Bank of Baroda
Addendum 2 dated 17th September 2021

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Router - Type 1 Annexure 12 A

Make and Model : DC Mumbai : 2; DR Hyderabad: 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 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 and switching. The processing engine architecture must be multi-processor **/ multi-core** based for enhanced performance.		
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	Router Architecture		
1	Architecture: The architecture of the router must be modular. 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.		
3	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.		
4	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.		
5	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.		
6	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.		
7	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.		
8	The router must have support for flash memory for configuration and OS backup.		
9	The Proposed model should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
10	**The router must be SD WAN compliant**		
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 (IMIX) **from Day 1 with in-box scalability upto 8 Gbps** for IPSEC performance and **7500 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		
b)	Software rollback feature		
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.** **6 x 10 GE Fiber** active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
3	The router card must support following interface: 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.		
2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
3	The router should support minimum **100 VRF instances** from day one		
4	The Router should have at-least **8 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 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The router should support for IPv6 Multicast.		
6	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	Should support IPv6 Quality of Service		
8	Should support IPv6 dual stack		
9	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	Should support SNMP over IPv6 for management.		
11	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The router must support router redundancy protocol like VRRP.		
13	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
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 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 **32k queues** 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		
I	Security Feature		
1	The router shall meet the following requirements for security –		
2	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.		
3	The router shall support time based ACL to reflect time based security and QoS policy.		
4	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The router shall support firewall service in hardware on all interfaces.		
6	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.		
7	The router shall support AAA features through RADIUS or TACACS+.		
8	The router shall support Control Plane Policing to protect the router CPU from attacks.		
9	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
10	The proposed router should have embedded support for 8000 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 trouble shooting		
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		
L	Certifications		
1	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
2	The proposed router should be **NDPP/EAL3 certified**		

Bank of Baroda			
Tender No.		**BCC:IT:PROC:113:30**	
Name of Work		**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder			
Router-Type 2 Annexure 12 B			
Make and Model : DC Mumbai : 2; DR Hyderabad: 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 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 and switching. The processing engine architecture must be multi-processor **/ multi-core** based for enhanced performance.		
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	Router Architecture		
1	Architecture: The architecture of the router must be modular. 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.		
3	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.		
4	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.		
5	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.		
6	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.		
7	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.		
8	The router must have support for flash memory for configuration and OS backup.		
9	The Proposed model should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
10	**The router must be SD WAN compliant**		

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 (IMIX) **from Day 1 with in-box scalability upto 8 Gbps** for IPSEC performance and **7500 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		
b)	Software rollback feature		
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.** 6 x 10 GE Fiber active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
3	The router card must support following interface: 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.		
2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
3	The router should support minimum **100 VRF instances** from day one		
4	The Router should have at-least **8 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 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The router should support for IPv6 Multicast.		
6	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	Should support IPv6 Quality of Service		
8	Should support IPv6 dual stack		
9	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	Should support SNMP over IPv6 for management.		
11	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The router must support router redundancy protocol like VRRP.		
13	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		

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 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 **32k queues** 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		
I	Security Feature		
1	The router shall meet the following requirements for security –		
2	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.		
3	The router shall support time based ACL to reflect time based security and QoS policy.		
4	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The router shall support firewall service in hardware on all interfaces.		
6	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.		
7	The router shall support AAA features through RADIUS or TACACS+.		
8	The router shall support Control Plane Policing to protect the router CPU from attacks.		
9	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
10	The proposed router should have embedded support for 8000 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		
K	Built-in trouble shooting		
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		
L	Certifications		
1	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
2	The proposed router should be **NDPP/EAL3 certified**		

Bank of Baroda

Tender No.	**BCC:IT:PROC:113:30**	
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder		
Router-Type 3 Annexure 12 C		
Make and Model : DC Mumbai : 4; DR Hyderabad: 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 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 and switching. The processing engine architecture must be multi-processor **/ multi-core** based for enhanced performance.		
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	Router Architecture		
1	Architecture: The architecture of the router must be modular. 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 -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.		
3	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.		
4	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.		
5	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.		
6	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.		
7	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.		
8	The router must have support for flash memory for configuration and OS backup.		
9	The Proposed model should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
10	**The router must be SD WAN compliant**		
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 (IMIX) **from Day 1 with in-box scalability upto 8 Gbps** for IPSEC performance and **7500 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		
b)	Software rollback feature		
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.** 4 x 10 GE Fiber active ports with Transreceiver and **3 x 1 GE Copper** active ports with Transreceiver from day one.		
3	The router card must support following interface: 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.		
2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
3	The router should support minimum **100 VRF instances** from day one		
4	The Router should have at-least **8 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 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The router should support for IPv6 Multicast.		
6	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	Should support IPv6 Quality of Service		
8	Should support IPv6 dual stack		
9	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	Should support SNMP over IPv6 for management.		
11	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The router must support router redundancy protocol like VRRP.		
13	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
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 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 **32k queues** 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		
I	Security Feature		
1	The router shall meet the following requirements for security –		
2	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.		
3	The router shall support time based ACL to reflect time based security and QoS policy.		
4	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The router shall support firewall service in hardware on all interfaces.		
6	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.		
7	The router shall support AAA features through RADIUS or TACACS+.		
8	The router shall support Control Plane Policing to protect the router CPU from attacks.		
9	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
10	The proposed router should have embedded support for 8000 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 trouble shooting		
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		
L	Certifications		
1	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
2	The proposed router should be **NDPP/EAL3 certified**		

