Bank Guarantee	50
ANNEXURE – 8 – Format of Non-Disclosure Agreement.....	52
ANNEXURE - 9 – Branch List with Router and Switch Models.....	55
ANNEXURE - 10 – Technical Specifications for SD-WAN and Switches.....	82

SUBMISSION OF PROPOSAL

StockHolding invites e-tenders via the GeM Portal in two bid system (Technical and Commercial bid), from firm/company/organisation with demonstrable experience, acquired within the last five (05) years, in the supply and implementation of SD-WAN solutions, along with the supply and installation of Layer 2 (L2) Managed Switches.

Submission of Bids:

The online bids will have to be submitted within the time specified on website <https://gem.gov.in/> the following manner:-

1. Eligibility/Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:

This “Invitation for bid” is for provision of implementation of Software Defined-Wide Area Network (SDWAN) solution and Branch L2 managed Switches at StockHolding as per the terms, conditions, and specifications indicated in this RFP and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.

Due Diligence:

The bidder is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the bidder’s risk and may result in rejection of the bid and the decision of StockHolding in this regard will be final and conclusive and binding.

Cost of Bidding:

The bidder shall bear all costs associated with the preparation & submission of its bid and StockHolding will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Contents of this RFP Document:

The requirements, bidding procedure, general terms & conditions are prescribed in this RFP document with various sections

- a Bidder Details – Annexure 1
- b Format for Eligibility Criteria - Annexure 2
- c Format for Technical Evaluation Criteria – Annexure 3
- d Format for Commercial Bids - Annexure 4
- e Integrity Pact (Text) - Annexure 5
- f Compliance Statement – Annexure 6
- g Format of Bank Guarantee – Annexure 7
- h Format of Non-Disclosure Agreement (NDA) – Annexure 8
- i Branch List with Router and Switch Models – Annexure 9
- j Technical Specifications for SD-WAN & Switches – Annexure 10

Clarifications regarding RFP Document:

- a Before bidding, the bidders are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to StockHolding for necessary clarifications.
- b A bidder requiring any clarification for their queries on this RFP may obtain such clarifications via email to CPCM@stockholding.com
- c StockHolding shall not be responsible for any external agency delays.
- d StockHolding reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
- e At any time before the deadline for submission of bids / offers, StockHolding may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.
- f StockHolding reserves the right to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on StockHolding.
- g StockHolding reserves the right to amend / cancel / postpone / pre-pone the RFP without assigning any reasons.
- h It may be noted that notice regarding corrigendum's/addendums/amendments/response to bidder's queries etc., will be published on StockHolding's website only. Prospective bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.

Validity of offer:

The offer should remain valid for a period of at least **90 days** from the date of submission

ELIGIBILITY CRITERIA (Documents to be Submitted Online)

Guidelines to be followed prior to applying-

Bidder should upload all supporting documents at the time of submission duly signed and stamped on their company's letter head.

Sr. No.	Criteria	Documents to be submitted by Bidder
1	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 or LLP with experience in implementation of SDWAN solution within the past 5 years.	Copy of Certificate of Incorporation issued by the Registrar of Companies or Partnership Deed and Self-declaration by the bidder for experience on its' Letter Head duly signed by the Authorized Signatory.
2	The Bidder / OEM should have supplied and implemented atleast One SD-WAN solution in BFSI Sector with minimum 210 branches (both for SD-WAN software & underlying Hardware) which OEM / Bidder is offering to Stockholding in the past 3 years as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email
3	The bidder must have supplied and installed a minimum of 200 L2 Managed Switches under a single contract within at least one (1) BFSI industry during the past three years in India, as of the RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email
4	Bidder should have an average annual turnover of at least ₹68 crores per annum for last three audited financial years (2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover or Balance Sheet for last three financial years.
5	Bidder should have Positive Net worth of at least ₹8 crores for all the last 03 (three) audited financial years i.e. 2022-23, 2023-24 and 2024-25.	Certificate from CA mentioning networth or Balance Sheet for last three financial years.
6	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
7	The bidder, in case of SI, should be OEM certified or authorized agent/reseller/partner of the OEM.	If the bidder is the OEM, a self-declaration must be provided confirming that the bidder is the original equipment manufacturer of the proposed solution; In case the bidder is not OEM of the offered solution, then a certificate from OEM certifying that Bidder is authorized partner of the OEM.

8	The proposed SD WAN solution and appliances of Branch/DC/DR quoted i.e. should be compatible with other OEM devices (e.g. Switches)	Self-declaration from bidder on letterhead duly signed by authorized signatory
9	Bidder must ensure that the equipment to be supplied will not reach End-of-Sale or End-of-Life status within the next 3 years and End of Support in next 7 years. In case proposed product goes end of support during contract period, then bidder will provide devices of equivalent or higher configuration approved by Stockholding.	Self-declaration from bidder on letterhead duly signed by authorized signatory
10	The bidder should have service/ support infra- structure at Mumbai MMR and should be able to provide efficient and effective support.	Office details along with escalation matrix to be submitted
11	The bidder must have qualified / certified / trained professionals in the proposed OEM's SDWAN solution on the payroll of the bidder as on RFP date.	• CVs or Resumes of proposed resources / Relevant certification copies • Self-declaration that proposed resources are on bidder's payroll
12	The Bidder of the proposed solution should be ISO 27001, 14001 and ISO 9001 certified.	Relevant Valid certificates to be submitted
13	The Bidder to submit signed & stamped Integrity Pact as per Annexure- 5	Self-declaration from bidder duly signed by authorized signatory

BIDS PREPARATION AND SUBMISSION DETAILS

The online bids will have to be submitted within the time specified on website <https://gem.gov.in/>. Bidders must familiarize (if not already) with the Portal and check/ fulfil the pre-requisites to access and submit the bid there.

Submission of Bids

- 1) The required documents for Eligibility Criteria, Commercial Bid must be submitted (uploaded) online on GeM portal. Eligibility Criteria and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document
- 2) The offer should be valid for a period of at least **90 days** from the date of submission of bid.
- 3) The Bidder shall fulfil all statutory requirements as described by the law and Government notices. The Bidder shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify StockHolding against all such liabilities, which are likely to arise out of the agency's failure to fulfil such statutory obligations.
- 4) The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP document(s). Failure to furnish all information required as mentioned in the RFP document(s) or submission of a proposal not substantially responsive to the RFP document(s) in every respect will be at the bidder's risk and may result in rejection of the proposal.
- 5) Delayed and/or incomplete bid shall not be considered.
- 6) There may not be any extension(s) to the last date of online submission of Eligibility Criteria details and commercial Price bids. This will be at the sole discretion of StockHolding.

Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. The eligibility bid submitted by the Bidder will be evaluated against the Eligibility criteria set forth in the RFP. The Bidder needs to comply with all the eligibility criteria mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of StockHolding would be final and binding on all the bidders to this document.

StockHolding may accept or reject an offer without assigning any reason what so ever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of StockHolding.

- a) Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.
- b) The information provided by the bidders in response to this RFP document will become the property of StockHolding.

Evaluation Process

First the 'Eligibility Criteria bid document' will be evaluated and only those bidders who qualify the requirements will be eligible for 'Technical bid'. In the second stage, for only those bidders who meets the 'Eligibility Criteria', technical bids will be evaluated, and a technical score would be arrived at. In third stage, only those bidders, who have qualified in the technical evaluation, shall be invited for commercial evaluation. The final price (L1) will be decided only on successful completion of the Online Reverse Auction for technically qualified bidders.

Eligibility Criteria Evaluation (Stage 1)

The bidder meeting the Eligibility Criteria as per **Annexure 2** will be considered for Technical

evaluation. Any credential/supporting detail mentioned in “**Annexure 2 – Eligibility Criteria**” and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

Technical Bid Evaluation (Stage 2)

The Technical bids of only those bidders shall be evaluated who have satisfied the eligibility criteria bid. StockHolding may seek clarifications from the any or each bidder as a part of technical evaluation requirements as mentioned in **Annexure 3**. All clarifications received by within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the StockHolding.

The proposal submitted by the bidders shall, therefore, be evaluated on the following criteria:

Sr. No.	Criteria	Supporting Documentation	Technical Score Matrix	Max Marks
A. Experience, Turnover & Resource Strength (70 Marks)				
1	The Bidder having an average annual turnover of at least ₹68 Crores per annum for all the last 03 (three) audited financial years i.e. 2022-23, 2023-24 and 2024-25. It should be of individual company and not of Group of Companies	A Certificate duly certified by the statutory auditor of the Bidder clearly mentioning the annual turnover of the bidder.	a) INR 68 Crores to INR 80 Crores: 12 Marks b) More than INR 80 Crores and less than INR 100 Crores: 15 Marks c) More than INR 100 Crores and less than INR 120 crores: 18 Marks d) More than INR 120 crores: 20 Marks	20 Marks
2	The Bidder / OEM should have supplied and implemented SD-WAN solution in BFSI Sector with minimum 210 branches (both for SD-WAN software & underlying Hardware) which OEM / Bidder is offering to Stockholding in the past 3 years as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email	a) 1 - 2 projects: 12 Marks b) 3 - 4 projects: 15 Marks c) More than 4 projects: 20 Marks	20 Marks
3	The bidder has supplied and installed a minimum of 200 L2 Managed Switches under a single contract within at least one (1) BFSI industry during the last three (3) years in India as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email	a) 1 - 2 projects: 12 Marks b) 3 - 4 projects: 15 Marks c) More than 4 projects: 20 Marks	20 Marks
	The bidder must have qualified / certified / trained	Self-Certificate on the letterhead of the bidder	a) 2 - 5 resources: 6 Marks	10 Marks

4	professionals in the proposed OEM's SDWAN solution on the payroll of the bidder as on RFP date.	signed by Authorized signatory with details of Relevant certifications and resource profiles to be submitted.	b) 5 - 8 resources: 8 Marks c) More than 8 resources: 10 Marks	
B. Technical Presentation (30 Marks)				
5	Bidder's capabilities in terms of solution expertise and experience in implementation related to project.	Technical Presentation delivered by Bidder	Following parameters will be considered for the evaluation: 1) Understanding of the project and StockHolding's requirement – 5 marks 2) Proposed SDWAN solution, its components and technologies used – 7 marks 3) Implementation approach, Project Timelines and Migration plan – 8 marks 4) Team Deployment Plan – 5 marks 5) SLA Management – 5 marks	30 Marks
Total Score				100 Marks

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- StockHolding shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks.
- The bidder to submit appropriate credentials [other than self- certification] in respect of each of the item.
- Technical proposals will be evaluated based on the total marks obtained across all technical evaluation criteria. Only those bidders who achieve a minimum cumulative score of 60 marks in the technical evaluation will qualify for the commercial bid evaluation.

Commercial Bid Evaluation (Stage 3)

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened.

Online Reverse Auction

The Bidder Whose Price Bid has not been rejected / disqualified by StockHolding will be asked to participate in the Reverse Auction, which will be conducted for determining the L1 bidder. The L-1 bidder will be determined on the basis of the lowest price quoted / offered in the Reverse Auction.

StockHolding may accept or reject the offer without assigning any reason what so ever at any stage of bid evaluation.

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

REQUIREMENT

1. Introduction

Stockholding, a subsidiary of IFCI Limited was promoted by the public financial institutions and incorporated as a public limited company on July 28, 1986. Stockholding is a Government Organization, being a subsidiary of IFCI. Stockholding, one of the largest Depository Participants (DP) and also largest premier Custodian in terms of assets under custody, provides post trading and custodial services to institutional investors, mutual funds, banks, insurance companies, etc. Stockholding acts as a Central Record Keeping Agency (CRA) for collection of stamp duty in 21 States and Union Territories on pan India basis. Stockholding is one of the largest Professional Clearing Members of the country. Stockholding has its registered office at Mumbai, main operations office at Navi Mumbai and operates through its over 200+ retail branches all over India.

2. Scope of Work

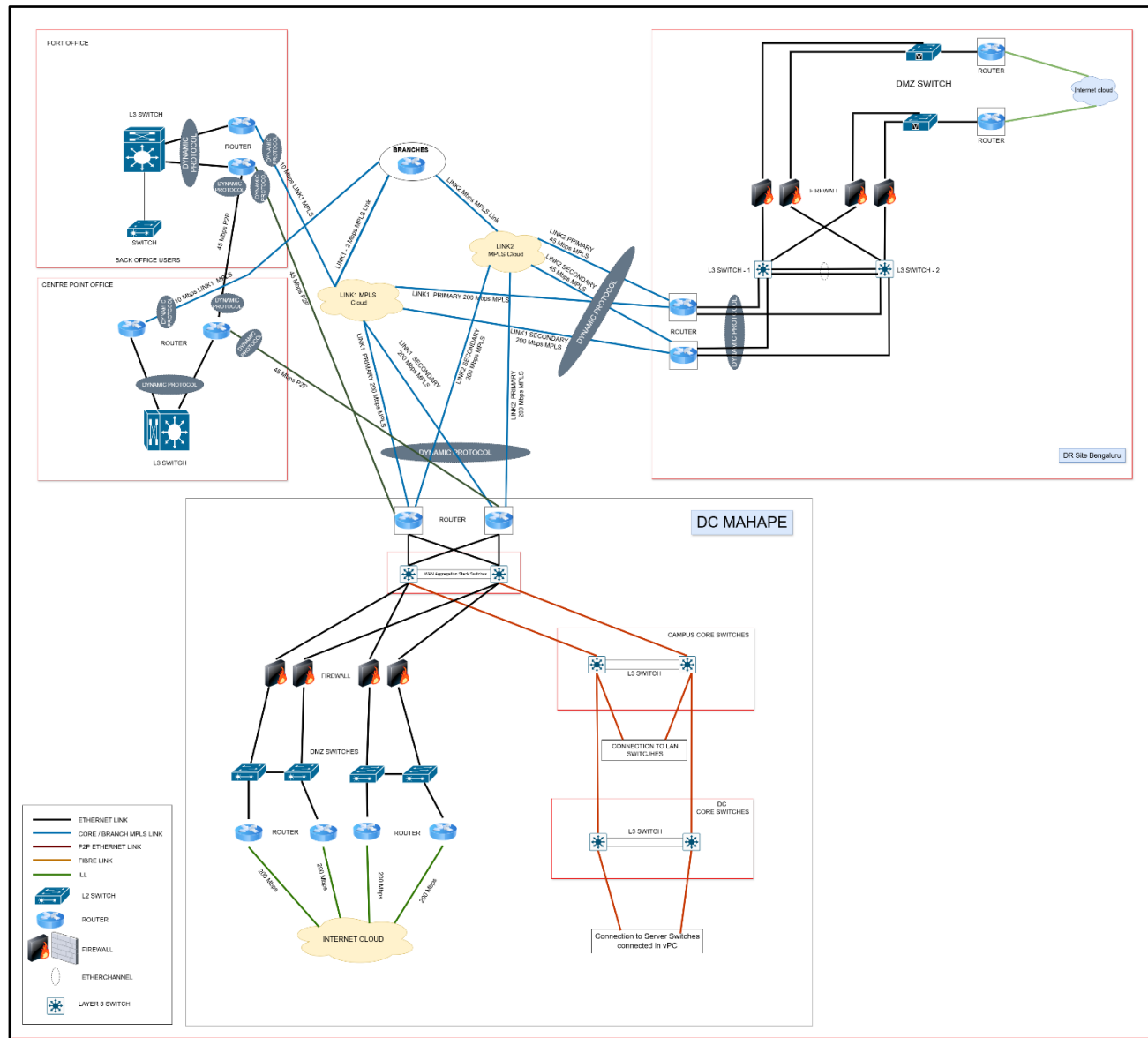
Stockholding proposes to deploy software defined wide area network (SD WAN) for its Data Center, Disaster Recovery Site (Colocation) and its branch offices across India. Apart from SD-WAN implementation, Stockholding also proposes to replace Branch switches across all its branch offices in India. The bidder is required to integrate the existing MPLS, ILL and local broadband lines at all the locations into the SD WAN solution in conformity with the technical specifications (Annexure 10 – Technical Specifications).

3. Current Architecture

- 1) **MPLS Connectivity** – Presently, Head Offices/DR/Branches of Stockholding are connected through a MPLS (WAN) provided by BSNL and Tata Communications (TCL) (Alternate). BSNL is the primary service provider for Stockholding while the secondary link is being managed by TCL. The secondary link may or may not be via MPLS Link. Branch Offices on MPLS to Main DC are connected via 2 Mbps bandwidth.
- 2) **Local Broadband Connectivity** – Since primary link of all branches connected to DC/DR is via MPLS link, many branch offices are also having broadband connections as secondary link.
- 3) **Internet Connectivity and Traffic Management:** To enable branch internet and application access at each Branch Office, the traffic routes to DC site through DC firewall and proxy via MPLS Link. Traffic for Internal applications accessed over WAN are also routed to DC via MPLS link.
- 4) **CISCO Internet Routers** – Currently, HO Data Centre is having CISCO 3945 Internet Routers (4 in DC Site and 2 in DR Site) where both primary and secondary internet links terminate. Both DC and DR Sites are in HA Configuration (1+1). At DC Site, there are 2 routers one for each line of business in HA Mode.
- 5) **CISCO WAN Routers** – Currently, HO Data Centre is having CISCO 4451 WAN Routers (2 in DC Site and 2 in DR Site). This is specifically for LAN traffic between branches and Data Centre. For Branches to connect to internet, the traffic is routed via branch routers and MPLS link to the WAN router, basis which access is given via proxy. To access LAN based applications, the traffic is routed via branch routers and MPLS link to the WAN router. Both DC and DR Sites are in HA Configuration (1+1).

- 6) **Branch Routers** – Currently, branches are having Routers as mentioned in Annexure 9 – Branch List with Router and Switch Models. Each branch has a single router commissioned.
- 7) **Branch Switches** – Currently, branches are having Switches models as mentioned in Annexure 9 – Branch List with Router and Switch Models. There are certain branches where multiple switches are commissioned.

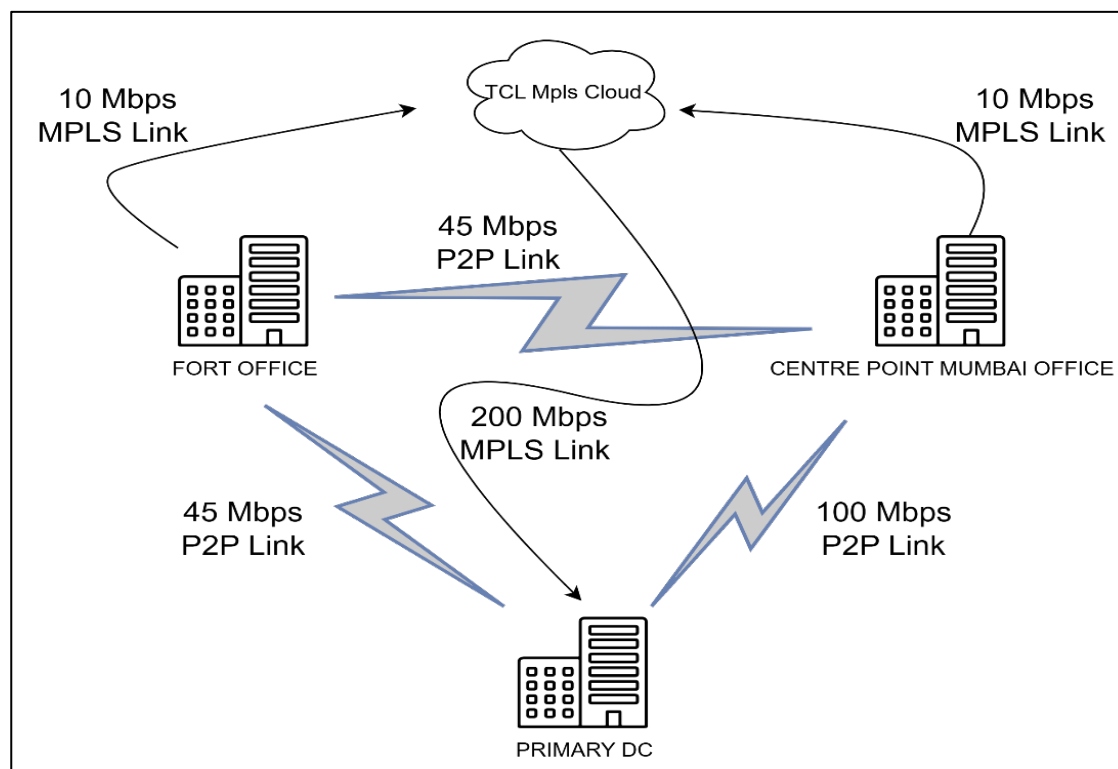
Diagram 1 - The detailed HO/Branch Office network is given below:



- 8) **Centre Point and Fort Offices** – These 2 offices i.e. Centre Point and Fort (both located in Mumbai) are considered critical offices and not considered as a regular branch. Centre point hosts close to 100 employees and Fort Office hosts close to 40 employees and also considered as a small DR site for extranet links.

Centre Point Office have CISCO 3945 routers (2 devices in HA mode) and CISCO 2921 and 2821 in Fort Office (in HA mode). These edge routers will have to be replaced as part of SD-WAN implementation. However, the switches are not required to be replaced.

Diagram 2 – Network connectivity between DC, Centre Point and Fort Office is depicted below:



9) Employee strength across offices

Location	Approximate Employee Count	Remarks
Branch	5	-
Regional Office	15	To be considered as Branch
Fort Office – Mumbai	40	-
Centre Point – Mumbai	100	-
Mahape – Navi Mumbai DC Site	1000	-
Bengaluru DR site	5	Co-located DR Site with 5 personnel seating capacity

4. Solution to be provided

The SD WAN solution should replace the existing routers and L2 managed switches by the edge devices proposed in this bid. However, the Perimeter Firewall at the DC and the DR site would remain.

