Addendum to the RFP's Eligibility Criteria & Installation:

Sr No.	Clause in RFP	Clarifications/ Changes made
1.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **C. Others:** 2. One Bidder can bid only with one OEM and If the OEM is bidding directly then they cannot submit another bid simultaneously with any other partner/bidder.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **C. Others:** **2. If the OEM is bidding directly then they cannot submit another bid simultaneously with any other partner/bidder. (Supporting document - Letter of confirmation from OEM (Should be on company letter head and must be signed by an authorized official only)**
2.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **D. Experience & Support Infrastructure** 1. The bidder should have supplied and maintained for at least 50 no's of proposed switches (Maximum 2 order) in past 3 Years to Commercial Banks / Financial Institutions / Government / PSU Organizations / IT & ITES / Manufacturing / Large Corporate in India.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **D. Experience & Support Infrastructure** 1. The bidder should have supplied and **installed** at least 50 no's of Switches (Maximum 2 order) in past 3 Years to Commercial Banks / Financial Institutions / Government / PSU Organizations / **Private Sector /** IT & ITES in India.
3.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **D. Experience & Support Infrastructure** 3. Must have adequate stock of spares of all items supplied and would be capable of providing replacement against faulty hardware as per the SLA.	**Annexure 2: Evaluation Terms** **A. Eligibility Criteria** **D. Experience & Support Infrastructure** 3. Must have adequate stock of spares of all items supplied and would be capable of providing replacement against faulty hardware as per the SLA. Supporting documents - Letter of undertaking (self-certified letter signed by authorized official of the bidder**/OEM**)
4.	**4. Installation** Network Hardware Installation at Bank's locations, including unpacking of cartons/ boxes, will be the responsibility of the vendor. Successful vendor will have to install the network hardware and hand it over to Bank for acceptance testing within 2	**4. Installation** Network Hardware Installation at Bank's locations, including unpacking of cartons/ boxes, will be the responsibility of the vendor. Successful vendor will have to install the network hardware and hand it over to Bank for acceptance testing within

Sr No.	Clause in RFP	Clarifications/ Changes made
	weeks from the date of delivery of the network hardware at Bank locations and Bank's notification for installation of the same. Vendor will have to pay late installation / implementation charges to the Bank @ 0.5% of the total Purchase Order Value per day or part thereof subject to maximum of 5% of the total purchase order value, for delay in installation, if the delay is caused owing to reasons attributable to the Vendor.	2 weeks from the date of delivery of the network hardware at Bank locations and Bank's notification for installation of the same. Vendor will have to pay late installation / implementation charges to the Bank @ 0.5% of the total Purchase Order Value **per week** or part thereof subject to maximum of 5% of the total purchase order value, for delay in installation, if the delay is caused owing to reasons attributable to the Vendor.

Technical Specifications:

A. Switch: 48 Port (Requirement: 77 Nos.):

S No.	Required Minimum Specifications	Bidder's Compliance (Yes/No)	Detail description how the solution /component would be compliant
1	Minimum of 48 port 10/100/1000 Mbps Ethernet auto sensing ports with 4*10 G uplink port from day one.		
2	The switch should have 176 Gbps of Switching Capacity and 130.9 Mpps Throughput Capacity		
3	The switch should be 1U and rack mountable in standard 19" rack.		
4	Full-Duplex Operation on Gig Ethernet		
5	The switch should have at least 4GB SDRAM and 4GB flash and have The switch should have Console Port , one OOBM port		
6	Switch should support stacking/MLAG and for stacking switch should have minimum 40 GBPS staking bandwidth		
7	Support for minimum of 32K MAC addresses		
8	Support for minimum of 750 active VLAN.		
9	The switch should have Internal redundant power supply and redundant Fan Tray from day one		
10	The Switch should support IEEE 802.3ad LACP supports up to 32 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm		
11	The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) or similar to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.		
12	RADIUS or TACACS + Support		
13	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
14	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
15	Support for Private VLAN to minimize broadcasts and maximize available bandwidth.		

