RFP for Network as a Service for LIC of India			
Name of bidder :			
CAMPUS SWITCH SPECIFICATIONS (8 Port)			
Sr.No	**Description**	**Compliance (Y/N)**	**Remarks**
	Publically available documents, as on the date of RFP, required for each point		
1	**Architecture**		
1.1	Shall be mounted on space provided by LIC	Select	
1.2	The switch should have dedicated Console Port	Select	
1.3	2GB memory and 2GB flash	Select	
1.4	The Switch should support 8000 MAC address	Select	
1.5	The switch should have minimum 512 Unicast Routes 512 Igmp Groups 1024 IPv4 host table (ARP)	Select	
1.6	The switch should have 8x ports 10/100/1000 BASE-T ports and 2x 1Gig SFP ports. The SFP ports should support both Copper and Fiber transceivers . The switch should have the capacity to terminate WAN link as well as LAN link. All downlink ports should be populated from Day1 and for uplink ports, kindly refer the SFP counts in the revised commercial Format.	Select	
1.7	The switch should have 20 Gbps of Switching Capacity and 14 Mpps throughput Capacity	Select	
1.8	Clause Deleted	Select	
1.9	Clause Deleted	Select	
2	**IPv6 feature**	Select	
2.1	IPv6 host enables switches to be managed in an IPv6 network	Select	
2.2	Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	Select	
2.3	MLD snooping forwards IPv6 multicast traffic to the appropriate interface	Select	
2.4	IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	Select	
2.5	IPv6 Static routing	Select	
2.6	Dynamic IPv6 lockdown or equivalent and ND snooping	Select	
3	**High Availability And Resiliency and Qos**	Select	
3.1	The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	Select	
3.2	The Switch should support IEEE 802.1s Multiple Spanning Tree, IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence.	Select	
3.3	The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), TCP/UDP port number, source port, and DiffServ,Rate limiting and graceful congestion management	Select	
4	**Management**	Select	
4.1	The Switch should support Built-in programability and support REST API or RESTCONF interface. The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB)	Select	
4.2	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	Select	
4.3	The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access. Switch should support TACACS+ and RADIUS	Select	
4.4	The Switch should support SNMP v3 with Min SHA2 Authentication and AES256 encryption alinged to RBI Guidelines	Select	
4.5	Switch should support monitoring and flow export protocols like RMON or sFlow (RFC 3176) or Netflow	Select	
4.6	The Switch should support TFTP and SFTP/SCP and support Debug and sampler utility support ping and traceroute for IPv4 and IPv6.	Select	
4.7	The Switch should support Network Time Protocol (NTPv3) and IEEE 802.1AB Link Layer Discovery Protocol (LLDP).	Select	

4.8	The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading and support Multiple configuration files which can be stored to a flash image.	Select	
4.9	The Switch should support Ingress and egress port monitoring and support Unidirectional link detection (UDLD) or equivalent protocol	Select	
4.1	OEM to further provide on-prem management solution to centrally manage and monitor the switches to provide Inventory, topology, Device health and centralised software upgrade	Select	
4.11	Management solution can be appliance or VM based; in case of VM , LIC will provide the VM resources like compute and Hypervisor licenses and any other license needed to ensure solution to run will be Bidders responsibility.	Select	
5	**Multicast**	Select	
5.1	The Switch should support IGMP Snooping and support Multicast Listener Discovery (MLD) MLD v1 and v2 and support and Any-Source Multicast (ASM) to manage IPv4 multicast networks	Select	
6	**Layer 2 Switching**	Select	
6.1	The switch must support 4,094 VLAN IDs (per IEEE 802.1Q) and be capable of configuring/operating at least 500 active VLANs.	Select	
6.2	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of up to 9198 bytes	Select	
6.3	The Switch should support Multiple Spanning Tree Protocol (MSTP) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	Select	
6.4	The Switch should support MVRP or equivalent VLAN registration protocol to allow automatic learning and dynamic assignment of VLANs	Select	
6.5	The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	Select	
6.6	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	Select	
7	**Security**	Select	
7.1	The Switch should support integrated hardware based trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Select	
7.2	The Switch should supportAccess control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	Select	
7.3	The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	Select	
7.4	The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks	Select	
7.5	The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch	Select	
7.6	The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	Select	
7.7	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	Select	
7.8	The Switch should support Dynamic IP lockdown or equivalent with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	Select	
7.9	The Switch should support Dynamic ARP protection or similar to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data.	Select	
7.10	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	Select	
7.11	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	Select	
7.12	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network	Select	
7.13	The Switch should support Source-port filtering to allow only specified ports to communicate with each other	Select	