1) Below is the minimum configuration expected –

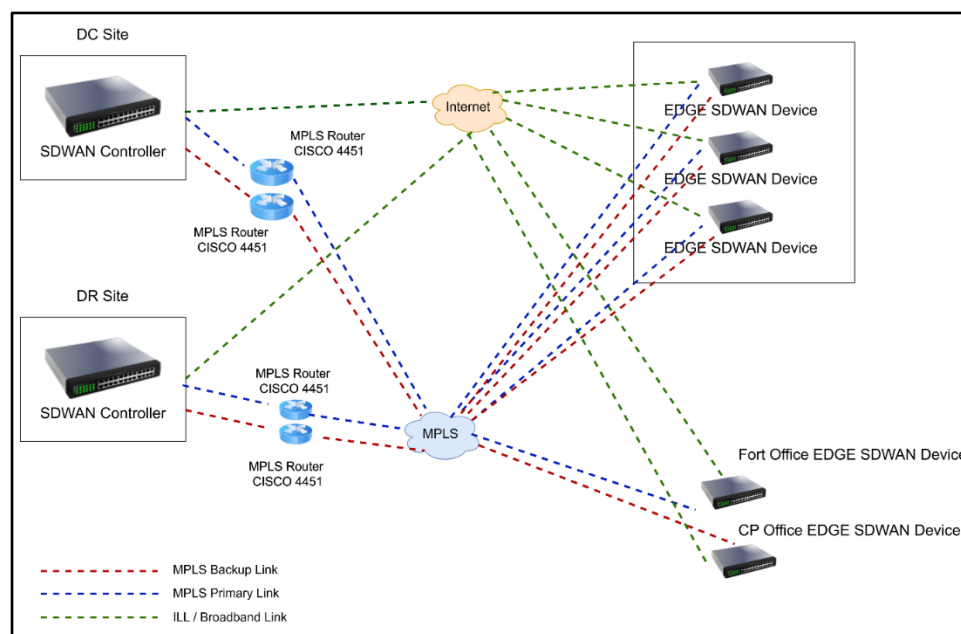
Location	Device Type	Minimum Required Device Specifications
Primary DC Site	SD-WAN Controller / Router in HA Mode	4 x 1/10 Gb port + 2 x 1Gb SFP + 2 x 10 GbE SPF+ (Any port can be configured as LAN/WAN/DMZ/MGMT or custom port) + 1 management port + 1 console port + 1 USB
DR Site		

		Port.
Branch Office	SD-WAN enabled Routers	5 x GE RJ45 ports (Any port can be configured as LAN/WAN/DMZ/MGMT or custom port). + 1 x USB and 1 x Console Port (RJ45)
Fort Office	SD-WAN enabled Routers in HA Mode	4 x 1 GE ports + 4 x 1/10GE (Any port can be configured as LAN/WAN/DMZ/MGMT or custom port) + 1 x USB and 1 x Console Port (RJ45)
Centre Point Office	SD-WAN enabled Routers in HA Mode	4 x 1 GE ports + 4 x 1/10GE (Any port can be configured as LAN/WAN/DMZ/MGMT or custom port) + 1 x USB and 1 x Console Port (RJ45)
Branch Office	L2 Network Switch	Layer 2 managed Switch at branches and in stack/MCLAG/cascade mode for certain branch offices – 24 port stackable/cascadable wherever required.

2) Broad Scope of Work includes the following –

a. Expected Network Diagram using SDWAN Technology

Diagram 3



b. SD-WAN Architecture

- 1) Delivery, Installation and commissioning of SD WAN solution along with SD-WAN enabled Routers on High Availability at each site (DC and DR Locations) on locations listed in Appendix W Annexure 9 – Branch List with Router and Switch Models in full High Availability (HA) configuration and subsequently.
- 2) The bidder shall study and understand the existing setup at Branches, Data Centre, DR site, NDR Site and prepare detailed implementation plan for integration. The bidder shall ensure that integration should be seamless and within stipulated timelines.
- 3) The number of locations may increase or decrease over the time. The solution/technology services will be required to be further extended to increased number of branches/offices across the country with the same rates and terms and

conditions in phased manner.

- 4) It is to be noted that there should be one single centralized management console for SDWAN solution irrespective of number of controllers, orchestrator/manager, analytics, or any other Head end devices installed to match Stockholding's scalability requirement. Further the existing setup (Devices/Servers/LAN/WAN/monitoring tools) should be able to manage using same centralized console with offering all required features including but not limited to Zero Touch Provisioning, Centralized updates, Patch and configuration management.
- 5) In case Stockholding opts to implement Full Mesh/partial mesh topology, all the communication between branches should be through encrypted IPsec Tunnels. It is also to be noted that all such tunnels should be formed dynamically without any kind manual intervention/configuration.
- 6) Bidder has to ensure that the Diagrams depicted in Diagram 2 is maintained at any point in time.
- 7) Bidder has to ensure that the proposed solution is as per Diagram 3 at any point in time.
- 8) Bidder shall supply the brand-new and genuine equipment's procured through this RFP at the Stockholding Locations as per the delivery schedule.
- 9) The proposed SD-WAN solution should be able to create dynamic VPN Tunnels In between Edge devices and the DC and DR so that the various applications of Stockholding can use the channel to other services to the beneficiaries of Stockholding and also for the day to day office tasks.
- 10) Bidder shall unpack and perform physical verification of the supplied equipment.
- 11) The bidder shall do the required passive cabling between the routers, existing network devices, racks and necessary arrangements for cage nuts, clamps etc. to make the proposed solution workable. Bidder shall also do the necessary labelling, dressing and tagging of power cables, Ethernet, Fiber Cables within the racks and inter-rack. The bidder shall perform the POST (Power ON Self-Test) for all supplied equipment's.
- 12) Any other miscellaneous/ major infrastructure upgrades requirements or extra work required to be performed due to existing hardware/software/structure limitation shall be provided by the successful bidder at no extra cost to Stockholding even if those items are not mentioned explicitly in this RFP related to the scope described in the RFP. Stockholding will not accept any plea of the Bidder at a later date for omission of services on the pretext that the same was not explicitly mentioned in the RFP.
- 13) Bidder shall provide all the power cords of proposed devices/ equipment's which are compatible with Indian sockets.
- 14) The selected bidder shall manage all the existing devices until replacement, without any additional cost to the Stockholding and arrange to provide equivalent or next higher version of the same device in case of device failure/faulty.
- 15) SD-WAN solution is to be implemented using Zero Trust Model. The thrust of the Zero Trust security approach is to stop trusting applications, users, networking devices, network by default and to implement continuous verification.
- 16) The SD-WAN solution should be capable of utilizing the links in following scenarios.
 - i. MPLS+MPLS
 - ii. MPLS+ILL
 - iii. MPLS + Broadband Internet
 - iv. ILL + Broadband Internet
 - v. Broadband Internet + Broadband Internet
 - vi. MPLS/ILL/ Broadband Internet link without backup.
 - vii. Only single Broadband Internet link
- 17) Existing WAN Routers both at DC and DR will continue as it is and shall not be

replaced. However, the proposed SD-WAN solution should be able to monitor the existing WAN routers as well.

- 18) The SD-WAN Solution provided by the successful bidder should be horizontally scalable. Scalability of the solution should be ensured through proper provisioning. The SDWAN device should have the required number of ports and throughput for commissioning the above-mentioned lines on the edge device.
- 19) The bidder has to ensure that the provisioning of the requisite hardware pertaining to the SDWAN solution considers future growth of 30% during the contract period.
- 20) The bidder should propose the architecture at the time of technical bid submission which must be vetted by OEM with high availability at all levels and redundancy in case DC fails and during DR drills as well. The same would also need approval from Stockholding IT team and any queries raised regarding architecture or traffic flow is to be clarified to Stockholding IT.
- 21) The proposed SD-WAN solution should have the capability to allow automatic/dynamic (without any manual configuration) encrypted IPSEC tunnels creation between branches (including branch offices, DC/DR) devices to enable branch to branch communication.
- 22) The devices (e.g. Switches), if required, for terminating the MPLS/ ILL/ Broadband connections onto the SDWAN devices and configuring it in HA has to be the part of the solution.
- 23) Successful bidder has to provide all components as part of the solution to implement the project successfully. All such components, if any, should be included in the bill of materials.
- 24) The SD-WAN Solution must be SASE Ready (universal/unified) for adoption by Stockholding as and when required during the course of contract without any change in CPE Hardware.
- 25) The SD-WAN equipment's should be supplied with Indian standard power cable. DC and DR devices should be supplied with redundant power supply and branch device should be supplied with single power supply.
- 26) SD-WAN Solution must be implemented in such a way that, incoming and outgoing traffic will be load balanced automatically across the network links at branches even in case primary link is not fully utilized. Traffic should be sent across network links even when link is not congested.
- 27) All proposed SD-WAN devices must be IPv6 Ready Logo Certified (from IPv6 Forum) and compliant with Government of India TEC/MTCTE certification requirements, including mandatory IPv6 support as per DoT guidelines.
- 28) The equipment's/applications used in DC/DR and critical locations should support high availability and redundancy at all levels from day 1. Locations such as DC & DR, Centre Point Office and Fort Office should always be in HA to avoid downtime. In case of primary device failure, the secondary appliance should take over the role of primary device without any downtime. For other locations where, single device will be installed, in case of failure of primary device, the same should be resolved/ replaced and should be in working condition within 1 day's downtime. The standby appliance should support immediate manual failover which can be used for troubleshooting/upgrades etc.
- 29) All the hardware supplied should be appliance based, RACK mountable and should be from the same OEM and must be supplied with all related accessories, power cables, mounting kit etc.
- 30) The proposed SD-WAN solution should support management via CLI, Web GUI administration interface and should support integration with various network management tools.
- 31) Bidder/OEM will be totally responsible for configuration, migration, installation, and best practices implementation at Stockholding's all locations including DC/DR.

- 32) Bidder/ OEMs should have service/ support infrastructure at across India and should be able to provide efficient and effective support PAN India.
- 33) All modules, licenses, power cables, ethernet/ fiber cable and all other sub-components should be bundled/mapped with parent device and warranty of these items should be co-terminus with warranty of parent devices.
- 34) The box should support integration with SOC monitoring tools, Antivirus, NAC solution, NMS etc. The box should also support for SASE using a single dashboard for SDWAN.
- 35) Application optimization shall be provided by the vendor for all the locations controlled centrally.
- 36) Security Features: The Branch edge device must have the following full featured firewall features:
 - i. IPS and IDS
 - ii. URL filtering
 - iii. Malware detection
 - iv. DDOS protection
 - v. Advanced Threat Prevention
 - vi. TLS/SSL decryption for HTTPS inspection
- 37) Centralized Management, Monitoring and Configuration: A central controller shall be provided, deployed & managed by successful bidder at Stockholding Data Center and at DR Site. The solution should provide for High Availability by leveraging the DC/DR Controller. All other Specifications in the technical evaluation document shall be applicable. The bidder shall ensure strict separation of management & control planes as a separate physical or virtual instance and data as separate instance to eliminate single points of failure.
- 38) Considering the CISCO 3945 routers (both at DC and DR site) for ILL also needs to be replaced, the BOQ proposed by the bidder should have the architecture solution encompassing either replacement of CISCO 3945 (both at DC and DR site) routers else the proposed solution should be sufficient enough to replace the CISCO 3945 without any additional hardware.
- 39) Stockholding also intends to commission 2 additional ILL links (Primary and Secondary) at DR Site to mirror DC Site. The entire solution should ensure that the additional 2 ILL Links (Primary and Secondary) at DR Site is accommodated without any new hardware deployment in the future.
- 40) Proposed BOQ by the bidder should have identical models and same count for both DC and DR site for SD-WAN solution. This is required so that if the DC site is shut down for whatever reasons, the DR Site should be fully functional without any change in the architecture. Branch Routers is not required in HA mode.

c. Existing Components replacement

Below are the components which shall be replaced in the proposed Solution:

Location	Needs Replacement	Remarks
Branch – Routers	Yes	Replace with SDWAN routers
Branch – Switches	Yes	Replace with new Switches
Regional Office – Routers	Yes	Replace with SDWAN routers
Regional Office – Switches	Yes	Replace with new Switches
Fort Office – Mumbai: ILL Router model # CISCO 2921 and 2821	Yes	Replace with SDWAN routers
Fort Office – Mumbai: Switches	No	-
Centre Point – Mumbai: ILL Router model # CISCO 3945	Yes	Replace with SDWAN routers

Centre Point – Mumbai: Switches	No	-
Mahape – Navi Mumbai DC Site – ILL Routers model # CISCO 3945	Yes	Replace with routers or part of the SDWAN DC controller appliance
Mahape – Navi Mumbai DC Site: Switches	No	-
Bengaluru DR site– ILL Routers model # CISCO 3945 and additional 2 routers to be onboarded for establishing 2 links	Yes	Replace with routers or part of the SDWAN DC controller appliance
Bengaluru DR site: Switches	No	-
Mahape – Navi Mumbai DC Site: WAN Routers model # CISCO 4451	No	-
Bengaluru DR site: WAN Routers model # CISCO 4451	No	-

Clarification: Bidder has to ensure that the proposed solution is seamlessly integrated with the components which do not need replacement.

d. Components under High Availability

Location	Needs HA at every site
Branch – Routers	NO
Branch – Switches	NO
Regional Office – Routers	NO
Regional Office – Switches	NO
Fort Office – Mumbai: ILL Router model # CISCO 2921 and 2821	YES
Centre Point – Mumbai: ILL Router model # CISCO 3945	YES
Mahape – Navi Mumbai DC Site – ILL Routers model # CISCO 3945	YES
Bengaluru DR site– ILL Routers model # CISCO 3945	YES
Mahape – Navi Mumbai DC Site: Management Appliance	NO
Mahape – Navi Mumbai DC Site: Reporting and Analytics Appliance	NO
Bengaluru DR site: Management Appliance (Incase DC Management Appliance is down, it should be managed from DR Management Appliance)	NO
Bengaluru DR site: Reporting and Analytics Appliance	NO

e. Branch Network Switches replacement

- 1) The bidder shall supply and install Layer-2 managed switches at branch/office locations. The switches must be fully compatible with, and seamlessly interoperable with, the proposed SD-WAN platform, supporting:
 - i. VLAN tagging and segmentation for SD-WAN traffic policies.
 - ii. Integration with SD-WAN CPE for routing and policy enforcement.
 - iii. Centralized configuration and monitoring (either via SD-WAN controller integration or standard management protocols such as SNMP, NETCONF, or equivalent).
- 2) The selected bidder will be responsible for supplying the required and configuring of switches.

- 3) It is crucial that the configuration includes testing the failover with crisscross connectivity to ensure seamless operation
- 4) The L2 managed network switches should come with the required licenses applicable for the entire contract period.
- 5) The Bidder/OEM can propose a single management console for both SD-WAN CPE's and Switches or separate consoles.
- 6) L2 Managed Switches can be of any OEM as compared to SD-WAN solution.
- 7) The bidder may propose a single Customer Premises Equipment (CPE) at the branch site capable of delivering both SD-WAN/routing functionalities and LAN switching functionalities. The bidder must clearly indicate if the proposed single-box solution meets both routing and switching requirements and specify any limitations compared to deploying separate router and switch devices.
- 8) For certain branch locations, there is a requirement of multiple switches to be placed in stack/MCLAG/cascade mode. The list of branches along with the count of switches for each location is mentioned in Annexure 9 – Branch List with Router and Switch Models.
- 9) Branch Network Switches is not required in HA mode.

f. Implementation

- 1) Setting up system as per SLA & Technical Specification given in Annexure 10 – Technical Specifications
- 2) Training (5 days) on operations and management of the SD WAN solution for five officials.

g. Operations and Maintenance Services

- 1) Should have Onsite Support for first 6 months after the implementation of the project for Working Days (Monday to Friday) in working Hours (9AM to 6PM) facilities to raise tickets, Coordination and customer support. Thereafter, there should be 24 X 7 facilities to raise tickets and customer support on Remote.
- 2) Bidder is also required to provide skilled resources that may be required for the successful completion of the project within stipulated timelines given in the RFP. The bidder should appoint and depute a dedicated Project Manager for the deployment of devices and providing support services who will act as a Single Point of Contact (SPOC) for the company. He shall be responsible for proper co-ordination with respective SPOC at each site for proper delivery, installation, and commissioning of the devices at locations mentioned in the PO.
- 3) Escalation matrix along with contact details to be provided within 15 days of commissioning the connectivity.
- 4) Should provide online performance monitoring reporting to Stockholding indicating bandwidth utilization, network latency, packet loss, jitter, link availability parameters as per SLA (Service Level Agreement).
- 5) Bidder will be responsible to provide the following to meet the Service Levels defined in this RFP till the Contract period.
 - i. Onsite comprehensive warranty
 - ii. AMC/ATS/subscription.
 - iii. Arrange back-to-back support from the respective OEM.
In Case of RMA, it is bidders' responsibility to replace the equipment as per SLA and to return the faulty equipment to the OEM warehouse at no extra cost to the Company during the tenure of the contract.
- 6) All network components of the SD-WAN (Hardware/Software) and Switches solution should be supported by same OEM during the tenure of contract.
- 7) Bidder should also take adequate care to avoid quoting network equipment going End-of-Sale within 1 year of date of supply of the equipment to the Company and network equipment going End-of-Support during the tenure of the contract.

- 8) Bidder should ensure that proposed network equipment should not go end-of-support within 5 years from the date of the Purchase Order. Bidder should produce an Authorization Letter in favor of Stockholding with reference to this RFP assuring full guarantee and warranty obligations for a MINIMUM period of Five years from the date of PO released.
- 9) The OEM/SI should provide onsite resources for smooth implementation, commissioning, and onboarding of locations to SD-WAN and Switches at no extra cost to the Company. If any major issue related to SD-WAN and Switches deployment arises due to which Company business is getting impacted during the implementation phase across all locations and bidder is not able to rectify the same within 24 hours, then OEM person should reach Stockholding's head office/DC and continue to be present till the issue is permanently resolved. Stockholding will provide necessary infra for that resource.
- 10) Bidder shall keep adequate stock of the spare equipment's or part thereof to maintain the SLA uptime. In case of device/part thereof gone faulty, the Selected Bidder shall replace the faulty device/part as per SOW & SLA defined in RFP. Further, bidder shall provide & install standby device of similar make model or equivalent device from the same OEM against faulty equipment at all circumstances to make the network functional within defined SLA during the tenure of contract. The standby device should not be EOL/EOS. In case of RMA, it is bidders' responsibility to replace the equipment as per SLA and to return the faulty equipment to the OEM warehouse at no extra cost to the company during the tenure of the contract.
- 11) Bidder must ensure OEM TAC support as and when required during the contract period. Additionally, bidder should arrange on-site OEM TAC support at DC, DR, and Head Office as per the company requirement. Bidder should provide login id details to company for logging to OEM portal for the call logging, support and log/view the status of calls/TAC cases raised by/for the Company. Company should be able to log calls 24*7 via phone/email/web-portal directly with OEM without any dependency on Bidder.
- 12) The Bidder should provide Configure/Re-configure devices and its configuration to fix Operational issues if any during the entire contract period.

h. Reports & Analytics

- 1) The bidder should propose storage for control plane data and analytics logs for SD-WAN, ensuring live monitoring logs are retained for minimum 180 days. Older logs should be archived to the Stockholding's archival storage.
- 2) SD-WAN solution should support export of DC/DR/Branch devices configuration for auditing purpose and its restoration as well. The solution should comply with SEBI, MEITY, CERT-In, etc. regulatory guidelines at all times.
- 3) The SD-WAN solution should provide role-based access control (RBAC) for reports and analytics dashboards, ensuring only authorized users can view/download sensitive data.
- 4) The reporting system should support customizable dashboards and scheduled reports (daily/weekly/monthly) delivered via email to designated stakeholders.
- 5) The bidder should ensure reports and analytics cover at least the following:
 - i. Link utilization, latency, jitter, and packet loss.
 - ii. Application performance visibility (business-critical vs. non-critical apps).
 - iii. User/branch-wise traffic patterns.
 - iv. Security events, including intrusion attempts, malware detection, policy violations.
- 6) The solution should provide real-time alerting and threshold-based notifications (via email/SMS/Syslog/REST API) for critical events (e.g., link failure, SLA breach, abnormal traffic patterns).

- 7) The solution should support integration with SIEM and log management tools using standard protocols (Syslog, APIs, etc.) for centralized monitoring.
- 8) The solution should provide an audit trail of all administrative/user activities (logins, configuration changes, policy modifications) with timestamp and user details.
- 9) The reporting/analytics system must ensure data integrity, immutability, and tamper-proof storage of logs as per SEBI/MEITY/CERT-In compliance requirements.

i. Performance Benchmarks

- 1) The SD-WAN solution shall meet or exceed the following minimum performance benchmarks. All figures must represent sustained encrypted IMIX throughput, Stateful Firewall, IDS/IPS, Anti-Malware, Application Recognition, URL/Domain Filtering, and SSL/TLS Inspection enabled concurrently with IPS for HTTPS.
- 2) All performance values must:
 - i. Be based on IMIX traffic profiles (real-world mixed packet sizes)
 - ii. Be achievable without any additional throughput or performance unlock licenses
 - iii. Be supported by OEM datasheets

Description	Minimum Requirement
Number of applications recognized (for application-aware routing)	≥ 5,000 (with regular updates)
Number of branches supported by solution	≥ 300 branches supported
NGFW + UTM/UTP + SD-WAN throughput (Firewall, IDS, IPS, Anti-malware and Domain/URL filtering) at Branch Level	≥ 1 Gbps
NGFW + UTM/UTP + SD-WAN throughput (Firewall, IDS, IPS, Anti-malware and Domain/URL filtering) at Fort Office	≥ 2 Gbps
NGFW + UTM/UTP + SD-WAN throughput (Firewall, IDS, IPS, Anti-malware and Domain/URL filtering) at Centre Point Office	≥ 2 Gbps
NGFW + UTM/UTP + SD-WAN throughput (Firewall, IDS, IPS, Anti-malware and Domain/URL filtering) at DC/DR Hub Level	≥ 10 Gbps

j. Warranty Clauses

- 1) **Commencement of Warranty:** The warranty for all supplied hardware, software licenses, and components (including but not limited to SD-WAN CPEs, controllers, management/orchestration platforms, and L2 managed switches) shall commence from either the Installation Date of the respective equipment/location or the Date of Final Acceptance and Go-Live, whichever ensures optimal coverage for the buyer.
- 2) **Adjustment for Early Installation:** In the event that warranty of the solution starts from the Installation Date, the time difference (gap period) between the Installation Date and the Final Acceptance and Go-Live Date shall be added on top of the actual standard warranty period requested by the buyer. This ensures StockHolding receives the full contractual duration of active operational warranty.
- 3) **Extension Due to Project Delays:** In case the Final Acceptance and Go-Live is

delayed for any reason, the bidder/OEM shall automatically extend the warranty period to the full extent of the delay, ensuring that the total warranty tenure remains uncompromised.