16	Rack mounting kit for securing the switch in standard rack are to be provided.		
17	The switch should have minimum		
	At Least 2K Ipv4 Unicast Routes and 1K Ipv6 Unicast Routes		
	750 IGMP Groups		
	1500 pv4 ingress ACL Entries.		
Layer 2 Features: -			
1	The Switch should support AT LEAST 4K VLAN IDs		
2	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of AT LEAST 9k bytes		
3	The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.		
4	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups		
5	The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
6	The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network.		
QoS Features: -			
1	Support for Classification and scheduling based on 802.1p/Q		
2	Support for 802.1p class-of-service (CoS). Ability to Mark/override 802.1P CoS per port		
3	Eight queues per egress port.		
4	DWRR/WRR for congestion avoidance or equivalent feature		
Multicast Support: -			
1	The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN		
2	The Switch should support Internet Group Management Protocol (IGMP)/IGMP Snooping / Any-Source Multicast (ASM) to manage IPv4		

	multicast networks; Integrate IGMPv1, v2, and v3		
Redundancy: -			
1	Link Aggregation		
2	Spanning Tree (802.1d) with support for spanning tree per VLAN		
3	Quick Failover over redundant links for improved network stability and reliability		
4	Support for IEEE rapid spanning tree.		
Security Features: -			
1	The Switch should support integrated trusted platform module (TPM) or similar for platform integrity. This ensures the boot process started from a trusted combination of switches.		
2	The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header		
3	The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis		
4	The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security		
6	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards		
7	The Switch should support Web-based authentication provides a browser-based environment or similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X		
8	The Switch should support MAC-based client authentication		
9	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications		

10	The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3		
13	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user		
14	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks		
15	The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing		
16	The Switch should support ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data		
17	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes		
18	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator		
19	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network		
20	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks		
21	The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch		
22	The Switch should support Secure FTP to allow secure file transfer to and from the switch and protect against unwanted file downloads or unauthorized copying of a switch configuration file		
23	The Switch should support Critical Authentication Role to ensure that important infrastructure devices are allowed network access even in the absence of a RADIUS server		

24	The Switch should support MAC Pinning or static MAC address configuration to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected		
25	The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, telnet/SSH, SSL, Web.		
26	The switch should support minimum 1500 Access control entry		
27	The Switch should support Security banner displays a customized security policy when users log in to the switch		
28	The Switch should support Green initiative for RoHS (EN 50581:2012) , WEEE regulations or similar		
Other Features:			
1	The switch should have integrate with Banks internal NMS.		
2	The management software should integrate with any EMS product suite.		
3	Layer 2 or Layer 3 traceroute feature to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
4	Should support Link layer Discovery Protocol		
5	Should Support DNS		
6	Secure access to switch management, limiting management applications from specific hosts only		
7	Should support BPDU guard to avoid topology loop.		
8	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
9	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
10	The operating system should have a self-healing mechanism /equivalent feature for the automatic recovery of the switch when a specified event occurs		
11	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime /equivalent.		
Network Management (Management Feature):-			
1	Embedded support for Web based management using standard secured web browser.		

2	Support for SNMP v1, SNMP v2c and SNMP v3		
3	Support for FTP/SFTP based software download/upload		
4	Support for port mirroring measurement using a network analyser or RMON probe.		
5	RMON: 4 Group (Statistics, Alarm, Events, History), on every port, no impact to performance		
6	Switch must be remotely managed via one telnet/SSH session for all module configuration		
7	Should have functionality to add new features like Firmware upgrades from central location, etc.		
8	Provisioned and Dynamic Policies at Layers 1-4 for QoS and Security		
9	Real Time Multi-Port Statistics		
10	Mac/IP Address Finder or equivalent feature		
11	Device and Port Groupings for Navigation and Policy Management		
12	Radius or TACACS+ server Support		
13	Administrative Access Right		
14	Traffic Volume/Error/Congestion Monitoring		
15	The Switch should be able to discover the neighbouring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
16	Should have Topology view features		
IEEE Standard Compliance: -			
1	802.1Q VLAN tagging		
2	802.1p Priority		
3	802.1D Spanning Tree		
4	802.3u Fast Ethernet		
5	802.3x Flow Control		
6	802.1x Authentication		
7	802.3ab Gigabit Interface		
8	Support for Remote Authentication Dialin User service (RADIUS) change of		
	authorization, URL Redirection and AAA		
9	Must have support to 802.1x network authentication and port security on a port		
	basis which will help to deploy Network Access Control (NAC)		
10	802.1x support with following features:		
	· 802.1x with VLAN Assignment		

