Technical Spec – Structured Cable

Make and Model : **Annexure 12 A**

Standard Compliance	Compliance Yes/No	Remarks
The Extended Product warranty and Application Assurance shall be for 25 years from the date of Installation.		
The Extended Product Warranty shall cover all passive Registered SCS components (i.e., cable and connectivity components that make up the passive data and telecommunications signal transmission infrastructure).		
The the Registered SCS compliant links/channels will meet or exceed the applicable requirements of the TIA 568-C series, and ISO/IEC 11801: 2002 standards for cabling links/channel configurations specified in these standards;		
Under the Extended Product Warranty, the supplier will (or will authorize an installer to) either repair or replace the defective Registered SCS product at the supplier's cost. The supplier will pay an installer for the cost of labor to repair or replace any such defective product on behalf of the supplier, provided, that such repair or replacement and associated labor costs receive the prior written approval of the supplier. If the supplier chooses to repair products, the supplier may use new or reconditioned replacement parts. If the supplier chooses to replace products, the supplier may replace such products with new or reconditioned products of the same or similar design.		
The Customer shall not be charged either the cost of the labor or the product at such an incident.		
Application Assurance		
The Application Assurance shall cover the Registered SCS compliant channels to support operations of the application(s) that the system was designed to support, as well as additional application(s) defined below. The supplier warrants that the Registered SCS will be free from defects that prevent operation of the specific application(s) for which the Registered SCS was initially designed as long as the design is in compliance with the SCS Performance Specifications for said applications and is in compliance with all other terms and conditions of this warranty.		
That all Passive Components in the Registered SCS meet or exceed the relevant component specification of the TIA 568-C series and ISO/IEC 11801: 2002 standards;		
The Application Assurance shall also cover the current (at the time of installation) and in accordance with application standards specifications, any application introduced in the future by recognized standards or user forums that use the relevant TIA/EIA 568-C series or ISO/IEC 11801 2nd edition (September 2002)		
The Supplier shall provide tools to Calculate the Insertion Loss (IL) of the system.		
The Supplier shall provide tools to calculate the Application performance for a given channel by calculating and Displaying the Optical loss.		
The Supplier Shall provide Document with details of Application Performance, for different topologies, Number of Connectors and Length of the Channel.		
Fiber channel shall support below specifications with guaranteed performance:		
40G Ethernet - BD support (QSFP-40G-SR-BD)		

OM4 with LC connection distance support (in mtr.)

# LC Connections* with:	1 MPOs	2 MPOs	3 MPOs	4 MPOs	5 MPOs	6 MPOs
0	155	155	155	155	155	155
1	155	155	155	155	155	150
2	155	155	155	155	150	150
3	155	155	155	150	150	145
4	155	155	155	150	145	145
5	155	155	150	150	145	140
6	155	150	150	145	145	140

* Number of connections excludes the connection to the active device at each end of the channel.

MPO connections support

Application	MPO connection	Distance (meter)
40 GBASE-SR4	1 MPO	175
	2 MPO	170
	3 MPO	165
	4 MPO	155
	5 MPO	150
	6 MPO	140
100 GBASE-SR4	1 MPO	130
	2 MPO	130
	3 MPO	130
	4 MPO	125
	5 MPO	120
	6 MPO	115

Technical Spec – CAT 6 A Cable

Make and Model :		**Annexure 12 B**
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
Channel Performance		
The Category 6A/ Class EA UTP SCS shall comply with the following standards		
a) ISO/IEC 11801:2010		
b) EN 50173 Part 1 through Part 5:2010 and 2011		
c) ANSI/TIA-568-C		
d) IEC 60603-7-4		
e IEEE 802.3 applications as outlined in section 2		
The Category 6A/ Class EA UTP system should support the following IEEE Ethernet applications		
a) 802.3e - 1BASE5		
b) 802.3i - 10BASE-T		
c) 802.3u - 100BASE-TX, 100BASE-T4		
d) 802.3y - 100BASE-T2		
e) 802.3z - 1000BASE-X		
f) 8023ab - 1000BASE-T		
g) 802.af - Power Over Ethernet (15.4W)		
h) 802.3at - Power Over Ethernet Enhancements (25.5W)		
i) 802.3az - Energy Efficient Ethernet		
802.3at - Power Over Ethernet Enhancements		
Additionally, the Category 6A/ Class EA UTP SCS shall be capable of supporting the following Fibre Channel Applications Standards, per Technical Committee 11 of INCITS:		
a) 1GFC-BASE-T		
b) 2GFC-BASE-T		
c) 4GFC-BASE-T		
It is critical that guaranteed worst-case values are provided to ensure the SCS can support 1G transmission without risk. “Average value” or “Typical Value” is not acceptable as they do not account for lower performance channels. The proposed Category 6A UTP SCS, when configured as a worst-case 100-meter channel shall provide performance headroom over limits specified by Cat6A		
NEXT - Minimum 3 dB above the standards;		
Should support a minimum of 4 connector Channel with a minimum 3 dB guaranteed NEXT		
Insertion Loss - 3%		
Return Loss - 1.0 db		
The SCS must consist of individual components provided by the same manufacturer. “Mix and Match” products are not allowed as there is no guarantee that the overall channel will meet Category 6A Channel requirements if constructed with components from different vendors.		
The Category 6A cable and Category 6A channel components shall be manufactured by a single manufacturer. The manufacturer shall warrant the Category 6A channel cable, components, and applications for a period of 25 years.		
The 25-year warranty shall be a transferable warranty and has component replacement policy in case of manufacturing defect		
The SCS must be tested by an ISP 17025 accredited 3rd Party test facility to EIA/TIA 568C, ISO/IEC 11801 Amendment 1 and for the channel testing must be provided as part of the bid response.		
The Category 6A system should support channels that are shorter than 15 meters for 2, 3, 4 connector channels without any minimum length requirements.		
Horizontal Cable		
The Cable should meet ANSI/TIA 568C.2 Category 6A Specifications		
Cables should have TRACKING Number to check the Genuity / details of the test reports		
The cable should consist of Eight 23 AWG copper conductors. Copper Clad Aluminum or any other combinations are not allowed		
The Cable should be round in shape		

The weight of the cable box of 1000 Feet should not be less than 34.7 lb		
The nominal Jacket thickness should be 0.05 inches		
The nominal Outside diameter should not be more than 0.285 inches		
The cable should support the installation temperature: 0 to 60 0 C		
It should support Operating temperature of -20 to 60 0 C		
The cable shall be available in Low-Smoke, Zero Halogen (LSZH) compatibility and		
The LSZH version must comply with the following Fire Safety standards:		
1) ISO/IEC 60332-3-22: Vertical Flame Spread		
2) ISO/IEC 60754-2: Acidity		
3) ISO/IEC 61034-2: Smoke Density		
Cable shall comply to below mechanical specifications:		
Conductor Material- Bare copper		
Insulation Material- Polyolefin		
Jacket Material- Low Smoke Zero Halogen (LSZH)		
Separator Material- Polyolefin		
Separator 2 Material-Polyolefin		
The cable and cordage shall be "True UTP" components that do not include internal or external shields, screened components or drain wires. No Special Grounding requirements.		
The horizontal cable shall have a unique print string on the cable jacket. This unique identifier shall also be used for on-line reference to a full set of factory tests that were performed on a sample from the same mater reel. The test parameters shall include NEXT, PSNEXT, Return Loss, Attenuation, ELFEXT and PSELFEXT. The on-line reference must be available on the SCS vendor public website, such that it can be accessed at any time.		

Technical Spec – CAT 6A Outlet		
Make and Model :		**Annexure 12 C**
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
The 8-pin modular (RJ-45) jacks shall comply with IEC 60603-7-4		
The Category 6A outlets shall be backward compatible with Category 6 and 5E cords and cables.		
The Category 6A outlets shall be of a universal design supporting T568 A & B wiring.		
The information outlet shall have a Current Rating of 1.5 A at 20°C		
The information outlet must support 90 degree cable termination. As some mounting hardware does not allow for cable entry directly from the rear, this capability is necessary		
3rd Party Verification test certificates shall be provided to show compliance to ISO/IEC 11801 Amendment 2 testing for Cat 6A components.		
The 8-pin modular (RJ-45) jacks shall comply with IEC 60603-7-4.		
The information outlet will have insertion life of 750 cycles minimum.		

Technical Spec – Copper Patch Chord		
Make and Model :		**Annexure 12 D**
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
SCS must support patch cord lengths of 1 meter minimum and equipment cords of 2 meter minimum and The Patch cords shall be available in 28 AWG reduced diameter LS-CM Dual Rated Cord complying to ISO/IEC 11801 Class EA | TIA/EIA-568 Cat 6A		
Cords shall be equipped with 8-pin modular plugs on each end.		
All cords shall be round, and consist of copper conductors, tightly twisted into individual pairs.		
Nominal cordage diameter shall not exceed 4.95 mm.		
Plugs shall be designed with an anti-snag latch to facilitate easy removal during move, add and change processes.		
The LSZH version must comply with the following Fire Safety standards:		
CM-LS & UL 1863		
The patch cord shall comply to below mechanical specification:		
Conductor Material- Copper Alloy, Polycarbonate		
Contact Plating Material- Gold over nickel		
Material Type- Phosphor Bronze		
The cordage shall be UTP components that do not include internal or external shields, screened components or drain wires.		
The patch cords will have insertion life of 750 cycles minimum.		

Technical Spec – Jack Panel		
Make and Model :		**Annexure 12 E**
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
24 or 48 Port Patch Panel		
The ganged adapter style patch panel will utilize increments of six RJ-45 style jacks in a common molded component.		
The ganged adapters shall have RJ45 jack in the front and Insulation Displacement Connector (IDC) at the rear of the module.		
The panel must be capable of supporting an upgrade to an intelligent system without any interruption to service due to patch cord removal or terminal block re-termination.		
Termination managers must be provided with the panel. These termination managers provide proper pair positioning, control, and strain relief features to the rear termination area of the panel.		
3rd Party Verification test certificates shall be provided to show compliance to ISO/IEC 11801 Amendment 2 testing for Cat 6A components.		
When configured in worst-case 100-meter channels with full cross-connects and consolidation points with the other products proposed in this tender, the panel shall be capable of delivering the minimum guaranteed channel performance		
The patch panel type shall be a 1U (24 port) or 2U (48 port) panel capable of supporting 24 or 48 unshielded modular 8-pin connectors compliant with IEC 60603-7-4 while meeting the Channel Performance as specified in Amendment 1 to ISO/IEC 11801:2002		

The panel shall be available in 24-port and 48-port configurations with universal A/B labeling and 110 connector terminations on rear of panel allowing for quick and easy installation of 22 to 24 AWG cable		
The panel shall be equipped with a removable rear mounted cable management bar and front and rear labels		
The panel shall be UL and cUL Listed		
Operating Temperature Range = 14°F to 140°F (-10°C to 60°C)		
Storage Temperature Range = -40°F to 158°F (-40°C to 70°C)		
Humidity = 95% (noncondensing)		
Nominal Solid Conductor Diameter = 0.025 to 0.020 in (0.64 to 0.51 mm) (22 to 24 AWG)		
Nominal Stranded Conductor Diameter:=0.025 to 0.020 in (0.64 to 0.51 mm (22 to 24 AWG)		
Insulation Types = All plastic insulates (including PVC, irradiated PVC, Polyethylene, Polypropylene, PTF Polyurethane, Nylon, and FEP)		
Insertion Life = 750 minimum insertions of an FCC 8-Position Telecommunications Plug		

Technical Spec – Fiber Cable		Annexure 12 F
Make and Model :		
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
IEC 60793-2-10, type A1a.3a | IEC 60793-2-10, type A1a.3b | TIA-492AAAD (OM4)		
TIA-492AAAD Detail Specification for 850-nm Laser-Optimized, 50-µm Core Diameter/125-µm Cladding Diameter Class la Graded-Index Multimode Optical Fibers Suitable for Manufacturing OM4 Cabled Optical Fiber		
TIA-455-220-A (FOTP-220), Differential Mode Delay Measurement of Multimode Fiber in the Time Domain, dated January 2003		
IEC 60793-2-10, type A1a.3a Edition 2.0, Optical fibre – Part 1-49: Measurement methods and test procedures – Differential mode delay		
IEC 60793-2-10, Edition 5.0, Optical fibres – Part 2-10: Product specifications – Sectional specification for category A1 multimode fibres (fiber model A1a.3, Sections D.3 and D.4)		
· Min OFL(LED)bandwidth@850nm 3500MHz.km		
· Min OFL(LED)bandwidth@1300nm 500MHz.km		
· Min EMB @850nm : 4700 MHz.Km		
· Max dispersion: 105 Ps/nm|*km		
· Certification : DMD(differential mode delay) test report from Intertek ETL test laboratory.		