Tender No.		**BCC:IT:PROC:113:30**	
Name of Work		**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder			
Router-Type 4 Annexure 12 D			
Make and Model : NDR Mumbai : 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 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 and switching. The processing engine architecture must be multi-processor **/ multi-core** based for enhanced performance.		
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	Router Architecture		
1	Architecture: The architecture of the router must be modular. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 12 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.		
3	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.		
4	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.		
5	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.		
6	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.		
7	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.		
8	The router must have support for flash memory for configuration and OS backup.		
9	The Proposed model should be supplied & supported in at least two commercial Bank / Financial Institutions / Govt Organization in India.		
10	**The router must be SD WAN compliant**		
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 (IMIX) **from Day 1 with in-box scalability upto 8 Gbps** for IPSEC performance and **7500 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		
b)	Software rollback feature		
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.** 6 x 10 GE Fiber active ports with Transreceiver and 4 x 1 GE Copper active ports with Transreceiver from day one.		
3	The router card must support following interface:		

	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.		
2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
3	The router should support minimum **100 VRF instances** from day one		
4	The Router should have at-least **8 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 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6		
4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The router should support for IPv6 Multicast.		
6	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	Should support IPv6 Quality of Service		
8	Should support IPv6 dual stack		
9	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	Should support SNMP over IPv6 for management.		
11	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The router must support router redundancy protocol like VRRP.		
13	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
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 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 **32k queues** 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		
I	Security Feature		
1	The router shall meet the following requirements for security –		
2	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.		
3	The router shall support time based ACL to reflect time based security and QoS policy.		
4	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The router shall support firewall service in hardware on all interfaces.		
6	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.		
7	The router shall support AAA features through RADIUS or TACACS+.		
8	The router shall support Control Plane Policing to protect the router CPU from attacks.		

9	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP.		
10	The proposed router should have embedded support for 8000 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 trouble shooting		
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		
L	Certifications		
1	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
2	The proposed router should be **NDPP/EAL3 certified**		

Tender No.	BCC:IT:PROC:113:30	
Name of Work	Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre	
Name of Bidder		
Switch -Type 1 Annexure 12 E		
Make and Model : DC Mumbai : 32; NDR Mumbai : 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 access switch-		
1	Switch should have 48 nos. of multispeed **1 GB Copper interfaces** and 2 nos. of 10 GE SFP+ uplink ports with line rate forwarding performance from day one		
2	Switch must have forwarding rate of at least 130.9 Mbps or more		
3	Switch should have Forwarding Bandwidth of 108 GBPS		
4	Switch should support Switching bandwidth 216 GBPS		
5	Switch must have capability to support for active **512 vlans**		
6	The offered product part codes have to be General Availability Part codes and not custom built Part Code. There should be cross reference to the Public website of the OEM with Enterprise grade switches capability		
7	2 Nos of Power Cord — Indian Localization to be prvided in day one.		
B	Features		
1	Switch should support STP-Spanning tree protocol (802.1D, 802.1W and 802.1S)		
2	Switch should support Dynamic Host Configuration Protocol (DHCP) auto configuration of multiple switches through a boot server eases switch deployment.		
3	Switch should support Auto-Negotiation on all ports automatically.		
4	Switch should support Dynamic Trunking Protocol (DTP) **or equivalent**		
5	Switch should support LACP for port bundling		
6	Switch should support Automatic Media-Dependent Interface Crossover.(MDIX) **or equivalent feature** automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.		
7	Switch must support Unidirectional Link Detection Protocol (UDLD), Aggressive UDLD, BPDU guard and root guard features **or equivalent**		
8	Switch should support Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge **or equivalent feature** to minimize broadcasts and maximize available bandwidth.		
9	Switch should support Internet Group Management Protocol (IGMP) Snooping for IPv4 and IPv6. It should support multicast IGMP V1, V2 and V3 support		
10	Switch should support Per-port Broadcast, Multicast, and Unicast Storm Control		
11	Switch should support dynamic VLANs and dynamic trunk configuration **or equivalent** across all switches.		
12	Switch must support Local and Remote Switch Port Analyzer (RSPAN) **or equivalent**. Also it must support feature such as Netflow/ SFLow / Jflow **or equivalent** from day one		
12	Switch should support Layer 2 Traceroute **or equivalent feature** for ease of troubleshooting		
14	Switch should support Trivial File Transfer Protocol (TFTP).		
15	Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification		
16	Switch must be Energy Efficient Ethernet or equivalent compliant.		
17	Switch should support optional internal or external redundant power supply		
18	**The management software should integrate with EMS (Microfocus) product suite.**		
C	Security & QOS		
1	Switch must support RADIUS change of authorization **or equivalent** feature which provides mechanism to change the attributes of an authentication, authorization and accounting (AAA) after it is authenticated		
2	RADIUS Change of Authorization (CoA) for Network Admission Control based on RFC 5176 **or equivalent** from day one		
3	Switch should support for Port Security.		
4	Switch should support for DHCP server, DHCP relay and DHCP Snooping.		
5	Switch should support for Dynamic ARP Inspection (DAI) **or equivalent** to ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
6	Switch should support IP source guard.		
7	The proposed switch should allow/disallow access to a particular user depending on the MAC Address or Active Directory **/ Any authentication solution** credentials to prevent unauthorized access,		
8	The RADIUS Change of Authorization Feature provides a mechanism to change the attributes of an Authentication, Authorization, and Accounting (AAA) session after it is authenticated.		
9	Switch must support for QOS trusted boundary, up to 8 egress queues per port and strict priority queuing, 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.		
10	Switch must support for access control list for IPv6 and IPv4 for security and QOS ACE		