7.14	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	Select	
7.15	The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	Select	
7.16	The Switch should support Security banner displays a customized security policy when users log in to the switch	Select	
7.17	Clause Deleted	Select	
8	**NAC functionality**	Select	
8.1	The switch should support Remote Authentication Dial-In User Service (RADIUS)	Select	
8.2	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	Select	
8.3	The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X	Select	
8.4	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	Select	
8.5	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user	Select	
8.6	The Switch should support Critical Authentication Role or equivalent to ensure that important infrastructure devices are allowed to access the network even in the absence of a RADIUS server.	Select	
8.7	The Switch should support RADIUS Change of Authorization (CoA) feature.	Select	
8.8	The switch should support 45 dACL (Access control entry/rules) per port and total 1000 rules per switch.	Select	
8.9	The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	Select	
9	**Certification**	Select	
9.1	Switch should support the below certifications (a) MTCTE/TCE or equivalent mandatory by DOT, Govt Of India (b) IPv6 logo certification/MTCTE certification to be provided . However ,feature alignment between IPv4 and IPv6 has to in place. (c) NDPP/NIAP/VAPT/Common Criteria certification or MTCTE certification to be provided confirming the security features and assurance of the software	Select	
10	**Product support**	Select	
10.1	The Warranty & AMC period should include technical support from the Bidder and back to back OEM support.	Select	
10.2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Select	
10.3	OEM should provide Case management tool, inventory management tool, field notice vulnerability updates and all relevant updates for all the modules procured as part of this RFP to ensure that the most updated details is available to the (customer) at any given point in time.	Select	
10.4	The Warranty & AMC period should include an OEM point of contact (POC) as a Trusted Advisor to LIC who would coordinate efforts across OEM/Partner teams to drive the adoption of the deployed products.	Select	
10.5	OEMs Trusted advisor would ensure that products procured as part of this RFP are delivering value to LIC and would create, own, and proactively communicate critical customer issues related to business or technical barriers and critical milestones.	Select	
11	**General Points**	Select	
11.1	The switch OEM must have been listed as a Leader or Challenger in the Gartner Magic Quadrant for Enterprise Network Switches in each of the last three years from the RFP date. This will not be applicable to OEMs falling under Make In India clause.	Select	
11.2	None of the switches or any of their components, including hardware and software, shall be announced as End-of-Sale as of the RFP submission date		

11.3	All switch hardware, software, and transceivers supplied under this RFP must be from the same OEM.	Select	

Name :

Date : **Designation :**

RFP for Network as a Service for LIC of India
Ref: CO/IT-BPR/NW/RFP/2025-26/02 Dated: 10.10.2025

Name of bidder :

CAMPUS SWITCH SPECIFICATIONS (24 Port)

Sr.No	Description	Compliance (Y/N)	Remarks
	Publically available documents, as on the date of RFP, required for each point		
1	**Architecture**	Select	
1.1	Shall be mounted on space provided by LIC	Select	
1.2	The switch should have dedicated Console Port	Select	
1.3	2GB memory and 2GB flash	Select	
1.4	The Switch should support 8000 MAC address	Select	
1.5	The switch should have minimum 512 Unicast Routes 512 Igmp Groups 1024 IPv4 host table (ARP)	Select	
1.6	The switch should have 24x ports 10/100/1000 BASE-T ports and 4x 1/10 Gig SFP ports. The SFP ports should support both Copper and Fiber transceivers . The switch should have the capacity to terminate WAN link as well as LAN link. All downlink ports should be populated from Day1 and for uplink ports, kindly refer the SFP counts in the revised commercial Format.	Select	
1.7	All downlink ports should be populated from Day1 and for uplinks , pls be guided by the SFP counts in the revised commercial Format.	Select	
1.8	It should be possible to stack switches with minimum 40 Gbps stack bandwidth and It should be possible to stack switches either using Front-plane port for stacking or dedicated stacking port. However no ports out of the 24 downlink ports should be used. Bidders have to factor additional SFPs / Stack Cables to implement stacking between switches	Select	
1.9	Clause Deleted	Select	
2	**IPv6 feature**	Select	
2.1	IPv6 host enables switches to be managed in an IPv6 network	Select	
2.2	Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	Select	
2.3	MLD snooping forwards IPv6 multicast traffic to the appropriate interface	Select	
2.4	IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	Select	
2.5	IPv6 Static routing	Select	
2.6	Dynamic IPv6 lockdown or equivalent and ND snooping	Select	
3	**High Availability And Resiliency and Qos**	Select	
3.1	The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	Select	
3.2	The Switch should support IEEE 802.1s Multiple Spanning Tree, IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence.	Select	
3.3	The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), TCP/UDP port number, source port, and DiffServ,Rate limiting and graceful congestion management	Select	
4	**Management**	Select	
4.1	The Switch should support Built-in programability and support REST API or RESTCONF interface. The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB)	Select	
4.2	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	Select	
4.3	The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access. Switch should support TACACS+ and RADIUS	Select	
4.4	The Switch should support SNMP v3 with Min SHA2 Authentication and AES256 encryption alinged to RBI Guidelines	Select	
4.5	Switch should support monitoring and flow export protocols like RMON or sFlow (RFC 3176) or Netflow	Select	
4.6	The Switch should support TFTP and SFTP/SCP and support Debug and sampler utility support ping and traceroute for IPv4 and IPv6.	Select	
4.7	The Switch should support Network Time Protocol (NTPv3) and IEEE 802.1AB Link Layer Discovery Protocol (LLDP).	Select	