Annexure 12 G

Technical Spec – Fiber MPO Trunk		
Make and Model :		
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
Construction material		
· Fiber type: OM4 multi-mode fiber complaint with IEC 60793-2-10, type A1a.3a | IEC 60793-2-10, type A1a.3b | TIA-492AAAD (OM4)		
· Jacket color: Aqua		
· Connector type: MPO-12/UPC		
Environmental specification		
· Installation temperature -20 °C to +60 °C (-4 °F to +140 °F)		
· Operating Temperature -20 °C to +70 °C (-4 °F to +158 °F)		
· Storage Temperature -40 °C to +70 °C (-40 °F to +158 °F)		
· Cable Qualification Standards ANSI/ICEA S-83-596 |Telcordia GR-409		
· EN50575 CPR Cable EuroClass Fire Performance Dca		
· EN50575 CPR Cable EuroClass Smoke Rating s1a		
· EN50575 CPR Cable EuroClass Droplets Rating d1		
· EN50575 CPR Cable EuroClass Acidity Rating a1		
· Environmental Space Low Smoke Zero Halogen (LSZH) | Riser		
· Flame Test Listing NEC OFNR-LS (ETL) and c(ETL)		
· Flame Test Method IEC 60332-3 |IEC 60754-2| IEC 61034-2 |IEEE 383 | UL 1666 | UL 1685		
MPO polarity		
· Connector A: method B, unpinned MPO		
· Connector B: method B, unpinned MPO		
Optical performance		
· All links shall meet or exceed the end to end loss performance specified to support the optic application guarantee		
· Fiber Components shall not exceed :		
· Insertion Loss, maximum 0.25 dB		
· Insertion Loss Change, mating 0.3dB		
· Return Loss, minimum 27.0 dB		
Mechanical performance		
· Compression 10 N/mm | 57.101 lb/in		
· Compression Test Method FOTP-41 | IEC 60794-1 E3		
· Flex 300 cycles		
· Flex Test Method FOTP-104 | IEC 60794-1 E6		
· Impact 5.88 N-m | 52.042 in lb		
· Impact Test Method FOTP-25 | IEC 60794-1 E4		
· Strain Test Method FOTP-33 | IEC 60794-1 E1		
· Twist 10 cycles		
· Twist Test Method FOTP-85 | IEC 60794-1 E7		
· Vertical Rise, maximum 500 m | 1,640.42 f		
· Ferrule Material Polymer		
Flame Test Specifications		

· Jacket flammability : available in OFNP and LSZH versions		
· Flame Test Listing NEC OFNR-LS (ETL) and c(ETL)		
· Flame Test Method IEC 60332-3 | IEC 60754-2 | IEC 61034-2 | IEEE 383 | UL 1666 | UL 1685		
Certification		
· RoHS 2011/65/EU compliant		
· ISO 9001:2015 Complaint		
· Fiber type: OM4 multiple mode fiber		
· Connector type: 2 x 12 LC fibers (Front) /2 x MPO-12 (Rear)		
· Support intelligence , support real-time monitoring and tracking of complex fiber connectivity including LC, MPO and breakout.		
· Connector type: LC-MPO		
· Color code: Aqua		
· Insertion Loss, maximum: 0.47 dB max		
· MPO Polarity : method B, Pinned		
· Fiber qty- 24 fiber		
· Front interface-LC		
· RoHS 2011/65/EU compliant		
· ISO 9001:2015 complaint		

Annexure 12 H

Technical Spec – Fiber Patch Chord		
Make and Model :		
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
· Fiber type :OM4 multiple mode fiber, complaint with TIA-492AAAD (OM4) & IEC IEC 60793-2-10, type A1a.3a | IEC 60793-2-10, type A1a.3b		
· Connector type: LC		
· Jacket flammability : LSZH		
· Jacket color : Aqua		
· Material : RoHS complaint		
· Outside diamter : 2.00 mm		
· Patch cords using Uniboot technology combine, modularity, flexibility with easy insertion and removal from connectivity		
· Uniboot connectors feature an adjustable polarity via a manual and independent rotation of each single connector body without exposing the fibers		
· Uniboot technology features a push-pull mechanism operated by squeezing the connector boot		

Annexure 12 I

Technical Spec – Fiber Shelf		
Make and Model :		
Standard Compliance	**Compliance (Yes/No)**	**Remarks**
The same Panel Shall should accommodate 4x 24F coupler plates for a total of 96 Fiber Termination or 4 x12F pigtail cassettes for a total of 48 fiber terminations/spliced in 1U height. The Panel Should have 2U and 4U Options to support Cassettes for a total of 144 duplex LC ports in 2U and 288 LC duplex ports to be supported 4U height Only.		
The width shall be 19 inches and height of 1U (1.75 inches), with a maximum of 19-inch depth.		
Panels shall have large, translucent window that provides a clear view of the patching field, must provide tool-less installation of rear trunk cables, and must provide split tray design to facilitate installation and minimize network downtime		
The shelf/LIU shall be sliding. 2U & 4U panel shall support split tray design for better access in high density environment.		
The Fiber shelf must be intelligent ready and must support field upgrade to intelligent fiber panels without removal of existing patch cords and without disruption of network services.		
The Shelf shall be able to Support splice trays to splice minimum 32 fibers, and Stackable tray support for 48 Splices/tray in 1U.		
Panel shall made up of steel material & flammability rating of UL 94 V-0.		
Panel shall support MPO adapters.		

Annexure 12 J

Technical Spec – SDN Fabric

Make and Model :

S. No.	Feature Set	Compliance (Yes/No)	Remarks
1	Fabric Defination		
1.1	Proposed fabric must be the Clos network topology architecture defined using Spine, Leaf switches with VXLAN overlay		
1.2	Fabric should have achieve following functionalities:		
1.2(a)	Flexibility : Should allow workload mobility anywhere in the DC, across the Data Center sites		
1.2(b)	Resiliency : The proposed fabric should be able to sustain multiple link and device (Leaf & Spine), Controller failures		
1.2(c)	Performance: The proposed fabirc should be able with use full cross sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi pathing		
1.2(d)	Solution should provide flow analytics and should be able show latency for the flow and packet drops in the network path which helps identify data path issues across fabric.		
1.2(e)	Mult-DataCenter design:- The proposed architecture should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across multiple Data centers.		
2	Hardware and Interface Requirement		
2.1	Fabric Connectivity should have the following properties:		
2.2	In the fabric, the leaf and spine switches quoted should be non-oversubscribed and perform at line rate		
2.3	All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking		
2.4	All switches or proposed Fabric must support for **500 VRF/Private** network without any additional component upgrade or design change		
3	Fabric Features		
3.1	Fabric manager must provide Centralised Management - Single pane of Glass for managing, monitoring and provisioning the entire Fabric.		
3.2	Fabric manager should not participate in Data plane and control plane path.		
3.3	Fabric manager shall support automated configuration changes (e.g. pushing common network changes across all devices, such as (QoS, security credentials or access control lists)		
3.6	Fabric manager must support a single GUI based network management tool for network and Trafic flow Visibility, management, Zero Touch Provisioning & replacement		
3.7	**Fabric manager must provide insight into the traffic flow patterns utilising standards like netflow or sFlow or IPIFX or equivalent Protocol Support**		
3.8	Fabric manager must have ability to automate VXLAN control plane and provide topology information of the fabric		
3.9	Fabric manager must support a single GUI based network management tool for automated state snapshot of fabric devices and change comparision between snapshots for simplified change verification.		
3.10	Fabric manager should provide dynamic device inventory of the Switches as well as current network topology of the Solution with ability to detect and depict the logical overlay networks over physical one.		
3.11	**Solution consisting of Fabric manager & Device manager to support integration with best of breed Physical and virtual firewall appliances for traffic rediversion**		
3.12	Fabric manager must run in "N + 1 or N + 2" redundancy, so that a single node fauilure does not impact genral working for the controller/manager.		
3.13	In the Event, ALL of the Fabric manager Fail Completely , the Switches must continue to function without any performance degradation and with the current configuration.		
3.14	Fabric manager shall support configuration compliance checking to detect config drift (e.g. manual configuration changes that no longer match templates or automated configs)		
3.15	Fabric manager must provide necessary report for compliance and audit, and security vulnerabilities (bugs, CVE, etc) in an automated way		
3.16	Fabric manager shall support software image compliance checking for feature and performance consistency		
3.17	**Solution should support proactive notifications for software bugs and security vulenrability specific to any deployment based on hardware platform, device configuration and deployed software version**		
3.18	Fabric manager should support support turnkey automated deployment and RMA operations using & Zero Touch Replacement procedures		
3.19	Fabric manager should support support network rollback to a previously known good state after a failed maintenance operation		
3.20	Fabric manager should support provide APIs that allow integration to custom or commercially available change management systems		
3.21	Fabric manager should support GUI based **solution** to carry operation task like upgrades and configuration change with ability to review those changes before deploying on fabric		
3.22	Fabric manager should support single GUI based network management tool for orchestration of automated software upgrades of Device software to minimize service disruption		
3.23	Fabric manager must support a single GUI based network management tool with role based access control.		
3.24	Fabric manager must support a single GUI based network management tool for provisioning of network features via custom configuration templates.		
3.25	Fabric manager must support a single GUI based network management tool with network wide state based rollback to known good state. Usefull during failed Operation Task		
3.26	Fabric manager should support a single GUI based network management tool for automated state snapshot for pre- and post- change management.		
3.27	Fabric manager must support a single GUI based network management tool for access to central database containing current and historical network based information and network state which can be queried by the customer for their own internal and external audit use and could be used to create a network view of all changes over time for troubleshooting and compliance needs.		
3.28	Fabric manager must support Topology view with details real time Badwidth Utilization; Traffic Throughput; Error Rates; etc		
3.29	Fabric managershall support sub-second state changes on the device to be captured.		
3.30	**Solution should support proactive notifications for software bugs specific to any deployment based on hardware platform, device configuration and deployed software version**		
3.31	**Fabric manager or devices shall support: ssh or JSON/HTTPS or OpenConfig or Netconf or SNMPv2c/v3 or any equivalent protocol support**		
3.32	Fabric manager shall support correlation of events to simplify troubleshooting and reduce unimportant alerts		
3.33	Fabric manager should provide open APIs to integrate custom developed or commercial third party tools		
3.34	Fabric manager should support event triggered email notification		
3.35	All devices must retain full CLI access for troubleshooting, management and configuration purposes even when controlled via a central management tool.		
3.36	All devices must support standard terminal transport services: SSHv2, Telnet , Tacacs+, Radius, Authentication and Authorization.		
3.37	All devices must support Network Management Logs and SNMP MIBs.		
3.38	**All devices must support netflow or sflow or telmetry**		
3.39	Fabric manager should support centralized network database, that leverages real-time state-streaming, to provide an aggregate view of the physical network state		
3.40	**Solution should leverage the centralized network database to provide network analytics**		

Annexure 12 K

Technical Specifications : Switch Type 1 (Modular Spine Switch)			
Make and Model :			
Sr.No	**Required Minimum Specifications**	**Compliance**	**Remarks**
1	**Hardware & Interface / Performance**		
	Switch should be chassis based with 2 Supervisor slots and minimum 8 Line Card slots with all Line Card slots capable of supporting 10G, 25G, 40G and 100G speeds.		
	Switch should be capable to scale upto 256 nos of 40/100G QSFP28 ports.		
	The switch must be populated with minimum of 5 line cards with 30 ports 40/100 G QSFP+ ports and all ports shall be fully populated with 40/100 Gbps QSFP+ from day one		
	Switch should have minimum 48 Tbps backplane switching capacity available from day 1		
	Switch should support wire-speed Layer-2 and Layer-3 forwarding.		
	Switch should have redundant Supervisors and Fully Poupulated Fabric modules to support scale requirements and future upgradability		
	Switch should support latency of 5microsec or less for high speed switching.		
	Switch should support minimum 40Mb Buffer Memory per Line Card for 40/100G Line Cards		
	Kindly change to "Switch Supervisor Engine Specs should have - Quad Core x86 CPU, 16Gb SDRAM and 4Gb Flash or 50G/100G SATA SSD"		
	Switch should support upto 280K MAC.		
	Switch should support upto 350K IPv4 Routes.		
	Switch should support upto 150K IPv6 Routes.		
	Switch should support upto 100K IPv4 Multicast entries.		
	Switch should support upto 140K IPv4 and 70K IPv6 Host Routes		
	Switch should have N+1 level of redundancy for power supply and fans		
	Switch should support AC Power supply with min 90% efficency or better		

	Switch should support in-line hot insertion and removal of different parts like Supervisor, power supplies, fan tray etc and should not require switch reboot & should not disrupt the functionality of the system		
	Switch should support Supervisior Redundancy or Routing Engine		
	Switch should support power budget of 3.5W per 10Gb of performance		
	Switch should have latency below 5microsec		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Switch OS should support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time State streaming of telemetry information		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		
	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		
3	**Layer 2**		
	Switch should support IEEE 802.1D Bridging and 802.1Q VLAN Tagging along with 4096 Vlans		
	Switch should support IEEE 802.1w and 802.1s and Rapid Per Vlan Spanning Tree(RPVST+)		
	Switch should support 802.3ad Link Aggregation LACP with up to 32 ports/channel and 512 Groups Per System		
	Switch should support 64 ports active/active layer2 LAG		
	Switch should support 802.1AB Link Layer Discovery Protocol (LLDP)		

	Switch should support 802.3x Flow Control		
	Switch should support Jumbo Frames 9216 Bytes		
	Switch should support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG		
	Switch should support IEEE 802.3ae 10 Gigabit Ethernet		
	Switch should support IEEE 802.3by 25 Gigabit Ethernet		
	Switch should support 802.3ba 40 and 100 Gigabit Ethernet		
4	**Layer 3**		
	Switch should support Dynamic Routing protcols like OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Switch should support Graceful restart for BGP,OSPF v2 and v3 and ISIS		
	Switch should support minimum 64-way ECMP routing for load balancing and redundancy		
	Switch should support PIM-SM or PIM-SSM or PIM-BiDi multicast routing or Anycast RP or MSDP along with Multicast Multipath		
	Switch should support BFD inclusive of BFD for Lag links, BFD for V4 and V6 VRF, Multi-hop BFD and BFD on IP unnumbered interfaces.		
	Switch Switch should support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP v4 and v6, Resilient ECMP, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking		
	Switch should support Traffic aware ECMP		
	Switch should support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
	Switch should support VxLAN with Routing and Bridging in Hardware.		