11	Switch must support Cross-stack QoS **or equivalent feature** to allow QoS to be configured across the entire stack		
12	Switch should be **IPv6 ready.**		
13	Network Time Protocol capability over IPv6		
D	Stacking		
1	The switch must support dedicated stacking ports **or equivalent feature** from day one		
2	Stacking **or equivalent feature** should enable all the switches to function as a single unit with single		
3	The Stacking module **or equivalent feature** should be Hot-swappable		
4	Stacking **or equivalent feature** should support upto maximum 8 nos. Of Switches		
5	Stacking **or equivalent feature** must support 70 Gbps or higher of throughput per switch		
6	Stacking **or equivalent feature** should support stacking cable length of 3m		
7	Switch should support cross stack Link aggregation protocols **or equivalent feature**.		
E	Standards of IEEE supported by the Switch		
1	IEEE 802.1D Spanning Tree Protocol		
2	IEEE 802.1p CoS Prioritization		
3	IEEE 802.1Q VLAN		
4	IEEE 802.1s		
5	IEEE 802.1w		
6	IEEE 802.1x		
7	IEEE 802.1AB (LLDP)		
8	IEEE 802.3ad		
9	IEEE 802.3ab 1000BASE-T specification		
F	Standards of RFC supported by the Switch		
1	RFC 768: UDP		
2	RFC 783: TFTP		
3	RFC 791: IP		
4	RFC 792: ICMP		
5	RFC 793: TCP		
6	RFC 826: ARP		
7	RFC 854: Telnet		
8	RFC 1542: BOOTP Extensions		
9	RFC 959: FTP		
10	RFC 1191 - Maximum Transmission Unit (MTU) Path Discovery IPv4		
11	RFC 1305: NTP		
12	RFC 1492: TACACS+		
13	RFC 2068 - HTTP		
14	RFC 2131 - DHCP		
15	RFC 2138 – RADIUS		
16	RFC 2236: IGMP Snooping		
17	RFC 2460 - IPv6		
18	RFC 2461 - IPv6 Neighbour Discovery		
19	RFC 2462 - IPv6 Auto configuration		
20	RFC 2463 - ICMP IPv6		
21	RFC 2597 - Assured Forwarding		
22	RFC 2598 - Expedited Forwarding **or Strict Priority Queuing PHB**		
23	RFC 2571 - SNMP Management		
24	RFC 2737: Entity MIB v2		
25	RFC 2819: RMON		
26	RFC 2863 - IF MIB v3		
27	RFC 3046 - DHCP Relay Agent Information Option		
28	RFC RFC 4291- IPv6 Addressing Architecture		
29	RFC 4594 - Configuration Guidelines for DiffServ Service Classes		
30	RFC 8201 - Maximum Transmission Unit (MTU) Path Discovery IPv6		

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Switch -Type 2 Annexure 12 F

