<u>CORRIGENDUM-2</u>

Sl No.	Item Details for reference in hosted Tender Document	Item Description in Hosted Tender Document	Corresponding amendment
01	Section – I, Clause – 1, Sl No 2 Pg No - 4 & Section -4, Sl no 2, page no-28 & Schedule – 3, Price Bid Form, Pg no-47 Sl No - 2 of Network Component Tables	Layer-3 24 Port Switch 10/100/1000 Mbps Network Managed Switch with 1 FX SFP Slots.	**Layer-2 24 Port Switch 10/100/1000 Mbps Network Managed Switch with 2 SX SFP Slots.**
02	Section – I, Clause – 1, Sl No 3 Pg No - 4 & Section -4, Sl no 3, page no-28 & Schedule – 3, Price Bid Form, Pg no-47 Sl No - 3 of Network Component Tables	Layer-2 48 Port 10/100/1000 Mbps Network Managed Switch with 1 FX SFP Slots.	**Layer-2 48 Port 10/100/1000 Mbps Network Managed Switch with 4 SX SFP Slots.**
03	Section – I, Clause – 1, Sl No 4 Pg No - 4 & Section -4, Sl no 4, page no-28 & Schedule – 3, Price Bid Form, Pg no-47 Sl No - 4 of Network Component Tables	Layer-2 8 Port 10/100/1000 Mbps Network Managed Switch with 1 FX SFP Slots.	**Layer-2 8 Port 10/100/1000 Mbps Network Managed Switch with 1 SX SFP Slot.**
04	Section – I, Clause – 1, Sl No 8 Pg No - 4 & Section -4, Sl no 8, page no-28 & Schedule – 3, Price Bid Form, Pg no-47 Sl No - 8 of Network Component Tables	I/O for work area side	**I/O for work area side(CAT6)**
05	Section – I, Clause – 1, Sl No 9 Pg No - 4 & Section -4, Sl no 9, page no-28 & Schedule – 3, Price Bid Form, Pg no-47 Sl No - 9 of Network Component Tables	I/O for patch panel	**I/O for patch panel side (CAT6)**
06	Section – I, Clause – 1, Sl No 7 Pg No - 4 & Section -4, Sl no 7, page no-28 & Schedule – 3, Price Bid Form, Pg no-48 Sl No - 21 of Fibre Component Tables	GLC Fibre Module	**1G SX SFP Trans receiver Module**
07	Section –I, Pg No 09, Note (Third Bullet Point)	"Extension of OGS-WAN – Technocommercial Bid due on xxxxxxxx" and "Extension of OGS-WAN – Price Bid due on xxxxxxxx"	**"Extension of OGS-WAN – Technocommercial Bid due on 07.06.2013" and "Extension of OGS-WAN – Price Bid due on 21.06.2013"**
08	Section – 2, Clause no-6, Pg No 10	Only those who have purchased the Specification can submit their tender. Tenders submitted by others will be rejected.	**Only those who have purchased the Tender Document can submit their tender. Tenders submitted by others will be rejected.**

Technical Specifications:

EDGE SWITCH (24 PORT)

The switches shall have following specifications / features:

Sl. No.	Description
1.1	The switch should have minimum 24 x 10/100/1000 Gigabit Ethernet and 4 Fiber uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.
1.2	Future support for Redundant Power supply
1.3	Should have fan for proper cooling
1.5	At least 56 Gbps switching fabric
1.6	Forwarding rate at least 41 Mpps
1.7	Configurable at least 8000 MAC addresses
1.8	Should support stacking (At least 20 Gbps bandwidth)
1.9	The device should be IPv6 ready from day one
1.10	Support for IEEE 802.1Q VLAN encapsulation. At least 250 VLANs should be supported & support for 4000 VLAN IDs.
1.11	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
1.12	Support for Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.
1.13	Spanning-tree Enhancements for fast convergence
1.14	Support for IEEE 802.1d, 802.1s, 802.1w, 802.3ad
1.15	Support for Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.
1.16	Support for IGMP snooping v3, Support for at least 250 IGMP Groups. IGMP filtering.
1.17	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.
1.18	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.
1.19	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.
1.20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.
1.21	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.
1.22	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.
1.23	Support for IEEE 802.1x to allow dynamic, port-based security, providing user authentication.
1.24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.
1.25	Support for SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
1.26	Support for 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.
1.27	Support for Port security to secure the access to an access or trunk port based on MAC address.
1.28	Support for Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.
1.29	Support for BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.
1.30	At least 500 ACL entries should be supported.
1.31	Support for Standard 802.1p CoS and DSCP
1.32	Support for Control- and Data-plane QoS ACLs
1.33	Four egress queues per port to enable differentiated management of up to four traffic types across the stack.
1.34	Support for Weighted tail drop (WTD) to provide congestion avoidance & Strict priority queuing mechanisms
1.35	There should not be any performance penalty for highly granular QoS functions.
1.36	Rate Limiting function should guarantee bandwidth in increments as small as 1 Mbps.

1.37	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.
1.38	At least 64 aggregate or individual polices should be available per Fast Ethernet or Gigabit Ethernet port.
1.39	Support for IPv6 Host which can provide basic IPv6 management such as IPv4/IPv6 dual stack, unicast address types, ICMPv6, IPv6 Aggregatable Address, Secure Shell (SSH) for v6, IPv6 Autoconfiguration, IPv6 neighbor discovery, Telnet, TFTP, SNMP, HTTP, HTTPS, Trace route, Syslog for v6.
1.40	Command Line Interface (CLI) support for configuration & troubleshooting purposes.
1.41	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.
1.42	Support for Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.
1.43	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.
1.44	Support for Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.
1.45	Support for Network Timing Protocol (NTP) to provide an accurate and consistent timestamp to all intranet switches.
1.46	Support for SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive inband management, and a CLI-based management console provides detailed out-of-band management.
1.47	Support for RMON I and II standards
1.48	Support for SNMPv1, SNMPv2c, and SNMPv3

EDGE SWITCH (48 PORT)

The switches shall have following specifications / features:

S/N	Description
1.1	The switch should have minimum 48 x 10/100/1000 Gigabit Ethernet and 4 Fiber uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.
1.2	Future support for Redundant Power supply
1.3	Should have fan for proper cooling
1.5	At least 104 Gbps switching fabric
1.6	Forwarding rate at least 77 Mpps
1.7	Configurable at least 8000 MAC addresses

1.8	Should support stacking (At least 20 Gbps bandwidth)
1.9	The device should be IPv6 ready from day one
1.10	Support for IEEE 802.1Q VLAN encapsulation. At least 250 VLANs should be supported. Support for 4000 VLAN IDs.
1.11	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
1.12	Support for Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.
1.13	Spanning-tree Enhancements for fast convergence
1.14	Support for IEEE 802.1d, 802.1s, 802.1w, 802.3ad
1.15	Support for Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.
1.16	Support for IGMP snooping v3, Support for at least 250 IGMP Groups. IGMP filtering.
1.17	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.
1.18	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.
1.19	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.
1.20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.
1.21	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.
1.22	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.
1.23	Support for IEEE 802.1x to allow dynamic, port-based security, providing user authentication.
1.24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.
1.25	Support for SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
1.26	Support for 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.
1.27	Support for Port security to secure the access to an access or trunk port based on MAC address.
1.28	Support for Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.
1.29	Support for BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU's are received to avoid accidental topology loops.
1.30	At least 500 ACL entries should be supported.
1.31	Support for Standard 802.1p CoS and DSCP
1.32	Support for Control- and Data-plane QoS ACLs
1.33	Four egress queues per port to enable differentiated management of up to four traffic types across the stack.
1.34	Support for Weighted tail drop (WTD) to provide congestion avoidance