- 4) **Definition of Final Acceptance and Go-Live:** “Final Acceptance and Go-Live” shall mean the successful installation, integration, testing, and commissioning of the entire SD-WAN solution and L2 Managed Switches (including branch devices, DC/DR hub devices, switches, controllers, and central management) in line with the scope of work, as officially confirmed by a Go-Live Certificate issued by Stockholding.
- 5) **Replacement Warranty & Coverage:** Any equipment or component replaced during the warranty period shall carry a warranty co-terminus with the overall solution warranty. The bidder/OEM shall ensure that comprehensive warranty coverage—including hardware replacement, software updates/patches, security signatures, and technical support—remains fully active throughout the extended warranty period.

5. Support

- 1) One contact number for all support (user/technical) needs would be preferred. Bidder should provide the address and telephone number for the general customer/ technical support location at Mumbai/MMR.
- 2) Bidder will depute 1 onsite FMS official for 12-month post Go-Live signoff. The duty hours of onsite qualified engineer would be 9.30 AM to 6 PM. In urgent circumstances, bidder will ensure the availability of Onsite Engineer for smooth operations and support services as and when required by Stockholding during the period of contract.
- 3) Bidder will ensure that deployed solution and all dependencies are under OEM warranty, as applicable, during the period of contract.
- 4) During period of contract, Bidder will provide support as per resolution matrix defined in this RFP. Non-adherence to resolution matrix will be considered as breach of SLA and dealt as per terms of RFP.
- 5) Bidder will ensure that at no given point of time during the period of contract the implemented solution or its component are out of OEM warranty/support.
- 6) The services shall be reviewed as per SLA.

6. OEM / SI Support

- 1) The solution should come with 24x7 OEM Support with dedicated account manager and toll-free number
- 2) The solution should show uptime status on GUI and should send monthly uptime reporting via email as and when required
- 3) The Bidder of the proposed solution should be ISO 27001, 14001 and ISO 9001 certified.
- 4) The Bidder of the proposed solution should also provide periodic custom attack summary and conduct configuration efficacy for configured web applications during the FMS support contract.

7. FMS Support Activities

- 1) The bidder has to ensure that the FMS resource deputed should be platform certified and should have minimum 3+ years' experience on SD-WAN platform.
- 2) FMS Support person should be stationed at Stockholding premises at Mahape – Navi Mumbai. FMS person should be available during working hours i.e. 8.00 AM to 5.00 PM Monday to Saturday.

- 3) The bidder has to ensure that any leaves or absence by the deputed FMS person should be replaced by an alternate resource.
- 4) Activities to be performed –
 - a. Provide post-deployment monitoring, troubleshooting, and tuning of SD-WAN performance.
 - b. Create and maintain operational documentation, configuration backups, and runbooks.
 - c. Provide knowledge transfer and training to the customer's network/admin teams.
 - d. Implement patching, firmware upgrades, and software updates of SD-WAN appliances.
 - e. Assist in incident management and resolution of network-related issues.
 - f. Generate periodic reports on network performance, uptime, and SLA compliance.
 - g. Participate in monthly/quarterly review meetings with stakeholders.
 - h. Suggest optimizations for bandwidth usage, cost efficiency, and application performance.
 - i. Ensure compliance with organizational security and audit policies.
 - j. Track and document lessons learned for future network expansion projects.

8. Documentation Deliverables

- 1) Project Documentation – Solution Architecture, Implementation & Roll-out plan.
- 2) SOP Document for operating all the solution components.
- 3) User Manual and/or Training material.

9. Buy-Back of Old Routers and Switches

- 1) Stockholding intends to give buy-back option to bidder the old routers which will be spare in lieu of up gradation/replacement by the new SD-WAN CPE's and which are lying at branches/offices.
- 2) The bidder has to quote the buy-back price of mentioned model in the Commercial bid form.
- 3) The bidder has to ensure erasing of stored data /all kind of the configuration/information on the buyback branch routers and switches and required log shall be shared with Stockholding by the centrally located team of the bidder in this regard.
- 4) A certificate with line of confirmation shall be submitted by the bidder to Stockholding in this regard.
- 5) The Bidder shall be fully responsible for un-installation and de-commissioning of the equipment and other related activities such as packing, unpacking, uncrating, inspection, logistic etc. for the old routers (which shall be picked up by bidder under buy back activity) without any extra cost to the Stockholding.
- 6) The numbers of buy back routers given in the price proposal are tentative and Stockholding shall reserve the rights to change the number of buy back routers as per current scenario.

10. Payment Milestones

Sr. No.	Milestone	Payment
1	Delivery of Hardware and Software	50% of 3 Year Cost (Line Items of Point 1,2, 3 and 6 as per Commercial Bid Format in Annexure-4).
2	Successful deployment of the SD WAN and	40% of 3 Year Cost (Line Items of Point 1,2,

	L2 Network switches and submission of project completion GO-Live report along and acceptance of the same by Stockholding.	3 and 6 as per Commercial Bid Format in Annexure-4).
3	Annual Payment for Uptime Availability for 3 year Warranty Period	An advance payment for the remaining 10% of 3 Year Cost (Line Items of Point 1,2, 3 and 6 as per Commercial Bid Format in Annexure-4) shall be made annually on a pro-rata basis for three years, after deducting any penalties incurred due to SLA deviations in the previous year.
4	One Time Implementation Cost	100% payment after successful Go-Live (Line Items of Point 4 as per Commercial Bid Format in Annexure-4).
5	User Training	100% payment after successful Training (Line Items of Point 5 as per Commercial Bid Format in Annexure-4).
6	AMC related payments for 4 th and 5 th Year	Advance Half Yearly payment after deduction of applicable penalty based on uptime calculations. Last payment will be done at the end of the contract period.

11. Delivery Schedule and Timelines

Sr. No.	Task	Expected period of delivery
1	Delivery of Hardware	Within 8 weeks from date of acceptance of Purchase Order
2	Commissioning of the Edge devices and GO-Live of the Project	Within 12 weeks from date of acceptance of Purchase Order
3	User Training	Within 14 weeks from date of acceptance of Purchase Order

12. Penalty Structure and Delivery Schedule

Sr. No.	Task	Penalty Structure	Maximum Penalty
1	Delivery of Hardware	If the Bidder fails to deliver any or all of the Systems and equipment's mentioned in the Purchase order (PO) within 6 weeks from the day of acceptance of Purchase Order, Stockholding shall deduct 0.5% percent per week or part thereof Line Items of Point 1, 2, 3 and 6 as per Commercial Bid Format in Annexure-4. Delivery Sign Off will be considered when all edge devices are delivered at the respective locations and shall be supported by delivery challans.	Subject to a maximum cap of 10% of the Total Cost for the Initial 3 Year Warranty Period
2	Successful deployment of the SD WAN and L2 Network switches and submission of project	If the Bidder fails to Successfully deploy SD WAN and L2 Network switches and make the project GO-Live mentioned in the Purchase order (PO)	

	completion GO-Live.	within 10 weeks from the day of acceptance of purchase order, Stockholding shall deduct 1% percent per week or part thereof Line Items of Point 1, 2, 3, 4 and 6 as per Commercial Bid Format in Annexure -4. Implementation Sign Off shall be considered when all edge devices are commissioned and the platform is Go-Live declared.	
3	User Training	If the Bidder fails to impart user training as mentioned in the Purchase order (PO) within 12 weeks from the day of acceptance of Purchase Order, Stockholding shall deduct 0.5% percent per week or part thereof User Training Cost (Point 5) as mentioned in the Commercial Bid Format in Annexure-4.	
4	Annual Payment for Uptime Availability for 3-year Warranty Period	Penalty shall be deducted as per uptime availability mentioned in Penalty for SD WAN Platform	
5	AMC related payments for 4 th and 5 th Year	Penalty shall be deducted as per uptime availability mentioned in PENALTY (AMC RELATED) – SD WAN Devices Platform	Subject to a maximum cap of 10% of the respective 4 th and 5 th Year AMC Period

13. Service Level Agreement

1) Resolution and Response Time

Severity Level	Criteria	Response Time	Resolution Time
High Severity Issues	A major network/ SDWAN/ Device failure having a serious impact on the operation and preventing the operations to function smoothly	Within 15 Mins	Vendor should fix the issue or provide workable solution in 4 hours from raising the issue. Any such workable solution recommendations should be acceptable to Stockholding post which it will be considered as a workable solution.
Medium Severity Issues	This is a problem that does not prevent the major network/ SDWAN/ Device being operable, but will have a serious impact on Stockholding's day to day operations. It only affects specific areas where a reasonable workaround can be utilized	Within 15 Mins	Vendor should fix the issue or provide workable solution in 24 hours from raising the issue. Any such workable solution recommendations should be acceptable to Stockholding post which it will be considered as a workable solution.

Low Severity Issues	This is a problem that does not prevent the network/ SDWAN/ Device being operable, but will have a minor impact on Stockholding's day to day operation of the system	Within 24 Hrs	Vendor should fix the issue or provide workable solution in 3 days from raising the issue. Any such workable solution recommendations should be acceptable to Stockholding post which it will be considered as a workable solution.
----------------------------	--	---------------	---

2) Penalty Structure – SDWAN Platform

Severity Level	Penalty Structure
High Severity Issues	₹ 25,000/- for every breach of the SLA.
Medium Severity Issues	₹ 10,000/- for every breach of the SLA.
Low Severity Issues	₹ 5,000/- for every breach of the SLA.

3) Penalty Structure – L2 Managed Network Switches

Severity Level	Penalty Structure
High Severity Issues	₹ 3,000/- for every breach of the SLA.
Medium Severity Issues	₹ 2,000/- for every breach of the SLA.
Low Severity Issues	₹ 1,000/- for every breach of the SLA.

The above penalty will be computed on monthly basis and will be deducted from the payable amount to the selected bidder.

Any component in network equipment that are reported to be down on a given date should be either fully repaired or replaced by substitute (of equivalent or higher configuration) as mention below

Uptime: The percentage uptime shall be calculated on monthly basis as follows:

$$\text{Availability} = \frac{(\text{Total No. of hours in a month} - \text{Total Outage Hours in Month}) \times 100}{(\text{Total No. of Hours in a Month})}$$

4) Penalty (Warranty Support Related)

1) Penalty for SD WAN Platform

In case if monthly uptime falls below the guaranteed level, StockHolding will impose a penalty as per below mentioned slab of that particular equipment value and same will be deducted from any bill payable to the vendor during the contract / warranty period.

Uptime (%)	Penalty of (%) of Initial 3 year Warranty Period
>=99.5	0
>=99 and < 99.5	1
>=98 and < 99	2
>=97 and < 98	3
>=96 and < 97	4
>=95 and < 96	5

< 95	10
------	----

StockHolding reserves the right to levy / waive off penalty considering various circumstances at that point in time.

Any such recovery of penalty shall not in any way relieve the Bidder from any of its obligations to complete the works/services or from any other obligations and liabilities under the Contract.

2) PENALTY (AMC RELATED) – SD WAN Devices Platform

Penalty for all the locations of Stockholding, if the uptime falls below the levels as tabulated below, Stockholding shall impose a penalty on the half yearly AMC charges for the specific critical network equipment for percent of loss of uptime below the guaranteed level as detailed under:

Uptime (%)	Penalty of (%) of Annual AMC Period of 4th and 5th Year
>=99.5	0
>=99 and < 99.5	1
>=98 and < 99	2
>=97 and < 98	3
>=96 and < 97	4
>=95 and < 96	5
< 95	10

3) PENALTY FOR FMS RESOURCE AVAILABILITY

If the bidder is not able to provide replace resource incase of absence of the already deputed FMS personnel, then Stockholding shall deduct Rs. 2,000 per day of absence.

14. Migration activities for change of location

In case Stockholding wishes to shift the network devices from one place to another anywhere within the City, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of network devices supplied by Service provider & hand-over to the concerned Stockholding Officials or Data Center, pre-shifting inspection, post-shifting inspection, re-installation etc. of all devices supplied by Service provider. All migration related activities to be done after Business / session hours /according to business convenience & the engineer has to be deployed as per the Stockholding requirements. Stockholding will bear all expenses for packing, shifting, insurance and other incidentals at actual.

Stockholding will not be responsible or liable for any losses, damages to the items of equipment tools and machinery while such dismantling, pre-shifting inspection, post-shifting inspection, and re-installation etc. is being carried out.

Bidder shall make available adequate alternative arrangement to ensure that the system functioning is neither affected nor dislocated during the shifting process. It is the responsibility of field engineer to integrate devices delivered for a Stockholding or Data Center & coordinate with Stockholding NOC to extend the reachability.

15. Site Not Ready Clause

To the extent that a material failure of performance of the obligations attributable solely to an act or omission of Stockholding (example SNR), causes the Bidder to fail to meet a time schedule for delivery and installation, the Bidder shall be entitled to a day-for-day extension of the applicable

delivery and installation date caused as a result of Stockholding delay.

However, if Stockholding desires to shift the equipment to a new site and install it thereof urgently, the Bidder shall be informed of the same immediately. Stockholding shall bear the charges for such shifting and the Bidder shall provide necessary arrangement to Stockholding in doing so. The terms of this agreement, after such shifting to the alternate site and reinstallation thereof would continue to apply and binding on the Bidder.

16. Contract Duration

- 1) Successful bidder shall enter into contract for the period of 05 (five) years with StockHolding.
- 2) StockHolding at its sole discretion may extend the contract for further period of two years, based on the satisfactory performance.

17. Payment Terms

- 1) Bidder to raise invoice for the payment duly certified by StockHolding.
- 2) Applicable TDS and/or CESS will be recovered (deducted) from the payment.
- 3) Payments will be released only after submission and verification of the required Bank Guarantee (BG). No payment will be made to successful bidder, until the BG verification is done.
- 4) Applicable GST payable at actual as per prevailing rate of taxes as per Government notification
- 5) In case of tax exemption or lower TDS; Bidder has to submit letter from Government Authority for tax exemption or lower TDS (to be submitted along with each of the invoice(s) (c) Applicable TDS will be deducted from payment(s).

18. Other Terms

Refund of Earnest Money Deposit (EMD)

- a) EMD will be refunded through NEFT or return of BG/FDR to the successful bidder on providing an acceptance confirmation against the PO issued by StockHolding.
- b) In case of unsuccessful bidders, the EMD will be refunded to them through NEFT or return of BG/FDR within 30 days after selection and confirmation of successful bidder, subject to internal approval of StockHolding.

Performance Bank Guarantee (PBG)

Successful Bidder shall, at own expense, deposit with the StockHolding, within fifteen (15) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% of the Contract Value from scheduled commercial banks as per Annexure - 7. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period and claim period shall be valid 12 months beyond the expiry of BG. No payment will be due to the successful bidder based on performance, until the BG is submitted. A penalty of Rs. 5,000 per day will be imposed on the successful bidder for any delay in issuing the PBG within the specified timeline.

Bank Guarantee may be discharged / returned by StockHolding upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee.

Stock Holding Corporation of India Limited reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

Neither the StockHolding nor the Bidder shall be responsible for any failure to fulfil any term or condition of the CONTRACT if and to the extent that fulfilment has been delayed or temporarily prevented by a Force Majeure occurrence, defined as "Force Majeure". For purposes of this clause, "Force Majeure" mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, strike, lock-outs beyond its control, labour disturbance not caused at the instance of the Party claiming Force Majeure, acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc.

The Party seeking to rely on Force Majeure shall promptly, within 5 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defence with particulars detailed in writing to the other Party and shall demonstrate that it has taken and is taking all reasonable measures to mitigate the events of Force Majeure. And, all Parties will endeavour to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure. Each PARTY shall bear its own cost in relation to the force majeure occurrence.

However, any failure or lapse on the part of the Bidder to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force Majeure, as set out above.

If the duration of delay exceeds ninety (90) consecutive or one hundred eighty (180) cumulative days, StockHolding and the Bidder shall hold consultations with each other in an endeavor to find a solution to the problem. Notwithstanding above, the decision of the StockHolding, shall be final and binding on the bidder.

Dispute Resolution

- a) All disputes or differences arising between the parties as to interpretation, operation, or effect of any clause in this RFP, shall be endeavoured to be resolved amicably through dialogues and discussions. However, disputes that cannot be mutually resolved shall be referred to arbitration.
- b) The arbitration proceedings shall be conducted by a sole arbitrator to be appointed by both the parties on mutual consent. In the event of failure to reach consensus on an arbitrator, each party shall appoint an arbitrator and both the arbitrators shall appoint a third arbitrator as referee arbitrator before the commencement of arbitration proceedings.
- c) The arbitration proceedings shall be governed by the provisions of The Arbitration and Conciliation Act, 1996. The venue of arbitration shall be Mumbai and the proceedings shall be conducted in English. The award of the arbitrator shall be final and binding on the Parties.

Governing Law and Jurisdiction:

Any dispute or difference arising out of or in connection with this Agreement shall be governed by and construed in accordance with the laws of India. Any disputes shall be subject to the exclusive

jurisdiction of the courts at Mumbai, Maharashtra.

Right to alter RFP

- a) StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.
- b) StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders.

Integrity Pact

The Bidder will have to enter in to an Integrity Pact with StockHolding. The format (text) for the Integrity Pact is provided as Annexure-5. The Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the bidder.

Sub-Contracting

The selected bidder / service provider/ vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required under this project.

Non-Disclosure Agreement (NDA)

The successful bidder shall execute Non-Disclosure Agreement (NDA) as per Annexure -8 in RFP, which contains all the services and terms and conditions of the services to be extended as detailed herein.

All the expenses related to execution of the document such as the applicable stamp duty and registration charges if any shall be borne by the successful bidder.

Indemnify

The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.

Termination of contract for convenience

StockHolding reserves the right to terminate the contract, in whole or in part, at any time and for its convenience, during the contract period, by providing 90 days' prior written notice. The notice of termination shall specify that termination is for StockHolding's convenience, the extent to which performance of the vendor under the contract is terminated and the date upon which such termination becomes effective. The vendor shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

Termination Clause

- a. StockHolding reserves right to terminate the contract without assigning any reason whatsoever by giving 90 days prior written notice to successful bidder, but not limited to
 - i. If the total penalty amount deducted exceeds ten percent (10%) of the Total Cost for the Initial 3 Year Warranty Period;
 - ii. If the total penalty amount deducted exceeds ten percent (10%) of the of the respective 4th and 5th Year AMC Period;
 - iii. If at any point of time, the services of bidders are found to be non-satisfactory;
- b. During the Termination notice period successful bidder must adhere to all the conditions mentioned in the 'Exit Management' clause.

- c. Notwithstanding the above, StockHolding reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.

Exit Management

- a. Purpose: In the case of termination of the Contract, the Exit Management procedure should start 90 days before the expiry or termination of contract.
- b. Plan: An Exit Management Plan, provided in writing by the Bidder to the StockHolding within 60 days of the acceptance of the Purchase Order/Contract, will outline the Bidder's support during the termination or expiration of the contract, along with the company's exit strategy. Following this, the exit plan must be reviewed and updated annually.
- c. Bidder shall provide the Termination/Expiration Assistance regardless of the reason for termination or expiration.
- d. Bidder shall fully and timely comply with the Exit Plan.
- e. Bidder shall not make any changes to the Services under this Agreement and shall continue to provide all Services to comply with the Service Levels.
- f. Confidential Information, Security and Data: The Bidder will promptly on the commencement of the exit management period supply to StockHolding the following:
- 1) Information relating to the current services rendered.
 - 2) Project Data and Confidential Information.
 - 3) All current and updated project data as is reasonably required for purposes of transitioning the services to its Replacement Bidder in a readily available format specified by StockHolding.

Options Order Clause

The Purchaser reserves the right to extend the contract period and/or increase the ordered quantum of goods/services up to 25 percent at any time till the completion date of the contract, by giving reasonable notice and reasonable extension in delivery period for increased quantum, even though the quantum ordered initially has been delivered in full before the completion period of contract.

Assignment

Either Party may, upon written approval of the other, assign its rights and obligations hereunder to: (i) its Parent Corporation (as defined below) or an Affiliate; and (ii) a third party entity in connection with the transfer of all or substantially all of the business and assets of that party to such entity. For purposes of this Agreement, a "Parent Corporation" shall mean a company or entity owning over 50% of a Party and an "Affiliate" shall mean a company directly or indirectly controlling, controlled by, or under common control with, a Party. Except as provided above in this Section, either Party may assign its rights and obligations under this Agreement to a third party only upon receiving the prior written consent of the other Party, which consent may be reasonably conditioned but will not be unreasonably withheld or delayed. The Parties agree that no assignments will be made unless the assignee agrees to accept in full the responsibilities and obligations of the assigning Party.