	· 802.1x Guest VLAN		
	· It should be compatible with 802.1x protocol.		
	without valid credentials to access a limited set of services which can be controlled by an administrator		
	· 802.1x - Auth Fail Open or equivalent. (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable.)		
	· 802.1x MAC-Auth-Bypass		
	· 802.1x with ACLS		
	· 802.1x Accounting		
	· Web Authentication for Non 802.1x Clients.		
	· Switch should support concurrent deployment of 802.1x and MAB		
	Authentication.		

B. Switch: 24 Port (Requirement: 10 Nos.)

S No	Required Minimum Specifications	Bidder's Compliance (Yes/No)	Detail description how the solution /component would be compliant
1	Minimum of 24 port 10/100/1000 Mbps Ethernet auto sensing ports with 4*10 G uplink port from day one.		
2	The switch should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity		
3	The switch should be 1U and rack mountable in standard 19" rack.		
4	Full-Duplex Operation on Gig Ethernet		
5	The switch should have at least 4GB SDRAM and 4GB flash and have The switch should have Console Port , one OOBM port		
6	Switch should support stacking/MLAG and for stacking switch should have minimum 40 GBPS staking bandwidth		
7	Support for minimum of 32K MAC addresses		
8	Support for minimum of 500 active VLAN.		
9	The switch should have Internal redundant power supply and redundant Fan Tray from day one		
10	The Switch should support IEEE 802.3ad LACP supports up to 32 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm		
11	The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) or smilar to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.		
12	RADIUS or TACACS + Support		
13	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
14	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
15	Support for Private VLAN to minimize broadcasts and maximize available bandwidth.		
16	Rack mounting kit for securing the switch in standard rack are to be provided.		
17	The switch should have minimum		

	At Least 2K Ipv4 Unicast Routes and 1K Ipv6 Unicast Routes		
	750 IGMP Groups		
	1500 pv4 ingress ACL Entries.		
Layer 2 Features: -			
1	The Switch should support AT LEAST 4K VLAN IDs		
2	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of AT LEAST 9k bytes		
3	The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.		
4	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups		
5	The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
6	The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network.		
QoS Features: -			
1	Support for Classification and scheduling based on 802.1p/Q		
2	Support for 802.1p class-of-service (CoS). Ability to Mark/override 802.1P CoS per port		
3	Eight queues per egress port.		
4	DWRR/WRR for congestion avoidance or equivalent feature		
Multicast Support: -			
1	The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN		
2	The Switch should support Internet Group Management Protocol (IGMP)/IGMP Snooping / Any-Source Multicast (ASM) to manage IPv4		

	multicast networks; Integrate IGMPv1, v2, and v3		
Redundancy: -			
1	Link Aggregation		
2	Spanning Tree (802.1d) with support for spanning tree per VLAN		
3	Quick Failover over redundant links for improved network stability and reliability		
4	Support for IEEE rapid spanning tree.		
Security Features: -			
1	The Switch should support integrated trusted platform module (TPM) or similar for platform integrity. This ensures the boot process started from a trusted combination of switches.		
2	The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header		
3	The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis		
4	The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security		
5	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards		
6	The Switch should support Web-based authentication provides a browser-based environment or similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X		
7	The Switch should support MAC-based client authentication		

8	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications		
9	The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3		
10	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user		
11	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks		
12	The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing		
13	The Switch should support ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data		
14	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes		
15	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator		
16	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network		
17	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks		
18	The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch		
19	The Switch should support Secure FTP to allow secure file transfer to and from the switch and protect against unwanted file downloads or unauthorized copying of a switch configuration file		