1.35	Strict priority queuing mechanisms
1.36	There should not be any performance penalty for highly granular QoS functions.
1.37	Rate Limiting function should guarantee bandwidth in increments as small as 1 Mbps.
1.38	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.
1.39	At least 64 aggregate or individual polices should be available per Fast Ethernet or Gigabit Ethernet port.
1.40	Support for IPv6 Host which can provide basic IPv6 management such as IPv4/IPv6 dual stack, unicast address types, ICMPv6, IPv6 Aggregatable Address, Secure Shell (SSH) for v6, IPv6 Autoconfiguration, IPv6 neighbor discovery, Telnet, TFTP, SNMP, HTTP, HTTPS, Trace route, Syslog for v6.
1.41	Command Line Interface (CLI) support for configuration & troubleshooting purposes.
1.42	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.
1.43	Support for Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.
1.44	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.
1.45	Support for Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.
1.46	Support for Network Timing Protocol (NTP) to provide an accurate and consistent timestamp to all intranet switches.
1.47	Support for SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive inband management, and a CLI-based management console provides detailed out-of-band management.
1.48	Support for RMON I and II standards
1.49	Support for SNMPv1, SNMPv2c, and SNMPv3

EDGE SWITCH (8 PORT)

The switches shall have following specifications / features:

Sl. No.	Description
1.1	The switch should have minimum 8 x 10/100/1000 Gigabit Ethernet and 2 x Dual purpose (Copper or Fiber) uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.
1.2	Switch should be 1 RU rack/wall mountable
1.3	Should have minimum 10 Gbps forwarding bandwidth
1.5	Should have minimum 13.2 Mpps forwarding rate
1.7	The device should be IPv6 ready from day one
1.8	Switch should support IEEE Standards of Ethernet: IEEE 802.1d, 802.1s, 802.1w etc.
1.9	Should have IEEE 802.1Q VLAN encapsulation and up to 250 active VLANs per switch

1.10	Should support IPv4 and IPv6 MLD v1 and v2 Snooping
1.11	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
1.12	Should have a mechanism to detect connectivity issues with both fiber and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues
1.13	Should have extensive debugging including layer 2 debugging and layer 2 trace route for troubleshooting
1.14	Should support for QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and help enable egress queue configuration.
1.15	Should support for autoconfiguration of multiple switches through a boot server eases switch deployment.
1.16	Should support for auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
1.17	Should support for dynamic trunk configuration across all switch ports
1.18	Should support for creation of Ethernet channeling with devices that conform to IEEE 802.3ad
1.19	Should support for automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
1.20	Should support for superior CLI for detailed configuration and administration.
1.21	switches should provide superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and ARP spoofing).
1.22	Support for multiple authentication mechanisms including 802.1X, MAC Authentication Bypass, and web authentication using a single, consistent configuration.
1.23	Suppoirt for RADIUS / TACACS+ Change of Authorization and Downloadable ACLs for comprehensive policy management capabilities.
1.24	Support for Port-Based ACLs for Layer 2 interfaces
1.25	Support for network security by encrypting administrator traffic during Telnet and SNMP sessions.
1.26	Support for multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
1.27	Support to prevent edge devices not in the network administrator's control from

	becoming Spanning Tree Protocol root nodes.
1.28	Support for implementation of VLAN Membership Policy Server client capability to provide flexibility in assigning ports to VLANs.
1.29	Support for atleast 64 Mb Flash memory & 128 Mb DRAM
1.30	Support for jumbo frames (9018 bytes)
1.31	Switch should support Reduction of Hazardous Substances (ROHS) 6

Technical Compliance:

EDGE SWITCH (48 PORT)

Sl. No	**Description**	**Bidder's response (Y/N)**	Remarks
1.1	The switch should have minimum 48 x 10/100/1000 Gigabit Ethernet and 4 Fiber uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.		
1.2	Future support for Redundant Power supply		
1.3	Should have fan for proper cooling		
1.5	At least 104 Gbps switching fabric		
1.6	Forwarding rate at least 77 Mpps		
1.7	Configurable at least 8000 MAC addresses		
1.8	Should support stacking (At least 20 Gbps bandwidth)		
1.9	The device should be IPv6 ready from day one		
1.10	Support for IEEE 802.1Q VLAN encapsulation. At least 250 VLANs should be supported. Support for 4000 VLAN IDs.		
1.11	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.		
1.12	Support for Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.		
1.13	Spanning-tree Enhancements for fast convergence		
1.14	Support for IEEE 802.1d, 802.1s, 802.1w, 802.3ad		
1.15	Support for Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.		
1.16	Support for IGMP snooping v3, Support for at least 250 IGMP Groups. IGMP filtering.		
1.17	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
1.18	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.		
1.19	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.		
1.20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize		