**ANNEXURE - 1 - Details of Bidder's Profile
(To be submitted along with bid on Company letter head)**

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Sl. No	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no.		
6	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office		
7	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID		
8	Years of experience in implementing and managing SDWAN Solution		
9	Financial parameters		
	Business Results (last three years)	Annual Turnover	Net Worth
		(₹ in Lakhs)	(₹ in Lakhs)
		2022-23	
		2023-24	
		2024-25	
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures)	(Mention the above Amount in INR only)	

N.B. Enclose copies of Audited Balance Sheet/CA Certificate along with enclosures

Dated this..... Day of 2026

(Signature)

ANNEXURE - 2 – Eligibility Criteria

Sr. No.	Criteria	Documents to be submitted by Bidder
1	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 or LLP with experience in implementation of SDWAN solution within the past 5 years.	Copy of Certificate of Incorporation issued by the Registrar of Companies or Partnership Deed and Self-declaration by the bidder for experience on its' Letter Head duly signed by the Authorized Signatory.
2	The Bidder / OEM should have supplied and implemented atleast One SD-WAN solution in BFSI Sector with minimum 210 branches (both for SD-WAN software & underlying Hardware) which OEM / Bidder is offering to Stockholding in the past 3 years as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email
3	The bidder must have supplied and installed a minimum of 200 L2 Managed Switches under a single contract within at least one (1) BFSI industry during the past three years in India, as of the RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email
4	Bidder should have an average annual turnover of at least ₹68 crores per annum for last three audited financial years (2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover or Balance Sheet for last three financial years.
5	Bidder should have Positive Net worth of at least ₹8 crores for all the last 03 (three) audited financial years i.e. 2022-23, 2023-24 and 2024-25.	Certificate from CA mentioning networth or Balance Sheet for last three financial years.
6	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
7	The bidder, in case of SI, should be OEM certified or authorized agent/reseller/partner of the OEM.	If the bidder is the OEM, a self-declaration must be provided confirming that the bidder is the original equipment manufacturer of the proposed solution; In case the bidder is not OEM of the offered solution, then a certificate from OEM certifying that Bidder is authorized partner of the OEM.
8	The proposed SD WAN solution and appliances of Branch/DC/DR quoted i.e. should be compatible with other OEM devices (e.g. Switches)	Self-declaration from bidder on letterhead duly signed by authorized signatory

9	Bidder must ensure that the equipment to be supplied will not reach End-of-Sale or End-of-Life status within the next 3 years and End of Support in next 7 years. In case proposed product goes end of support during contract period, then bidder will provide devices of equivalent or higher configuration approved by Stockholding.	Self-declaration from bidder on letter head duly signed by authorized signatory
10	The bidder should have service/ support infra- structure at Mumbai MMR and should be able to provide efficient and effective support.	Office details along with escalation matrix to be submitted
11	The bidder must have qualified / certified / trained professionals in the proposed OEM's SDWAN solution on the payroll of the bidder as on RFP date.	- CVs or Resumes of proposed resources / Relevant certification copies - Self-declaration that proposed resources are on bidder's payroll
12	The Bidder of the proposed solution should be ISO 27001, 14001 and ISO 9001 certified.	Relevant Valid certificates to be submitted
13	The Bidder to submit signed & stamped Integrity Pact as per Annexure- 5	Self-declaration from bidder duly signed by authorized signatory

Note:

- All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
- Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this..... Day of 2026
(Signature)

(In the capacity of)

Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE - 3 – Technical Evaluation Criteria

Sr. No.	Criteria	Supporting Documentation	Technical Score Matrix	Max Marks
A. Experience, Turnover & Resource Strength (70 Marks)				
1	The Bidder having an average annual turnover of at least ₹68 Crores per annum for all the last 03 (three) audited financial years i.e. 2022-23, 2023-24 and 2024-25. It should be of individual company and not of Group of Companies	A Certificate duly certified by the statutory auditor of the Bidder clearly mentioning the annual turnover of the bidder.	a) INR 68 Crores to INR 80 Crores: 12 Marks b) More than INR 80 Crores and less than INR 100 Crores: 15 Marks c) More than INR 100 Crores and less than INR 120 crores: 18 Marks d) More than INR 120 crores: 20 Marks	20 Marks
2	The Bidder / OEM should have supplied and implemented SD-WAN solution in BFSI Sector with minimum 210 branches (both for SD-WAN software & underlying Hardware) which OEM / Bidder is offering to Stockholding in the past 3 years as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email	a) 1 - 2 projects: 12 Marks b) 3 - 4 projects: 15 Marks c) More than 4 projects: 20 Marks	20 Marks
3	The bidder has supplied and installed a minimum of 200 L2 Managed Switches under a single contract within at least one (1) BFSI industry during the last three (3) years in India as on RFP date.	• Work Orders / Purchase Orders / Contracts copy • Completion certificate / Client reference letter OR Go-live / acceptance email	a) 1 - 2 projects: 12 Marks b) 3 - 4 projects: 15 Marks c) More than 4 projects: 20 Marks	20 Marks
4	The bidder must have qualified / certified / trained professionals in the proposed OEM's SDWAN solution on the payroll of the bidder as on RFP date.	Self-Certificate on the letterhead of the bidder signed by Authorized signatory with details of Relevant certifications and resource profiles to be submitted.	a) 2 - 5 resources: 6 Marks b) 5 - 8 resources: 8 Marks c) More than 8 resources: 10 Marks	10 Marks
B. Technical Presentation (30 Marks)				
5	Bidder's capabilities in terms of solution expertise and experience in implementation related to project.	Technical Presentation delivered by Bidder	Following parameters will be considered for the evaluation: 1) Understanding of the project and StockHolding's requirement – 5	30 Marks

			marks 2) Proposed SDWAN solution, its components and technologies used – 7 marks 3) Implementation approach, Project Timelines and Migration plan – 8 marks 4) Team Deployment Plan – 5 marks 5) SLA Management – 5 marks	
Total Score				100 Marks

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- StockHolding shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks.
- The bidder to submit appropriate credentials [other than self- certification] in respect of each of the item.
- Technical proposals will be evaluated based on the total marks obtained across all technical evaluation criteria. Only those bidders who achieve a **minimum cumulative score of 60 marks** in the technical evaluation will qualify for the commercial bid evaluation.

ANNEXURE - 4 – Commercial Bid Format

Table A – SD WAN solution and Switches

Sr. No.	Description	Quantity	Unit Rate in ₹	Total Cost (3 Year Warranty) in ₹	AMC/ATS Charges in ₹ (4th Year)	AMC/ATS Charges in ₹ (5th Year)	2 Years AMC/ATS Total Cost in ₹	Total Cost (Warranty + AMC) in ₹
1	SD-WAN Managers / Controllers / Orchestrators / Data planes devices – DC + DR in HA mode with Edge Devices in DC / DR Hub Site, Mumbai – Centre Point and Mumbai – Fort Office in HA Mode along with SD-WAN Software solution Licenses (all locations)	1						
2	SD-WAN Edge Devices at Branch	204						
3	Branch Network Switches	222						
4	One Time Implementation Cost	1	-		-	-	-	
5	User Training	1	-		-	-	-	
6	Additional network / server equipment, if any	1						
7	Total Cost in ₹	-	-					

Note –

- 1) OEM/SI to ensure that the Unit Rate per router/switch is given to Stockholding incase of Branch Expansion during the contract period. The unit rate shall be adhered for the whole duration of the contract period.
- 2) Support, Management, Maintenance etc. Costing for 5 years' period. The contract is extendable up to another 2 years or part there of (beyond the above 5 years) at the discretion of Stockholding. Accordingly, the prices for the additional 2 years also need to be provided separately ([Refer Table E](#)).
- 3) Bidder shall also provide unit rate of SD-WAN CPE and switch for each year for the entire duration of contract period incase number of branches are increased. Unit Rate shall be inclusive of transportation, delivery and installation charges.

Table B – Price Schedule for Buy Back of existing branch routers and switches

The selected bidder should take over the existing old routers and switches from branches on a buyback arrangement. The bidder should quote buyback amount for the existing equipment in the price bid mentioned below –

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



Sr. No.	Product Name	Unit Price (₹)	Approx. Quantity	Total Price (₹)
8	Router		As mentioned in Branch List with Router and Switch Models	
9	Switch			
10	Grand Total			

Note –

- 1) The quantity mentioned above in tentative and amount will be deposited by the bidder in respect of actual quantity.
- 2) All Stockholding related configuration shall be erased by the bidder before respective Stockholding authorities. A document of undertaking shall be submitted by the bidder for the same.
- 3) Stockholding undertakes that Quantities are indicative and may vary.

Table C – Total Price and TCO for 5 Years

Description	Total Cost in ₹
Total Cost for Warranty and Support for 5 Years – Row 07 as in Table A	
Total Buy Back – Row 10 as in Table B	
Grand Total Cost excluding GST in ₹	Row 07 – Row 10
GST in ₹	
Grand Total Cost including GST in ₹	

Note:

- a) Price to be quoted is for contract period of 05 (five) years including GST while uploading financial bids on GeM portal.
- b) Taxes extra, as applicable.
- c) Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled in correctly.
- d) All payments will be made in INR.

Table D – Unit Rate of Devices

Description	SD-WAN Edge Devices at Branch with requisite Software Licenses	SD-WAN Edge Devices at non-Branch and non-hub site with requisite Software Licenses	L2 Managed Branch Network Switches with requisite software Licenses
Year 1 Cost in ₹			
Year 2 Cost in ₹			

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



Year 3 Cost in ₹			
Year 4 Cost in ₹			
Year 5 Cost in ₹			
Year 6 Cost in ₹			
Year 7 Cost in ₹			

Note – Any additional devices taken in between the contract period shall co-terminate with the end date of the original contract period.

Table E – AMC for 6th and 7th Year (Optional)

Description	Total Cost in ₹
6 th Year AMC – SD WAN Solution with licenses	
6 th Year AMC – L2 Managed Branch Network Switches with licenses	
7 th Year AMC – SD WAN Solution with licenses	
7 th Year AMC – L2 Managed Branch Network Switches with licenses	
Total Cost in ₹	

Table F – FMS Resource (Optional)

Description	Unit Rate in ₹
FMS Resource for 12 months	

Note: Price to be quoted under Table D, Table E & Table F are ‘Optional Cost Component’ and will not be considered for evaluation. Those components are required on need basis. StockHolding may avail these components during the contract period at the same rate proposed by the selected bidder as part of commercial proposal during the bid submission.

ANNEXURE – 5 – Integrity Pact

(_____ Name of the Department / Office) RFP No. _____
for _____

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on _____ day of the _____, between, on one hand, StockHolding ., a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. B R Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s. _____

_____ (with complete address and contact details) represented by Shri _____ (i.e. Bidders hereinafter called the **`Counter Party`**) which expression shall mean and include , unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with Bidder(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board 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 tenor of the contract to be entered into with a view to “- Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of 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 PRINCIPAL 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:

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or

services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.

b) The Principal/Owner will, during the Tender (RFP) Process treat all Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party (ies) the same information and will not provide to any Bidder(s)/Counter Party (ies) confidential / additional information through which the Bidder(s)/Counter Party (ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.

c) The Principal / Owner shall endeavor to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / StockHolding will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/Bidders

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / Bidders commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.

2. The Counter Party 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 PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3. The Counter Party 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 Principal / StockHolding or otherwise in procurement 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 Principal / StockHolding for forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Principal / StockHolding.

4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.

5. Bidder / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.

6. The Bidder / Counter Party has to further confirm and declare to the Principal / StockHolding that the Bidder / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / StockHolding or any of its functionaries whether officially or unofficially to the award of the contract to the Bidder / Counter Party 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.

7. The Bidder / Counter Party has to submit a Declaration along with Eligibility Criteria, as given at **Annexure**. If bids are invited through a Consultant a Declaration has to be submitted along with the Eligibility Criteria as given at **Annexure**.
8. The Bidder / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of StockHolding /Principal, 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.
9. The Bidder / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / StockHolding as part of the business relationship, regarding plans, proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
13. The Bidder / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / Counter Party, either directly or indirectly, is a relative of any of the official / employee of Principal / StockHolding, or alternatively, if any relative of an official / employee of Principal / StockHolding has financial interest / stake in the Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / Counter Party at the time of filing of tender (RFP).
15. The term "relative" for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The Bidder / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / StockHolding
17. The Bidder / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the Bidder(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / StockHolding is entitled to disqualify the Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / Counter Party / Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity

of transgression and determined by Principal / StockHolding. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / StockHolding.

2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / StockHolding's absolute right to resort to and impose such exclusion.

3. Apart from the above, the Principal / StockHolding may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / StockHolding.

4. The Bidder / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner / StockHolding may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / StockHolding / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / StockHolding / Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / StockHolding / Owner has disqualified the Bidder(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / StockHolding / Owner apart from exercising any legal rights that may have accrued to the Principal / StockHolding / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the Bidder / Contractor / Counter Party.

2. Criminal Liability: If the Principal / Owner / StockHolding obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / Counter Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / StockHolding has substantive suspicion in this regard, the Principal /

StockHolding / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

V. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Bidder(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its sub-contractors / sub-bidders.

2. The Principal / StockHolding / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.

3. The Principal / StockHolding / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / StockHolding and the Bidder/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / StockHolding has appointed Shri Shekhar Prasad Singh, IAS (Retd.) as Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.

2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, StockHolding Ltd.
3. The Bidder(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / StockHolding / Owner including that provided by the Contractor(s) / Bidder / Counter Party. The Counter Party / Bidder / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-Contractor's Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 50 lakhs or more , the Principal / StockHolding / Owner will provide the IEM sufficient information about all the meetings among the parties related to the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.
5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /StockHolding and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit nonbinding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, StockHolding. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / StockHolding and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, StockHolding Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO&MD, StockHolding has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer.
8. The word `IEM` would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD StockHolding

VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the StockHolding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.

4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / StockHolding in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses:-

(For and on behalf of Principal / Owner / StockHolding)

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES:

1. _____ (Signature, name and address)

2. _____ (Signature, name and address)

Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



**ANNEXURE – 6 – Compliance Statement
(To be submitted on Company Letter Head)**

**Sub: RFP REF NO: CPCM-47/2026-27 dated 14-Oct-2026 - Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by StockHolding. We also agree that StockHolding reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

Sr. No.	Item / Clause of the RFP	Compliance (Yes / No)	Remarks / Deviations (if any)
1	Objective of the RFP		
2	Scope of Work		
3	Eligibility Criteria		
4	Service Level Agreement (SLA)		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Requirement		
11	Technical Specifications for SDWAN and Switches as in Annexure-10		

(If Remarks/Deviations column is left blank it will be construed that there is no deviation from the specifications given above)

Date:

Signature with seal

Name & Designation:

ANNEXURE – 7– Format of Bank Guarantee

This Bank Guarantee is executed by the ----- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at ----- and branch office at ----- (hereinafter referred to as the “Bank”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at ----- in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as “StockHolding”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of -----, a Company incorporated under the Companies Act, 1956 and having its Registered Office at ----- (hereinafter referred to as the “Service Provider”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

- A. StockHolding has, pursuant to the Tender No. _____, issued the Purchase Order dated _____ to the Service Provider for providing _____
- B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. _____ /- (Rupees _____ only) till _____ (date).
- C. The Bank has, at the request of the Service Provider, agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

- 1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.
- 2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. _____/- (Rupees _____ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider.
- 3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing whatsoever as the liability of the Bank under these presents being absolute and unequivocal.
- 4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.

5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. _____/- (Rupees _____ only).
2. This Bank Guarantee will be valid for a period up to _____ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before _____ (date) is the only condition precedent for payment of part/full sum under this guarantee.

For Issuing Bank

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID:

ANNEXURE – 8 – Format of Non-Disclosure Agreement

This Non-Disclosure Agreement (hereinafter “Agreement”) is executed on this _____ day of _____, 20xx by and between

Stock Holding Corporation of India Limited, a company incorporated under the Companies Act, 1956 and having its registered office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400012 (hereinafter referred to as “**StockHolding**” which expression shall mean and include its successors and assigns), of the One Part;

And

Company Name, a company incorporated under the Companies Act, 1956 and having its registered office / corporate office at **Complete Address** (hereinafter referred to as “**Company Name**” which expression shall mean and include its successors and assigns), of the Other Part. (StockHolding and **Company Name** are individually referred to as ‘Party’ and collectively as ‘Parties’.)

The Party disclosing Confidential Information under this Agreement shall be referred to as Disclosing Party and the Party receiving Confidential Information shall be referred to as Receiving Party.

1. **Purpose:** Whereas, the Parties wish to explore possible business opportunity, during which either Party will be required to disclose certain Confidential Information to the other.
2. **Confidential Information and Exclusions:** Confidential Information shall mean and include (a) any information received by the Receiving Party which is identified by Disclosing Party as confidential or otherwise; (b) all information including technical, data security, cyber security business, financial and marketing information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, know-how, ideas, concepts, strategies, trade secrets, product or services, results obtained by using confidential information, prototype, client or vendor list, projects, employees, employees skills and salaries, future business plans disclosed by Disclosing Party whether orally or as embodied in tangible materials. Confidential Information shall however exclude any information which a) is in the public domain; (b) was known to the Party of such disclosure or becomes known to the Party without breach of any confidentiality agreement; (c) is independently developed by the Party without use of Confidential Information disclosed herein; (d) is disclosed pursuant judicial order or requirement of the governmental agency or by operation of law, provided that the recipient party gives disclosing party a written notice of any such requirement within ten (10) days after the learning of any such requirement, and takes all reasonable measure to avoid disclosure under such requirement.
3. **Confidentiality Obligations:** The Receiving Party shall, at all times maintain confidentiality and prevent disclosure of Confidential Information of Disclosing party with at least the same degree of care as it uses to protect its own confidential information but in no event with less than reasonable care. The Receiving Party shall keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party. The Receiving Party agrees not to disclose, transmit, reproduce or make available any such Confidential Information to any third parties and shall restrict disclosure of Confidential Information only to a limited group of Recipient's directors, concerned officers, employees, attorneys or professional advisors who need to have access to the Confidential Information for the purposes of maintaining and supporting the services and each of whom shall be informed by Receiving Party of the confidential nature of Confidential Information and agree to observe the same terms and conditions set forth herein as if specifically named a Party hereto. The Receiving Party shall not, unless otherwise agreed herein, use any such Confidential Information and Confidential Materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their

projects. The Receiving Party shall not use the Confidential Information in any way to create a derivative work out of it or reverse engineer or use for any commercial purpose or for any purpose detrimental to the Disclosing Party. The Receiving Party shall not make copies of Confidential Information unless the same are reasonably necessary. The Receiving Party shall immediately notify Disclosing Party in the event of any unauthorized use or disclosure of the Confidential Information and reasonably support Disclosing Party in taking necessary remedial action.

4. **No Warranty:** All Confidential Information is provided 'as is.' Neither Party makes any warranty, express, implied or otherwise, regarding its accuracy, completeness or performance.

5. **No License:** Each Party recognizes that nothing in this Agreement is construed as granting it any proprietary rights, by license or otherwise, to any Confidential Information or to any intellectual property rights based on such Confidential Information.

6. **Return:** The Receiving Party who receives the Confidential Information and Confidential Materials agrees that on receipt of a written demand from the Disclosing Party:

a. Immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control; (SUCH RETURN OF DOCUMENTS SHOULD BE DONE BY SIGNING A LETTER).

b. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;

c. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and

d. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.

e. Receiving party will attempt to maintain, to the best possible extent, physical and logical segregation of the Confidential Information of the data of the Receiving party from data of any third party.

7. **Term:** The term of this Agreement shall be ____ (____) years from _____ (the Effective Date). Either Party may terminate this Agreement by giving a thirty (30) days written notice to the other. The confidentiality obligations stated in this Agreement shall survive for a period of three (3) years from the date of termination or expiration of this Agreement.

8. **Remedies:** The Confidential Information and Confidential Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.

The Parties acknowledge and agree that the Disclosing Party will suffer substantial and irreparable damage, not readily ascertainable or compensable in monetary terms, in the event of any breach of any provision of this Agreement by the Receiving Party. The Receiving Party therefore agrees that, in the event of any such breach, the Disclosing Party shall be entitled, without limitation of any other remedies otherwise available to it, to obtain an injunction or other form of equitable relief from any court of competent jurisdiction.

9. **Governing Law and Jurisdiction:** This Agreement may be governed and construed in accordance with the laws of India and shall be subject to the jurisdiction of courts in Mumbai, India.

10. **Miscellaneous:** This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior commitments/ understanding in this regard and may not be amended or modified except by a writing signed by a duly authorized representative of the respective Parties. This Agreement may be executed in several counterparts (physical or electronic form), each of which shall be deemed an original, but all of which together

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



shall constitute one and the same instrument. This Agreement may not be assigned or transferred except by a mutual written consent of both the Parties.