Make and Model : DC Mumbai : 6

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 access switch:		
1	Minimum of 48 port 1/10/25 Gbps port and 6 nos. of 40/100 Gbps ports, with minimum 1280 Gbps switching backplane		
2	1GBE Copper Transreceiver - 10 Nos on day 1		
3	10G SFP+LC SR Transreceiver - 20 Nos on day 1		
4	40GbE QSFP+ Transreceiver - 4 Nos on day 1		
5	100GbE QSFP+ Transreceiver - 2 Nos on day 1		
6	QSFP+ to QSFP+ 3 mts DAC cable		
7	SFP+ to SFP+ 3 mts DAC cable		
8	Full-Duplex Operation on GbE		
9	Multiple Load Sharing Trunks		
10	Minimum of **4 GB** SDRAM and **4 GB** Flash memory, packet buffer size: **24 MB**		
11	**Redundant and Hot Swappable Platinum rated Power Supplies** (Port side intake)		
12	Fan Tray - 2 Nos **(Redundant Hot swappable fan)**		
13	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
14	Minimum throughput of 250 million pps		
15	Minimum routing/switching capacity should be **2.56 Tbps**		
16	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
17	Support for minimum of 128000 MAC addresses		
18	RFC 1027 Proxy ARP RFC 1091 Telnet Terminal-Type Option RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
19	Should support TACACS/TACACS+		
20	High MTBF Support		
21	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
22	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
23	Rack mounting kit for securing the switch in standard rack are to be provided.		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		
2	**Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification**		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		
C	Security & QOS Features		
1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Support Configuration Change Tracking		
6	Support System Event Logging		
7	Support Syslog		
8	Support SNMP v1, v2c, v3 compatible		
D	Other Features		

1	Switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		
2	The management software should integrate with EMS **(Microfocus)** product suite.		
3	Switch should seamlessly integrate with existing network equipments		
4	Layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
5	Switch should support Link layer Discovery Protocol		
6	Switch should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Switch should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L3 features		
E	Network Management (Management Feature)		
1	Embedded support for Web based management using standard secured web browser **or management of switch should be supported using EMS (Microfocus) product suite.**		
2	**Support all features of SNMP v3.**		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer 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 session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Should support QoS and Security at Layers 1-4		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Radius or TACACS+ server Support		
13	Private and Enterprise MIB / MIB		
14	Administrative Access Right		
15	Traffic Volume/Error/Congestion Monitoring		
16	TFTP **or equivalent mode for** Download / Upload Software		
17	Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
F	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		
G	RFC (Request for Comment) Support		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Switch -Type 3 Annexure 12 G

Make and Model : DC Mumbai : 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 access switch-		
1	Minimum of 48 port 1/10/25 Gbps port and 6 nos. of 40/100 Gbps ports, with minimum 1280 Gbps switching backplane		
2	1GBE Copper Transreceiver - 10 Nos on day 1		
3	10G SFP+LC SR Transreceiver - 20 Nos on day 1		
4	40GbE QSFP+ Transreceiver - 4 Nos on day 1		
5	100GbE QSFP+ Transreceiver - 1 Nos on day 1		
6	QSFP+ to QSFP+ 3 mts DAC cable		
7	SFP+ to SFP+ 3 mts DAC cable		
8	Full-Duplex Operation on GbE		
9	Multiple Load Sharing Trunks		
10	Minimum of **4 GB** SDRAM and **4 GB** Flash memory, packet buffer size: **24 MB**		
11	**Redundant and Hot Swappable Platinum rated Power Supplies** (Port side intake)		
12	Fan Tray - 2 Nos **(Redundant Hot swappable fan)**		
13	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
14	Minimum throughput of 250 million pps		
15	Minimum routing/switching capacity should be **2.56 Tbps**		
16	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
17	Support for minimum of 128000 MAC addresses		
18	RFC 1027 Proxy ARP RFC 1091 Telnet Terminal-Type Option RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
19	Should support TACACS/TACACS+		
20	High MTBF Support		
21	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
22	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
23	Rack mounting kit for securing the switch in standard rack are to be provided.		
24	**Should be a Data Center Class Switch**		
25	**All the Data Center class Switches (Switch Type 2 to Type 7) must be of the same OEM make**		
26	**The switch should support 12,000 IPv4 and IPv6 route entries in the routing table including multicast routes**		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		
2	**Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification**		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		