4.8	The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading and support Multiple configuration files which can be stored to a flash image.	Select	
4.9	The Switch should support Ingress and egress port monitoring and support Unidirectional link detection (UDLD) or equivalent protocol	Select	
4.10	OEM to further provide on-prem management solution to centrally manage and monitor the switches to provide Inventory, topology, Device health and centralised software upgrade	Select	
4.11	Management solution can be appliance or VM based; in case of VM , LIC will provide the VM resources like compute and Hypervisor licenses and any other license needed to ensure solution to run will be Bidders responsibility.	Select	
5	**Multicast**	Select	
5.1	The Switch should support IGMP Snooping and support Multicast Listener Discovery (MLD) MLD v1 and v2 and support and Any-Source Multicast (ASM) to manage IPv4 multicast networks	Select	
6	**Layer 2 Switching**	Select	
6.1	The switch must support 4,094 VLAN IDs (per IEEE 802.1Q) and be capable of configuring/operating at least 500 active VLANs.	Select	
6.2	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of up to 9198 bytes	Select	
6.3	The Switch should support Multiple Spanning Tree Protocol (MSTP) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	Select	
6.4	The Switch should support MVRP or equivalent VLAN registration protocol to allow automatic learning and dynamic assignment of VLANs.	Select	
6.5	The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	Select	
6.6	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	Select	
7	**Security**	Select	
7.1	The Switch should support integrated hardware based trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Select	
7.2	The Switch should supportAccess control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	Select	
7.3	The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	Select	
7.4	The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks	Select	
7.5	The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch	Select	
7.6	The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	Select	
7.7	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	Select	
7.8	The Switch should support Dynamic IP lockdown or equivalent with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	Select	
7.9	The Switch should support Dynamic ARP protection or similar to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data.	Select	
7.10	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	Select	
7.11	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	Select	
7.12	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network	Select	
7.13	The Switch should support Source-port filtering to allow only specified ports to communicate with each other	Select	
7.14	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	Select	
7.15	The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	Select	