For Stock Holding Corporation of India Limited	For Company Name
Name:	Name:
Title:	Title:
In the Presence of	
Name:	Name:
Title:	Title:

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**

ANNEXURE - 9 – Branch List with Router and Switch Models



Sr. No	State	Branch	Address	Pin Code	Router Model	Router Count	Switch Model	Switch Count	Remarks
1	Andhra Pradesh	Guntur	2nd Floor, Raghu Mansion 4th Line, 1st Cross Road Brodipet, Guntur PIN : 522001	522001	Cisco 2801	1	WS-C2960-24TC-S	1	
2	Andhra Pradesh	Kakinada	Door No. 5-1-61/1 , Ayyappa Towers, 2nd Floor, Main Road, Suryaroa Peta Kakinada PIN : 533001	533001	Cisco 2801	1	WS-C2960-24TC-S	1	
3	Andhra Pradesh	Kurnool	Plot No. A 10 , 1st Floor, 40-383 Bhupal Residency, Park Road Kurnool PIN : 518001	518001	Cisco 2901	1	WS-C2960-24TC-S	1	
4	Andhra Pradesh	Nellore	16/1102, Ground Floor Moon Land Apartments, K V Agraharam, Pogathota, Nellore PIN : 524001	524001	Cisco 2901	1	WS-C2960-24TC-L	1	
5	Andhra Pradesh	Rajamundry	Door No.7-28-32, Second Floor T.Nagar, Jupudi Complex Rajahmundry PIN : 533101	360007	Cisco 2901	1	WS-C2960-24TC-S	1	
6	Andhra Pradesh	Tirupathi	Shop no. 10, Sridevi Complex, Tilak Road, Tirupathi - 517501	517501	Cisco 2901	1	WS-C2960-24TC-S	1	
7	Andhra Pradesh	Vijaywada	D.No. 27-14-47, Opp. Buckingham Post Office, Rajagopalachari Street, Vijaywada PIN : 520002	520002	Cisco 2911	1	WS-C2960-24TC-S	1	
8	Andhra Pradesh	Vizag	2nd Floor, C-6, 30-15-158, Pavan Enclave, Daba	530020	Cisco 2901	1	WS-C2960+24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Gardens, Vishakaptanam – 530020.						
9	Assam	Guwahati	Blue Dart Complex ,1st floor Maniram Dewan Lane, G.S. Road Ulubari, Guwahati PIN : 781007	781007	Cisco 2901	1	WS-C2960+24TC-S	1	
10	Assam	Jorhat	K.D. Building,1st Floor Rupahi Ali Garali, Jorhat PIN : 785001	785001	Cisco 2811	1	WS-C2960-24TC-S	1	
11	Assam	Silchar	Progressive Heights, Shop No. 16-17, Ground Floor, Hospital Road, Silchar - 788005	788005	Cisco 2801	1	WS-C2960-24TC-S	1	
12	Assam	Tinsukia	Shyam Kunj Complex, Opp Hero Honda Showroom, Chirwapatty, Tinsukia PIN : 786125	786125	Cisco 2801	1	WS-C2960-24TC-S	1	
13	Bihar	Bhagalpur	Bharti Bhawan,1st floor,Patal Babu Road, Bhagalpur, , Pin Code- 812001	812001	Cisco 2811	1	WS-C2960-24TC-S	1	
14	Bihar	Muzaffarpur	SBJ Tower,Ground floor,Jawaharlal Road, Muzaffarpur-842001	842001	Cisco 2811	1	WS-C2960-24TC-S	1	
15	Bihar	Patna	329, Kidwaipuri First Floor, Main Road,Near Surya Hospital Kidwaipuri, Patna Kidwaipuri First Floor, Main Road,Near Surya Hospital Kidwaipuri, Patna 800001	800001	Cisco 2901	1	WS-C2960-24TC-S / WS-C2960S-24TS-L	2	
16	Chattisgarh	Raipur	Office no 102, First floor,Sky Park Complex,Infront of	492001	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Bhantia Nursing Home,Ravi Nagar, RAIPUR - 492001						
17	Chattisgarh	Bilaspur	Shop No F-8, First Floor, T M Business ParkShrikant Verma Marg, Bilaspur-495001	495001	Cisco 2811	1	WS-C2960-24TC-S	1	
18	Goa	Panaji	2nd Floor, Tamba Building Dr. Atmaram Borkar Road Panaji – Goa PIN : 403001	403001	Cisco 2801	1	WS-C2960-24TC-S	1	
19	Gujarat	Adajan	H – 207, “Manthan” , First floor, Muktanand nagar, Opp – Gujarat Gas Circle , Adajan Road, Adajan , Surat – 395009	395009	Cisco 2901	1	WS-C2960-24TC-S	1	
20	Gujarat	Ahmedabad Hub	03, IFCI BHAVAN , 4th Floor, C.G Road , Near Lal Bunglow, Ahmedabad – 380006	380006	Cisco 2801	1	WS-C3560E-24TD-E / WS-C2960-24TC-S / WS-C2960-48TC-L	2	
21	Gujarat	Ahmedabad Satelite	FF-5 Jyoti Plaza Complex, Shyamal Cross Roads , Satellite , Ahmedabad - 380015	380015	Cisco 2801	1	WS-C2960+24TC-S	1	
22	Gujarat	Anand	204 Jay Ambe Gold, Second Floor,Near Circuit House, Amul Dairy Road, Anand – 388001.	388001	Cisco 2801	1	WS-C2960-24TC-S	1	
23	Gujarat	Ashram Road	Shop No: 106 - First floor , Sukh Sagar Complex, Near Fortune Land Mark Hotel , Usmanpura, Ashram	380005	Cisco 2901	1	WS-C2960-24TC-L	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Road , Ahmedabad – 380005						
24	Gujarat	Baroda (Sayajiganj)	305-308, Paradise Complex, 3rd Floor, Sayajiganj, Vadodara PIN : 390005	305308	Cisco 2901	1	WS-C2960-24TC-L	1	
25	Gujarat	Bharuch	119/A, 1st Floor, Bluechip Complex, Sevashram Road, Bharuch – 392001	392001	Cisco 2901	1	WS-C2960-24TC-S	1	
26	Gujarat	Bhavnagar	1st Floor, G-2 Vasundhra Complex, Opp. Dakshinamurty School, Waghawadi Road, Bhavnagar - 364002.	364002	Cisco 2901	1	WS-C2960-24TC-S	1	
27	Gujarat	Ellorapark	FF - 12, First Floor, Trident Complex, Racecourse Road, Baroda – 390007	390007	Cisco 2801	1	WS-C2960-24TC-S	1	
28	Gujarat	Gandhidham	Shop No 5, Ground Floor, Om Corner, Banking Area, Gandhidham – 370201	370201	Cisco 2901	1	WS-C2960-24TC-S	1	
29	Gujarat	Gandhinagar	Plot No.447,Second Floor, Sector-16,GH-5,Near Pragna Petrol Pump,Gandhinagar.	382810	Cisco 2811	1	WS-C2960-24TC-S	1	
30	Gujarat	Harni Warasia	SHCIL , Shruti Avenue 1st Floor, Office no: 8-9, Near Jyoti Park, Water,Tank Road Karelibaug, Vadodara- 390018	390018	Cisco 2901	1	WS-C2960-24TC-S	1	
31	Gujarat	Jamnagar	Shop No 6, 7 and 8, Madhav Darshan Complex, Opp. Cricket	361003	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Bungalow, Gurudwara Road, Jamnagar PIN : 361003						
32	Gujarat	Junagadh	Platinum Complex, Jayshree Talkies Road, Behind Aroon, Opposite Mahasagar Travels, Kalwa Chowk, Junagarh - 362001	362001	Cisco 2801	1	WS-C2960-24TC-S	1	
33	Gujarat	Maninagar	101,first floor, ratna complex, Maninagar char rasta Ahmedabad 380008	380008	Cisco 2911	1	WS-C2960-24TC-S	1	
34	Gujarat	Mehsana	Office No. 27, 28, 29, 1st Floor, Sheth Punjiram Chambers, Radhanpur, Road, Mehsana - 384002	384002	Cisco 2801	1	WS-C2960-24TC-S	1	
35	Gujarat	Motera	209, Shukan Mall, Near Virat Petrol Pump, Motera, Sabarmati, Ahmdabad-05	395003	Cisco 2801	1	WS-C2960-24TC-S	1	
36	Gujarat	Navsari	FF Nanu Vishnu Dham, Swami Vivekanand Road, Kansarawad, Navasari- 396445	396445	Cisco 2801	1	WS-C2960-24TC-L	1	
37	Gujarat	Porbandar	Purusharth, Ground Floor, Behind Aroon Photo Studio, M.G Road, Porbandar, PIN : 360575	360575	Cisco 2901	1	WS-C2960-24TC-L	1	
38	Gujarat	Rajkot Hub	Shree Sadguru Complex, 1st Floor, Opp. Tirupati Petrol Pump, Kalawad Road, Rajkot PIN : 360007	360007	Cisco 3945	1	WS-C2960-24TC-S / WS-C2960-24TC-S	2	
39	Gujarat	Surat Ring Road	201, Shree Shyam Chambers, Opp. Sub Jail	395002	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			, Ring Road , Surat - PIN : 395002						
40	Gujarat	Surat Citilight	UG-7, Upper Ground Floor, Eco Futurz, New Citylight Road, Surat – 395007	395007	Cisco 2801	1	WS-C2960-24TC-S	1	
41	Gujarat	Visnagar	Stock Holding Corporation of I Ltd. 1st Floor, Shop No 5 & 6, M N College Road, Jyot Complex, Visnagar : 384315	384315	Cisco 2801	1	WS-C2960-24TC-S	1	
42	Gujarat	GiftCity	308 A , Signature Building , 3rd Floor Block 13 B Zone 1 Giftcity Gandhinagar Ahmedabad GUJARAT India 382355	382355	Cisco 1921	1	WS-C2960+24TC-S	1	
43	Gujarat	Morbi	Shop No. 2, First Floor, Yadunandan Complex, Ravapar Road, Morbi - 363641,.	363641	Cisco 2801	1	WS-C2960-24TT-L	1	
44	Haryana	Ambala	5502, Nicholson Road 1 St Floor, Opp. Nigar Cinema Surya Tower, Ambala Cantt PIN : 133001	133001	Cisco 2911	1	WS-C2960-24TC-L	1	
45	Haryana	Gurgaon	Shop No. 251, Central Arcade, 1st Floor, Opposite To Sahara Mall, Dlf Phase Ii, Gurgaon, PIN : 122002	122002	Cisco 2801	1	WS-C2960-24TC-S	1	
46	Haryana	Karnal	Ist Floor,16, Mahila Ashram Complex, Behind Main Bus Stand, Karnal PIN : 132001	132001	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



47	Haryana	Panchkula	SCO 48 First Floor Sector 11 Panchkula 134112	134112	Cisco 2811	1	WS-C2960-24TC-S	1	
48	Himachal Pradesh	Shimla	P.C. Chambers, Ridge, Ritz Cinema Road, Near Mall Road, Shimla, PIN : 171001	171001	Cisco 2801	1	WS-C2960-24TC-S	1	
49	Himachal Pradesh	Haldwani	U-38, Phase-II, Durga city Centre, Bhotia Parao, Haldwani-263139	263139	Cisco 2901	1	WS-C2960-24TC-S	1	
50	Himachal Pradesh	Solan	Platinum Mall,Ground Floor South Enclave, Saproon Bye Pass- Solan PIN : 173211	173211	Cisco 2901	1	WS-C2960-24TC-S	1	
51	Jammu Kashmir	Jammu	83 - A/D Extn Near Police Lines Gandhi Nagar, Jammu PIN : 180004	180004	Cisco 2901	1	WS-C2960-24TC-S	1	
52	Jammu Kashmir	Srinagar	Prince Residency , 1st Floor , BB Cant., Broadway, Sonwar (Batwara) Srinagar - J & K , PIN- 190004	190004	Cisco 2901	1	WS-C2960-24TT-L	1	
53	Jharkhand	Bokaro	C1-22C , Sector IV, City Centre, Bokaro Steel City , Bokaro - 827004	827004	Cisco 2801	1	WS-C2960-24TC-S	1	
54	Jharkhand	Dhanbad	101, 1st floor,Shanti Bhavan, Bank More street , Dhanbad PIN : 826001	826001	Cisco 2811	1	WS-C2960-24TC-S	1	
55	Jharkhand	Hazaribagh	Above Central Bank Of India Bodam Bazar Malviya Marg, Hazaribagh PIN : 825301	825301	Cisco 2801	1	WS-C2960S-24TS-S	1	
56	Jharkhand	Jamshedpur	Shanti Niketan Bldg., 2nd Floor , I.S.B Shop Area,	831001	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Bistupur Main Road, Jamshedpur PIN : 831001						
57	Jharkhand	Ranchi	5, Arjan Place, 3rd Floor, Main Road, Ranchi PIN : 834001	533101	Cisco 2901	1	WS-C2960-24TC-S	1	
58	Karnataka	Bangalore Hub	Bangalore Stock Exchange Ltd., Stock Exchange Towers, 51, 1st Cross, J.C. Road, Bangalore, PIN : 560027	560027	Cisco 3945	1	WS-C2960-24TC- S/WS-C2960-24TC- S/WS-C2960-24TC- S	3	
59	Karnataka	Belgaum	Basavakrupa 1, Club Road , Opp. Civil Hospital, Near Hansraj Supermarket, Belgaum, PIN : 590002	390005	Cisco 2801	1	WS-C2960-24TC-S	1	
60	Karnataka	Bellary	D No.342/1 A/1 CHIRANJEEVI NILAYA SHUBHA MAHAL 1st CROSS , GANDHI NAGAR, Bellary 583101	583101	Cisco 2811	1	WS-C2960-24TC-L	1	
61	Karnataka	Bhagalkot	Melligeri Towers , Shop No Upper Ground floor 37 and 38, Bagalkot 587101.	587101	Cisco 2901	1	WS-C2960-24TC-S	1	
62	Karnataka	Davangare	1st Floor, Above Mahalakshmi Book Depot, AVK College Road, P. J. Extension, Davangere-577002	577002	Cisco 2901	1	WS-C2960-24TC-S	1	
63	Karnataka	Dharwad	Sri Ranga Tower, Ground Floor, Opp NTTF, Near Ramnagar Cross P B Road, Dharwad - 580001	580001	Cisco 2801	1	WS-C2960-24TC-S	1	
64	Karnataka	Gulbarga	G1 And G2, Shruti Arcade Opp.St.Mary"S Chruch, Court Road Off S	585102	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			B Temple Road, Gulbarga PIN : 585102						
65	Karnataka	Hassan	Door No.2324/2110, First Floor, Dyuthi Arcade, Opp. KEB Office, 2nd Main, KR Puram, Hassan – 573201	573201	Cisco 2801	1	WS-C2960-24TC-S	1	
66	Karnataka	Hubli	1st Floor, Varsha Complex, Next To Corporation Bank, Behind Bhavani Arcade, Opp Basava Vana, Near Old Bus Stand, Hubli PIN : 580029	580029	Cisco 2911	1	WS-C2960+24TC-S	1	
67	Karnataka	Jayanagar	Shop No.7, 1st Floor, #44, 33rd Cross, Jayanagar, 4th T Block, Bangalore PIN : 560011	560011	Cisco 2811	1	WS-C2960-24TC-S	1	
68	Karnataka	Karkala	SHOP NO 12 , D NO 127/23, FIRST FLOOR, SHARADA PALACE, MARKET ROAD, KARKALA - 574104	574104	Cisco 2901	1	WS-C2960-48TC-L	1	
69	Karnataka	Koramangala	Ahad Chambers,No.406, Ground Floor,Koramangala, 7th Block Bangalore - 560095	560095	Cisco 2801	1	WS-C2960-24TC-S	1	
70	Karnataka	Kundapur	Door No. 433/1/51, Near Manunath Nursing Home, Mastikatte Main Road, Kundapur PIN : 576201	576201	Cisco 2801	1	WS-C2960-24TC-L	1	
71	Karnataka	Malleswaram	No. 10, 1 floor, 3rd cross, Malleswaram - Bangalore – 560003	560003	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



72	Karnataka	Mangalore	2nd Floor, Manasa Towers, M G Road,Mangalore PIN : 575003	575003	Cisco 2801	1	WS-C2960-24TC-S	1	
73	Karnataka	Mysore	Lakshman Plaza, 442/3 & 4, 1st Floor, Near Ramaswami Circle, Chamaraja Double Road, Mysore PIN : 570024	570024	Cisco 2811	1	WS-C2960-24TC-S	1	
74	Karnataka	Raichur	59/A-1, Shreyansh Towers 1st Floor, Above Bank Of Maharastra M.G Road, Raichur PIN : 584101	584101	Cisco 2801	1	WS-C2960-24TC-S	1	
75	Karnataka	Shimoga	1st Floor, Sangappa Complex, Garden Area, 3rd Cross , Beside State Bank Of Hyderabad, Shimoga PIN : 577201	577201	Cisco 2901	1	WS-C2960+24TC-S	1	
76	Karnataka	Udupi	Laxmi Prasad Building, 1st Floor, Opp: MESCOM, MarutiVeethika Road, Udupi PIN : 576101	576101	Cisco 2901	1	WS-C2960-24TC-S	1	
77	Karnataka	Yelahanka	Ankad Building no 960 ,LIG ,B sector,1st floor ,Yelahanka new town,Bangalore, 560064	560064	Cisco 2901	1	WS-C2960-24TT-L	1	
78	Kerala	Calicut	Metro Towers, 19/2084-B/20, 1st Floor, P.V. Swamy Road, Chalappuram P.O., Calicut PIN : 673002	673002	Cisco 2901	1	WS-C2960-24TC-S	1	
79	Kerala	Kannur	2nd Floor K.V.R. Towers, South Bazar Kannur PIN : 670002	670002	Cisco 2811	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



80	Kerala	Kochi Hub	Safeena Mansion, Ground Floor, Ravipuram Junction. Opp: Deepa Theatre, (Behind Central Bank of India) M G Road, Ernakulam . 682016	682016	Cisco 2801	1	WS-C2960-24TC-S	2	
81	Kerala	Kollam	E-2-24/25 2nd Floor, Commercial Complex, East Block Bishop Jerome Nagar, Chinnakada PIN : 691001	691001	Cisco 2811	1	WS-C2960-24TC-S	1	
82	Kerala	Kottayam	Madappallil, Room No: 572 F , 1st Floor, Sasthri Road , Kottayam - 680001	680001	Cisco 2801	1	WS-C2960-24TC-S	1	
83	Kerala	Trichur	Pooma Complex, 3rd Floor M G Road, Trichur PIN : 680001	680001	Cisco 2901	1	WS-C2960-24TC-S	1	
84	Kerala	Trivandrum	T.C No:16/1999 (1),Ground Floor , Suha Residency, situate, lying and being at Poonthi Road,Kumarapuram,Medical College P O. Thiruvananthapuram - 695011	695011	Cisco 2901	1	WS-C2960-24TC-S	1	
85	Madhya Pradesh	Bhopal	Alankar Comple,Plot No. 11, First Floor, Shop no 6, M.P.Nagar, Zone - II,Bhopal (M.P.) 462011	462011	Cisco 2901	1	WS-C2960-24TC-S	2	
86	Madhya Pradesh	Gwalior	Ground Floor , Plot No. 11 , Orion Tower ,City Centre ,Gwalior - 474011	474011	Cisco 2811	1	WS-C2960-24TC-S	1	
87	Madhya Pradesh	Indore	201-202, 2nd Floor, D.M. Towers, Race Course	452001	Cisco 2901	1	WS-C2960-24TC-L	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Road, Janjirwala Square, INDORE - 452001						
88	Madhya Pradesh	Jabalpur	7 Ankita Complex, 2nd Floor, Opp. Prabhu Vandana Talkies, Civic Center , Jabalpur PIN : 482001	482001	Cisco 2901	1	WS-C2960-24TC-S	1	
89	Madhya Pradesh	Ujjain	Office Number: 4, 1st Floor , Siddhi Vinayak Trade Centre, Opposite To Shaheed Park, Freeganj, Ujjain PIN : 456001	456001	Cisco 2801	1	WS-C2960-24TT-L	1	
90	Maharashtra	Ahmednagar	House No. 2440, First Floor,Above Indusind Bank, Telikhunt, Ahmednagar, Maharashtra - 414001	414001	Cisco 2801	1	WS-C2960-24TC-S	1	
91	Maharashtra	Amravati	Block No 82,Glushan Market Mofussil Plots, Near Panchasheel Talkies, Jaistambh Chowk, Amravati PIN : 444601	444601	Cisco 2901	1	WS-C2960-24TC-L	1	
92	Maharashtra	Aurangabad	Ragbhir Chambers, Above Idbi Bank, 1st Floor, Vidya Nagar, Jalna Road, Aurangabad PIN : 431005	431005	Cisco 2901	1	WS-C2960-24TC-S	1	
93	Maharashtra	Chandrapur	2nd Flr Raghuvanshi Complex Near Azad Garden Main Road PIN : 442702	442702	Cisco 2901	1	WS-C2960-24TC-S	1	
94	Maharashtra	Dombivali	Swanand building First floor, Above Bank of	421201	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Baroda ATM , Rajaji Path Road Ramnagar, Dombivli (East) - 421201						
95	Maharashtra	Ghatkopar	Shop No. 2/3, Ground Floor Vishwa Nagar Co. Hsg. Soc. , Ghatkopar(E), Mumbai - 400077	400077	Cisco 2901	1	WS-C2960-24TC-L	1	
96	Maharashtra	Goregaon	G-2 Unique Tower, Ground Floor, Gaiwadi Indl. Estate, Near Kamats Club , Off S V Road , Goregaon(West) - 400622	400622	Cisco 2901	1	WS-C2960-24TC-S	1	
97	Maharashtra	Jalgaon	OM Chambers, 3 and 4, Ground Floor, Court Street , Jalgaon - 425001	425001	Cisco 2801	1	WS-C2960-24TC-S	1	
98	Maharashtra	Kalyan	Shop No 1, Ground Floor, Gayatri Sankul, Oak Baug, Opp Railway Station, Kalyan West, Thane - 421 301	421301	Cisco 2911	1	WS-C2960-24TC-S	1	
99	Maharashtra	Kharghar	Shop No-3,Ground Floor,Ambika Heritage CHS,Plot No-1,Sector- 1,Opp Kharghar Railway Station,Kharghar,Navi Mumbai-410210	410210	Cisco 1841	1	WS-C2960G-24TC-L	1	
100	Maharashtra	Kolhapur	Ayodhya Towers, 4th Floor, 511 Kh, E - Ward, Near Dabolkar Corner , Station Road, Kolhapur PIN : 416001	416001	Cisco 2901	1	WS-C2960-24TC-S	1	
101	Maharashtra	Nagpur – 1 (Dhantoli)	3rd Floor, Saraf Court, Opposite Yashwant Stadium, Dhantoli, Nagpur - 440012	570024	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