C	Security & QOS Features		
1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Support Configuration Change Tracking		
6	Support System Event Logging		
7	Support Syslog		
8	Support SNMP v1, v2c, v3 compatible		
D	Other Features		
1	Switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		
2	The management software should integrate with EMS **(Microfocus)** product suite.		
3	Switch should seamlessly integrate with existing network equipments		
4	Layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
5	Switch should support Link layer Discovery Protocol		
6	Switch should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Switch should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L3 features		
E	Network Management (Management Feature)		
1	Embedded support for Web based management using standard secured web browser **or management of switch should be supported using EMS (Microfocus) product suite.**		
2	**Support all features of SNMP v3.**		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer 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 session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Should support QoS and Security at Layers 1-4		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Radius or TACACS+ server Support		
13	Private and Enterprise MIB / MIB		
14	Administrative Access Right		
15	Traffic Volume/Error/Congestion Monitoring		
16	TFTP **or equivalent mode for** Download / Upload Software		
17	Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
F	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		
G	RFC (Request for Comment) Support		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

Tender No.		**BCC:IT:PROC:113:30**	
Name of Work		**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder			
Switch -Type 4 Annexure 12 H			
Make and Model : DC Mumbai : 4			
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 access switch:		
1	Minimum of 48 port 1/10/25 Gbps port and 6 nos. of 40/100 Gbps ports, with minimum 1280 Gbps switching backplane		
2	1GBE Copper Transreceiver - 10 Nos on day 1		
3	10G SFP+LC SR Transreceiver - 20 Nos on day 1		
4	40GbE QSFP+ Transreceiver - 4 Nos on day 1		
5	QSFP+ to QSFP+ 3 mts DAC cable		
6	SFP+ to SFP+ 3 mts DAC cable		
7	Full-Duplex Operation on GbE		
8	Multiple Load Sharing Trunks		
9	Minimum of **4 GB** SDRAM and **4 GB** Flash memory, packet buffer size: **24 MB**		
10	**Redundant and Hot Swappable Platinum rated Power Supplies** (Port side intake)		
11	Fan Tray - 2 Nos **(Redundant Hot swappable fan)**		
12	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
13	Minimum throughput of 250 million pps		
14	Minimum routing/switching capacity should be **2.56 Tbps**		
15	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
16	Support for minimum of 128000 MAC addresses		
17	RFC 1027 Proxy ARP RFC 1091 Telnet Terminal-Type Option RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
18	Should support TACACS/TACACS+		
19	High MTBF Support		
20	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
21	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
22	Rack mounting kit for securing the switch in standard rack are to be provided.		
23	**Should be a Data Center Class Switch**		
24	**All the Data Center class Switches (Switch Type 2 to Type 7) must be of the same OEM make**		
25	**The switch should support 12,000 IPv4 and IPv6 route entries in the routing table including multicast routes**		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		
2	**Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification**		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		
C	Security & QOS Features		

1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Support Configuration Change Tracking		
6	Support System Event Logging		
7	Support Syslog		
8	Support SNMP v1, v2c, v3 compatible		
D	Other Features		
1	Switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		
2	The management software should integrate with EMS **(Microfocus)** product suite.		
3	Switch should seamlessly integrate with existing network equipments		
4	Layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
5	Switch should support Link layer Discovery Protocol		
6	Switch should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Switch should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L3 features		
E	Network Management (Management Feature)		
1	Embedded support for Web based management using standard secured web browser **or management of switch should be supported using EMS (Microfocus) product suite.**		
2	**Support all features of SNMP v3.**		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer 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 session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Should support QoS and Security at Layers 1-4		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Radius or TACACS+ server Support		
13	Private and Enterprise MIB / MIB		
14	Administrative Access Right		
15	Traffic Volume/Error/Congestion Monitoring		
16	TFTP **or equivalent mode for** Download / Upload Software		
17	Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
F	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		
G	RFC (Request for Comment) Support		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Switch -Type 5 Annexure 12 I

Make and Model : DC Mumbai : 8; DR Hyderabad : 8

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 access switch-		
1	Minimum of 48 port 1/10/25 Gbps port and 6 nos. of 40/100 Gbps ports, with minimum 1280 Gbps switching backplane		
2	1GBE Copper Transreceiver - 4 Nos on day 1		
3	10G SFP+LC SR Transreceiver - 8 Nos on day 1		
4	40GbE QSFP+ Transreceiver - 2 Nos on day 1		
5	QSFP+ to QSFP+ 3 mts DAC cable		
6	SFP+ to SFP+ 3 mts DAC cable		
7	Full-Duplex Operation on GbE		
8	Multiple Load Sharing Trunks		
9	Minimum of **4 GB** SDRAM and **4 GB** Flash memory, packet buffer size: **24 MB**		
10	**Redundant and Hot Swappable Platinum rated Power Supplies** (Port side intake)		
11	Fan Tray - 2 Nos **(Redundant Hot swappable fan)**		
12	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
13	Minimum throughput of 250 million pps		
14	Minimum routing/switching capacity should be **2.56 Tbps**		
15	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
16	Support for minimum of 128000 MAC addresses		
17	RFC 1027 Proxy ARP RFC 1091 Telnet Terminal-Type Option RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
18	Should support TACACS/TACACS+		
19	High MTBF Support		
20	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
21	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
22	Rack mounting kit for securing the switch in standard rack are to be provided.		
23	**Should be a Data Center Class Switch**		
24	**All the Data Center class Switches (Switch Type 2 to Type 7) must be of the same OEM make**		
25	**The switch should support 12,000 IPv4 and IPv6 route entries in the routing table including multicast routes**		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		
2	**Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification**		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		
C	Security & QOS Features		