	Switch should support VxLAN routing and bridging must also be supported in overlay VRFs.		
	~~**Switch should support Accumulated IGP Metric (AIGP), BGP Monitoring Protocol (BMP) and BGP Prefix Origin Validation with Resource Public Key Infrastructure (RPKI)**~~		
	Switch should support VxLAN+EVPN leaf-spine overlay technology supporting type-1 to type-8 routes		
	Switch should have support IRB with EVPN with distributed gateway functionality		
	Switch should support IGMP v2/v3,PIM-SM / PIM-SSM, Anycast RP (RFC 4610), VRF Support for IP Multicast, Multicast Source Discovery Protocol (MSDP)and IP Multicast Multipath.		
	Switch should support RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	Switch should support RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	Switch should support RFC 4862 IPv6 Stateless Address Autoconfiguration		
	Switch should support RFC 4443 Internet Control Message Protocol (ICMPv6) for the IPv6 Specifications		
	Switch should support RFC 1981 Path MTU Discovery for IP version 6		
	Switch should support RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
	Switch should support RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IPv4)		
5	**Quality of Service (QoS)**		
	Switch should support 8 queues per port		
	Switch should support 802.1p based classification		
	Switch should support DSCP based classification and remarking		
	Switch should support Rate limiting; Policing or Shaping		

	Switch should support Strict Priority Queuing		
	Switch should support Explicit Congestion Notification(ECN)		
	Switch should support Per Priority Flow Control(PFC)		
	Switch should support DCBX Support - Data Center Bridging Extension		
	Switch should support ACL Based DSCP Marking and Policing		
	Switch should support Egress queue scheduling and shaping and WRR and WRED		
6	**Security and Network Management**		
	Switch should support Security ACLs Ingress and Egress with upto L4 filtering capabilties.		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Switch should support TACACS+/RADIUS		
	Switch should support Management over IPv4, IPv6		
	Switch should provide remote login for administration using Telnet and SSHv2		
	Switch should support Syslog and Syslog over TLS		
	Switch should support AAA with accounting to AAA servers		
	Switch should support sFlow / NetFlow		
	Switch should support for management and monitoring status using SNMP v1,v2,v3		
	Switch should support Filtering of Management Traffic(SNMP,SSHv2) with Service ACL.		
	Switch should support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support central time server synchronization using Network Time Protocol		
7	**Monitoring, Provisioning and Automation**		
	Switch should support secure Zero Touch Provisioning with options to provision Certificates artifacts on the device when it boots.		

	Switch should support Advance Event Management for pro-active network monitoring or equivalent		
	Switch should support Restoration of Operating System & Configuration from USB		
	Switch should monitor output queue lengths for all Device interfaces and log and stream events related to congestion		
	Switch should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using Two-Way Active Measurement Protocol		
	Switch should have programability and automation with Anisble, python, bash.		
	Switch should support sampling of flows at every switch, aggregates them and sends the samples to a collector with path and latency information.		
	Switch should support tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purpose.		
8	**Data Center Features - Virtualization and SDN**		
	Solution should support integration with Open Stack.		
	Switch should support multi OEM hypervisor environment		
	Solution should support integration with Open Stack.		
	Switch should have capability to run Docker container on switch.		
9	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All required licenses to support full layer 2 and layer 3 shall be provided from day one		

Annexure 12 L

Technical Specifications :Switch Type 2 (Spine Switch)			
Make and Model :			
Sr.No	**Required Minimum Specifications**	**Compliance**	**Remarks**
1	**Hardware & Interface / Performance**		
	Switch must have at least 64 x 40/100G QSFP+ and 2 SFP+ with minimum switching throuput of 12.8 Tbps		
	The switch shall be fully populated with 40/100 Gb QSFP+ fromd day one		
	Switch should support packet throughput of 4.2 Bpps or above		
	Switch should be provided with 19" Rack mountable with necessary mounting kit		
	Switch should have N+1 redundant, hot-swappable fan modules and power supplies with power cords provided as per site requirement		
	Switch should support both AC and DC power supply options.		
	Switch should have 1 Gigabit RJ45 Port for OOB Management in separate VRF		
	The switch should support port to port latency of 800 ns		
	Switch hardware should be capable of supporting at least: 1. 136K IPv4 host routes 2. 256K MAC addresses 3. 68K IPv6 Host Routes 4. 100 VRFs		
	Switch should have 32 Mb of Dynamic buffer		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Switch OS should support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time State streaming of telemetry information		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		
	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		
3	**Layer 2**		
	Switch should support IEEE 802.1D Bridging and 802.1Q VLAN Tagging along with 4096 Vlans		
	~~Switch should support IEEE 802.1w and 802.1s and Rapid Per Vlan Spanning Tree(RPVST+)~~		
	Switch should support 802.3ad Link Aggregation LACP with up to 32 ports/channel and 512 Groups Per System		
	Switch should support 32 ports active/active layer2 LAG		
	Switch should support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Switch should support 802.3x Flow Control		
	Switch should support Jumbo Frames 9216 Bytes		
	Switch should support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG		
	Switch should support IEEE 802.3ae 10 Gigabit Ethernet		
	Switch should support IEEE 802.3by 25 Gigabit Ethernet		
	Switch should support 802.3ba 40 and 100 Gigabit Ethernet		
4	**Layer 3**		
	Switch should support Dynamic Routing protcols like OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Switch should support Graceful restart for BGP,OSPF v2 and v3 and ISIS		
	Switch should support minimum 64-way ECMP routing for load balancing and redundancy		
	Switch should support PIM-SM or PIM-SSM or PIM-BiDi multicast routing or Anycast RP or MSDP along with Multicast Multipath		
	Switch should support BFD inclusive of BFD for Lag links, BFD for V4 and V6 VRF, Multi-hop BFD and BFD on IP unnumbered interfaces.		

	Switch Switch should support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP v4 and v6, Resilient ECMP, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking		
	Switch should support Traffic aware ECMP		
	Switch should support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
	Switch should support VxLAN with Routing and Bridging in Hardware.		
	Switch should support VxLAN routing and bridging must also be supported in overlay VRFs.		
	~~Switch should support Accumulated IGP Metric (AIGP), BGP Monitoring Protocol (BMP) and BGP Prefix Origin Validation with Resource Public Key Infrastructure (RPKI)~~		
	Switch should support VxLAN+EVPN leaf-spine overlay technology supporting type-1 to type-5 routes		
	Switch should have support IRB with EVPN with distributed gateway functionality.		
	Switch should support IGMP v2/v3,PIM-SM / PIM-SSM, Anycast RP (RFC 4610), VRF Support for IP Multicast, Multicast Source Discovery Protocol (MSDP)and IP Multicast Multipath.		
	Switch should support RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	Switch should support RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	Switch should support RFC 4862 IPv6 Stateless Address Autoconfiguration		
	Switch should support RFC 4443 Internet Control Message Protocol (ICMPv6) for the IPv6 Specifications		
	Switch should support RFC 1981 Path MTU Discovery for IP version 6		
	Switch should support RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
	Switch should support RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IPv4)		
5	**Quality of Service (QoS)**		
	Switch should support 8 queues per port		
	Switch should support 802.1p based classification		
	Switch should support DSCP based classification and remarking		
	Switch should support Rate limiting; Policing or Shaping		
	Switch should support Strict Priority Queuing		
	Switch should support Explicit Congestion Notification(ECN)		
	Switch should support Per Priority Flow Control(PFC)		
	Switch should support DCBX Support - Data Center Bridging Extension		
	Switch should support ACL based or equivalent protocol based DSCP Marking and Policing		
	Switch should support Egress queue scheduling and shaping and WRR and WRED		
6	**Security and Network Management**		
	Switch should support Security ACLs Ingress and Egress with upto L4 filtering capabilties.		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Switch should support TACACS+/RADIUS		
	Switch should support Management over IPv4, IPv6		
	Switch should provide remote login for administration using Telnet and SSHv2		
	Switch should support Syslog and Syslog over TLS		
	Switch should support AAA with accounting to AAA servers		
	Solution should support sflow/Netflow/telemetry		
	Switch should support for management and monitoring status using SNMP v1,v2,v3		
	Switch should support Filtering of Management Traffic(SNMP,SSHv2) with Service ACL.		
	Switch should support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support central time server synchronization using Network Time Protocol		
7	**Monitoring, Provisioning and Automation**		
	Switch should support secure Zero Touch Provisioning with options to provision Certificates artifacts on the device when it boots.		
	Switch should support Advance Event Management for pro-active network monitoring or equivalent		
	Switch should support Restoration of Operating System & Configuration from USB		
	Switch should monitor output queue lengths for all Device interfaces and log and stream events related to congestion		
	Switch should have programability and automation with Anisble, python, bash.		
	Switch should support sampling of flows at every switch, aggregates them and sends the samples to a collector with path and latency information.		

	Switch should support tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purpose.		
8	**Data Center Features - Virtualization and SDN**		
	Solution should support integration with Open Stack.		
	Switch should support multi OEM hypervisor environment		
	Solution must support visibilty via intergration into Container Workloads		
	Switch should have capability to run Docker container on switch.		
9	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		

Annexure 12 M

Technical Specifications :Switch Type 3 (Leaf Switch)			
Make and Model :			
Sr. No	**Required Minimum Specifications**	**Bidder's compliance (Yes/No)**	**Bidder's Remarks**
1	**Hardware & Interface / Performance**		
	Switch should have 96 ports (single non-blocking switch) or more, capable of 1/10/25 GbE SFP+ and minimum of 8x 40/100G uplinks		
	The switch should be populated with all the 96 x 10/25 SFPs and all 8x100 G QSFPs from day 1 itself		
	Switch should support minimum 6.4 Tbps switching capacity/throughput or more		
	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding on every port		
	For SFP/SFP+, shall support 10/25 GBE and 25GBASE-MR-XSR, MultiRate SFP		
	Switch should support minimum 1 Micro sec or less of latency for high speed switching.		
	Switch should have console port		
	Switch should have management interface for Out of Band Management with support for 100M/1G Speeds.		
	Shall Support USB port		
	Switch must support minimum 32Mb Intelligent Buffer with support for Dynamic Buffer allocation, also this buffer should not be split into multiple slices.		
	Switch should have all the license enable for integrating with VXLAN based controller.		
	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel/LAG, multi chassis port channel etc		

	Control Plane should comprise - Quad Core x86 CPU, 8Gb DRAM and 8Gb Flash		
	Shall support min 256K MAC.		
	Shall support upto 350K IPv4 Routes.		
	Shall support upto 190K or more IPv6 Unicast entries.		
	Shall support upto 100K IPv4 Multicast entries.		
	Switch should have N+1 level of redundancy for power supply and fans		
	Switch should support AC Power supply with min 90% efficency or better		
	Should support both Front-to-back and back-to-front reversible airflow for optimized cooling		
	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc and should not require switch reboot & should not disrupt the functionality of the system		
	Switch should have Max Power Consumption of 500W or less		
	Switch must support Precision Time Protocol helps in synchronizing visibility of data flow across the fabric device.		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Industry standard CLI		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Shall support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time Telemetry for streaming of telemetry information		
	Should support Configuration roll-back and check point		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		
	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		

	~~Should support user applications to run as a VM or Container to support modern DC troubleshooting and monitoring.~~		
3	**Layer 2**		
	Shall Support IEEE 802.1Q VLAN Tagging		
	Shall Support IEEE 802.1w Rapid Spanning Tree		
	Shall Support IEEE 802.1s Multiple Spanning Tree Protocol		
	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN		
	Switch should support basic Multicast IGMP v2, v3		
	~~Shall support Rapid Per VLAN Spanning Tree (RPVST+)~~		
	Shall support 802.3ad Link Aggregation LACP with up to 32 ports/channel		
	Shall support 128 Link Aggregation Groups (LAG)		
	Shall support 32 ports active/active layer2/Layer3 multipathing redundancy		
	Shall support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Shall support Port Mirroring		
	Shall support 802.3x Flow Control		
	Shall support Jumbo Frames 9216 Bytes		
	Shall support active/active layer-2 topology without STP where host are dual homed to leaf switch using vPC or MLAG or ESI-LAG or equivalent protocol standard		
	Switch must support resilient L2 Hashing and ECMP		
	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using VRRP or equivalent		
	Shall Support IEEE 802.1D Bridging and Spanning Tree		
	Shall Support IEEE 802.3ab 1000BASE-T		
	Shall Support IEEE 802.3z Gigabit Ethernet		
	Shall Support IEEE 802.3ae 10 Gigabit Ethernet		
	Shall Support IEEE 802.3by 25 Gigabit Ethernet		
	Switch must 802.3ba 40 and 100 Gigabit Ethernet		
4	**Layer 3**		
	Shall support basic Layer-3 Routing		

