S/N	24 Ports L2 Switch Technical Specifications	Compliance (Yes/ No)
	Specification	
	General Features	
1	The switch should have minimum 24 x 10/100/1000 Base-T Ports & 4 x 1000 Base-X SFP slots populated with 1 x 1000 Base-LX/LH (SM) Modules	
2	Future support for Redundant Power supply	
3	Should have fan for proper cooling.	
	Performance	
4	At least 100 Gbps switching bandwidth	
5	Forwarding rate – At least 70 Mpps.	
6	Configurable at least 16000 MAC addresses	
7	The switch should support stacking with 80 Gbps Stacking bandwidth to stack upto 8 switches into a single virtual switch. Stacking is not required from day 1, but stacking should be supported on the proposed switch model.	
8	DRAM 512 MB and 128 MB Flash	
	Layer-2 Features	
9	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.	
10	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.	
11	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.	
12	Spanning-tree Enhancements for fast convergence	
13	IEEE 802.1d, 802.1s, 802.1w, 802.3ad,	
14	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.	
15	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.	
16	Link Aggregation Protocol (LACP)	
17	Support for UDLD (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.	
18	The 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.	
19	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.	

21	Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.	
	Network Security Features	
22	Support for mechanisms to improve the network's ability to automatically identify, prevent, and respond to security threats and also to enable the switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. Thus preventing the spread of Viruses & worms.	
23	IEEE 802.1x to allow dynamic, port-based security, providing user authentication.	
24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.	
25	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
26	Bidirectional data support on the Mirrored port to allow the intrusion detection system (IDS) to take action when an intruder is detected.	
27	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
28	MAC address notification to allow administrators to be notified of users added to or removed from the network.	
29	DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.	
30	Port security to secure the access to an access or trunk port based on MAC address.	
31	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.	
32	BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.	
33	Should support 500 ACL entries	
	Quality of Service (QoS) & Multicast	
34	Standard 802.1p CoS and DSCP	
35	Control- and Data-plane QoS ACLs, Cross-stack QoS	
36	Up to eight egress queues per port	
37	Strict priority queuing mechanisms	
38	There should not be any performance penalty for highly granular QoS functions.	
39	Committed information rate (CIR) function to provide bandwidth in increments of 8 Kbps	

40	Rate limiting should be provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
41	Flow-based rate limiting and up to 256 aggregate or individual policers per port	
42	Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance.	
43	2000 IPv4 & IPv6 Unicast Direct Routes	
44	1000 Multicast Groups	
	Management	
45	Superior manageability Features	
46	Command Line Interface (CLI) support for configuration & troubleshooting purposes.	
47	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.	
48	Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.	
49	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.	
50	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.	
51	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.	
52	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.	
53	RMON I and II standards	
	Certification:	
54	The switch should be Common Criteria EAL4 or NDPP certified and IPv6 Ready Logo certified (The supporting URL and certification link need to be attached with the Bid)	
55	Switch OEM should be in the Gartner's Leaders or Challengers quadrant for Wired and Wireless LAN Access Infrastructure	