7.16	The Switch should support Security banner displays a customized security policy when users log in to the switch	Select	
7.17	Clause deleted	Select	
8	**NAC functionality**	Select	
8.1	The switch should support Remote Authentication Dial-In User Service (RADIUS)	Select	
8.2	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	Select	
8.3	The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X	Select	
8.4	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	Select	
8.5	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user	Select	
8.6	The Switch should support Critical Authentication Role or equivalent to ensure that important infrastructure devices are allowed to access the network even in the absence of a RADIUS server.	Select	
8.7	The Switch should support RADIUS Change of Authorization (CoA) feature.	Select	
8.8	The switch should support 45 dACL (Access control entry/rules) per port and total 1080 rules per switch.	Select	
8.9	The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	Select	
9	**Certification**	Select	
9.1	Switch should support the below certifications (a) MTCTE/TCE or equivalent mandatory by DOT, Govt Of India (b) IPv6 logo certification/MTCTE certification to be provided . However ,feature alignment between IPv4 and IPv6 has to in place. (c) NDPP/NIAP/VAPT/Common Criteria certification or MTCTE certification to be provided confirming the security features and assurance of the software	Select	
10	**Product support**	Select	
10.1	The Warranty & AMC period should include technical support from the Bidder and back to back OEM support.	Select	
10.2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Select	
10.3	OEM should provide Case management tool, inventory management tool, field notice vulnerability updates and all relevant updates for all the modules procured as part of this RFP to ensure that the most updated details is available to the (customer) at any given point in time.	Select	
10.4	The Warranty & AMC period should include an OEM point of contact (POC) as a Trusted Advisor to LIC who would coordinate efforts across OEM/Partner teams to drive the adoption of the deployed products.	Select	
10.5	OEMs Trusted advisor would ensure that products procured as part of this RFP are delivering value to LIC and would create, own, and proactively communicate critical customer issues related to business or technical barriers and critical milestones.	Select	
11	**General Points**	Select	
11.1	The switch OEM must have been listed as a Leader or Challenger in the Gartner Magic Quadrant for Enterprise Network Switches in each of the last three years from the RFP date. This will not be applicable to OEMs falling under Make In India clause.		
11.2	None of the switches or any of their components, including hardware and software, shall be announced as End-of-Sale as of the RFP submission date	Select	
11.3	All switch hardware, software, and transceivers supplied under this RFP must be from the same OEM.	Select	

Name :

Date : **Designation :**

RFP for Network as a Service for LIC of India
Ref: CO/IT-BPR/NW/RFP/2025-26/02 Dated: 10.10.2025

Name of bidder :

CAMPUS SWITCH SPECIFICATIONS (48 Port)

Sr.No	Description	Compliance (Y/N)	Remarks
	Publically available documents, as on the date of RFP, required for each point		
1	**Architecture**	Select	
1.1	Shall be mounted on space provided by LIC	Select	
1.2	The switch should have dedicated Console Port	Select	
1.3	2GB memory and 2GB flash	Select	
1.4	The Switch should support 8000 MAC address	No	
1.5	The switch should have minimum 512 Unicast Routes 512 Igmp Groups 1024 IPv4 host table (ARP)	Select	
1.6	The switch should have 48x ports 10/100/1000 BASE-T ports and 4x 1/10 Gig SFP ports. The SFP ports should support both Copper and Fiber transceivers . The switch should have the capacity to terminate WAN link as well as LAN link. All downlink ports should be populated from Day1 and for uplink ports, kindly refer the SFP counts in the revised commercial Format.	Select	
1.7	The switch should have 104 Gbps of Switching Capacity and 77 Mpps throughput Capacity	Select	
1.8	It should be possible to stack switches with minimum 40 Gbps stack bandwidth and It should be possible to stack switches either using Front-plane port for stacking or dedicated stacking port. However no ports out of the 48 downlink ports should be used. Bidders have to factor additional SFPs / Stack Cables to implement stacking between switches	Select	
1.9	Proposed switch should be provided with an internal redundant power supply from Day 1.	Select	
2	**IPv6 feature**	Select	
2.1	IPv6 host enables switches to be managed in an IPv6 network	Select	
2.2	Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	Select	
2.3	MLD snooping forwards IPv6 multicast traffic to the appropriate interface	Select	
2.4	IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	Select	
2.5	IPv6 Static routing	Select	
2.6	Dynamic IPv6 lockdown or equivalent and ND snooping	Select	
3	**High Availability And Resiliency and Qos**	Select	
3.1	The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	Select	
3.2	The Switch should support IEEE 802.1s Multiple Spanning Tree, IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence.	Select	
3.3	The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), TCP/UDP port number, source port, and DiffServ,Rate limiting and graceful congestion management	Select	
4	**Management**	Select	
4.1	The Switch should support Built-in programability and support REST API or RESTCONF interface. The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB)	Select	
4.2	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	Select	
4.3	The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access. Switch should support TACACS+ and RADIUS	Select	
4.4	The Switch should support SNMP v3 with Min SHA2 Authentication and AES256 encryption alinged to RBI Guidelines	Select	
4.5	Switch should support monitoring and flow export protocols like RMON or sFlow (RFC 3176) or Netflow	Select	
4.6	The Switch should support TFTP and SFTP/SCP and support Debug and sampler utility support ping and traceroute for IPv4 and IPv6.	Select	