1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Support Configuration Change Tracking		
6	Support System Event Logging		
7	Support Syslog		
8	Support SNMP v1, v2c, v3 compatible		
D	Other Features		
1	Switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		
2	The management software should integrate with EMS **(Microfocus)** product suite.		
3	Switch should seamlessly integrate with existing network equipments		
4	Layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
5	Switch should support Link layer Discovery Protocol		
6	Switch should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Switch should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L3 features		
E	Network Management (Management Feature)		
1	Embedded support for Web based management using standard secured web browser **or management of switch should be supported using EMS (Microfocus) product suite.**		
2	**Support all features of SNMP v3.**		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer 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 session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Should support QoS and Security at Layers 1-4		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Radius or TACACS+ server Support		
13	Private and Enterprise MIB / MIB		
14	Administrative Access Right		
15	Traffic Volume/Error/Congestion Monitoring		
16	TFTP **or equivalent mode for** Download / Upload Software		
17	Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
F	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		
G	RFC (Request for Comment) Support		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Switch -Type 6 Annexure 12 J

Make and Model : NDR Mumbai : 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 access switch-		
1	Minimum of 48 port 1/10/25 Gbps port and 6 nos. of 40/100 Gbps ports, with minimum 1280 Gbps switching backplane		
2	1GBE Copper Transreceiver - 4 Nos on day 1		
3	10G SFP+LC SR Transreceiver - 40 Nos on day 1		
4	40GbE QSFP+ Transreceiver - 2 Nos on day 1		
5	QSFP+ to QSFP+ 3 mts DAC cable		
6	SFP+ to SFP+ 3 mts DAC cable		
7	Full-Duplex Operation on GbE		
8	Multiple Load Sharing Trunks		
9	Minimum of **4 GB** SDRAM and **4 GB** Flash memory, packet buffer size: **24 MB**		
10	**Redundant and Hot Swappable Platinum rated Power Supplies** (Port side intake)		
11	Fan Tray - 2 Nos **(Redundant Hot swappable fan)**		
12	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
13	Minimum throughput of 250 million pps		
14	Minimum routing/switching capacity should be **2.56 Tbps**		
15	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
16	Support for minimum of 128000 MAC addresses		
17	RFC 1027 Proxy ARP RFC 1091 Telnet Terminal-Type Option RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
18	Should support TACACS/TACACS+		
19	High MTBF Support		
20	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
21	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
22	Rack mounting kit for securing the switch in standard rack are to be provided.		
23	**Should be a Data Center Class Switch**		
24	**All the Data Center class Switches (Switch Type 2 to Type 7) must be of the same OEM make**		
25	**The switch should support 12,000 IPv4 and IPv6 route entries in the routing table including multicast routes**		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		
2	**Switch should support Network Timing Protocol (NTP), SNMPV1,V2,V3 and Mac address notification**		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		
C	Security & QOS Features		

1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Support Configuration Change Tracking		
6	Support System Event Logging		
7	Support Syslog		
8	Support SNMP v1, v2c, v3 compatible		
D	Other Features		
1	Switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		
2	The management software should integrate with EMS **(Microfocus)** product suite.		
3	Switch should seamlessly integrate with existing network equipments		
4	Layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.		
5	Switch should support Link layer Discovery Protocol		
6	Switch should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Switch should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L3 features		
E	Network Management (Management Feature)		
1	Embedded support for Web based management using standard secured web browser **or management of switch should be supported using EMS (Microfocus) product suite.**		
2	**Support all features of SNMP v3.**		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer 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 session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Should support QoS and Security at Layers 1-4		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Radius or TACACS+ server Support		
13	Private and Enterprise MIB / MIB		
14	Administrative Access Right		
15	Traffic Volume/Error/Congestion Monitoring		
16	TFTP **or equivalent mode for** Download / Upload Software		
17	Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
F	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		
G	RFC (Request for Comment) Support		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

Bank of Baroda

Tender No.	**BCC:IT:PROC:113:30**
Name of Work	**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**
Name of Bidder	