	available bandwidth.		
1.21	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.		
1.22	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.		
1.23	Support for IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
1.24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
1.25	Support for SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
1.26	Support for 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.		
1.27	Support for Port security to secure the access to an access or trunk port based on MAC address.		
1.28	Support for Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.		
1.29	Support for BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU’s are received to avoid accidental topology loops.		
1.30	At least 500 ACL entries should be supported.		
1.31	Support for Standard 802.1p CoS and DSCP		
1.32	Support for Control- and Data-plane QoS ACLs		
1.33	Four egress queues per port to enable differentiated management of up to four traffic types across the stack.		
1.34	Support for Weighted tail drop (WTD) to provide congestion avoidance		
1.35	Strict priority queuing mechanisms		
1.36	There should not be any performance penalty for highly granular QoS functions.		

1.37	Rate Limiting function should guarantee bandwidth in increments as small as 1 Mbps.		
1.38	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.		
1.39	At least 64 aggregate or individual polices should be available per Fast Ethernet or Gigabit Ethernet port.		
1.40	Support for IPv6 Host which can provide basic IPv6 management such as IPv4/IPv6 dual stack, unicast address types, ICMPv6, IPv6 Aggregatable Address, Secure Shell (SSH) for v6, IPv6 Autoconfiguration, IPv6 neighbor discovery, Telnet, TFTP, SNMP, HTTP, HTTPS, Trace route, Syslog for v6.		
1.41	Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
1.42	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.		
1.43	Support for Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
1.44	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.		
1.45	Support for Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
1.46	Support for Network Timing Protocol (NTP) to provide an accurate and consistent timestamp to all intranet switches.		
1.47	Support for SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive inband management, and a CLI-based management console provides detailed out-of-band management.		
1.48	Support for RMON I and II standards		
1.49	Support for SNMPv1, SNMPv2c, and SNMPv3		

EDGE SWITCH (24 PORT)

Sl. No.	**Description**	**Bidder's response (Y/N)**	Remarks
1.1	The switch should have minimum 24 x 10/100/1000 Gigabit Ethernet and 4 Fiber uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.		

1.2	Future support for Redundant Power supply		
1.3	Should have fan for proper cooling		
1.5	At least 56 Gbps switching fabric		
1.6	Forwarding rate at least 41 Mpps		
1.7	Configurable at least 8000 MAC addresses		
1.8	Should support stacking (At least 20 Gbps bandwidth)		
1.9	The device should be IPv6 ready from day one		
1.10	Support for IEEE 802.1Q VLAN encapsulation. At least 250 VLANs should be supported & support for 4000 VLAN IDs.		
1.11	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors		
1.12	Support for Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.		
1.13	Spanning-tree Enhancements for fast convergence		
1.14	Support for IEEE 802.1d, 802.1s, 802.1w, 802.3ad		
1.15	Support for Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.		
1.16	Support for IGMP snooping v3, Support for at least 250 IGMP Groups. IGMP filtering.		
1.17	Support for Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
1.18	Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.		
1.19	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.		
1.20	Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.		
1.21	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.		
1.22	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.		
1.23	Support for IEEE 802.1x to allow dynamic, port-based security, providing user authentication.		
1.24	Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.		
1.25	Support for SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
1.26	Support for 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.		
1.27	Support for Port security to secure the access to an access or trunk port based on MAC address.		
1.28	Support for Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.		
1.29	Support for BPDU Guard to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDU’s are received to avoid accidental topology loops.		
1.30	At least 500 ACL entries should be supported.		
1.31	Support for Standard 802.1p CoS and DSCP		
1.32	Support for Control- and Data-plane QoS ACLs		
1.33	Four egress queues per port to enable differentiated management of up to four traffic types across the stack.		
1.34	Support for Weighted tail drop (WTD) to provide congestion avoidance & Strict priority queuing mechanisms		
1.35	There should not be any performance penalty for highly granular QoS functions.		
1.36	Rate Limiting function should guarantee bandwidth in increments as small as 1 Mbps.		
1.37	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.		
1.38	At least 64 aggregate or individual polices should be available per Fast Ethernet or Gigabit Ethernet port.		