	Shall support minimum 128-way ECMP routing for load balancing and redundancy		
	Shall support OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Shall support PIM-SM or SSM multicast routing		
	Shall support BFD v4 and v6 VRF Aware		
	Shall support BFD for LAG Link and Multihop BFD		
	Shall support Route Maps		
	Shall support Anycast RP		
	Shall support EVPN		
	Switch should support Dynamic Load Balancing Feature		
	Switch should support Traffic aware ECMP		
	Switch shall support IEEE 1588 PTP(Precision Time Protocol) with PTP Modes (Transparent Clock and Boundary Clock)		
	Switch must support uRPF		
	~~Switch must support NAT~~		
	Switch must support VxLAN with Routing and Bridging in Hardware in single pass		
	RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	RFC 4862 IPv6 Stateless Address Autoconfiguration		
	RFC 4443 Internet Control Message Protocol (ICMPv6) for the Ipv6 Specifications		
5	**Quality of Service (QoS)**		
	Up to 8 queues per port		
	802.1p based classification		
	DSCP based classification and remarking		
	Rate limiting		
	Switch should support for different type of QoS features for real time traffic differential treatment using Strict Priority Queuing		
	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
	Explicit Congestion Notification(ECN)		

	Switch must support Per Priority Flow Control(PFC)		
	DCBX Support - Data Center Bridging Extension		
	ACL based or equivalent protocol based DSCP Marking		
	ACL based or equivalent protocol based Policing		
	Policing Shaping		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Shall Support IEEE 802.1p QOS/COS		
6	**Security and Network Management**		
	Shall Support security ACLs		
	Shall Support TACACS+/RADIUS		
	Switch should support IP Source guard, ARP inspection, DHCP Snooping		
	Shall Support SNMP v2, v3		
	Shall Support Management over IPv4, IPv6		
	Switch should provide remote login for administration using:		
	a. Telnet		
	b. SSHV2		
	Shall Support Syslog		
	Shall Support AAA		
	Shall Support Port Mirroring		
	Shall Support sFlow / NetFlow		
	Switch should support for management and monitoring status using different type of Industry standard NMS using:		
	a. SNMP V1 and V.2		
	b. SNMP V.3		
	c. Filtration of SNMP using Access list		
	d. SNMP MIB support for QoS		
	Switch should support for basic administrative tools like:		
	a. Ping		
	b. Traceroute		

	Shall support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
	Switch should support central time server synchronization using Network Time Protocol		
	Switch should provide different privilege for login in to the system for monitoring and management		
7	**Monitoring, Provisioning**		
	Shall support Advance Event Management for pro-active network monitoring or equivalent		
	Shall support Restoration of Operating System & Configuration from USB		
	Shall support CLI schedular, Shell script, for timed automation, and event managert for triggered automation		
	Shall support centralized script/system to configure a switch without user intervention		
8	**Automation and Extensibility**		
	Switch must open APIs to be managed from any northbound controller.		
	Switch must support all devops tools like Ansible, Chef, Puppet and Salt stack.		
	Switch must support Openconfig		
9	**Data center Advanced Features and Network Virtulization**		
	Fabric Device must support Vxlan routing/bridging in hardware.		
	Solution should support integration with Open Stack and Vmware NSX		
	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically; with complete visibiltiy.		
	Solution must support visibilty via intergration into Container Workloads.		

	Vxlan routing and switching must also be supported in non default or default VRFs for multitenancy		
	Switch should have capability to run Docker container on switch.		
10	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All licenses and OS required for full layer 2/ layer 3 features shall be provided from day one		

Annexure 12 N

Technical Specifications :Switch Type 4 (Leaf Switch)			
Make and Model :			
Sr.No	**Required Minimum Specifications**	**Compliance**	**Remarks**
1	**Hardware & Interface / Performance**		
	Switch should have 48 ports or more, capable of 1/10G *48 RJ-45 Ports and 8*40/100G QSFP+ Uplinks the switch should be populated with all 40/100 Gbps QSFP+ from day one		
	Switch should support minimum 1.5 Tbps or more switching capacity/throughput		
	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding		
	Switch should support minimum 3micro sec or less of latency for high speed switching.		
	Switch must support minimum 32Mb Buffer Memory		
	Control Plane should comprise - Multi Core x86 CPU, 4Gb DRAM and 4Gb Flash		
	Shall support min 44K MAC.		
	Shall support upto 16K IPv4 Routes.		
	Shall support upto 22K IPv4 Multicast entries.		
	Switch should have N+1 level of redundancy for power supply and fans		
	Switch should support AC Power supply with 90% Efficency		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Switch OS should support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time State streaming of telemetry information		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		
	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		

3	**Layer 2**		
	Switch should support IEEE 802.1D Bridging and 802.1Q VLAN Tagging along with 4096 Vlans		
	~~Switch should support IEEE 802.1w and 802.1s and Rapid Per Vlan Spanning Tree(RPVST+)~~		
	Switch should support 802.3ad Link Aggregation LACP with up to 32 ports/channel and 50 Groups Per System		
	Switch should support 32 ports active/active layer2 LAG		
	Switch should support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Switch should support 802.3x Flow Control		
	Switch should support Jumbo Frames 9216 Bytes		
	Shall support active/active layer-2 topology without STP where host are dual homed to leaf switch using vPC or MLAG or ESI-LAG or equivalent protocol standard		
	Shall Support IEEE 802.1D Bridging and Spanning Tree		
	Shall Support IEEE 802.3ab 1000BASE-T		
	Shall Support IEEE 802.3z Gigabit Ethernet		
	Shall Support IEEE 802.3ae 10 Gigabit Ethernet		
4	**Layer 3**		
	Shall support basic Layer-3 Routing		
	Shall support minimum 64-way ECMP routing for load balancing and redundancy		
	Shall support OSPF, OSPFv3, BGP, IS-IS, and RIPv2		
	Shall support PIM-SM or SSM multicast routing		
	Shall support Route Maps		
	Switch must support uRPF		
5	**Quality of Service (QoS)**		
	Up to 8 queues per port		
	802.1p based classification		
	DSCP based classification and remarking		

	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
	Explicit Congestion Notification(ECN)		
	ACL based or equivalent protocol based Policing		
	Policing Shaping		
	Rate Limiting		
6	**Security and Network Management**		
	Switch should support Security ACLs Ingress and Egress with upto L4 filtering capabilties.		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Switch should support TACACS+/RADIUS		
	Switch should support Management over IPv4, IPv6		
	Switch should provide remote login for administration using Telnet and SSHv2		
	Switch should support Syslog and Syslog over TLS		
	Switch should support sFlow / NetFlow		
	Switch should support for management and monitoring status using SNMP v1,v2,v3		
	Switch should support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support central time server synchronization using Network Time Protocol		
7	**Monitoring, Provisioning**		
	Shall support Advance Event Management for pro-active network monitoring or equivalent		
	Shall support Restoration of Operating System & Configuration from USB		
	Shall support CLI schedular, Shell script, for timed automation, and event managert for triggered automation		
	Shall support centralized script/system to configure a switch without user intervention		
8	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All licenses and OS required for full layer 2/ layer 3 features shall be provided from day one		

Annexure 12 O

Technical Specifications : Switch Type 5 (Leaf Switch)			
Make and Model :			
Sr. No	**Required Minimum Specifications**	**Bidder's compliance (Yes/No)**	**Bidder's Remarks**
1	**Hardware & Interface / Performance**		
	Switch should have 48 ports or more, capable of 1/10/25 GbE SFP+ and 8x40/100G uplinks		
	All ports should be populated with 48 x 1Gbps Copper SFP from day one and should support a mix of 1 G and 10/25 G SFP in future with mere replacement of SFPs by the Bank and all 8x 40/100 GB QSFP should be populated from day one		
	Switch should support minimum 4 Tbps switching capacity/throughput or more		
	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding		
	For SFP/SFP+, shall support 10/25 GBE and 25GBASE-MR-XSR, MultiRate SFP		
	Switch should support minimum 1 Micro sec or less of latency for high speed switching.		
	Switch should have console port		
	Switch should have management interface for Out of Band Management with support for 100M/1G Speeds.		
	Shall Support USB port		
	Switch must support minimum 24Mb Intelligent Buffer with support for Dynamic Buffer allocation, also this buffer should have option to be split into multiple slices if desired		
	Switch should have all the license enable for integrating with VXLAN based controller.		

	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel/LAG, multi chassis port channel etc		
	Control Plane should comprise - Quad Core x86 CPU, 8Gb DRAM and 8Gb Flash		
	Shall support min 256K MAC.		
	Shall support upto 350K IPv4 Routes.		
	Shall support upto 190K or more IPv6 Unicast entries.		
	Shall support upto 100K IPv4 Multicast entries.		
	Switch should have N+1 level of redundancy for power supply and fans		
	Switch should support AC Power supply with min 90% efficency or better		
	Should support both Front-to-back and back-to-front reversible airflow for optimized cooling		
	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc and should not require switch reboot & should not disrupt the functionality of the system		
	Switch should have Max Power Consumption of 305W or less		
	Switch must support Precision Time Protocol helps in synchronizing visibility of data flow across the fabric device.		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Industry standard CLI		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Shall support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time Telemetry for streaming of telemetry information		
	Should support Configuration roll-back and check point		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		

	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		
	~~Should support user applications to run as a VM or Container to support modern DC troubleshooting and monitoring.~~		
3	**Layer 2**		
	Shall Support IEEE 802.1Q VLAN Tagging		
	Shall Support IEEE 802.1w Rapid Spanning Tree		
	Shall Support IEEE 802.1s Multiple Spanning Tree Protocol		
	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN		
	Switch should support basic Multicast IGMP v2, v3		
	~~Shall support Rapid Per VLAN Spanning Tree (RPVST+)~~		
	Shall support 802.3ad Link Aggregation LACP with up to 32 ports/channel		
	Shall support 128 Link Aggregation Groups (LAG)		
	Shall support 32 ports active/active layer2/Layer3 multipathing redundancy		
	Shall support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Shall support Port Mirroring		
	Shall support 802.3x Flow Control		
	Shall support Jumbo Frames 9216 Bytes		
	Shall support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG		
	Switch must support resilient L2 Hashing and ECMP		
	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using VRRP or equivalent		
	Shall Support IEEE 802.1D Bridging and Spanning Tree		
	Shall Support IEEE 802.3ab 1000BASE-T		
	Shall Support IEEE 802.3z Gigabit Ethernet		
	Shall Support IEEE 802.3ae 10 Gigabit Ethernet		
	Shall Support IEEE 802.3by 25 Gigabit Ethernet		

	Switch must 802.3ba 40 and 100 Gigabit Ethernet		
4	**Layer 3**		
	Shall support basic Layer-3 Routing		
	Shall support minimum 128-way ECMP routing for load balancing and redundancy		
	Shall support OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Shall support PIM-SM or SSM multicast routing		
	Shall support BFD v4 and v6 VRF Aware		
	Shall support BFD for LAG Link and Multihop BFD		
	Shall support Route Maps		
	Shall support Anycast RP		
	Shall support EVPN		
	Switch should support Dynamic Load Balancing Feature		
	Switch should support Traffic aware ECMP		
	Switch shall support IEEE 1588 PTP(Precision Time Protocol) with PTP Modes (Transparent Clock and Boundary Clock)		
	Switch must support uRPF		
	~~Switch must support NAT~~		
	Switch must support VxLAN with Routing and Bridging in Hardware in single pass		
	RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	RFC 4862 IPv6 Stateless Address Autoconfiguration		
	RFC 4443 Internet Control Message Protocol (ICMPv6) for the Ipv6 Specifications		
5	**Quality of Service (QoS)**		
	Up to 8 queues per port		
	802.1p based classification		
	DSCP based classification and remarking		
	Rate limiting		

	Switch should support for different type of QoS features for real time traffic differential treatment using Strict Priority Queuing		
	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
	Explicit Congestion Notification(ECN)		
	Switch must support Per Priority Flow Control(PFC)		
	DCBX Support - Data Center Bridging Extension		
	ACL based or equivalent protocol based DSCP Marking		
	ACL based or equivalent protocol based Policing		
	Policing Shaping		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Shall Support IEEE 802.1p QOS/COS		
6	**Security and Network Management**		
	Shall Support security ACLs		
	Shall Support TACACS+/RADIUS		
	Switch should support IP Source guard, ARP inspection, DHCP Snooping		
	Shall Support SNMP v2, v3		
	Shall Support Management over IPv4, IPv6		
	Switch should provide remote login for administration using:		
	a. Telnet		
	b. SSHV2		
	Shall Support Syslog		
	Shall Support AAA		
	Shall Support Port Mirroring		
	Shall Support sFlow / NetFlow		
	Switch should support for management and monitoring status using different type of Industry standard NMS using:		
	a. SNMP V1 and V.2		
	b. SNMP V.3		
	c. Filtration of SNMP using Access list		

	d. SNMP MIB support for QoS		
	Switch should support for basic administrative tools like:		
	a. Ping		
	b. Traceroute		
	Shall support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
	Switch should support central time server synchronization using Network Time Protocol		
	Switch should provide different privilege for login in to the system for monitoring and management		
7	**Monitoring, Provisioning**		
	Shall support Advance Event Management for pro-active network monitoring or equivalent		
	Shall support Restoration of Operating System & Configuration from USB		
	Shall support CLI schedular, Shell script, for timed automation, and event managert for triggered automation		
	Shall support centralized script/system to configure a switch without user intervention		
8	**Automation and Extensibility**		
	Switch must open APIs to be managed from any northbound controller.		
	Switch must support all devops tools like Ansible, Chef, Puppet and Salt stack.		
	Switch must support Openconfig		
9	**Data center Advanced Features and Network Virtulization**		
	Fabric Device must support Vxlan routing/bridging in hardware.		