Switch-Type 7 Annexure 12 K

Make and Model :DC Mumbai : 2

S/N	Required Minimum Specifications (Per Device)	Bidder's compliance (Yes / No)	Bidder's remarks
	The following are the functional requirements to be met by the core switch-		
A	**Interface/Performance**		
1	Should be modular chassis.		
2	Shall support at least **30 Terabits** or higher per second fabric capacity		
3	Shall support at least 2 Terabits or more per second per line card		
4	Shall support 1G Copper, 10G Fiber, 40G Fiber and 100 G Fiber ports		
5	Shall support minimum 800 Mpps per line card		
6	Shall support less than 5 Micro second latency		
7	Shall support Non-blocking architecture		
8	Shall support up to **256 -** 40/100 Gbe ports		
9	1GBE Copper Transreceiver - 48 Nos on day 1		
10	10G SFP+LC SR Transreceiver - 24 Nos on day 1		
11	40GbE QSFP+ Transreceiver - 4 Nos on day 1		
12	100GbE QSFP+ Transreceiver - 8 Nos on day 1		
13	Should support 40G long range and short range QSFPs.		
14	Switch should have console port for local management		
15	Switch should have management interface for Out of Band Management		
16	Switch should support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc		
17	Switch should be rack mountable and support side rails, if required		
18	Switch should support VLAN tagging (IEEE 802.1q)		
19	Switch should support IEEE Link Aggregation or Ethernet Bonding		
20	The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG		
21	The switch should support 1,20,000 IPv4 and IPv6 routes entries in the routing table with multicast routes		
22	Switch should have wire rate switching capacity including the services:		
	a. Switching		
	b. IP Routing (Static/Dynamic)		
	c. IP Forwarding		
	d. Policy Based Routing		
	e. QoS		
	f. ACL and Global Control Plane Policing.		
	g. IP V.6 host and IP V.6 routing		
23	Switch should support minimum 32 VRF instances		
24	**Should have minimum 4 line card slots with a future inbuilt slot scalability of additional 50%**		
B	**Operating System**		
1	Shall support modern modular operating system designed for data center scalability and reliability		
2	Shall support auto process recovery from failures		
3	Shall support Health monitoring and self healing		
4	Shall support Single Operating System binary image for all switch models		
5	Shall support Industry standard CLI		
C	**Resilient Control Plane**		
1	Quad Core x86 CPU		
2	16GB DRAM		
3	4GB Flash		
4	24 Mb buffer per line card		
5	The switch should support dual supervisor and seamless switchover in case of failure		
D	**Layer 2 features**		
1	Shall support 120K MAC entries		
2	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)		
3	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN		
4	Switch should support basic Multicast IGMP v1, v2, v3		
5	Shall support Rapid Per VLAN Spanning Tree (RPVST+)		
6	Shall support 802.3ad Link Aggregation LACP with up to 16 ports/channel		
7	Shall support up to **32** ports per Link Aggregation Group (LAG)		
8	Shall support 256 Link Aggregation Groups (LAG)		
9	Shall support 64 ports active/active layer2/Layer3 multipathing redundancy		
10	Shall support 802.1AB Link Layer Discovery Protocol (LLDP)		
11	Shall support Port Mirroring		
12	Shall support 802.3x Flow Control		

13	Shall support Jumbo Frames 9216 Bytes		
14	Shall support IGMP v2/v3 snooping		
15	Shall support active/active layer-2 topology without STP where host are dual homed to switch		
E	**Layer 3 features**		
1	Shall support 100K IPv4 Unicast entries		
2	Shall support 8K or More IPv6 Unicast entries		
3	Shall support 10K IPv4 Multicast entries		
4	Shall support 4K ACL		
5	Shall support basic layer-3 routing – static routes, **RIP v2**		
6	Shall support VRRP or equivalent		
7	Shall support 64-way ECMP routing for load balancing and redundancy		
8	Shall support OSPF v2 with MD5 auth, BGP v4 with MD5 auth, ISIS using MD5 Authentication and MP BGP		
9	Shall support PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) multicast routing, IGMP V.1, V.2 and V.3		
10	Shall support Route Maps		
11	Shall support Anycast RP		
F	**Data center Advanced Features and Network Virtualization**		
1	Shall be VxLAN ready.		
2	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN		
3	Switch should support VXLAN and EVPN or equivalent to optimize the east - west traffic flow inside the data center		
4	Switch should support Open Flow/Open Day light/Open Stack controller		
5	Switch should support Data Center Bridging		
6	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically, may be using orchestation layer		
G	**Quality of Service (QoS) Features**		
1	Up to 8 queues per port		
2	802.1p based classification		
3	DSCP based classification		
4	DSCP based classification and remarking		
5	Rate limiting		
6	Switch should support for different type of QoS features for ream time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing		
7	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
H	**Security and Network Management features**		
1	Shall Support ACLs using Layer 2, Layer 3, Layer 4 fields		
2	Shall Support MAC Security		
3	Shall Support TACACS+ / RADIUS		
4	Shall Support SNMP v2, v3		
5	Shall have 100/1000 management port		
6	Shall Support RS-232 serial console port		
7	Shall Support USB port		
8	Shall Support Management over IPv4, IPv6		
9	Switch should support DHCP Snooping		
10	Switch should provide remote login for administration using: a. Telnet b. SSHV2		
11	Shall Support Syslog		
12	Shall Support AAA		
13	Industry Standard CLI		
14	Shall Support Port Mirroring		
15	Shall Support sFlow / netFlow		
16	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 with encryption c. Filtration of SNMP using Access list d. SNMP MIB support for QoS		
17	Switch should support for basic administrative tools like: a. Ping b. Traceroute		
18	Shall support built in TCP Dump or Wireshark trouble shooting tool or equivalent		
19	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring		
20	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
21	Switch should support central time server synchronization using Network Time Protocol NTP V.4		
22	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces		
23	Switch should provide different privilege for login in to the system for monitoring and management		
24	Protection from unnecessary or DoS traffic by control plane protection policy		