20	The Switch should support Critical Authentication Role to ensure that important infrastructure devices are allowed network access even in the absence of a RADIUS server		
21	The Switch should support MAC Pinning or static MAC address configuration to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected		
22	The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, telnet/SSH, SSL, Web.		
23	The switch should support minimum 1500 Access control entry		
24	The Switch should support Security banner displays a customized security policy when users log in to the switch		
25	The Switch should support Green initiative for RoHS (EN 50581:2012), WEEE regulations or smillar		
Other Features:			
1	The switch should have integrate with Banks internal NMS.		
2	The management software should integrate with any EMS product suite.		
3	Layer 2 or Layer 3 traceroute feature to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
4	Should support Link layer Discovery Protocol		
5	Should Support DNS		
6	Secure access to switch management, limiting management applications from specific hosts only		
7	Should support BPDU guard to avoid topology loop.		
8	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
9	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
10	The operating system should have a self-healing mechanism /equivalent feature for the automatic recovery of the switch when a specified event occurs		
11	The software should have a mechanism to proactively detect and address potential		

	hardware and software faults during runtime /equivalent.		
Network Management (Management Feature): -			
1	Embedded support for Web based management using standard secured web browser.		
2	Support for SNMP v1, SNMP v2c and SNMP v3		
3	Support for FTP/SFTP based software download/upload		
4	Support for port mirroring measurement using a network analyser or RMON probe.		
5	RMON: 4 Group (Statistics, Alarm, Events, History), on every port, no impact to performance		
6	Switch must be remotely managed via one telnet/SSH session for all module configuration		
7	Should have functionality to add new features like Firmware upgrades from central location, etc.		
8	Provisioned and Dynamic Policies at Layers 1-4 for QoS and Security		
9	Real Time Multi-Port Statistics		
10	Mac/IP Address Finder or equivalent feature		
11	Device and Port Groupings for Navigation and Policy Management		
12	Radius or TACACS+ server Support		
13	Administrative Access Right		
14	Traffic Volume/Error/Congestion Monitoring		
15	The Switch should be able to discover the neighbouring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
16	Should have Topology view features		
IEEE Standard Compliance: -			
1	802.1Q VLAN tagging		
2	802.1p Priority		
3	802.1D Spanning Tree		
4	802.3u Fast Ethernet		
5	802.3x Flow Control		
6	802.1x Authentication		
7	802.3ab Gigabit Interface		
8	Support for Remote Authentication Dialin User service (RADIUS) change of		

	authorization, URL Redirection and AAA		
9	Must have support to 802.1x network authentication and port security on a port		
	basis which will help to deploy Network Access Control (NAC)		
10	802.1x support with following features:		
	· 802.1x with VLAN Assignment		
	· 802.1x Guest VLAN		
	· It should be compatible with 802.1x protocol.		
	without valid credentials to access a limited set of services which can be controlled by an administrator		
	· 802.1x - Auth Fail Open or equivalent. (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable.)		
	· 802.1x MAC-Auth-Bypass		
	· 802.1x with ACLS		
	· 802.1x Accounting		
	· Web Authentication for Non 802.1x Clients.		
	· Switch should support concurrent deployment of 802.1x and MAB		
	Authentication.		

C. Router: 4 Port (Requirement: 15 Nos.):

S No	Required Minimum Specifications	Bidder's Compliance (Yes/No)	Detail description how the solution /component would be compliant
1	The following are the functional requirements to be met by the access router: -		
2	Router shall have 1:1/1:N PSU redundancy from day one		
3	The processing engine architecture must be multi-processor / multi-core based for enhanced processing		
4	The router must support traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
5	The router must support flow-based traffic analysis feature.		

6	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
7	Rack mounting kit for securing the router in standard rack are to be provided.		
8	Architecture: The architecture of the router must be modular.		
9	The router should provide 10 gbps throughput.		
10	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.		
11	The router processing engine architecture must be multi-processor / multi-core based for enhanced processing.		
12	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode or able to store dual software image to ensure high availability of the system. The router in the event of failure of any one OS or control module It should possible to boot router from redundant OS or redundant control module.		
13	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.		
14	The router must sync to the Network Time Protocol (NTP) server.		
15	The router must have support for flash memory for configuration and OS backup.		
16	The router must have minimum 8 GB DRAM and 8 GB flash memory for configuration and OS backup. Router should have provision to add SSD drives for extra storage requirement		
18	Router Performance Parameter		
19	The router must support minimum 1,500,000 IPv4 or 1,500,000 IPv6 routes entries in the routing table and should be scalable.		
20	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		