	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically; with complete visibiltiy.		
	Solution must support visibilty via intergration into Container Workloads.		
	Vxlan routing and switching must also be supported in non default or default VRFs for multitenancy		
	Switch should have capability to run Docker container on switch.		
10	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All licenses and OS required for full layer 2/ layer 3 features shall be provided from day one		

Annexure 12 P

	Technical Specifications :Switch Type 6 (Leaf Switch)		
	Make and Model :		
Sr.No	**Required Minimum Specifications**	**Bidder's compliance (Yes/No)**	**Bidder's Remarks**
1	**Hardware & Interface / Performance**		
	Switch should be fixed 1RU based configuration to support atleast 48*10/25 GbE SFP+ and minimum of 12*100G uplinks with all SFPs populated from day one		
	Switch should support minimum 4.8 Tbps switching capacity/throughput or more		
	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding on every port		
	Switch should support minimum 1 Micro sec or less of latency for high speed switching.		
	Switch must support minimum 24Mb Intelligent Buffer with support for Dynamic Buffer allocation, also this buffer should have option to be split into multiple slices if desired		
	Control Plane should comprise - Quad Core x86 CPU, 8Gb DRAM and 8Gb Flash		
	Shall support min 256K MAC.		
	Shall support upto 350K IPv4 Routes.		
	Shall support upto 100K IPv4 Multicast entries.		
	Switch should have N+1 level of redundancy for power supply and fans with both front to rear and rear to front airflow		
	Switch should support AC Power supply with min 90% efficency or better		
	Switch should support Hitless upgrade & reloads in MLAG or VPC or Virtual Chassis or other supported protocol setup, without adversely afecting the fowarding plane with sub second data outage during upgrade		
	Should support both Front-to-back and back-to-front reversible airflow for optimized cooling		
	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc and should not require switch reboot & should not disrupt the functionality of the system		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		

	Switch OS should support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time State streaming of telemetry information		
	Should support programming in python, C++,GO or other supported protocol for programming the switch		
	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		
3	**Layer 2**		
	Switch should support IEEE 802.1D Bridging and 802.1Q VLAN Tagging along with 4096 Vlans		
	~~Switch should support IEEE 802.1w and 802.1s and Rapid Per Vlan Spanning Tree(RPVST+)~~		
	Switch should support 802.3ad Link Aggregation LACP with up to 32 ports/channel and 512 Groups Per System		
	Switch should support 32 ports active/active layer2 LAG		
	Switch should support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Switch should support 802.3x Flow Control		
	Switch should support Jumbo Frames 9216 Bytes		
	Switch should support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG		
	Switch should support IEEE 802.3ae 10 Gigabit Ethernet		
	Switch should support IEEE 802.3by 25 Gigabit Ethernet		
	Switch should support 802.3ba 40 and 100 Gigabit Ethernet		
4	**Layer 3**		
	Switch should support Dynamic Routing protcols like OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Switch should support Graceful restart for BGP,OSPF v2 and v3 and ISIS		
	Switch should support minimum 64-way ECMP routing for load balancing and redundancy		
	Switch should support PIM-SM or PIM-SSM or PIM-BiDi multicast routing or Anycast RP or MSDP along with Multicast Multipath		
	Switch should support BFD inclusive of BFD for Lag links, BFD for V4 and V6 VRF, Multi-hop BFD and BFD on IP unnumbered interfaces.		
	Switch Switch should support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP v4 and v6, Resilient ECMP, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking		
	Switch should support Traffic aware ECMP		

	Switch should support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
	Switch should support VxLAN with Routing and Bridging in Hardware.		
	Switch should support VxLAN routing and bridging must also be supported in overlay VRFs.		
	~~Switch should support Accumulated IGP Metric (AIGP), BGP Monitoring Protocol (BMP) and BGP Prefix Origin Validation with Resource Public Key Infrastructure (RPKI)~~		
	Switch should support VxLAN+EVPN leaf-spine overlay technology supporting type-1 to type-8 routes		
	Switch should have support IRB with EVPN with distributed gateway functionality.		
	Switch should support IGMP v2/v3,PIM-SM / PIM-SSM, Anycast RP (RFC 4610), VRF Support for IP Multicast, Multicast Source Discovery Protocol (MSDP)and IP Multicast Multipath.		
	~~Switch should support Dynamic NAT options like Many-to-Many NAT and Many-to-One NAT (PAT) at line rate with no additional latency.~~		
	Switch should support RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	Switch should support RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	Switch should support RFC 4862 IPv6 Stateless Address Autoconfiguration		
	Switch should support RFC 4443 Internet Control Message Protocol (ICMPv6) for the IPv6 Specifications		
	Switch should support RFC 1981 Path MTU Discovery for IP version 6		
	Switch should support RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
	Switch should support RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IPv4)		
5	**Quality of Service (QoS)**		
	Switch should support 8 queues per port		
	Switch should support 802.1p based classification		
	Switch should support DSCP based classification and remarking		
	Switch should support Rate limiting; Policing or Shaping		
	Switch should support Strict Priority Queuing		
	Switch should support Explicit Congestion Notification(ECN)		
	Switch should support Per Priority Flow Control(PFC)		
	Switch should support DCBX Support - Data Center Bridging Extension		
	Switch should support ACL based or equivalent protocol based DSCP Marking and Policing		
	Switch should support Egress queue scheduling and shaping and WRR and WRED		
6	**Security and Network Management**		

	Switch should support Security ACLs Ingress and Egress with upto L4 filtering capabilties.		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Switch should support TACACS+/RADIUS		
	Switch should support Management over IPv4, IPv6		
	Switch should provide remote login for administration using Telnet and SSHv2		
	Switch should support Syslog and Syslog over TLS		
	Switch should support AAA with accounting to AAA servers		
	Switch should support sFlow / NetFlow		
	Switch should support for management and monitoring status using SNMP v1,v2,v3		
	Switch should support Filtering of Management Traffic(SNMP,SSHv2) with Service ACL.		
	Switch should support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support central time server synchronization using Network Time Protocol		
	Switch should support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.		
7	**Monitoring, Provisioning and Automation**		
	Switch should support secure Zero Touch Provisioning with options to provision Certificates artifacts on the device when it boots.		
	Switch should support Advance Event Management for pro-active network monitoring or equivalent		
	Switch should support Restoration of Operating System & Configuration from USB		
	Switch should support advanced mirroring features : Mirror to CPU, ACL filters and truncation on Mirror sessions, and tunneling of mirror packets to remote servers.		
	Switch should monitor output queue lengths for all Device interfaces and log and stream events related to congestion		
	Switch should automatically mirror taffic queued in event of congetion/latency or micro burst and send mirrored traffic to CPU, directly connected server and remote server as per usecase.		
	Switch should have programability and automation with Anisble, python, bash.		
	Switch should support sampling of flows at every switch, aggregates them and sends the samples to a collector with path and latency information.		
	Switch should support tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purpose.		
8	**Data Center Features - Virtualization and SDN**		
	Solution should support integration with Open Stack.		
	Switch should support multi OEM hypervisor environment		

	Solution must support visibilty via intergration into Container Workloads.		
	Switch should have capability to run Docker container on switch.		
9	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All licenses and OS required for full layer 2/ layer 3 features shall be provided from day one		

Annexure 12 Q

Technical Specifications : Switch Type 7 (Leaf Switch)			
Make and Model :			
Sr. No	**Required Minimum Specifications**	**Bidder's compliance (Yes/No)**	**Bidder's Remarks**
1	**Hardware & Interface / Performance**		
	Switch should have 48 ports or more, capable of 1/10/25 GbE SFP+ and 8x40/100G uplinks		
	All ports should be populated with 24 x 1Gbps Copper SFP and 24x 10/25 Gbps SFP+ multimode fiber from day one and should support a mix of 1 G and 10/25 G SFP in future with mere replacement of SFPs by the Bank and all 8x 100 GB SFP should be populated from day one		
	Switch should support minimum 4 Tbps switching capacity/throughput or more		
	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding		
	For SFP/SFP+, shall support 10/25 GBE and 25GBASE-MR-XSR, MultiRate SFP		
	Switch should support minimum 1 micro sec or less of latency for high speed switching.		
	Switch should have console port		
	Switch should have management interface for Out of Band Management with support for 100M/1G Speeds.		
	Shall Support USB port		
	Switch must support minimum 32Mb Intelligent Buffer with support for Dynamic Buffer allocation, also this buffer should not be split into multiple slices.		
	Switch should have all the license enable for integrating with VXLAN based controller.		

	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel/LAG, multi chassis port channel etc		
	Control Plane should comprise - Quad Core x86 CPU, 8Gb DRAM and 8Gb Flash		
	Shall support min 256K MAC.		
	Shall support upto 350K IPv4 Routes.		
	Shall support upto 190K or more IPv6 Unicast entries.		
	Shall support upto 100K IPv4 Multicast entries.		
	Switch should have N+1 level of redundancy for power supply and fans		
	Switch should support AC Power supply with min 90% efficency or better		
	Should support both Front-to-back and back-to-front reversible airflow for optimized cooling		
	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc and should not require switch reboot & should not disrupt the functionality of the system		
	Switch should have Max Power Consumption of 305W or less		
	Switch must support Precision Time Protocol helps in synchronizing visibility of data flow across the fabric device.		
2	**Operating System**		
	Should support modern modular operating system designed for Performance, scalability and reliability based on Statefull Architecture		
	Should support Industry standard CLI		
	Should support Software Fault Containment and Stateful Fault Repair of individual agents(processes) running on the OS		
	Shall support Self Healing of Agent(processes) using Health Monitoring Mechanism		
	Should support Real Time Telemetry for streaming of telemetry information		
	Should support Configuration roll-back and check point		
	Should support programming in python, C++,GO or other supported protocol for programming the switch.		

	Should provide direct access to the Linux bash where Linux general utilities/commands can be executed		
	~~Should support user applications to run as a VM or Container to support modern DC troubleshooting and monitoring.~~		
3	**Layer 2**		
	Shall Support IEEE 802.1Q VLAN Tagging		
	Shall Support IEEE 802.1w Rapid Spanning Tree		
	Shall Support IEEE 802.1s Multiple Spanning Tree Protocol		
	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN		
	Switch should support basic Multicast IGMP v2, v3		
	~~Shall support Rapid Per VLAN Spanning Tree (RPVST+)~~		
	Shall support 802.3ad Link Aggregation LACP with up to 32 ports/channel		
	Shall support 128 Link Aggregation Groups (LAG)		
	Shall support 32 ports active/active layer2/Layer3 multipathing redundancy		
	Shall support 802.1AB Link Layer Discovery Protocol (LLDP)		
	Shall support Port Mirroring		
	Shall support 802.3x Flow Control		
	Shall support Jumbo Frames 9216 Bytes		
	Shall support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG		
	Switch must support resilient L2 Hashing and ECMP		
	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using VRRP or equivalent		
	Shall Support IEEE 802.1D Bridging and Spanning Tree		
	Shall Support IEEE 802.3ab 1000BASE-T		
	Shall Support IEEE 802.3z Gigabit Ethernet		
	Shall Support IEEE 802.3ae 10 Gigabit Ethernet		
	Shall Support IEEE 802.3by 25 Gigabit Ethernet		
	Switch must 802.3ba 40 and 100 Gigabit Ethernet		