102	Maharashtra	Nagpur – 2 (Vishnu Complex)	1st Floor, Vishnu Complex, Opp. Rahate Hospital C. A. Road, Nagpur – 440008	440008	Cisco 2901	1	WS-C2960-24TC-S	1	
103	Maharashtra	Nanded	Shop No-05, Kothari Complex, First Floor, Shivaji Nagar, Nanded – 431602	431602	Cisco 2901	1	WS-C2960-24TC-S	1	
104	Maharashtra	Nashik	F8, 1st Floor, Suyojit Sankul, Adj. To Rajiv Gandhi Bhavan (Nmc), Saharanpur Road, Nasik PIN : 422002	422002	Cisco 2901	1	WS-C2960-24TC-S	1	
105	Maharashtra	Pune – 3	5/33, Agarkar Nagar, CTS No. 12 & 12/1(Part), Bund Garden Road, Near Alankar Theatre, Pune – 411001	411001	Cisco 2901	1	WS-C2960-24TC-S	1	
106	Maharashtra	Pune JM Road	Unit No. 102, 1st Floor, Kamayani Tower, V M Joshi Marg , Off J M Road Pune - 411005	411005	Cisco 2911	1	WS-C2960-24TC-S	1	
107	Maharashtra	Pune Akurdi (Chinchwad)	Shop No. 40, ground floor, Tapasvi Plaza, Near Khandoba Chowk, Bombay Pune Road, Akurdi, ,Pune 411019	411019	Cisco 2801	1	WS-C2960-24TC-S	1	
108	Maharashtra	Pune Pimple Saudagar	Shop No. 171, First Floor, Vision 9 Mall, Roseland Residency Road, Pimple Saudagar, Pimpri-Chinchwad 411027	411027	Cisco 2811	1	WS-C2960-24TC-S	1	
109	Maharashtra	Sangli	Gomtesh Padmavati 111/112 Mahaveer Nagar	416416	Cisco 2811	1	WS-C2960-24TT-L	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Sangli PIN : 416416 (Maharastra)						
110	Maharashtra	Vashi	C1/12/0.2, Ground Floor, Sector -2, Near Abudaya bank, Opp. Shanti Center-Vashi , Navi Mumbai - 400 703	400703	Cisco 2801	1	WS-C2960-24TC-S	1	
111	Maharashtra	Vikhroli	25 Hazari Baug, Ground Floor, Station Road, Vikhroli West, Mumbai – 400083	400083	Cisco 2901	1	WS-C2960-24TC-S	1	
112	Maharashtra	Yawatmal	Shop No. 18,19,20,21 1st Floor Super Bazaar, Sbi Square Yawatmal PIN : 445001	445001	Cisco 2801	1	WS-C2960-24TC-S	1	
113	Maharashtra	Andheri	Shop No. 4,Parsian Apartments,V.P. Road Next To Zorostrrian Co-Op. Bank Ltd. Off S. V. Road, Andheri(West) PIN : 400058	400058	Cisco 2811	1	WS-C2960-24TC-S	1	
114	Maharashtra	Borivali	Shop No.3, Tulsi Baug CHSL, MayFair 14,Behind Prabhodhankar Thackeray Naatya Mandir,Ramdas Surtale Marg, Off Chandavarkar Road, Borivali West , Mumbai - 400 092.	400920	Cisco 2801	1	WS-C2960-24TC-S	1	
115	Maharashtra	Chembur	First Floor, Ramesh Niwas, Road No. 20, Near SBI ,Chembur, Mumbai – 400071	400071	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



116	Maharashtra	Dadar	Trisandhya CHS, G2 - B303 , Gr. Floor, Dadasaheb Phalke Road, Dadar East, Mumbai - 400014	400014	Cisco 2801	1	WS-C2960-24TC-S	1	
117	Maharashtra	Mahalaxmi	Orbit Height , 'E'-Wing , Shop No. 5 ,Ground Floor, Javji Dadaji Marg, Mahalaksmi Mumbai MAHARASHTRA India. 400007	400007	Cisco 2911	1	WS-C2960-24TC-S	1	
118	Maharashtra	Mulund	Shop No.11, Ground Floor , Manisha Pride, J. Nehru Road, Mulund – West , Mumbai 400 080	400800	Cisco 2901	1	WS-C2960-24TC-S	1	
119	Maharashtra	Thane	shop no 8 and 9 , ground floor, Pride Enclave , Apollo society , Vishnu Nagar, Naupada , Thane West, vishnu nagar , Naupada, Thane - 400602	400602	Cisco 2911	1	WS-C2960-24TC-S	1	
120	Maharashtra	Vileparle	104 , Shyam Kamala, Opp Vile Parle Station Vile Parle(E) , Mumbai - 400 057	400570	Cisco 2901	1	WS-C2960-24TC-S	1	
121	Maharashtra	Raheja Chambers	Raheja Chambers, Office Number 15,Ground Floor, Nariman Point, Mumbai – 400021	400021	Cisco 2811	1	WS-C2960-24TC-S	1	
122	Maharashtra	Parel	4,Tirupati CHS,Ground Floor,Dr. S. S. Rao Raod, Parel, Mumbai - 400012	400012	Cisco 2901	1	WS-C2960-24TC-S	1	
123	Maharashtra	Sify Airoli	C/O Airoli IDC, 5th, 6th & 7th Floor, Reliable Plaza, Plot No. K- 10, Kalwa	400706	Cisco 2901	1	WS-C2960-24TC-S	1	Switches Not to be replaced

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Industrial Area, Airoli, Navi Mumbai - 400706.						
124	Maharashtra	Fort	UTI Building, 12/14 Bank Street, Cross Lane, Fort, Mumbai – 400023	400023	Cisco 2821 / Cisco 2921	2	WS-C3850-48T-E	4	Switches Not to be replaced
125	Maharashtra	Center Point- Parel	Centre Point, Unit No. 301, 3rd Floor, Dr. B. Ambedkar Road, Parel, MUMBAI- 400012	400012	Cisco 3945	2	WS-C3850-48T-E	6	Switches Not to be replaced
126	New Delhi	Bhikaji Cama Place	Gr. Flr., Shop # Gf-13, Bldg No. 3, Ansal Chambers - I, Bikaji Cama Place, New Delhi PIN : 110066	110066	Cisco 2811	1	WS-C2960-24TC-S	1	
127	New Delhi	Delhi Hub	5th Floor(Half), A-Wing, IFCI Tower, 61 Nehru Place, New Delhi - 110019	110019	Cisco 3945	1	WS-C2960-24TC-S	3	
128	New Delhi	Janakpuri	103, 1st Floor, Suneja Tower-1, Janakpuri District Centre, Janakpuri, New Delhi PIN : 110058	110058	Cisco 2901	1	WS-C2960-24TC-S	1	
129	New Delhi	Janpath	68/2 (Above Mehrasons Jewellers), Janpath, New Delhi PIN : 110001 (New Delhi)	110001	Cisco 2801	1	WS-C2960-24TC-S	1	
130	New Delhi	Karkardooma	401, Fourth Floor,Ashish Corporate Tower Community Centre, Karkardooma, Vikas Marg, New Delhi PIN : 110092 (New Delhi)	110092	Cisco 2801	1	WS-C2960-24TC-S	1	
131	New Delhi	Milap	Milap Bldg., Gr. Flr., Bahadur Shah Zafar	110002	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Marg, New Delhi PIN : 110002 (New Delhi)						
132	New Delhi	Pitampura	504, 5th Floor, B-08, Gditi, Netaji Subash Place, Pitampura, Delhi PIN : 110034 (New Delhi)	110034	Cisco 2811	1	WS-C2960-24TC-S	1	
133	Meghalaya	Shillong	Parkside Building, Ground Floor, Barik, Shillong- 793001, Meghalaya Parkside Building, Ground Floor, Barik, Shillong 793001	793001	Cisco 2811	1	WS-C2960-24TT-L	1	
134	Odisha	Agartala	88, Motor Station Road, 1st Floor, Opposite Petrol Pump, Agartala - 799001 (Tripura)	799001	Cisco 2901	1	WS-C2960-24TC-S	1	
135	Odisha	Bhubaneshwar	No 101, First Floor , TKR Business Center, Plot no 2132/4711(Above ICICI Bank ltd) Vivekanand Marg Po: Old town Bhubaneshwar 751002	751002	Cisco 2811	1	WS-C2960-24TC-S	1	
136	Odisha	Cuttack	1st Floor Sumitra Plaza , Cuttack - 753012	753012	Cisco 2811	1	WS-C2960-24TC-S	1	
137	Odisha	Rourkela	Plot No. 307/2050, Behind Pani Market Complex, Udit Nagar, Rourkela : 769012	769012	Cisco 2801	1	WS-C2960-24TC-S	1	
138	Odisha	Angul	Ground Floor, Om Tower, Shankar Cinema Road, Angul -759122 ,Odisha	759122	Cisco 2801	1	WS-C2960-24TC-L	1	
139	Puducherry	Pondicherry	1st Floor, 201 Mission Street, Above Bharat	605001	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Overseas Bank, Pondicherry PIN : 605001						
140	Punjab	Amritsar	4-Deep Complex, 1st Floor, Court Road, Amritsar-143001	143001	Cisco 2901	1	WS-C2960-24TC-S	1	
141	Punjab	Bhatinda	MC.4373, 1st Floor, Opp. Indian Overseas Bank, Kikar Bazar, Bhatinda PIN : 151005	151005	Cisco 2801	1	WS-C2960-24TC-S	1	
142	Punjab	Chandigarh	Second Floor, Sco 154- 155, Sector 17 C , Chandigarh - PIN : 160017	160017	Cisco 2901	1	WS-C2960-24TC-S	1	
143	Punjab	Jalandhar	SCO 33 , Multani Tower, PUDA Complex, Opp Tehsil Complex, Jalandhar -144001	144001	Cisco 2911	1	WS-C2960-24TC-S	1	
144	Punjab	Ludhiana	Cabin No. 501, 5th Floor, Sco 18, Feroze Gandhi Market, Ludhiana PIN : 141001	141001	Cisco 2901	1	WS-C2960-24TC-S	1	
145	Punjab	Moga	Nifd Campus, 531/9, New Town, Opp D.M. College Moga PIN : 142001	142001	Cisco 2801	1	WS-C2960-24TC-S	1	
146	Punjab	Mohali	S.C.F 33, First Floor, Phase 5, Mohali PIN : 160059	160059	Cisco 2811	1	WS-C2960-24TC-S	1	
147	Punjab	Pathankot	Manav Complex,SCO:S7 39:40,Upper Ground Floor Patel Chowk,Pathankot Punjab 145001	145001	Cisco 2801	1	WS-C2960-24TC-S	1	
148	Punjab	Patiala	Shop No. 6 & 7, Leela Bhawan Market Patiala PIN : 147001	147001	Cisco 2901	1	WS-C2960-24TC-S	1	
149	Punjab	Phagwara	OHRI Towers, 1st Floor, Above ICICI Bank, G.T.	144401	Cisco 2811	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Road Phagwara Punjab 144401.						
150	Rajasthan	Ajmer	Mudgal Height Ground floor, Opposite Swastik HP petrol pump, Rajendrapura Agra Gate, Jaipur Road, Ajmer - 305001	305001	Cisco 2901	1	WS-C2960+24TC-S	1	
151	Rajasthan	Alwar	Siddhivinayak Corporate, 1st Floor, Plot No 6, Lajpat Nagar, Scheme No. 2, Alwar - 301001	301001	Cisco 2901	1	WS-C2960-24TC-S	1	
152	Rajasthan	Bikaner	Opp. Drm House Near Railway Stadium Bikaner PIN : 334001	334001	Cisco 2901	1	WS-C2960-24TC-S	1	
153	Rajasthan	Jaipur (Nawal Tower)	Unit No.C First Floor, Nawal Tower, A-1, Jawahar Lal Nehru Marg, Jaipur 302017	302017	Cisco 2801	1	WS-C2960-24TC-S	1	
154	Rajasthan	Jaipur (Sangam Tower)	Sangam Tower, 2nd Floor Office No. 213, Church Road, Jaipur PIN : 302001	302001	Cisco 2901	1	WS-C2960-24TC-S	1	
155	Rajasthan	Jodhpur	1st Floor, Gulab Bhavan Chopasni Rd., Near Kankariya Bldg. Jodhpur PIN : 342003	342003	Cisco 2901	1	WS-C2960-24TC-S	1	
156	Rajasthan	Kota	Mewara Plaza, 344, Shopping Centre Rawat Bhata-Guman Pura Road Kota PIN : 324007	324007	Cisco 2801	1	WS-C2960-24TC-S	1	
157	Rajasthan	Sriganganagar	SHCIL , 3rd Floor, 53 B – Block, Agarwal Building, Near Ravindra Path Main Road, Sriganganagar 335001	335001	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



158	Rajasthan	Udaipur	11-12, Ground Floor, Anand Plaza, Near Ayad Bridge, University Road, Udaipur-313001	313001	Cisco 2901	1	WS-C2960-24TC-S	1	
159	Tamilnadu	Adayar	51/25,first Floor,Gandhi Nagar, 1st Main Road,Adyar Business court ,adyar, chennai- 600020	600020	Cisco 2811	1	WS-C2960-48TT-S	1	
160	Tamilnadu	Anna Nagar	Old No. W-101 , New No. 46 And 48 Second Avenue , Annanagar Chennai PIN : 600040	600040	Cisco 2801	1	WS-C2960-24TC-S	1	
161	Tamilnadu	Chennai Hub	Justice Basheer Ahmed Sayeed Bldg, 3rd Flr, 45, Moore Street , Second Line Beach, Chennai PIN : 600001	600001	Cisco 3945	1	WS-C2960-24TC-S / WS-C2960-24TC-S / WS-C2960-24TC-S	3	
162	Tamilnadu	Coimbatore	A - 108,1st Floor,Raheja Center, 1073/ 74 Avinashi Road, Coimbatore PIN : 641018	641018	Cisco 2901	1	WS-C2960-24TC-S	1	
163	Tamilnadu	Erode	159 A , First Floor , Parimalam Complex , Mettur Road , Erode – 638011	638011	Cisco 2801	1	WS-C2960-24TC-S	1	
164	Tamilnadu	Karaikudi	No.45, 3rd Floor, SPK Corporate Centre,Shanmugha Raja Road, Karaikudi -630001	630001	Cisco 2801	1	WS-C2960-24TC-S	1	
165	Tamilnadu	Karur	128 A, Vanitha Towers First Floor, Covai Road, Karur PIN : 639002	639002	Cisco 2801	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



166	Tamilnadu	Madurai	C-1, 3rd Floor,, A.R. Plaza 16-17 North Veli Street, Madurai PIN : 625001	625001	Cisco 2901	1	WS-C2960-24TC-S	1	
167	Tamilnadu	Mylapore	Shop No : 1b, 4/180 Tnhb Complex, Luz Corner, Mylapore , Chennai PIN : 600004	600004	Cisco 2801	1	WS-C2960-24TC-S	1	
168	Tamilnadu	Porur	Arut Jothi Towers, 1st Floor, No.2 And 9, Shakthi Nagar, Mount Ponnamalle High Rode, Porur, Chennai PIN : 600116	600116	Cisco 2901	1	WS-C2960-24TC-S	1	
169	Tamilnadu	Salem	5 / 1 , First Floor , Sri Lakshmi Complex, No 76, Cherry Road, Opp to Government Arts College, Salem - 636007.	636007	Cisco 2801	1	WS-C2960-24TC-S	1	
170	Tamilnadu	T. Nagar	202, 2nd Floor, Challa Malli Complex, 11/11/A, Sir Theagaraya Road, T Nagar Chennai PIN : 600017	600017	Cisco 2801	1	WS-C2960-24TC-S	1	
171	Tamilnadu	Tambaram	Branch Shop No 8 And 9, First Floor, 68/22 A, Kakkan Street, Tambaram West, Chennai PIN : 600045	600045	Cisco 2811	1	WS-C2960-24TC-S	1	
172	Tamilnadu	Trichy	Ramanathan Arcade,First Floor, No:16,K.C Road Thennur,Trichy – 620017.	620017	Cisco 2901	1	WS-C2960-24TC-S	1	
173	Tamilnadu	Tuticorin	Anbu Medical Complex, 285/8d, 1st Floor, W.G.C	628002	Cisco 2811	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Road, Tuticorin PIN : 628002						
174	Tamilnadu	Velachery	No.3A, 1st floor , Taramani 100 feet road,Tansi Nagar, Velachery,Landmark: Near Derby Showroom,Chennai- 600042	600042	Cisco 2911	1	WS-C2960+24TC-S	1	
175	Tamilnadu	West Mambalam	Navin Iswarya, ground floor New No:84: old no 48,Brindavan street, West Mambalam,Chennai 600033	600033	Cisco 2911	1	WS-C2960-24TC-S	1	
176	Telangana	Dilsukhnagar	1st floor, LEGEND RINDA CAPITAL, Moosaram bagh, Hyderabad, -500036 Phone : 040 - 24151197 & 21451203	500036	Cisco 2811	1	WS-C2960-48TT-S	1	
177	Telangana	Himayatnagar	3-6-269, G-6 And 7, Ground Floor Opp Telugu Academy,Himayath Nagar Hyderabad PIN : 500029	500029	Cisco 2901	1	WS-C2960-24TC-L	1	
178	Telangana	Hyderabad Hub	G6- G10, East Block Swarana Jayanthi Commercial Complex, Beside Huda Maitrivanam, Ameerpet,Hyderabad : 500038	500038	FORTINET	1	WS-C2960-24TC-S / WS-C2960-24TC-S / WS-C2960-24TC-L	3	
179	Telangana	Kukatpally	Shop No.5, Siddhartha Towers, 3-3-6, Sumithra Nagar,Opp. Metro Pillar	500072	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			No. 789, Kukatpally, Hyderabad - 500072						
180	Telangana	Nizamabad	Block E, 1st Floor, Kavita Complex, Go Down Road Nizamabad PIN : 503001	503001	Cisco 2811	1	WS-C2960-24TC-S	1	
181	Telangana	Secunderabad	Sona Accord Ground Floor, No.9-1-199/2/55/B St. Mary's Road, Secunderabad - 500003	500003	Cisco 2901	1	WS-C2960-24TC-S	1	
182	Telangana	Warangal	Shop No. 16, 1st Floor H No 5-9-36,37 Lashkar Bazar Hanamkonda Main Road, Warangal PIN : 506001	506001	Cisco 2801	1	WS-C2960-24TC-L	1	
183	Uttar Pradesh	Agra	6, Awagarh House, M.G. Road, Civil Lines, Agra PIN : 282001 (Uttar Pradesh)	282001	Cisco 2901	1	WS-C2960-24TC-S	1	
184	Uttar Pradesh	Bareilly	167,Civil Lines,1st Floor,Station Road,Bareilly-243001	243001	Cisco 2801	1	WS-C2960X-24TS-L	1	
185	Uttar Pradesh	Ghaziabad	18/3, First Floor, Above IDBI Bank, Model Town East, Ghaziabad – 201001 (Uttar Pradesh)	201001	Cisco 2801	1	WS-C2960-24TC-L	1	
186	Uttar Pradesh	Greater Noida	Room No-303,3rd Floor,K Son's,Alfa Commercial Belt-1,Uttar Pradesh,Greater Noida- 201308	201308	Cisco 2901	1	WS-C2960-24TT-L	1	
187	Uttar Pradesh	Jhansi	Shanti Complex,372, Civil Lines,1st Floor,Gwalior Road,Jhansi,UP-284001	284001	Cisco 2801	1	WS-C2960X-24TS-L	1	
188	Uttar Pradesh	Meerut	T-306, 3rd Floor, Ganga Plaza, Begum Bridge	250002	Cisco 2901	1	WS-C2960-24TC-S	1	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



			Road, Meerut PIN : 250002 (Uttar Pradesh)						
189	Uttar Pradesh	Noida	208, Ocean Plaza, Sector - 18, Noida PIN : 201301 (Uttar Pradesh)	201301	Cisco 2901	1	WS-C2960-24TC-S	1	
190	Uttar Pradesh	Mathura	Tera Tower 1stFloor Bhuteshwar Road, Mathura, U.P – 281004	281004	Cisco 2901	1	WS-C2960G-24TCL	1	
191	Uttar Pradesh	Moradabad	Das Building, Ground Floor Raj Mahal Road Moradabad- 244001	244001	Cisco 2811	1	WS-C2960-24TC-S	1	
192	Uttar Pradesh	Saharanpur	Thrill Market F-10 First floor court road Saharanpur U.P- 247001	247001	Cisco 2901	1	WS-C2960-24TC-S	1	
193	Uttar Pradesh	Aligarh	Manglam Complex, 1st flood,32A-1F, Samad Road, Aligarh - U.P. - 202001	202001	Cisco 2801	1	WS-C2960G-24TC-L	1	
194	Uttar Pradesh	Allahabad	G-4, L.D.A. Center, Ground Floor, 2 , Sardar Patel Marg, Civil Lines Allahabad PIN : 211001 (Uttar Pradesh)	211001	Cisco 2911	1	WS-C2960-24TC-S	1	
195	Uttar Pradesh	Gorakhpur	Office No. 16,17,18, III Floor The Mall , Cross Road, Bank Road ,Gorakhpur PIN : 273001 (Uttar Pradesh)	273001	Cisco 2901	1	WS-C2960-24TC-S	1	
196	Uttar Pradesh	Kanpur Hub	Ground Floor Krishna Towers 15/63 Civil Lines, Kanpur PIN : 208001 (Uttar Pradesh)	208001	Cisco 3945	1	WS-C2960-48TT-S / WS-C2960-48TT-S	2	
197	Uttar Pradesh	Lucknow – 1 (SapruMarg)	36/15, 1st floor, Opp. Rohit Bhawan, Sapru Marg , Lucknow -226001 (Uttar Pradesh)	226001	FORTINET	1	WS-C2960-24TC-S / WS-C2960-24TC-L	2	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