25	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes		
26	**The management software should integrate with EMS (Microfocus) product suite.**		
I	**Standards Compliance**		
1	Shall Support IEEE 802.1D Bridging and Spanning Tree		
2	Shall Support IEEE 802.1p QOS/COS		
3	Shall Support IEEE 802.1Q VLAN Tagging		
4	Shall Support IEEE 802.1w Rapid Spanning Tree		
5	Shall Support IEEE 802.1s Multiple Spanning Tree Protocol		
6	Shall Support IEEE 802.1AB Link Layer Discovery Protocol		
7	Shall Support IEEE 802.3ad Link Aggregation with LACP		
8	Shall Support IEEE 802.3x Flow Control		
9	Shall Support IEEE 802.3ba 40/100 Gigabit Ethernet		
J	**Monitoring, Provisioning**		
1	Shall support Advance Event Management for pro-active network monitoring or equivalent		
2	Shall support Restoration of Operating System & Configuration from USB		
3	Shall support CLI schedular, Shell script, for timed automation, and event managert for triggered automation		
4	Shall support sFlow or Netflow or equivalent		
5	Shall support centralized script/system to configure a switch without user intervention		
K	**Virtualization and Next Gen DC features**		
1	Virtualization switch should communicate with vSphere 4.0 and above, and vCenter **or with any other market standard virtualization environment** to support adaptive network virtualization		
2	VLAN auto provision - Auto create/configure VM VLAN when new VM is created in vCenter **or equivalent virtualized environment**		
3	VM Auto Discovery – Find exactly which ESX Hosts **or equivalent virtualized environment** and VMs are on a given port in the network. Displays the full Physical Port to Virtual Switch to VM Binding.		
4	Should Dynamically create VLAN policy based on VM movement.		
5	Should be able to extract vNIC information from the VM Host.		
6	VmWare Multi-Tenancy – Connecting up to 4 separate vCenter administrative domain **or equivalent feature in other virtualized environment**		
7	**The hardware should have inbuilt capability or through an additional hardware / solution to support the above features**		
L	**Hardware High Availability**		
1	Switch should have redundant **Platinum rated** power supply and fans		
2	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 non disrupt the functionality of the system		
3	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP		
4	Switch should support for BFD For Fast Failure Detection as per RFC (5880)		
5	Switch should support Graceful Restart for OSPF, BGP etc.		
M	**Data Center Class Design**		
1	Shall provide front to back air flow with **port side intake.**		
2	**Should be a Data Center Class Switch**		
3	**All the Data Center class Switches (Switch Type 2 to Type 7) must be of the same OEM make**		
N	**Misc**		
1	Switch should support the complete STACK of IP V4 and IP V6 services		
2	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied		
3	Switch should support Configuration roll-back and check point		
4	Switch should support for BFD For Fast Failure Detection as per RFC (5880)		
5	The transcievers should be from same OEM of the proposed switch		

Bank of Baroda			
Tender No.		**BCC:IT:PROC:113:30**	
Name of Work		**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder			
Firewall -Type 1 Annexure 12 L			
Make and Model : DC Mumbai : 2; DR Hyderabad : 2			
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		

Bank of Baroda			
Tender No.		**BCC:IT:PROC:113:30**	
Name of Work		**Request for Proposal for Selection of Vendor for Supply, Installation & Maintenance of Network Hardware at Data Centre**	
Name of Bidder			
Firewall -Type 2 Annexure 12 M			
Make and Model : NDR Mumbai : 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		