4	**Layer 3**		
	Shall support basic Layer-3 Routing		
	Shall support minimum 128-way ECMP routing for load balancing and redundancy		
	Shall support OSPF, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
	Shall support PIM-SM or SSM multicast routing		
	Shall support BFD v4 and v6 VRF Aware		
	Shall support BFD for LAG Link and Multihop BFD		
	Shall support Route Maps		
	Shall support Anycast RP		
	Shall support EVPN		
	Switch should support Dynamic Load Balancing Feature		
	Switch should support Traffic aware ECMP		
	Switch shall support IEEE 1588 PTP(Precision Time Protocol) with PTP Modes (Transparent Clock and Boundary Clock)		
	Switch must support uRPF		
	Switch must support NAT		
	Switch must support VxLAN with Routing and Bridging in Hardware in single pass		
	RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
	RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)		
	RFC 4862 IPv6 Stateless Address Autoconfiguration		
	RFC 4443 Internet Control Message Protocol (ICMPv6) for the Ipv6 Specifications		
5	**Quality of Service (QoS)**		
	Up to 8 queues per port		
	802.1p based classification		
	DSCP based classification and remarking		
	Rate limiting		
	Switch should support for different type of QoS features for real time traffic differential treatment using Strict Priority Queuing		

	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
	Explicit Congestion Notification(ECN)		
	Switch must support Per Priority Flow Control(PFC)		
	DCBX Support - Data Center Bridging Extension		
	ACL based or equivalent protocol based DSCP Marking		
	ACL based or equivalent protocol based Policing		
	Policing Shaping		
	Switch should support control plane policing to protect switch CPU from DoS attack		
	Shall Support IEEE 802.1p QOS/COS		
6	**Security and Network Management**		
	Shall Support security ACLs		
	Shall Support TACACS+/RADIUS		
	Switch should support IP Source guard, ARP inspection, DHCP Snooping		
	Shall Support SNMP v2, v3		
	Shall Support Management over IPv4, IPv6		
	Switch should provide remote login for administration using:		
	a. Telnet		
	b. SSHV2		
	Shall Support Syslog		
	Shall Support AAA		
	Shall Support Port Mirroring		
	Shall Support sFlow / NetFlow		
	Switch should support for management and monitoring status using different type of Industry standard NMS using:		
	a. SNMP V1 and V.2		
	b. SNMP V.3		
	c. Filtration of SNMP using Access list		
	d. SNMP MIB support for QoS		
	Switch should support for basic administrative tools like:		

	a. Ping		
	b. Traceroute		
	Shall support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
	Switch should support central time server synchronization using Network Time Protocol		
	Switch should provide different privilege for login in to the system for monitoring and management		
7	**Monitoring, Provisioning**		
	Shall support Advance Event Management for pro-active network monitoring or equivalent		
	Shall support Restoration of Operating System & Configuration from USB		
	Shall support CLI schedular, Shell script, for timed automation, and event managert for triggered automation		
	Shall support centralized script/system to configure a switch without user intervention		
8	**Automation and Extensibility**		
	Switch must open APIs to be managed from any northbound controller.		
	Switch must support all devops tools like Ansible, Chef, Puppet and Salt stack.		
	Switch must support Openconfig		
9	**Data center Advanced Features and Network Virtulization**		
	Fabric Device must support Vxlan routing/bridging in hardware.		
	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically; with complete visibiltiy.		

	Solution must support visibilty via intergration into Container Workloads		
	Vxlan routing and switching must also be supported in non default or default VRFs for multitenancy		
	Switch should have capability to run Docker container on switch.		
10	**Mandatory Compliance :**		
	All categories of Switches, Transceivers & Switch OS should be from same OEM		
	All active managed proposed switches/switch OS should be EAL / NDcPP Common criteria certified.		
	All licenses and OS required for full layer 2/ layer 3 features shall be provided from day one		

Load Balancer			Annexure 12 R
Make and Model :			
S/N	**Required Minimum Specifications**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
A	**Platform**		
1	Must be an appliance with hardened OS		
2	Platform should be a full proxy architecture and must perform reverse proxy		
3	**Should support 10 virtual instances which have full fault isolation and resource reservation between each virtual instance. Hyper visor should not be an open source. The same can be further upgraded to 55 virtual instances.**		
4	Should have a dedicated out-of-band Ethernet management port		
5	Should have full support IPv6. It should support all IPv6 scenarios:		
6	a. IPv4 on the inside and IPv6 on the outside (Phase – II certified)		
7	b. IPv6 on the inside and IPv4 on the outside		
8	c. IPv6 on the inside and outside		
9	Should support VLAN, LACP & Trunking		
10	Should be a high performance purpose built hardware based solution with a minimal of intel quad core processor or better		
11	Should have a memory of 160 GB from Day 1		
12	Proposed Hardware must have 10 x 1/10 Gbps SFP+ and 4 x 40G QSFP+ optical ports Fully populated from day one with 10G and 40G Multi-Mode modules. Without use of any Splitout/ Breakout cable		
13	Should have Dual Power Supply & SSD Disk		
B	**Performance**		
1	Platform should have "L7" throughput of minimum 100 Gbps L7 throughput from day one		
2	The Proposed Appliance should support minimum 3 Million Layer 7 RPS (Request Per second)		
3	**The Proposed Appliance should support minimum 2.4 Million Layer 4 CPS (Connection Per second)**		
4	The Proposed Appliance should have and support 100,000 SSL CPS of RSA 2048 bit key strength and upto 45,000 SSL CPS of ECDSA-P256 bit key strength. (1TPS =1CPS)		
5	Should have SSL Throughput of minimum 40 Gbps		
6	Should have Compression throughput of minimum 10 Gbps		
7	Should support configurable TCP Optimization features for client- side and server-side connection		
C	**Security features**		
1	Proposed solution should contain an internal geo location database from day one		
2	Proposed Solution should support client NAT & server NAT		
3	Proposed solution should support HTTP Header manipulation on client requests and server responses to hide server identities		
4	Proposed Solution should have Advance Denial of Service protection		
D	**Server Load Balancing**		
1	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, hardware/software/firmware based SSL offload and hardware based server side compression		
2	Dual TCP Stack for client side as well as server side for optimizing TCP traffic towards both sides		
3	Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts		
4	Should have 2048 and 4096 bit key for SSL certificate support		
5	Should have capability to support ECC, RSA and ECC+RSA (Hybrid) Certificates for SSL offload		
6	Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive and observed		
7	Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1		
8	The Device should support Advanced Web Performance		
E	**Global Server Load Balancing**		
1	The Proposed Solution must have Global Server Load Balancing supported on the same appliance		
2	The Proposed Solution must have performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.		

3	The Proposed Solution must have global response time optimization in real-time through advanced load and proximity measurements		
4	The Proposed Solution must have providing failover capability between data centers in active-active or active-backup modes		
5	The Proposed Solution must have global redirection based on DNS		
6	The Proposed Solution should support DNSSEC functionality		
7	The Proposed Solution should support 1K DNS QPS (Query Per Second)		
F	**Optimization**		
1	The Device should support Application Performance Monitoring for advanced end to end reporting for every application transaction for all Virtual Service without any limitation with below details a. Session Anomaly b. Client Side Latency, Server Side Latency c. SSL Ciphers used d. End Device used to access the application e. End-to-End Latency for perticular session		
G	**Device Administration**		
1	Should provide HTTPS interface management for administering the device		
2	For device management and administration appliance should have internal user database as well as must support external user database of RADIUS/ TACACS+/ Microsoft AD/ LDAP and ClientCertificate LDAP		
3	Should provide SSH interface management for administering the device		
4	Should provide troubelshooting and traffic analysis tool like tcpdump		
5	Should support role based admin access with roles like no access, Guest,Operator,Application editior,Resource Administrator and Administrator		
6	Should have a live dashboard with graphical reporting		
	a. CPU Usage		
	b. Memory Usage		
	c. Connections Statistics		
	d. Throughput Statistics		
	e. Virtual Server Status		
	f. Pool Status		
	g. Node Status		
7	Should provide historical graphical reporting for the last 30 days on appliance itself or using external reporting solution seamlessly.		
8	Should have a built-in tool to take a snapshot of the unit for trobleshooting and analysis purpose		
9	Vendor should provide a service to upload this snapshot and get feedback on the heatlh of the unit & missing Hotfixes and best practices		
10	Appliance should support multiple configuration backup on appliance itself, also as when configuration restore happens it should backup last running config automatically and administrator should be able to go back to at least 4 restoration points		
11	The Proposed Appliance should support Network Isolation as well as Management isolation		
H	**Centralised Management**		
1	Proposed Solution must have Unified (Centralized) Consolidated Management (Hardware or Software based.) Incase of Software, required hardware will be provided. OS /software to be provided by vendor.		
2	Configuration Management		
3	SSL Cerificate Management		
4	Configuration Auditing , Reporting etc.		
I	**High Availability**		
1	Should have active-active and active-backup high availability with TCP/IP connection mirroring.		
2	Should have transparent failover between 2 devices, the failover should be transparent to other networking devices		
3	Should support network based failover for session mirroring, connection mirroring and heartbeat check		
4	Should support config autosync, manual sync to and from active and backup unit		
5	Should support the feature to force the active device to standby and back to active state; or force a device to offline mode		
6	Should support MAC masquerading		
J	**Reporting Features**		
1	Should have a Reporting Engine built-in		
2	Should support High Speed Logging to a syslog server		
3	Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc..		
K	**Service ,Support & Training**		
1	6 Hrs CTR support.		
2	Vendor operates 24/7/365 global Technical Assistance Center (TAC) in India		
3	The AMC warrenty should include all the components supplied as part of the solution including transreceivers,breakout cables etc.		

Make and Model : **Annexure 12 S**

Technical Spec – Router Type 1			
Sr. No	Specifications	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the access router:-		
1	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
2	The router must be based on architecture which does hardware based forwarding andswitching. The processing engine architecture must be multi-processor / multi-core based for enhanced processing		
3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
4	The router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.		
5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
6	Rack mounting kit for securing the router in standard rack are to be provided.		
7	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
B	Architecture: The architecture of the router must be modular.		
1	**The router should provide 120 Mpps of forwarding speed**		
2	The router must have redundant power supply module. The router must support 220V AC or -2 48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails. Router should be proposed with AC power supply.Power Supply: The router must have redundant power supply module. The router must support 220V AC power supply module. There should not be any impact on the router performance in case of one power supply fails.		
3	Router Processor Architecture: The router processor architecture must be multi-processor /Multi-core based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
4	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.		
5	Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
6	Clock: The router must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.		
7	The router must have support for flash memory for configuration and OS backup.		
8	The proposed solution should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
C	**Router Performance Parameter**		
1	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
3	**Router must support 5 Gbps of Crypto throughput for IPSEC performance and minimum of 4000 IPSEC tunnels from day 1 (internal/external).**		
4	The Router solution must be a enterprise grade Equipment supporting the following:		
	a) In-band and out-band management		
	c) Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
5	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism		
6	The router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path		
D	**Physical Parameters**		
1	The router must have the following interface as defined in the IEEE, ITU-T:		
2	**The Router shouold support 36x 1G Copper SFP and 8 X 10G SFP+ port multimode and should be populated with all ports from day one**		
E	**Layer 3 Routing Protocols**		
1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support		
2	both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
3	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
4	The router should support minimum 100 VRF instances from day one		
5	The Router should have at-least 2 GB of DRAM from day one		
F	IPv6 Support		
1	Should support IP version 6 in hardware.		
2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6		
4	Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
5	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
6	The router should support for IPv6 Multicast.		

7	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
8	Should support IPv6 Quality of Service		
9	Should support IPv6 dual stack		
10	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	Should support SNMP over IPv6 for management.		
12	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
13	The router must support router redundancy protocol like VRRP/ HSRP		
G	Multicast		
1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
2	~~The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.~~		
3	The multicast implementation must support source specific multicast.		
4	The router must support multicast load balancing traffic across multiple interfaces.		
5	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP)		
H	**Quality of Service**		
1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.		
2	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.		
3	The router shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter.		
4	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.		
5	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
6	The router should have support for minimum 8 queues per port		
7	Scheduling should allow for round robin and weighted round robin.		
8	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.		
9	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
10	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type		
11	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.		
12	**The router shall support at least 4k queues per interface to offer granular QoS, policing and shaping capabilities."**		
13	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
14	IPSec packets should be marked with QoS security feature		
15	The router shall meet the following requirements for security –		
16	The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc.		
17	The router shall support time based ACL to reflect time based security and QoS policy.		
18	The router shall support unicast RPF (uRPF) or similar feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
19	The router shall support firewall service in hardware on all interfaces.		
20	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
21	The router shall support AAA features through RADIUS or TACACS+.		
22	The router shall support Control Plane Policing to protect the router CPU from attacks.		
23	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
24	**The proposed router should have embedded support for 4000 IPsec tunnels from day one, which should be activated from day 1.**		
J	System Management and Administration		
1	Routers should support configuration rollback		
2	Support for accounting of traffic flows for Network planning and Security purposes		
3	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic		
4	Routers should support Software upgrades		
5	Routers should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The management software should integrate with EMS (Microfocus) product suite.		
K	Built-in troubleshooting		
1	Extensive debugs on all protocols		
2	Shall support Secure Shell for secure connectivity		
3	Should have to support Out of band management through Console and an external modem for remote management		
4	Pre-planned scheduled Reboot Facility		

5	Real Time Performance Monitor – service-level agreement verification probes/alert		
I	**Certifications**		
1	The proposed router should be NDPP/EAL3/EAL4 or FCC certified		