198	Uttar Pradesh	Mughalsarai	Shop No-1, 1st Floor, B.N.Complex, G.T Road, Circus Mod,Mugalsarai,Chauda uli - 232101(uttar Pradesh)	232101	Cisco 2901	1	WS-C2960+24TC-S	1	
199	Uttar Pradesh	Varanasi – 1	D-58/2, 4th Floor, Kuber Complex, Rath Yatra, Varanasi PIN : 221010 (Uttar Pradesh)	221010	Cisco 2901	1	WS-C2960-24TC-S	1	
200	Uttar Pradesh	Varanasi – 2	Hashmi Complex, S 2 / 639 – 18, Near J.P. Mehta Inter College, Club Road , Varanasi - 221002 (Uttar Pradesh)	221002	Cisco 2811	1	WS-C2960+24TC-S	1	
201	Uttarakhand	Dehradun	59/3, 1st Floor Rajpur Road., Above IDBI Bank, Dehradun - 248001 (Uttarakhand)	248001	Cisco 2901	1	WS-C2960-24TC-S	1	
202	Uttarakhand	Haridwar	Kumar Complex, First Floor Ranipur More, Chandracharya Chowk, Haridwar-249407 (Uttaranchal)	249407	Cisco 2801	1	WS-C2960-24TC-S	1	
203	West Bengal	Kalyani Naihati	NO. B- 9/ 21 (CA), KALYANI TOWNSHIP,GROUND FLOOR, NEEMTALA ROAD, KALYANI - 741235,DIST – NADIA STATE- WEST BENGAL.	741235	Cisco 2811	1	WS-C2960-24TC-L	1	
204	West Bengal	Kolkatta Hub	4th Floor, National Insurance Building,8 India Exchange Place Kolkata 700001	700001	Cisco 3945	1	WS-C2960-24TC-S / WS-C2960-24TC-S / WS-C2960-24TC-S / WS-C2960-24TT-L / WS-C2960-24TT-L	5	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



205	West Bengal	Rashbehari	Purabi Apartment, Ground Floor - GA 28 Rashbehari Avenue, Kolkata - 700026	700026	Cisco 2901	1	WS-C2960-24TC-S	1	
206	West Bengal	Salt lake	Unit No. 107, WEBEL Tower 1, IT Park, BN4, Sector 5, Salt Lake, Kolkata- 700091.	700091	Cisco 2811	1	WS-C2960-24TT-L	1	

SDWAN Features-

Sr. No.	Section	Description	Mandatory / Optional	Compliance by OEM/ Bidder (Yes/No)
1	Section A: General Requirements & Architecture	All proposed SD-WAN devices must be compliant with Government of India TEC/MTCTE certification requirements	Mandatory	
2		Proposed SDWAN solution should have management-based architecture and if management appliances/solution goes offline the SDWAN solution should keep on functioning without any issues. Each SDWAN appliance must support built-in GUI as well for any changes if required.	Mandatory	
3		The proposed solution shall be based on a true Software Defined Network (SDN) architecture, ensuring separation of Management, Control, and Data planes. Management and Data plane components must be deployable on separate physical or virtual instances, with no shared compute, storage, or operating system dependencies, such that failure or compromise of one plane does not impact the availability or security of the other. The solution shall support centralized management and centralized control, with logical and role-based isolation to support multi-tenant environments. The solution must ensure logical separation of Management, Control, and Data planes.	Mandatory	
4		The solution shall include centralized orchestration, SD-WAN control functionality on branch edge devices and hub/gateway devices implemented using either centralized or distributed architectures and should not mandate a dedicated controller appliance.	Mandatory	
5		System should support a centralized single plane of management system to allow device configuration, policy provisioning, software updates and assurance capabilities for all components including firewall and IPS.	Mandatory	
6		System should support the secure overlay fabric with all SD-WAN software elements without direct route peering and secure overlay fabric management protocols to simplify control plane processing such as routing and secure keys distribution.	Mandatory	
7		System should support grouping based upon site-wise/device-wise etc. with dashboard for monitoring.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



8	Solution should provide an abstraction of policy orchestration between control, data, and application policies.	Mandatory	
9	System should support any kind of transport such as Multiprotocol Label Switching (MPLS), P2P, Internet, Broadband and ILL	Mandatory	
10	The solution should support multi-tenant architecture that provides isolation using RBAC between different sub-tenants/business units. Traffic isolation and privacy must be achieved for both Control and Forwarding plane using per tenant secure overlay network.	Mandatory	
11	The data plane at branch locations, data center & DR should be programmable from the central software defined network controller.	Mandatory	
12	The communication between the software defined network controller and branch devices should be secure and encrypted.	Mandatory	
13	The tunnel creation should be automatic without any manual configuration on the edges and controller, for all topologies including Hub & Spoke, Partial Mesh and Full Mesh.	Mandatory	
14	WAN path Selection at branch locations should be based on near real-time analysis of WAN Links Capacity & Quality (Packet loss, Latency & Jitter).	Mandatory	
15	The architecture should allow for internet breakout at local branch, centralized location, or remote entity based on application and policy defined in the controller.	Mandatory	
16	The system architecture should be transport agnostic and support MPLS, ILL, BB. 4G/5G support with tethering	Mandatory	
17	The SD-WAN should support SNMP V3, IPFix, Syslog exporter, etc for monitoring and reporting purpose.	Mandatory	
18	The SD-WAN solution must apply QoS policies to all traffic including both optimized and non-optimized traffic flows, including TCP, UDP and other non-TCP traffic types.	Mandatory	
19	The SD-WAN solution should include a QoS mechanism that protects delay sensitive flows like Voice, Video, and VDI.	Mandatory	
20	The SD-WAN should support IPv4 & IPv6 dual stack from Day-1.	Mandatory	
21	The SD-WAN should support 802.1Q and 802.1X.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



22	System should support end-to-end segmentation to securely isolate Intranet departments and Business Partner traffic within a single appliance. All configuration should be done through central orchestrator. Segmentation to be done in such a way that all control traffic and data traffic of each segment is completely segregated end-to-end. Segmentation should be done from the central controller. The solution shall ensure that branch devices support multiple network segments, while data center and disaster recovery devices support a significantly higher number of segments to accommodate large-scale enterprise requirements.	Mandatory	
23	The software defined network controller must have REST APIs available for 3rd party integration or integration with custom automation tools.	Mandatory	
24	SD-WAN solution should support tenancy separation allowing branch and 3rd party vendor networks to utilize same physical CPE, WAN circuit and central components with total isolation across management, control and data plane.	Optional	
25	SD-WAN solution should support route manipulation on LAN, WAN and Overlay to achieve various hybrid network integration requirements.	Mandatory	
26	SD-WAN solution should support native firewall (stateful) to secure branches with Direct Internet Access for LAN or Guest users.	Mandatory	
27	The SD-WAN solution shall support Site-to-Site IPSec and GRE tunnels on both LAN and WAN interfaces, with interoperability across any third-party IPSec/GRE capable appliance, to enable hybrid deployments. The solution shall further provide integrated secure controls such as encryption, authentication, and policy enforcement to ensure confidentiality, integrity, and compliance in multi-vendor environments.	Mandatory	
28	SD-WAN solution must come with deep analytical capabilities with support for on-premise deployment for detailed logging and audit purpose.	Mandatory	
29	SD-WAN solution should build dynamic IPSEC tunnels using Asymmetric encryption (DH group) and generate unique key for each site for better security. Solution shall support DH Groups 14 and higher, including ECDH groups (19, 20, 21) for key exchange in IPSec and GRE tunnels	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



30	SD-WAN solution should have capability to mitigate packet drop effects in underlay using Forward Error Correction and Packet Replication to improve end-user experience.	Mandatory	
31	The SD-WAN solution shall support automatic zero-touch provisioning of overlay tunnels, including automatic assignment of BGP AS numbers and secure IPsec authentication credentials. The solution shall also allow administrators the option to manually configure BGP AS numbers and IPsec authentication parameters where required.	Mandatory	
32	Automatic Policy Configuration: The SD-WAN solution shall automatically configure routing and security policies to enable end-to-end communication across all LAN networks over the SD-WAN, in accordance with the selected network topology, while also allowing administrators to manually modify or configure policies if required.	Mandatory	
33	There must be minimum two-factor authentication between Controllers and central/branch devices before establishing communication.	Mandatory	
34	The SD-WAN solution shall have the capability to intelligently route voice and video traffic based on real-time quality metrics, such as MOS (Mean Opinion Score) for voice and equivalent QoE (Quality of Experience) scores for video, to ensure optimal application performance and user experience.	Mandatory	
35	The SD-WAN solution shall support the creation of multiple virtual networks or segments to enable secure traffic isolation, enforce granular policies per department or application, support multi-tenant environments, and simplify scalable connectivity across branches, data centers, and cloud environments.	Mandatory	
36	The system should allow time-based refresh of encryption key for each virtual private network.	Mandatory	
37	The SD-WAN solution shall support the creation of dynamic overlay tunnels between branch and hub devices, enabling automatic tunnel establishment, path selection, and failover. The solution shall also allow administrators the option to manually configure static overlay tunnels where required for specific use cases or compliance requirements.	Mandatory	
38	Dynamic VPN Path Creation: The system must make virtual private network paths dynamically on power on without using routing protocols on WAN side.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



39	The SD-WAN solution shall automatically form secure overlay tunnels between branch and DC/Hub/DR sites whenever a new WAN link is added, without requiring manual changes at individual branch devices. The solution shall also allow administrators the option to manually override or configure overlays if required for specific operational or compliance needs.	Mandatory	
40	The SD-WAN solution shall support IPSec and GRE or equivalent tunneling mechanism encapsulation types for overlay tunnels and shall automatically establish tunnels between branch and hub sites without requiring manual configuration. The solution shall also allow administrators the option to manually configure tunnels where necessary for specific use cases or compliance requirements.	Mandatory	
41	The system should support SHA-256 or higher authentication algorithms for Data Integrity.	Mandatory	
42	The system should support AES256, AES256-CBC or equivalent encryption algorithms for Data Security.	Mandatory	
43	System should support Zero Touch Provisioning (ZTP) of CPE device respective of any location with minimum touch provisioning for rapid site provisioning and deployment, considering a closed environment with MPLS/ILL/BB or any other transport	Mandatory	
44	The SD-WAN solution shall support automatic fallback to the underlay MPLS network in the event of overlay tunnel failure, ensuring uninterrupted data-plane operation. The solution shall also allow administrators the option to manually control or override failover behavior if required for specific operational or compliance needs.	Mandatory	
45	All HQ and branch SD-WAN devices shall support automatic configuration backups to a centralized manager without manual intervention. The solution shall also allow administrators to initiate manual backups or restore configurations as needed for operational or compliance purposes.	Mandatory	
46	There should not be any impact on SDWAN data forwarding capability in case of complete disconnection of management console.	Mandatory	
47	Management architecture should support rich policy constructs to manipulate routing information, access control, segmentation, extranets	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



48	Solution should provide transport independence and should allow to use any transport like MPLS, Internet, 3G/4G/5G, Point to Point link	Mandatory	
49	SDWAN solution should support performance SLA based on latency, packet loss, jitter or all 3 combined	Mandatory	
50	SD-WAN solution must support rule-based routing based on application, source and destination. Support for user and user-group based routing (via AD/LDAP/RADIUS integration or equivalent) is desirable/preferred	Mandatory	
51	The SD-WAN solution shall allow creation of traffic-handling rules based on applications, source IP/subnet, destination IP/subnet, or Fully Qualified Domain Names (FQDNs). Each rule shall have the option to associate a specific performance probe or monitor (e.g., latency, jitter, packet loss, MOS) to enable dynamic path selection and ensure optimal application performance.	Mandatory	
52	The SD-WAN solution shall provide the provision for an optional built-in WiFi hardware module at branch devices. The WiFi module, when deployed, shall support multiple SSIDs, modern encryption standards (WPA3/WPA2-Enterprise), 802.1X authentication, and integration with SD-WAN software for secure traffic segmentation, policy enforcement, zero-touch provisioning, and real-time monitoring. If the solution does not provide an embedded Wi-Fi module, the bidder shall propose an OEM Wi-Fi access point integrated with the SD-WAN solution offering equivalent centralized management, segmentation and ZTP	Mandatory	
53	The proposed SD-WAN solution must provide security capabilities from Day-1 like IPS and IDS, URL filtering Malware detection DDOS protection for all locations (Branch / DC / Cloud), either natively integrated within the SD-WAN appliance or through a tightly integrated OEM security stack centrally managed through the same management platform.	Mandatory	
54	The SD-WAN device should have an inbuilt Layer 7 Stateful firewall that provides Stateful application-based firewalling. Stateful Firewall Services with Access Lists and/or Time-based Access lists to provide supervision and control. The device should support NAT and PAT.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



55		The solution must have a Deep Packet Inspection (DPI) engine to match applications (Layers 3 through 7) so that the corresponding business policy and firewall rules can be configured. The SD-WAN appliance should identify minimum 1000 or more applications using a DPI engine. The solution should also have the ability to add custom applications to be used in firewall rules/ business policy. The solution must support identification of applications over encrypted traffic using one or more of the following methods: SSL/TLS certificate / SNI based identification or DPI classification without decryption or Selective SSL/TLS decryption where supported	Mandatory	
56	Section B: Network Performance, Traffic Management & Path Steering	The system should be able to prioritize inbound and outbound traffic using QOS to ensure critical traffic is prioritized	Mandatory	
57		The system should select optimum path based on network parameters like Latency, Jitter, packet loss and network available bandwidth	Mandatory	
58		The system should support packet classification, marking, and bandwidth allocation between SD-WAN devices.	Mandatory	
59		The solution should support adaptive shaping capability that helps avoid congestion at Hub locations. Adaptive shaping allows a device (branch or hub) to enforce dynamic egress shaping rate on any other device sending traffic.	Mandatory	
60		The system should ensure sessions are not impacted when switching between paths. In case of blackout or brownout scenarios, traffic convergence to alternate path should be within 1 sec failover time.	Mandatory	
61		SLA management should have fallback mechanism - if both links at branch location fail to meet SLA, traffic should not drop.	Mandatory	
62		The solution should manage flapping links by removing a link from overlay for traffic forwarding if link is frequently flapping with incremental timeout periods.	Mandatory	
63		The solution should measure SLA parameters such as Latency, Packet loss and Jitter. Each device should do independent SLA calculation towards each remote SDWAN device (bi-directional) on all available paths.	Mandatory	

64	The proposed SD-WAN solution shall support the automatic and dynamic establishment of encrypted tunnels between branch devices to facilitate full-mesh branch-to-branch communication, without requiring manual configuration. Additionally, the solution shall provide the capability for manual tunnel configuration to accommodate specific network policies, custom topologies, or exceptional connectivity requirements.	Mandatory	
65	The proposed SD-WAN solution should ensure that any change in physical connectivity (change in service provider or IP address) does not require any change in virtual private network configuration in SD-WAN CPEs.	Mandatory	
66	The SD-WAN overlay VPN configuration must be decoupled from physical/virtual WAN interfaces and WAN IP addressing. Solution must support dynamic WAN IP and automatic tunnel re-establishment across available WAN transports without manual reconfiguration.	Mandatory	
67	The SD-WAN solution must support selective application-based local breakout for SaaS applications with automatic detection of associated public IPs and FQDNs to make necessary decisions for implementing local breakout.	Mandatory	
68	The solution must support SaaS Application monitoring to check liveness and determine best path selection towards such applications for intelligent routing decisions.	Mandatory	
69	The solution shall ensure high WAN/LAN link performance with TCP optimization, FEC, packet duplication, dynamic path selection, link load balancing, QoS, adaptive shaping, compression, optimized encryption, CRC error monitoring, and automated SLA-based failover, with telemetry and reporting for proactive management.	Mandatory	
70	The configured aggregated MPLS/ILL/BB or any transport pipe should show up as one consolidated virtual pipe/connection with all traffic shaping, steering, weights, QoS, quotas, security policies assigned to that consolidated virtual pipe.	Mandatory	
71	Apart from MPLS/ILL/BB or any transport pipe working as aggregated pipe, SD-WAN should provide failover capabilities between connections/links in aggregated MPLS/ILL/BB or any other transport pipe, such as Active/Active, Active/Passive and backup during blackouts and brownouts.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



72	The SD-WAN vendor shall confirm which of the following methods the proposed solution identifies application traffic for steering:	Mandatory	
73	Source/Destination IP Address		
74	FQDN		
75	Source/Destination Subnet		
76	Destination Port #		
77	Differentiated Services Code Point (DSCP)		
78	VLAN Tag		
79	Application signature		
80	The SD-WAN vendor shall identify the granularity at which the product steers traffic to a given path:	Mandatory	
81	Must support per-packet or per-session steering with sub-second failover based on real-time link quality		
82	Flow-by-flow		
83	Session-by-session		
84	The SD-WAN vendor shall identify the traffic management policies that can be used to steer traffic:	Mandatory	
85	Load balanced		
86	Explicit (forced)		
87	Automatic failover		
88	Automatic fail-back		
89	The SD-WAN vendor shall describe the proposed solution's support for the following features:	Mandatory	
90	Jumbo frames		
91	802.1q (VLAN) Configuration & Processing		
92	Inbound QOS Identification and Classification		
93	Outbound QOS Identification and Classification		
94	Traffic Shaping based on Interface, Tunnel, VLAN, QOS, Application, IP Address, Subnet, or MAC address (indicate all that apply)	Mandatory	
95	Guaranteed minimum / maximum bandwidth by VLAN, QOS, Application or Flow, class	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



96		Traffic Shaping based on the percentage of interface bandwidth for each classified traffic.	Mandatory	
97		The SD-WAN vendor shall describe the ways by which the proposed solution allows to block a traffic flow and at which layers can enforcement be applied:	Mandatory	
98		Source/Destination IP Address		
99		URL/FQDN		
100		Source/Destination Subnet		
101		Source/Destination Port #		
102		Differentiated Services Code Point (DSCP)		
103		VLAN Tag		
104		Application		
105		User		
106	Section C: Authentication, Authorization and Accounting (AAA)	The central management system should authenticate and authorize every administrator/user accessing Central/branch device using RADIUS/TACACS+ for user authentication and authorization.	Mandatory	
107		All configuration change activities should be logged and stored for audit purpose.	Mandatory	
108		The solution should support 802.1x mechanism for network access control, and integrate with existing NAC solution to allow only trusted devices accessing network.	Mandatory	
109		The management platform must support MFA login.	Mandatory	
110		Branch SD-WAN appliances must be securely accessed via SSH/GUI only from authorized SD-WAN manager and not directly to reduce threat surface.	Mandatory	
111	Section D: Management & Orchestration	The Solution should have simplified orchestration placed in DC and DRC for provisioning, automation to control and push configuration for all devices.	Mandatory	
112		The solution should provide a web-based administration interface and GUI for intuitive management. All device configurations must be possible through the GUI, while CLI access should also be available for advanced configuration, troubleshooting, and scripting requirements.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



113	The solution must support high availability within the DC (node-level HA), ensuring uninterrupted services in case of component failure. In the event of a complete DC failure, the solution must automatically failover to DR, with management, control, and data planes seamlessly taken over by DR infrastructure. The design should ensure minimal disruption, with heartbeat-based monitoring for real-time detection and automatic failover between DC and DR.	Mandatory	
114	The system must support intelligent alerting and event notification to external systems. All events such as faults, alarms, and threshold breaches should be reported through industry-standard mechanisms including Syslog messages, SNMP (preferably SNMPv3) traps, and Telemetry streams. The alerting system should incorporate threshold-based monitoring with re-arming logic to prevent repetitive notifications until conditions return to normal, thereby minimizing false positives and alarm flooding	Mandatory	
115	The system must send e-mail notification for events and alerts.	Mandatory	
116	Proposed SDWAN solution should have capabilities to push software update/patches from central devices like Controller/Orchestrator/Manager. Option to disable local OS upgrade should be available for all devices. Should support graceful software upgrade/rollback (Zero Downtime upgrades) with version control.	Mandatory	
117	Proposed Orchestrator should be able to push/ pull the configuration to dynamically selected device groups as per the predefined tags in any permutation and combination. Accordingly, the push/ pull of the configuration should apply to the selected group of devices only.	Mandatory	
118	The proposed Orchestrator should be capable of monitoring any configuration mismatch between orchestrator and branch device.	Mandatory	
119	Proposed Orchestrator should have scheduling mechanism to push templates to dynamically selected group or for dynamically selected group to pull configuration from templates defined centrally.	Mandatory	

120	SD-WAN devices must support active (ICMP, UDP, TCP, BFD, TWAMP, SaaS) and passive (NetFlow/IPFIX, DPI) probes for latency, jitter, and packet loss, with 1-second polling and on-demand probing for troubleshooting. Metrics must be historically stored, GUI-accessible, exportable via APIs/Syslog/Telemetry, and integrated with intelligent threshold-based alerting with re-arming.	Mandatory	
121	SD-WAN device should automatically switchover existing session in concurrence with branch device to alternate superior link in case of current link degradation at branch or data center end. In any case of session switchover, reverse and forward path should be symmetric.	Mandatory	
122	The policy should include traffic steering based on WAN link type (MPLS, ILL,BB etc; or any type of WAN link) available at branch location.	Mandatory	
123	The SD-WAN solution must support the definition and enforcement of traffic forwarding policies for LAN-to-WAN traffic at branch locations. Policies must be based on applications, application categories, source and destination subnets, and specific IP addresses. The solution should allow traffic prioritization, path selection, and blocking as per defined policies, ensuring optimal performance, security, and SLA compliance	Mandatory	

124	The proposed SD-WAN solution shall provide centralized policy enforcement and governance through a single management platform. It must support standardized configuration templates / profiles that can be applied consistently across all branch, DC and cloud SD-WAN devices. The solution shall continuously and automatically validate device configurations against defined corporate security and network policies, detecting configuration drift and deviations including (but not limited to): 1. Missing or incorrect firewall/security rules 2. Incorrect routing policies / segmentation policies 3. Non-standard WAN link settings, QoS, or SLA policies 4. Unauthorized configuration changes / local CLI changes 5. Non-compliant software/firmware versions or weak crypto settings (if applicable) Upon detecting non-compliance, the system must: 1. Generate alerts/notifications (dashboard + email/SIEM integration), and 2. Support automated remediation by re-applying the approved template/policy (auto rollback / auto push), or enforce a “block change unless approved” mechanism. 3. The solution must maintain audit logs of policy violations, remediation actions, and user activity for security audit readiness.	Mandatory	
125	The system should allow definition and enforcement of traffic forwarding policies that allow encapsulation of traffic with IPSEC or UDP or GRE or no Encapsulation for all traffic passing through device.	Mandatory	
126	The system should allow monitoring of Packet loss ratio, Delay, Jitter, and Bandwidth utilization of each WAN link. Administrator should be able to use these parameters to define traffic steering policies and monitor policy violations during threshold breach.	Mandatory	