4.7	The Switch should support Network Time Protocol (NTPv3) and IEEE 802.1AB Link Layer Discovery Protocol (LLDP).	Select	
4.8	The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading and support Multiple configuration files which can be stored to a flash image.	Select	
4.9	The Switch should support Ingress and egress port monitoring and support Unidirectional link detection (UDLD) or equivalent protocol	Select	
5	**Multicast**	Select	
5.1	The Switch should support IGMP Snooping and support Multicast Listener Discovery (MLD) MLD v1 and v2 and support and Any-Source Multicast (ASM) to manage IPv4 multicast networks	Select	
6	**Layer 2 Switching**	Select	
6.1	The switch must support 4,094 VLAN IDs (per IEEE 802.1Q) and be capable of configuring/operating at least 500 active VLANs.	Select	
6.2	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of up to 9198 bytes	Select	
6.3	The Switch should support Multiple Spanning Tree Protocol (MSTP) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	Select	
6.4	The Switch should support MVRP or equivalent VLAN registration protocol to allow automatic learning and dynamic assignment of VLANs	Select	
6.5	The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	Select	
6.6	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	Select	
7	**Security**	Select	
7.1	The Switch should support integrated hardware based trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	Select	
7.2	The Switch should supportAccess control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	Select	
7.3	The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	Select	
7.4	The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks	Select	
7.5	The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch	Select	
7.6	The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	Select	
7.7	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	Select	
7.8	The Switch should support Dynamic IP lockdown or equivalent with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	Select	
7.9	The Switch should support Dynamic ARP protection or similar to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data.	Select	
7.10	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	Select	
7.11	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	Select	
7.12	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network	Select	
7.13	The Switch should support Source-port filtering to allow only specified ports to communicate with each other	Select	
7.14	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	Select	
7.15	The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	Select	
7.16	The Switch should support Security banner displays a customized security policy when users log in to the switch	Select	
7.17	Clause deleted	Select	

8	**NAC functionality**	Select	
8.1	The switch should support Remote Authentication Dial-In User Service (RADIUS)	Select	
8.2	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	Select	
8.3	The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X	Select	
8.4	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	Select	
8.5	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user	Select	
8.6	The Switch should support Critical Authentication Role or equivalent to ensure that important infrastructure devices are allowed to access the network even in the absence of a RADIUS server.	Select	
8.7	The Switch should support RADIUS Change of Authorization (CoA) feature.	Select	
8.8	The switch should support 45 dACL (Access control entry/rules) per port and total 1080 rules per switch.	Select	
8.9	The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	Select	
9	**Certification**	Select	
9.1	Switch should support the below certifications (a) MTCTE/TCE or equivalent mandatory by DOT, Govt Of India (b) IPv6 logo certification/MTCTE certification to be provided . However ,feature alignment between IPv4 and IPv6 has to in place. (c) NDPP/NIAP/VAPT/Common Criteria certification or MTCTE certification to be provided confirming the security features and assurance of the software	Select	
10	**Product support**	Select	
10.1	The Warranty & AMC period should include technical support from the Bidder and back to back OEM support.	Select	
10.2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Select	
10.3	OEM should provide Case management tool, inventory management tool, field notice vulnerability updates and all relevant updates for all the modules procured as part of this RFP to ensure that the most updated details is available to the (customer) at any given point in time.	Select	
10.4	The Warranty & AMC period should include an OEM point of contact (POC) as a Trusted Advisor to LIC who would coordinate efforts across OEM/Partner teams to drive the adoption of the deployed products.	Select	
10.5	OEMs Trusted advisor would ensure that products procured as part of this RFP are delivering value to LIC and would create, own, and proactively communicate critical customer issues related to business or technical barriers and critical milestones.	Select	
11	**General Points**	Select	
11.1	None of the switches or any of their components, including hardware and software, shall be announced as End-of-Sale as of the RFP submission date	Select	
11.2	All switch hardware, software, and transceivers supplied under this RFP must be from the same OEM.	Select	
11.3	Clause Deleted	Select	
11.4	OEM to further provide on-prem management solution to centrally manage and monitor the switches to provide Inventory, topology, Device health and centralised software upgrade	Select	
11.5	Management solution can be appliance or VM based; in case of VM , LIC will provide the VM resources like compute and Hypervisor licenses and any other license needed to ensure solution to run will be Bidders responsibility.	Select	
11.6	The switch OEM must have been listed as a Leader or Challenger in the Gartner Magic Quadrant for Enterprise Network Switches in each of the last three years from the RFP date. This will not be applicable to OEMs falling under Make In India clause.	Select	

Place :

Authorized Signatory Name

Date : **Designation :**