Annexure 12 T

Technical Spec – Router -2			
Sr. No	**Specifications**	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the access router:-		
1	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
2	The router must be based on architecture which does hardware based forwarding andswitching. The processing engine architecture must be multi-processor / multi-core based for enhanced processing		
3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
4	The router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.		
5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
6	Rack mounting kit for securing the router in standard rack are to be provided.		
7	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
B	Architecture: The architecture of the router must be modular.		
1	Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 20 Gbps on Day 1 and should be scalable to 40 Gbps in future.		
2	The router must have redundant power supply module. The router must support 220V AC or -2 48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails. Router should be proposed with AC power supply.Power Supply: The router must have redundant power supply module. The router must support 220V AC power supply module. There should not be any impact on the router performance in case of one power supply fails.		
3	Router Processor Architecture: The router processor architecture must be multi-processor /Multi-core based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
4	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.		
5	Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
6	Clock: The router must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.		
7	The router must have support for flash memory for configuration and OS backup.		
8	The proposed solution should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
C	**Router Performance Parameter**		
1	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
4	The Router solution must be a enterprise grade Equipment supporting the following:		
	a) In-band and out-band management		
	c) Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
5	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism		
6	The router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path		
D	**Physical Parameters**		
1	The router must have the following interface as defined in the IEEE, ITU-T:		
2	Minimum of 8 x 10 GE Fiber and 4 x 1 GE Copper ports. 8 x 10 GE Fiber active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
E	**Layer 3 Routing Protocols**		
1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
3	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
4	The router should support minimum 100 VRF instances from day one		
5	The Router should have at-least 4GB of DRAM from day one		
F	IPv6 Support		
1	Should support IP version 6 in hardware.		
2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6		
4	Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
5	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
6	The router should support for IPv6 Multicast.		
7	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
8	Should support IPv6 Quality of Service		
9	Should support IPv6 dual stack		
10	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	Should support SNMP over IPv6 for management.		
12	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
13	The router must support router redundancy protocol like VRRP/ HSRP		
G	**Multicast**		
1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
2	~~The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.~~		
3	The multicast implementation must support source specific multicast.		
4	The router must support multicast load balancing traffic across multiple interfaces.		
5	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.		
H	**Quality of Service**		
1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.		

2	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.		
3	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.		
4	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
5	The router should have support for minimum 8 queues per port		
6	Scheduling should allow for round robin and weighted round robin.		
7	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.		
8	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
9	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type		
10	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.		
11	The router shall support at least 32k queues to offer granular QoS, policing and shaping capabilities.		
12	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
13	IPSec packets should be marked with QoS security feature		
14	The router shall meet the following requirements for security –		
15	The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc.		
16	The router shall support time based ACL to reflect time based security and QoS policy.		
17	The router shall support unicast RPF (uRPF) or similar feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
18	The router shall support firewall service in hardware on all interfaces.		
19	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
20	The router shall support AAA features through RADIUS or TACACS+.		
21	The router shall support Control Plane Policing to protect the router CPU from attacks.		
22	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
23	The proposed router should have embedded support for 4000 IPsec tunnels from day one, which should be activated from day 1.		
J	**System Management and Administration**		
1	Routers should support configuration rollback		
2	Support for accounting of traffic flows for Network planning and Security purposes		
3	Should support extensive support for SLA monitoring for metrics like delay, latency,		
4	Routers should support Software upgrades		
5	Routers should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The management software should integrate with EMS (Microfocus) product suite.		
K	Built-in troubleshooting		
1	Extensive debugs on all protocols		
2	Shall support Secure Shell for secure connectivity		
3	Should have to support Out of band management through Console and an external modem for remote management		
4	Pre-planned scheduled Reboot Facility		
5	Real Time Performance Monitor – service-level agreement verification probes/alert		
I	**Certifications**		
1	The proposed router should be NDPP/EAL3/EAL4 or FCC certified		

Annexure 12 U

Technical Spec – Router -3			
Sr. No	**Specifications**	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the access router:-		
1	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
2	The router must be based on architecture which does hardware based forwarding andswitching. The processing engine architecture must be multi-processor / multi-core based for enhanced processing		
3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
4	The router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.		
5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
6	Rack mounting kit for securing the router in standard rack are to be provided.		
7	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
B	Architecture: The architecture of the router must be modular.		
1	Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 8 Gbps on Day 1 and should be scalable to 40 Gbps in future.		
2	The router must have redundant power supply module. The router must support 220V AC or -48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails. Router should be proposed with AC power supply.Power Supply: The router must have redundant power supply module. The router must support 220V AC power supply module. There should not be any impact on the router performance in case of one power supply fails.		
3	Router Processor Architecture: The router processor architecture must be multi-processor /Multi-core based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
4	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.		
5	Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
6	Clock: The router must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.		
7	The router must have support for flash memory for configuration and OS backup.		
8	The proposed solution should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
C	**Router Performance Parameter**		
1	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
3	The Router solution must be a enterprise grade Equipment supporting the following:		
	a) In-band and out-band management		
	b) Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
6	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism		
7	Router must support 5 Gbps of Crypto throughput (IMIX) from Day 1 with in-box scalability upto 8 Gbps for IPSEC performance and 7500 IPSEC tunnels from day 1 (internal/external).		
8	The router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path		
D	**Physical Parameters**		
1	The router must have the following interface as defined in the IEEE, ITU-T:		
2	Minimum of 8 x 10 GE Fiber and 4 x 1 GE Copper ports. 8 x 10 GE Fiber active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
E	**Layer 3 Routing Protocols**		
1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
3	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
4	The router should support minimum 100 VRF instances from day one		
5	The Router should have at-least 4GB of DRAM from day one		
F	IPv6 Support		
1	Should support IP version 6 in hardware.		
2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6		
4	Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
5	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
6	The router should support for IPv6 Multicast.		
7	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
8	Should support IPv6 Quality of Service		
9	Should support IPv6 dual stack		
10	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	Should support SNMP over IPv6 for management.		
12	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		

13	The router must support router redundancy protocol like VRRP/ HSRP		
G	**Multicast**		
1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
2	The multicast implementation must support source specific multicast.		
3	The router must support multicast load balancing traffic across multiple interfaces.		
4	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.		
H	**Quality of Service**		
1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.		
2	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.		
3	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.		
4	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
5	The router should have support for minimum 8 queues per port		
6	Scheduling should allow for round robin and weighted round robin.		
7	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.		
8	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
9	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type		
10	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.		
11	The router shall support at least 32k queues to offer granular QoS, policing and shaping capabilities.		
12	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
13	IPSec packets should be marked with QoS security feature		
14	The router shall meet the following requirements for security –		
15	The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc.		
16	The router shall support time based ACL to reflect time based security and QoS policy.		
17	The router shall support unicast RPF (uRPF) or similar feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
18	The router shall support firewall service in hardware on all interfaces.		
19	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
20	The router shall support AAA features through RADIUS or TACACS+.		
21	The router shall support Control Plane Policing to protect the router CPU from attacks.		
22	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
23	The proposed router should have embedded support for 4000 IPsec tunnels from day one, which should be activated from day 1.		
J	**System Management and Administration**		
1	Routers should support configuration rollback		
2	Support for accounting of traffic flows for Network planning and Security purposes		
3	Should support extensive support for SLA monitoring for metrics like delay, latency,		
4	Routers should support Software upgrades		
5	Routers should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The management software should integrate with EMS (Microfocus) product suite.		
K	Built-in troubleshooting		
1	Extensive debugs on all protocols		
2	Shall support Secure Shell for secure connectivity		
3	Should have to support Out of band management through Console and an external modem for remote management		
4	Pre-planned scheduled Reboot Facility		
5	Real Time Performance Monitor – service-level agreement verification probes/alert		
I	**Certifications**		
1	The proposed router should be NDPP/EAL3/EAL4 or FCC certified		

Annexure 12 V

Technical Spec – Router -4			
Sr. No	**Specifications**	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the access router:-		
1	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
2	The router must be based on architecture which does hardware based forwarding andswitching. The processing engine architecture must be multi-processor / multi-core based for enhanced processing		
3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
4	The router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.		
5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
6	Rack mounting kit for securing the router in standard rack are to be provided.		
7	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
B	**Architecture: The architecture of the router must be modular.**		
1	Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 10 Gbps on Day 1 and should be scalable to 40 Gbps in future.		
2	The router must have redundant power supply module. The router must support 220V AC or -2 48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails. Router should be proposed with AC power supply.Power Supply: The router must have redundant power supply module. The router must support 220V AC power supply module. There should not be any impact on the router performance in case of one power supply fails.		
3	Router Processor Architecture: The router processor architecture must be multi-processor /Multi-core based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
4	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.		
5	Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
6	Clock: The router must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.		
7	The router must have support for flash memory for configuration and OS backup.		
8	The proposed solution should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
C	**Router Performance Parameter**		
1	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
4	The Router solution must be a enterprise grade Equipment supporting the following:		
	a) In-band and out-band management		
	c) Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
5	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism		
6	The router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path		
7	Router must support 5 Gbps of Crypto throughput (IMIX) from Day 1 with in-box scalability upto 8 Gbps for IPSEC performance and 7500 IPSEC tunnels from day 1 (internal/external).		
D	**Physical Parameters**		
1	The router must have the following interface as defined in the IEEE, ITU-T:		
2	Minimum of 8 x 10 GE Fiber and 4 x 1 GE Copper ports. 4 x 10 GE Fiber active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
3	Fast Ethernet, Gigabit Ethernet, 10G Fiber Ethernet Ports.		
E	**Layer 3 Routing Protocols**		
1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
3	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
4	The router should support minimum 100 VRF instances from day one		
5	The Router should have at-least 4GB of DRAM from day one		
F	IPv6 Support		
1	Should support IP version 6 in hardware.		
2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6		
4	Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
5	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
6	The router should support for IPv6 Multicast.		
7	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
8	Should support IPv6 Quality of Service		
9	Should support IPv6 dual stack		
10	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	Should support SNMP over IPv6 for management.		
12	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
13	The router must support router redundancy protocol like VRRP/ HSRP		
G	**Multicast**		
1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
3	The multicast implementation must support source specific multicast.		
4	The router must support multicast load balancing traffic across multiple interfaces.		
5	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.		
H	**Quality of Service**		
1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.		
2	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.		
3	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.		
4	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
5	The router should have support for minimum 8 queues per port		

6	Scheduling should allow for round robin and weighted round robin.		
7	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.		
8	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
9	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type		
10	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.		
11	The router shall support at least 32k queues to offer granular QoS, policing and shaping capabilities.		
12	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
13	IPSec packets should be marked with QoS security feature		
14	The router shall meet the following requirements for security –		
15	The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc.		
16	The router shall support time based ACL to reflect time based security and QoS policy.		
17	The router shall support unicast RPF (uRPF) or similar feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
18	The router shall support firewall service in hardware on all interfaces.		
19	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
20	The router shall support AAA features through RADIUS or TACACS+.		
21	The router shall support Control Plane Policing to protect the router CPU from attacks.		
22	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
23	The proposed router should have embedded support for 4000 IPsec tunnels from day one, which should be activated from day 1.		
J	**System Management and Administration**		
1	Routers should support configuration rollback		
2	Support for accounting of traffic flows for Network planning and Security purposes		
3	Should support extensive support for SLA monitoring for metrics like delay, latency,		
4	Routers should support Software upgrades		
5	Routers should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The management software should integrate with EMS (Microfocus) product suite.		
K	Built-in troubleshooting		
1	Extensive debugs on all protocols		
2	Shall support Secure Shell for secure connectivity		
3	Should have to support Out of band management through Console and an external modem for remote management		
4	Pre-planned scheduled Reboot Facility		
5	Real Time Performance Monitor – service-level agreement verification probes/alert		
	The management software should integrate with EMS (Microfocus) product suite.		
I	**Certifications**		
1	The proposed router should be NDPP/EAL3/EAL4 or FCC certified		