21	Router must support 5 Gbps of Crypto throughputs for IPSEC performance and minimum of 4000 IPSEC tunnels from day 1 (internal/external).		
22	The Router solution must be a enterprise grade Equipment supporting the following:		
23	a) In-band and out-band management		
24	c) Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
25	The proposed router should support modular OS upgrade mechanism		
26	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		
27	Physical Parameters		
28	The router must have the following interface as defined in the IEEE, ITU-T or equivalent		
29	The Router should support 4x 1G Copper SFP / Port and 4 X 10G SFP+ port multimode and should be populated with all ports from day one Router should have free slots to add additional Ethernet ports in future		
30	Router should support variety of interface like Ethernet 1Gig, 10Gig , FE.		
31	Layer 3 Routing Protocols		
32	The router must support the IPv4 and IPv6 stack in hardware and software. It must support		
33	both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
34	The router must support RIPv1 / RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
35	The router should support minimum 100 VRF instances from day one		
36	The Router should have at-least 8 GB of DRAM from day one		
37	IPv6 Support		
38	Should support IP version 6 in hardware.		
39	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
40	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6		
41	Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
42	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		

43	The router should support for IPv6 Multicast.		
44	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
45	Should support IPv6 Quality of Service		
46	Should support IPv6 dual stack		
47	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
48	Should support SNMP over IPv6 for management.		
49	The router must perform GRE tunnelling as per RFC 1701 and RFC 1702..		
50	The router must support router redundancy protocol like VRRP/ HSRP		
51	Multicast		
52	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) or Sparse Mode (PIM-SM) or similar		
53	The multicast implementation must support source specific multicast.		
54	The router must support multicast load balancing traffic across multiple interfaces.		
55	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP)		
56	Quality of Service		
57	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.		
58	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 .		
59	The router shall support Strict Priority Queuing or Low Latency or similar Queuing to support real time application like Voice and Video with minimum delay and jitter.		
60	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.		
61	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
62	The router should have support for minimum 8 queues per port		

63	Scheduling should allow for round robin and weighted round robin or similar		
64	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.		
65	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
66	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		
67	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.		
68	The router shall support at least 16k queues to offer granular QoS, policing and shaping capabilities or similar features		
69	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
70	IPSec packets should be marked with QoS security feature		
71	The router shall meet the following requirements for security –		
72	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.		
73	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.		
74	The router shall support firewall service in hardware on all interfaces.		
75	The router should have support for Network Address Translation (NAT) or Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
76	The router shall support AAA features through RADIUS or TACACS+.		
77	The router shall support Control Plane Policing to protect the router CPU from attacks.		
78	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS,BGP.		
79	The proposed router should have embedded support for 4000 IPsec tunnels from day one, which should be activated from day 1.		
80	Router shall support 256-bit encryption		
81	System Management and Administration		

82	Routers should support configuration rollback		
83	Support for accounting of traffic flows for Network planning and Security purposes		
84	Should support extensive support for SLA monitoring for metrics like delay/latency/ jitter/ packet loss or RTP-Based VoIP traffic		
85	Routers should support Software upgrades		
86	Routers should support SNMPv2 and SNMPv3		
87	Device should have Console, Telnet, SSH1 and SSH2 support for management		
88	The management software should integrate with EMS (Microfocus) product suite.		
89	Built-in troubleshooting		
90	Extensive debugs on all protocols		
91	Shall support Secure Shell for secure connectivity		
92	Should have to support Out of band management through Console and an external modem for remote management		
93	Pre-planned scheduled Reboot Facility		
94	Real Time Performance Monitor – service-level agreement verification probes/alert		
95	Certifications		
96	The proposed router should be NDPP/EAL3/EAL4 or FCC certified		

Clarification of Pre-bid queries is enclosed separately.

All other Terms & Conditions are same as per our RFP Bid no. GEM/2024/B/4885083Dated 24th April 2024 for Supply, Installation and Maintenance of Network Switch and Router with 5 Years Warranty.