1.39	Support for IPv6 Host which can provide basic IPv6 management such as IPv4/IPv6 dual stack, unicast address types, ICMPv6, IPv6 Aggregatable Address, Secure Shell (SSH) for v6, IPv6 Autoconfiguration, IPv6 neighbor discovery, Telnet, TFTP, SNMP, HTTP, HTTPS, Trace route, Syslog for v6.		
1.40	Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
1.41	For enhanced traffic management, monitoring, and analysis, upto four RMON groups (history, statistics, alarms, and events) must be supported.		
1.42	Support for Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
1.43	Domain Name System (DNS) support to provide IP address resolution with user-defined device names.		
1.44	Support for Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
1.45	Support for Network Timing Protocol (NTP) to provide an accurate and consistent timestamp to all intranet switches.		
1.46	Support for SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive inband management, and a CLI-based management console provides detailed out-of-band management.		
1.47	Support for RMON I and II standards		
1.48	Support for SNMPv1, SNMPv2c, and SNMPv3		

EDGE SWITCH (8 PORT)

Sl. No.	**Description**	**Bidder's response (Y/N)**	Remarks
1.1	The switch should have minimum 8 x 10/100/1000 Gigabit Ethernet and 2 x Dual purpose (Copper or Fiber) uplinks (uplink port should support 1000 Base SX, 1000 Base ZX, 1000 Base LX.		
1.2	Switch should be 1 RU rack/wall mountable		
1.3	Should have minimum 10 Gbps forwarding bandwidth		
1.5	Should have minimum 13.2 Mpps forwarding rate		
1.7	The device should be IPv6 ready from day one		
1.8	Switch should support IEEE Standards of Ethernet: IEEE 802.1d,		

	802.1s, 802.1w etc.		
1.9	Should have IEEE 802.1Q VLAN encapsulation and up to 250 active VLANs per switch		
1.10	Should support IPv4 and IPv6 MLD v1 and v2 Snooping		
1.11	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		
1.12	Should have a mechanism to detect connectivity issues with both fiber and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues		
1.13	Should have extensive debugging including layer 2 debugging and layer 2 trace route for troubleshooting		
1.14	Should support for QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and help enable egress queue configuration.		
1.15	Should support for autoconfiguration of multiple switches through a boot server eases switch deployment.		
1.16	Should support for auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.		
1.17	Should support for dynamic trunk configuration across all switch ports		
1.18	Should support for creation of Ethernet channeling with devices that conform to IEEE 802.3ad		
1.19	Should support for automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.		
1.20	Should support for superior CLI for detailed configuration and administration.		
1.21	switches should provide superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and ARP spoofing).		
1.22	Support for multiple authentication mechanisms including 802.1X, MAC Authentication Bypass, and web authentication using a single, consistent configuration.		
1.23	Suppoirt for RADIUS / TACACS+ Change of Authorization and Downloadable ACLs for comprehensive policy management capabilities.		

1.24	Support for Port-Based ACLs for Layer 2 interfaces		
1.25	Support for network security by encrypting administrator traffic during Telnet and SNMP sessions.		
1.26	Support for multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.		
1.27	Support to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
1.28	Support for implementation of VLAN Membership Policy Server client capability to provide flexibility in assigning ports to VLANs.		
1.29	Support for atleast 64 Mb Flash memory & 128 Mb DRAM		
1.30	Support for jumbo frames (9018 bytes)		
1.31	Switch should support Reduction of Hazardous Substances (ROHS) 6		