127		The SD-WAN solution must support the aggregation of multiple WAN links, including multiple MPLS links or an MPLS link combined with a public Internet link, into a single logical connection. The system should dynamically distribute traffic across these links based on link quality, application requirements, and defined policies, ensuring high availability, bandwidth optimization, and seamless failover in case of link degradation or failure	Mandatory	
128		The SD-WAN must integrate transparently into existing routing infrastructure. Solution should have capability to coexist with existing routing protocols (e.g. OSPF, BGP (iBGP and eBGP), IPSEC etc.).	Mandatory	
129		The system should allow plug and play installation of branch devices without requiring manual configuration or minimal manual configuration at remote location.	Mandatory	
130		The system should allow automatic software/patch/version upgrades (Zero Downtime upgrade) from software defined network controller across all deployed devices or group of devices in branch offices, data center and cloud. “Zero Downtime Upgrade must be supported for HA deployments (Active/Standby or equivalent). For branches since it is not in HA mode, upgrade should be automated with minimal disruption and scheduled maintenance windows.”	Mandatory	
131		The system should allow scheduling upgrade of devices either individually or in batches as per requirement and process should be completely automated. In case upgrade fails, device should be rolled back to previous stable configuration.	Mandatory	
132		The SD-WAN solution must support non-disruptive software upgrades, ensuring that branch devices remain fully operational and continue to forward traffic while new software or firmware is being downloaded and installed from the central SD-WAN controller. This capability should enable rolling upgrades across multiple sites without impacting business applications or WAN connectivity	Mandatory	
133	Section E: Security features	The system should implement stateful firewall with Access Lists and/or Time-based Access lists to provide supervision and control on branch device, centrally provisioned and managed from software defined network controller.	Mandatory	

134	The SD-WAN device should detect and mitigate common DDoS attacks like UDP floods or Ping of Death, protecting the branch and WAN connectivity without impacting legitimate traffic.	Mandatory	
135	The proposed SD-WAN solution must provide integrated security services at all branch and DC locations, either natively within the SD-WAN appliance or through tightly integrated security stack under the same centralized management platform. The solution must support, at minimum, the following security capabilities: IP filtering / firewall (L3–L4), URL filtering / web filtering, Anti-Virus / Anti-Malware, DNS filtering / secure DNS, Intrusion Prevention System (IPS). These features must be centrally managed through a single console with policy templates, logging and reporting.	Mandatory	
136	The SD-WAN solution must provide Intrusion Prevention System (IPS) capabilities at all branches, supporting a comprehensive, daily-updated signature database covering critical CVEs from day-1 to cover common and critical threats. The system must allow centralized IPS signature updates from the SD-WAN controller, either periodically or on-demand, ensuring timely protection against emerging vulnerabilities without impacting device performance.	Mandatory	
137	The proposed SD-WAN solution must support DNS filtering to block access to potentially malicious websites at both hub and branch locations. Additionally, it should include DNS sinkholing capabilities to intercept and redirect DNS queries for known malicious domains, preventing users from accessing harmful content.	Mandatory	
138	The solution must support file filtering to protect against viruses and vulnerabilities associated with various file types and blocks potentially dangerous file transfers, applications, files with specific sizes/protocols, and traffic direction.	Mandatory	
139	Controller and device should be accessible only through web-based interface for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



140		SD-WAN Devices should communicate with cloud console only at the management layer level for licenses, upgrades, signatures, etc. For all other purpose of traffic inspection, networking routing , etc. there should be no communication with cloud pertaining to control / data planes placed by OEM in cloud in case of fully on-prem deployment.	Mandatory	
141	Section F: Visibility, Analytics, Monitoring & Reporting	Centralized Management system should support multiple administrators with administrative rights based on their roles and provide Audit Trail of changes.	Mandatory	
142		The system must monitor and report Top Users/IPs by applications accessed/bandwidth usage in branch location. Data must be stored by controller for minimum 30 days.	Mandatory	
143		The dashboards must have following visibility features: Reports for Link availability, Device availability, HA pair of DC availability, SLA reports of latency, Packet loss, Jitter and link usage Distinguish between SDWAN overlay traffic and local internet breakout link usage SDWAN reports including topology map, application visibility per branch, per link and URL categories and other custom user defined applications System utilization capturing CPU, DISK, Memory and session load	Mandatory	
144		The Solution must display security and SD-WAN reports in same management platform with logs for each feature delivered.	Mandatory	
145		The proposed SDWAN dashboard solution should have visibility of all other SDWAN components/elements deployed across all data centers and branches.	Mandatory	
146		Centralized reporting server/tools must be capable of scheduling all reporting mechanisms including ad-hoc reports.	Mandatory	
147		The system should provide mechanism to monitor performance for Links and Virtual Private Network.	Mandatory	
148		The system must monitor ISP link parameters like link quality, link usage and link congestion and provide historical data for minimum 30 days.	Mandatory	
149		The system should support application-level monitoring and traffic control to improve business-critical application performance, facilitate capacity management and planning, and reduce network operating costs.	Mandatory	
150		The system should support ability to automatically detect applications, report application traffic, and allow for marking and filtering via policy.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



151	The system should allow user to define custom application based on multiple parameters such as protocol values, ports, patterns etc and tag application by family and sub-family like business, non-business, SaaS, by Risk categories etc. Should have capability to define traffic policies for such applications and categories.	Mandatory	
152	The system should allow administrators to be grouped with well-defined roles assigned to them. Should support monitoring only user role, network change administrator role and overall system administrator role with permissions to manage software defined network controller.	Mandatory	
153	The SD-WAN should support granular Real-Time/near real-time Monitoring and Historical Reporting like: Statistic bandwidth usage of available links Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization	Mandatory	
154	The SD-WAN should generate reports for: Traffic statistics of all included paths Specific application utilization Path performance	Mandatory	
155	The SD-WAN MUST provide following reports of Individual Link Quality on daily, weekly, monthly, yearly or configurable period basis: Packet loss in the links Jitter on the links Latency of Links	Mandatory	
156	The solution must generate notifications for: Link Flaps at remote branch location ISP link quality degrade Link utilization along with threshold CPU, Memory and Disk Utilization of Branch Device	Mandatory	
157	Notifications generated by software defined network controller must be forwarded as email to pre-configured email address and reflected on Dashboard.	Mandatory	
158	The system must monitor and report top 20 applications by usage across all branch locations, in branch locations along with data rate and flow usage. Data must be stored by controller for minimum 30 days.	Mandatory	
159	The system must monitor and report Top 10 LAN users by bandwidth usage and applications accessed by them in branch location along with data rate and flow usage. Data must be stored by controller for minimum 30 days.	Mandatory	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



160		Administration should be able to drill down these reports for troubleshooting, e.g., applications accessed by specific users along with bandwidth consumed during defined amount of time.	Mandatory	
161	Section H: Hardware Specification for Branch Locations	The device must incorporate a hardware-based Root of Trust (RoT) or a dedicated secure cryptographic module (such as TPM, Secure Element, or equivalent) to provide secure storage for encryption keys (e.g., IPsec), ensure device identity attestation, and protect against physical and unauthorized tampering	Mandatory	
162		Device should support protocols like IPv4, IPv6, VRRP, Static Routes, OSPF, BGP, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling from Day-1.	Mandatory	
163		Dynamic Host Control Protocol (DHCP) server/relay/client.	Mandatory	
164		Should support debugging capabilities to assist in problem Resolution	Mandatory	
165		Support for the following IP v6 features: OSPF v3, BGP Support for V6, IP V6 Dual Stack, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6	Mandatory	
166		Devices should support Configuration rollback feature	Mandatory	
167		Shall have Secure Shell for secure connectivity	Mandatory	
168		Extensive debugs on all protocols	Mandatory	
169		Should be at least EAL3/EAL4 /NDcPP/FIPS 140-2/NIAP/TEC Certified	Mandatory	
170		Device should be with IPv6 Ready/compliant.	Mandatory	
171		The Device should be TEC/MTCTE certified	Mandatory	

Switch Specifications:

Sr. No	Mandatory Feature	Description	Compliance (Yes/No)
	General Requirement		
1	Integration with existing network	Product should work in a heterogeneous network consisting of various devices from different OEMs using standard protocols for Uplink/downlink connection, VTP, VLAN and STP etc.	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



2	Integration with existing network	Device should have support for all standard/open industry protocols to use in environment where the uplink and downlink switches are from different manufactures / OEM. The bidder / OEM shall not demand any change in the existing deployed network components or endpoints while providing seamless integration with heterogeneous network environment.	
3	Enterprise Grade Product	"Enterprise" Grade means that OEM has declared the proposed model as enterprise grade on their public website and it will work for an enterprise and can satisfy mission critical tasks.	
4	Rack Mountable	The Layer 2 Network switch should be standard rack mountable with clamps.	
5	Hardware Dimension	Platform must be enterprise grade in 1 RU form-factor with internal power-supply.	
6	MTBF and MTTR	Should have (MTBF) Mean Time Between Failure of 70,000 hours or higher to ensure long life of switch hardware. Should have (MTTR) Mean Time To Repair as 4 hours for the provided switch.	
7	Additional feature list	Please submit a list of all features provided by the product that will be available to the StockHolding without any additional charges and will be under support. These features will be treated at par with other features mentioned in the RFQ.	
Licensing Requirement			
8	Enterprise licensing	Product should have enterprise license without any restrictions to use the features mentioned in the RFQ from day one. If during the contract, Product is not performing as per specifications in this RFQ, bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to StockHolding.	
9	Enterprise licensing	Bidder/OEM has to provide the access of a central portal (credential based) where StockHolding can cross verify the allotted licenses to the StockHolding with the relevant	
10	No limit licensing	Product and its various features like switching and other inbuilt features etc. should not have any licensing restriction on number of users, concurrent connections, total connections, new connections, number of VLANs, zones, number of policies, number of appliances, other network parameters, number of equipment/servers etc. as per the RFQ specification.	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



11	Product part code availability	The offered product Part Codes have to be General Availability Part codes and not custom-built Part Code for the StockHolding. There should be cross reference to the public website of the OEM.	
	Capacity		
12	Port requirement (24- port switches)	Switch should support 24 x 1000 Mbps Base TX access ports from day one. Switch should support 4 x 1G from day One. All uplink port should support LR and SR transceiver from day one.	
13	Console Port	Switch should have a console port (RJ45 or USB) for local administration.	
14	Auto MDI and MDI-X	Auto MDI-X (Medium-Dependent Interface Crossover) automatically detects the required cable connection type and configures the connection appropriately, removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer.	
15	Auto and Manual Speed Negotiation Performance	Auto MDI-X (Medium-Dependent Interface Crossover) automatically detects the required cable connection type and configures the connection appropriately, removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. Negotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support. In the OSI model, auto negotiation resides in the physical layer.	
16	Line rate forwarding	The switch shall have a minimum of 100 Gbps no blocking switching capacity for 24 ports. Supports for Virtual Output Queuing VoQ is good to have. Virtual output queueing (VOQ) is a technique used in certain network switch architectures where, rather than keeping all traffic in a single queue, separate queues are maintained for each possible output location. It addresses a common problem known as head-of-line blocking.	
17	MAC Address	Shall have minimum 16K MAC Addresses. Switch must have Store and Forward Switching Feature.	

18	System requirement	The switch must possess sufficient internal Flash memory and DRAM to concurrently store at least two full production firmware images and configuration files, supporting seamless dual-boot failover capability during upgrades. Memory architecture must fully support the maximum scaled limits of the MAC address, ARP, and routing tables without performance degradation till end of support is not declared by the OEM	
	Layer2 Features		
19	STP	Spanning Tree Protocol (802.1d, 802.1w, 802.1s)	
20	VLAN Trunking	Should support 802.1q for carrying multiple VLAN's over a link.	
21	Multicast	Multicast IGMP v1, v2, v3 should be supported. Internet Group Management Protocol (IGMP) filtering to provide multicast authentication by filtering out nonsubscribers and to limit the number of concurrent multicast streams available per port.	
22	per-VLAN MAC learning	Per-VLAN / interface MAC learning.	
23	Layer 2 trace route	Layer 2 / Layer 3 trace route.	
24	MTU	9198 Bytes to avoid any Application performance issue. MTU size should be configurable parameters on each port.	
25	Jumbo frames support	Switch should support for Jumbo Frames	
26	Voice VLAN	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN.	
27	Neighbor discovery	The switch should support discovery of the neighboring device of the same vendor giving the details about the plat form, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.	
28	VLAN	Should support 4094 VLAN and 256 Active VLANs	
29	L2 Qos/Cos Support	The Layer 2 switches should support Quality of Service (QoS) features, including 802.1p Class of Service (CoS) marking, traffic prioritization per VLAN, and queuing mechanisms to ensure efficient handling of network traffic at the access layer	
	Availability		
30	Uplink Redundancy & Bandwidth Aggregation	Switch should allow redundancy in uplinks. Uplink bundling/aggregation should be supported using LACP.	
31	Storm Control (Broadcast/Multicast)	F2/ Storm control (Broadcast, Multicast).	

	Security		
32	IEEE 802.1x Based Security	Switch must have 802.1x based endpoint authentication and port security to implement and run Network Access Control (NAC) solution. 1. IEEE802.1x 2. 802.1x with VLAN Assignment 3. 802.1x Guest VLAN 4. 802.1x - Auth-Fail VLAN or equivalent (An auth fail VLAN allows users without valid credentials to access a limited set of services which can be controlled by an administrator. Please note that at present the StockHolding is using dACLs to achieve this functionality.) 5. 802.1x - Auth Fail Open or equivalent (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable or to allow specific sets of services even in case of radius reject profile.) 6. 802.1x MAC-Auth Bypass 7. 802.1x MAC-Auth-Bypass for voice VLAN 8. 802.1x with ACLs 9. 802.1x with Port Security 10. 802.1x Accounting 11. NAC - L2 IEEE 802.1x 12. Web Authentication for Non 802.1x Clients 13. Multi Domain Authentication (802.1x for IP phone + 1 host behind phone) 14. Switch should support concurrent deployment of 802.1x and MAB authentication. Where 802.1x is the priority protocol and MAB is fall back option or vice versa. 15. Switch should function as “Authenticator” in 802.1x based authentication as well as switch port (for example: uplink/downlink ports) shall simultaneously support 802.1x supplicant mode.	

33	IEE 802.1 X, EAP, Radius and MAB support	Switch shall have the capability to support modern and latest protocols associated with network access control technology like 802.1x, EAP and Radius with configurable features. The following configurable parameters are examples for reference. 1. EAP protocol supports maximum number of attempts, time out and number of attempts etc. with supplicant. 2. Radius protocol related parameters like, primary & secondary radius server configuration, radius time out, maximum number of attempt and fail open in case all the configured radius server is unreachable. After a number of EAP failures or no response received from client machine or supplicant then the switch shall auto fail over to MAB authentication. In MAB authentication, the endpoint MAC learned on port shall be used as credential automatically for authentication.	
34	Radius: IETF	Switch should support all the standard definitions and attributes of Radius as per the RFC2865 and RFC3575. For example: The switch should at least support below mentioned radius attribute types and its associated value implementation. RADIUS Attribute: (6) Service-Type A. (1) Login B. (2) Framed C. (8) Authenticate Only D. (10) Call Check (61) NAS-Port-Type E. (15) Ethernet F. (19) Wireless - IEEE 802.11 (29) Termination-Action G. (0) Default H. (1) Radius Request (49) Acct-Terminate-Cause I. All practical values of this attribute.	

35	Radius accounting packets	IEEE 802.1X RADIUS accounting relays important events to the RADIUS server (such as the supplicant's connection session). This session is defined as the interval beginning when the supplicant is authorized to use the port and ending when the supplicant stops using the port. A RADIUS accounting-request packet contains one or more Attribute-Value (AV) pairs to report various events and related information to the RADIUS server. The following are the examples of AV-pairs that should be at least supported by the switch. i) NAS-IP-Address ii) NAS-Port iii) Service-Type iv) Framed-IP-Address v) Class vi) Called-Station-ID vii) Calling-Station-ID viii) Acct-Status-Type ix) Acct-Session-ID x) Acct-Session-Time xi) Acct-Terminate-Cause xii) NAS-Port-Type xiii) Acct-Authentic Etc.	
36	Port Based access control lists for Layer2 Interface	For Layer 2 interfaces allow security policies to be applied on individual switch ports using layer 2, layer3 and layer 4 parameter(s). The access control list based on IP addresses should be supported as statically configured on switch or remotely deployed from Radius server in form of downloadable/dynamic ACL.	
37	MAC Address Notification on workstation join into the network.	Audit trails and logging.	
38	Port security	Ability to control and possibly restrict end points in the network. Secures access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.	

39	RADIUS Change of Authorization (CoA) for Network Access Control	The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. a. RADIUS COA. b. URL Redirection for posture, VLAN and ACL assignment. Note: To utilize the COA or disconnect/reconnect functionality (when the state of the port need be changed on switch port after successful authentication) the attributes and dictionaries shall be provided by the bidder to incorporate in the Radius server/NAC server/ authentication server deployed in the StockHolding.	
40	Downloadable Access Control List (ACLs)	The switch shall have the capabilities to support a minimum of 45 lines of dACL per port concurrently on all the access ports of the switch if no logical port is mentioned. For example, if 24 ports switch then minimally 45 lines of dACL will be applied concurrently on all 24 ports (each) either through a single named dACL or through multiple named dACL. a. Switches should support dACLs per port. b. Number of rules per dACL = 45 where each rule line can have IP subnet or individual IP. c. Should support downloading of dACLs created on a central NAC server or Radius server. Note: 1) Please provide documentary evidence / reference in support of this clause along with the technical bid (data sheet will also be considered subject to its availability on public domain). 2) The switch should have capacity to handle number of ACL rules for mentioned number of dACL in this clause and other ACLs mentioned in this technical specification sheet combined. e.g., dACL: (24*45) + SNMP_ACL NTP_ACL+ SSH_ACL_SNMP_ACL etc.	
41	AAA services	Support for Authentication databases (TACACS or RADIUS).	

42	DHCP Snooping	DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.	
43	IP Source Guard	IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.	
44	Spanning tree Root protection	Prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes	
45	Unknown unicast and unknown multicast blocking and unknown unicast rate limiting	To enable unicast and/or multicast blocking on a switch port to suppress the flooding of frames being forwarded out through that port.	
46	Dynamic ARP Inspection	Dynamic ARP Inspection (DAI) is a security feature that verifies address resolution protocol (ARP) requests and responses in a network.	
47	Spanning tree BPDU protection.	For avoiding network loops	
48	Spanning Tree BPDU	For Edge port protection.	
49	Multidomain authentication	to allow an IP phone and a PC to authenticate on the same switch port while being placed on the appropriate voice and data VLANs.	
	Manageability		
50	Embedded RMON Support.	Ability to collect performance statistics	

51	SSH2 and above version-based Administration on IPV4	Secure and remote administration of switches at the branch over SSH2 protocol. 1. Switch shall have the capabilities to support the remote version upgrade through SFTP and SSH. 2. Configuration backup shall be supported from the external servers or solution which will require the mentioned protocols. 3. Configuration change/modification or addition/deletion shall be supported by remote process automation tools over ssh. Switch shall support control on SSH based access to the switch using named access control list. SSH shall support standard and higher version of encryption or cryptographic algorithm like SHA-2 etc.	
52	SNMP V3 and above version, based Administration and Monitoring over IPv4	Basic Network management and monitoring capabilities shall be available for switch with secure and latest standard protocols. Switch should support SNMP V3 with AES-256 or higher version of encryption. It should also support SHA based authentication on SNMP. Switch should support named access control list- based filtering or equivalent control mechanism for allowing authorized SNMP servers communication. Specific Object Identifier (OID) for device monitoring like, CPU, memory and FAN status shall be provided by the bidder/OEM so that device can be integrated with external network monitoring systems.	
53	LLDP & LLDP - MED Support	Link layer media protocol to identify endpoints in the network. For example, IP Phones.	
54	Network Time Protocol (NTP V2 and above version) over IPv4	To sync time on all network devices to synchronize the log collection and events. Switch shall support specified access list- based control for NTP servers. The device should have secure NTP functionality with authentication and encryption support. The NTP should support MD5 and SHA.	
55	DHCP based Auto config	Auto configuration of switches at the branches to aid error free IP configuration and up gradation.	
56	SYSLOG over IPv4	Syslog is a way for network devices to send event messages to a logging server – known as a Syslog server using syslog protocol.	

**Request for Proposal (RFP) for Implementation of Software Defined-Wide
Area Network (SDWAN) and Branch L2 Managed Switches**



57	Local and remote port mirroring for packet captures	Local and remote port mirroring for packet captures	
58	Device access	Should support management CLI and web UI over SNMP, RJ-45 or USB ports.	
59	Operating Temperature	Switch should support Operating Temperature range 0 to +45 degC Considering the Indian climatic condition. Switch shall have perforation to provide sufficient ventilation.	
60	Management and configuration guide	Bidder / OEM need to submit the PDF or hard copy of Management & Configuration guide and CLI reference guide for the make and model proposed against this RFP along with information on operating system version. There should be a publicly available management & configuration guide for the hardware and software version.	
	IPv6 features		
61	IPv6 and dual layer compatible.	Switch should be compatible for IPv4 and IPv6 traffic.	
62	MIBs for IPv6 traffic	Switch should support MIB for IPv6 management	
63	IPv6: HTTP, HTTPS, ICMPv6, TCP/UDP over IPv6, Domain Name Resolution	IPv6 access capability	
64	IPv6 Stateless Auto Config.	Ability to provide auto configured IPv6 address	
65	IPv6: Option processing and fragmentation	Advance IPv6 capabilities	
66	IPv6 MLD v1 and higher version snooping	MLD is used in IPv6 equivalent to IGMP for discovering multicast listeners on a directly attached line.	
67	IPv6 Applications: Ping/Traceroute/ VTY/TFTP	IPv6 Applications: Ping/ Traceroute/ VTY/ TFTP/ Telnet/ SSH	
68	IPv6	The Device should be on the IPv6 Ready Logo or higher certification.	