Annexure 12 W

Firewall Type -1

S/N	Required Minimum Specifications (Per Device) [Any model other than Checkpoint]	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the firewall-		
1	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework		
2	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded:		
	a. Prevention against Malware		
	b. Prevention against Bot & Botnets,		
	c. Prevention against malware hosting URL, Prevention against risky web2.0 apps		
	d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
3	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
4	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
5	Proposed solution should have a Unified Policy Frame work for application, user, data awareness, etc in a single rule.		
6	Licensing should be a per device and not limited to user/IP based (should support unlimited users)		
7	Firewall Architecture should be on distributed framework – NGFW with Threat Prevention Policy Management, Logging, Reporting, Dashboard and should be managed from a centralised console.		
8	The communication between all the components should be encrypted with SSL or PKI.		
9	Security effectiveness should be recommended/certified by NSS **/ Forrester** NGFW **last published** test report		
10	Proposed Solution framework should have IPSec VPN (Site to Site VPN) functionalities for Secure Remote access to corporate application over the internet		
11	Solution should have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
12	The proposed solution of appliances should support the dynamic routing protocols with readiness for BGPv4 & OSPF		
13	Appliance should have a capability to support for more than 500 VLAN.		
14	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.		
15	Firewall Appliances should deployed for Active – Active architecture for both Firewall & VPN.		
16	It should support the system authentication with TACACS+ **/** RADIUS.		
17	IPSec VPN should support the Authentication Header / **ESP** Protocols		
18	IPSec ISAKMP methods should support Diffie-Hellman Group 1,2,5,14 & 19, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 2048		
19	Should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
B	Performance Requirement		
1	The proposed solution should have an integrated solution for IPSEC, site to site		
2	Proposed solution should support IPSec functionality		
3	Solution should support minimum **200,000** new sessions per second processing		
4	Firewall should support atleast **15,000,000 concurrent sessions**		
C	Hardware and Interface Requirements		
1	Firewall appliance should have Console port and USB Ports		
2	Solution should support VLAN Tagging and Link Aggregation (IEEE 802.3ad) to achieve higher bandwidth		
3	Solution should support Dual Stack with Ipv4 and Ipv6 functionality		
4	Solution should support Ipv6 NAT functionality NAT64 and NAT46		
5	Firewall should have Hardware Sensor Monitoring capabilities.		
6	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
7	Every Gateway Security control (like Firewall or any other feature **including URL filtering, Anti-Malware etc.** required to meet **the mentioned** specification) must not have any licensing restriction on number of users **as and when the licenses are being utilised by the Bank**		

8	Each Appliance should have at least 8x10 GE fiber and 4 x 1 G Copper interface. All mentioned ports should be active and populated with required transceivers from day one. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. **HA and Management ports are to be factored additionally, over and above the mentioned interface quantity.**		
9	Should support atleast **20 Gbps from day 1** of production performance (http based) / multiprotocol & multipacket combined, Firewall & IPS throughput **and should be scalable to 30 Gbps in future.**		
10	**Hot Swapability: The hardware must have redundant and Hot swappable power supply and Redundant Hot swappable fan.**		
11	**The hardware should have at-least 64 GB of DRAM from day one**		
D	Firewall Filtering & Web Control [Application Control +URL Filtering] Requirements		
1	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
2	The Firewall must provide state engine support for all common protocols of the TCP/IP stack		
3	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
4	The Firewall should be able to filter traffic even if the packets are fragmented		
5	The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net-.		
6	The Firewall should provide advanced NAT capabilities, supporting all applications and services		
7	Local access to firewall modules should support role based access		
8	Solution should support Application Detection and Usage Control.		
9	Application Control Databases should have sizable application and widget control list		
10	Solution should have an option of creating custom categories for URL and Application control.		
11	Should provide Seamless integration with Active Directory /LDAP (Agent-less deployment is preferable)		
12	Should be Managed Centrally from Single Dashboard via user friendly interface.		
13	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats		
14	**Application Control and URL Filtering licenses are not required from day 1 and may not be included as part of the proposed device.**		
E	Anti-Malware & Anti-bot		
1	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
2	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
3	The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
4	The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
5	The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations		
6	The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities		
7	The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
8	The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.		
9	Solution should be able to discover the Bot infected machine		
10	Solution should be able to provide with Forensic tools which give details like Infected Users/Device,Malware type,Malware action etc		
11	Anti-virus scanning should support proactive and stream mode **or equivalent**		
12	Solution should be able to create a protection scope for the inspection		
13	Proposed solution should have an option of configuring Exception		
14	Anti-spyware for pattern based blocking at the gateway		
15	The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
16	The proposed solution should be able to detect & prevent the malware by scanning of different file types.		
17	Proposed solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		

18	The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP		
19	The proposed solution should prevent the users to access the malware hosting websites and/or web resources		
20	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) or any other internationally supported format		
21	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at bank's data center.		
22	**Anti-Malware & Anti-bot licenses are not required from day 1 and may not be included as part of the proposed device.**		
F	Application Visibility and Awareness		
1	Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement		
2	Firewall should support the Identity based logging, application detection and usage controls		
3	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.		
4	Should have Categories like Business Applications, IM, File Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Search Engine, Virtual Worlds, Webmail etc.		
5	The proposed solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).		
6	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
7	Identity Access should be able to distinguish between employee and other like guests and contractors.		
8	Should have provide out of box Categories based on Application types, Security Risk level etc. Should include filtering of application names based on Application types, Security Risk level etc.		
9	Application Control Library should covering most of the Web 2.0 application signatures		
G	Administration, Management and Logging		
1	Management Should support automation & Orchestration using Open REST API Support.		
2	The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.		
3	Solution should be able provide auditing view / report for FW changes, Rule addition/Deletion & other network changes		
4	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.		
5	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
6	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.		
7	Role based administration with multiple administrators & Separation of duties should be supported. Config conflict should be avoided when multiple administrators works together.		
8	Management should provide role based access on policy configuration to cater separation of duties.		
9	Management should have log indexing capability for faster log search & log optimization.		
10	The Firewall administration software must provide a means of viewing, filtering and managing the log data. Monitoring logs in single console per policy will be plus		
11	The Firewall logs must contain information about the firewall policy rule that triggered the log.		
12	Should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
13	Management should alert administrator in case if any configuration error or Misconfiguration.		
14	The centralized management solution should support integration with the Microsoft AD or LDAP, NAC/IDAM.		
15	The Solution should be able to ingest the Intelligence shared over STIX **/** TAXII **/ API** from the SIEM solution		
16	Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework.		

17	It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
18	It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
19	Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.		
20	All proposed components NGFW, Logging, Reporting etc. should be managed from centralised management framework and if not then vendor need to provide additional components if any		
21	Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework		
22	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc. need to be provided with Real-Time and Historical reporting all the components.		
23	IPS signatures should support more than 7000+ excluding custom signatures.		
24	Centralized Management Server should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
25	**The management software should integrate with EMS (Microfocus) product suite.**		
H	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Separate Management **solution along with License (in HA mode) to be provisioned each** for DC, Mumbai and DR, Hyderabad **and also separately for each type of Firewall.**		
3	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
4	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
5	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided		
I	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
J	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
H	**URL Filtering**		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		

Annexure 12 X

Firewall -Type 2

S/N	Required Minimum Specifications (Per Device)	Bidder's compliance (Yes / No)	Bidder's remarks
A	The following are the functional requirements to be met by the firewall-		
1	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework		
2	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded: a. Prevention against Malware b. Prevention against Bot & Botnets, c. Prevention against malware hosting URL, Prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
3	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
4	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
5	Proposed solution should have a Unified Policy Frame work for application, user, data awareness, etc in a single rule.		
6	Licensing should be a per device and not limited to user/IP based (should support unlimited users)		
7	Firewall Architecture should be on distributed framework – NGFW with Threat Prevention Policy Management, Logging, Reporting, Dashboard and should be managed from a centralised console.		
8	The communication between all the components should be encrypted with SSL or PKI.		
9	Security effectiveness should be recommended/certified by NSS **/ Forrester** NGFW **last published** test report		
10	Proposed Solution framework should have IPSec VPN (Site to Site VPN) functionalities for Secure Remote access to corporate application over the internet		
11	Solution should have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
12	The proposed solution of appliances should support the dynamic routing protocols with readiness for BGPv4 & OSPF		
13	Appliance should have a capability to support for more than 500 VLAN.		
14	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.		
15	Firewall Appliances should deployed for Active – Active architecture for both Firewall & VPN.		
16	It should support the system authentication with TACACS+ **/** RADIUS.		
17	IPSec VPN should support the Authentication Header / **ESP** Protocols		
18	IPSec ISAKMP methods should support Diffie-Hellman Group 1,2,5,14 & 19, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 2048		
19	Should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
B	Performance Requirement		
1	The proposed solution should have an integrated solution for IPSEC, site to site		
2	Proposed solution should support IPSec functionality		
3	Solution should support minimum **200,000** new sessions per second processing		
4	Firewall should support atleast **15,000,000 concurrent sessions**		
C	Hardware and Interface Requirements		
1	Firewall appliance should have Console port and USB Ports		
2	Solution should support VLAN Tagging and Link Aggregation (IEEE 802.3ad) to achieve higher bandwidth		
3	Solution should support Dual Stack with Ipv4 and Ipv6 functionality		
4	Solution should support Ipv6 NAT functionality NAT64 and NAT46		
5	Firewall should have Hardware Sensor Monitoring capabilities.		
6	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
7	Every Gateway Security control (like Firewall or any other feature **including URL filtering, Anti-Malware etc.** required to meet **the mentioned** specification) must not have any licensing restriction on number of users **as and when the licenses are being utilised by the Bank**		
8	Each Appliance should have at least 8x10 GE fiber and 4 x 1 G Copper interface. All mentioned ports should be active and populated with required transceivers from day one. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. **HA and Management ports are to be factored additionally, over and above the mentioned interface quantity.**		
9	Should support atleast **20 Gbps from day 1** of production performance (http based) / multiprotocol & multipacket combined, Firewall & IPS throughput **and should be scalable to 30 Gbps in future.**		
10	**Hot Swapability: The hardware must have redundant and Hot swappable power supply and Redundant Hot swappable fan.**		

11	**The hardware should have at-least 64 GB of DRAM from day one**		
D	Firewall Filtering & Web Control [Application Control +URL Filtering] Requirements		
1	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
2	The Firewall must provide state engine support for all common protocols of the TCP/IP stack		
3	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
4	The Firewall should be able to filter traffic even if the packets are fragmented		
5	The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net-.		
6	The Firewall should provide advanced NAT capabilities, supporting all applications and services		
7	Local access to firewall modules should support role based access		
8	Solution should support Application Detection and Usage Control.		
9	Application Control Databases should have sizable application and widget control list		
10	Solution should have an option of creating custom categories for URL and Application control.		
11	Should provide Seamless integration with Active Directory /LDAP (Agent-less deployment is preferable)		
12	Should be Managed Centrally from Single Dashboard via user friendly interface.		
13	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats		
14	**Application Control and URL Filtering licenses are not required from day 1 and may not be included as part of the proposed device.**		
E	Anti-Malware & Anti-bot		
1	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
2	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
3	The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
4	The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
5	The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations		
6	The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities		
7	The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
8	The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.		
9	Solution should be able to discover the Bot infected machine		
10	Solution should be able to provide with Forensic tools which give details like Infected Users/Device,Malware type,Malware action etc		
11	Anti-virus scanning should support proactive and stream mode **or equivalent**		
12	Solution should be able to create a protection scope for the inspection		
13	Proposed solution should have an option of configuring Exception		
14	Anti-spyware for pattern based blocking at the gateway		
15	The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
16	The proposed solution should be able to detect & prevent the malware by scanning of different file types.		
17	Proposed solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		
18	The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP		
19	The proposed solution should prevent the users to access the malware hosting websites and/or web resources		
20	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) or any other internationally supported format		
21	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at bank's data center.		
22	**Anti-Malware & Anti-bot licenses are not required from day 1 and may not be included as part of the proposed device.**		
F	Application Visibility and Awareness		
1	Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement		
2	Firewall should support the Identity based logging, application detection and usage controls		
3	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.		

4	Should have Categories like Business Applications, IM, File Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Search Engine, Virtual Worlds, Webmail etc.		
5	The proposed solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).		
6	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
7	Identity Access should be able to distinguish between employee and other like guests and contractors.		
8	Should have provide out of box Categories based on Application types, Security Risk level etc. Should include filtering of application names based on Application types, Security Risk level etc.		
9	Application Control Library should covering most of the Web 2.0 application signatures		
G	Administration, Management and Logging		
1	Management Should support automation & Orchestration using Open REST API Support.		
2	The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.		
3	Solution should be able provide auditing view / report for FW changes, Rule addition/Deletion & other network changes		
4	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.		
5	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
6	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.		
7	Role based administration with multiple administrators & Separation of duties should be supported. Config conflict should be avoided when multiple administrators works together.		
8	Management should provide role based access on policy configuration to cater separation of duties.		
9	Management should have log indexing capability for faster log search & log optimization.		
10	The Firewall administration software must provide a means of viewing, filtering and managing the log data. Monitoring logs in single console per policy will be plus		
11	The Firewall logs must contain information about the firewall policy rule that triggered the log.		
12	Should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
13	Management should alert administrator in case if any configuration error or Misconfiguration.		
14	The centralized management solution should support integration with the Microsoft AD or LDAP, NAC/IDAM.		
15	The Solution should be able to ingest the Intelligence shared over STIX **/** TAXII **/ API** from the SIEM solution		
16	Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework.		
17	It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
18	It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
19	Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.		
20	All proposed components NGFW, Logging, Reporting etc. should be managed from centralised management framework and if not then vendor need to provide additional components if any		
21	Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework		
22	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc. need to be provided with Real-Time and Historical reporting all the components.		
23	IPS signatures should support more than 7000+ excluding custom signatures.		
24	Centralized Management Server should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
25	**The management software should integrate with EMS (Microfocus) product suite.**		
H	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Separate Management **solution along with License (in HA mode) to be provisioned** for NDR, Mumbai **and also separately for each type of Firewall.**		
3	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
4	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		

5	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided		
I	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
J	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
H	**URL Filtering**		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		