**Annexure-IV (A)**

| ** Please provide make and model no of the quoted items | | | |
|---|---|---|---|
| **TECHNICAL SPECIFICATIONS - Switching** | | | |
| **L3 Switch 52 Port** | | | |
| **1- Technical clauses:** | | | |
| **SI No** | **Desired Specification/Qualitative Requirement** | **Compliance (Yes/No)** | **Remarks ** ** |
| **1** | **Core / Distribution Switches -52 port (Layer 3)** | | |
| **1.1** | Architecture | | |
| **(a)** | Switch should have 48 10/100/1000Base-T ports + 4 10GE SFP+ ports for uplink to Switch or Servers for Stacking. | | |
| **(b)** | Switch should provide option of Redundant power supply | | |
| **(c)** | Switch shall have Min. 256 MB SD RAM & 128 MB Flash Memory | | |
| **(d)** | Switch shall have SD Card slot for easy file store & restoration like firmware, configuration file, boot image, syslog etc. | | |
| **(e)** | Switch shall provide digital I/O design through external alarm port to have better security protection. | | |
| **(f)** | Switch shall be able to receive events detected by external sensors (e.g. temperature, smoking or anti-theft sensor). The switch shall be able to send a trap/log out to report the issue. | | |
| **(g)** | Switch shall be able to activate external air-conditioner/fan or ring the bell based on the condition defined by the user | | |
| **1.2** | Network Media | | |
| **(a)** | SFP's 1000BaseSX,1000BaseLX,1000BaseTX,1000Base Lx WDM | | |
| **1.3** | Performance | | |
| **(a)** | The Switch shall have Non-blocking wire speed switch fabric | | |
| **(b)** | The Switch shall have Minimum 176 Gbps Back plane or more | | |
| **(c)** | The Switch shall have Minimum 130 million pps or more | | |
| **(d)** | The Switch shall support Min. 32K Mac address or more | | |
| **(e)** | The Switch shall support Min. 4000 VLANs | | |
| **(f)** | The Switch shall support IPv4/IPv6 Routing including IPv6 Tunnel, ICMPv6, IPv6 Neighbour Discovery(ND), DHCPv6, RIPng and OSPFv3 | | |
| **(g)** | The Switch shall have 40 Gigabit Stacking Backplane | | |

| | | | |
|---|---|---|---|
| **(h)** | The Switch shall be able to do Physical Stack up to 10 units per stack or more | | |
| **(i)** | The Switch shall be able to do IP Stacking up to 30 units per IP | | |
| **(j)** | The Switch Should support Jumbo Frame (up to 9216 Bytes) | | |
| **1.4** | Layer 3 Features | | |
| **(a)** | The Switch should have RIPv1(RFC1058)/RIPv2(RFC2453),RIPng,OSPFv2, OSPFv3, MPLS,MPLS VPN, VPLS | | |
| **(b)** | The Switch should have Policy Based Routing ,BGP 4 & VRRP | | |
| **(c)** | The Switch should have DVMRP v3, PIM-DM/SM/SDM for IPv4 | | |
| **(d)** | The Switch should have IPv6 Tunnelling | | |
| **(e)** | The Switch should have Up to 256 IP Interfaces & 10K route entries or more | | |
| **(f)** | The Switch should have Multi Path Routing support for Equal cost & Weighted Cost | | |
| **(g)** | The Switch should have Per port Limit IP Multicast Address Range for Control Packet | | |
| **1.5** | Layer 2 Features | | |
| **(a)** | The Switch should have IGMP Snooping v1,v2,v3 & MLD Snooping | | |
| **(b)** | The Switch should have Spanning tree 802.1d,802.1w,802.1s | | |
| **(c)** | The Switch should have 802.3ad Link Aggregation Up to 30 groups per device | | |
| **(d)** | The Switch should have Port Mirroring One to one/Many to One & RSPAN | | |
| **(e)** | The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment | | |
| **(f)** | The Switch shall have the capability to build the trunk across stack | | |
| **(g)** | The Switch shall support IEEE 802.3ah, IEEE 802.1ag, 802.1AX & ITU-T Y.1731 | | |
| **(h)** | It shall support LLDP and LLDP-MED including client location information. It shall exchange link and device information in multi-vendor networks | | |
| **1.6** | VLAN | | |

| | | | |
|---|---|---|---|
| **(a)** | The LAN switch shall have IEEE 802.1Q VLAN encapsulation. Up to 255 VLANs per switch and up to 4000 VLAN IDs. | | |
| **(b)** | It shall have Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors. | | |
| **(c)** | It shall have centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the others switches automatically, thus reducing the overhead of creating/modifying/deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting. | | |
| **(d)** | It shall have support for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops | | |
| **(e)** | It shall support 802.1v & Q-in-Q Vlan | | |
| **1.7** | Quality of Service | | |
| **(a)** | It shall support 802.1p Priority Queues (8 Queues) | | |
| **(b)** | Queue Handling mode: WRR & Strict Mode | | |
| **(c)** | Granular Rate Limiting functions on per port & flow based to guarantee bandwidth in increments shall be as low as 64 Kilobits per Second. | | |
| **d)** | Switch shall support three color marker with CIR/PIR minimum granularity of 1 kbps | | |
| **(e)** | Class of service shall be based on Switch port, DSCP, Vlan ID,TCP/UDP port, Protocol type,802.1p queues, IPv4/v6 address, IPv6 flow label & User defined packet content | | |
| **1.8** | Access Control List | | |
| **(a)** | The Lan Switch shall have the capability to apply access list control based on IPv4/v6 address, Protocol type,IPv6 flow label, Time based ACL, Vlan-ID, MAC-ID, DSCP, IPv6 traffic class, TCP/UDP Port, Switch port & user defined packet content | | |
| **(b)** | The Switch shall support up to 1600 Access Control Entries minimum | | |
| **1.9** | Network Security | | |
| **(a)** | The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication. | | |

| | | | |
|---|---|---|---|
| **(b)** | The LAN switch shall support for Admission Control features 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 such as Microsoft for security-policy compliance and enforcement before a host is permitted to access the network | | |
| **(c)** | It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions. | | |
| **(d)** | It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration. | | |
| **(e)** | It shall support 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. | | |
| **(f)** | It shall support DHCP Interface Tracker (Option 82) to augment a host IP address request with the switch port ID. | | |
| **(g)** | It shall support that each end node can be isolated from each other and they should be able to connect to shared ports such as Internet and servers | | |
| **(h)** | It shall support port security to secure the access to an access or trunk port based on MAC address. After a specific timeframe, the aging feature should remove the MAC address from the switch to allow another device to connect to the same port.(up to 14 MAC-ID per port) | | |
| **(i)** | It shall have MAC-IP-Port binding up with support for ACL mode to 475 Entries per device | | |
| **(j)** | It shall have Web & MAC Based Access Control | | |
| **(k)** | It shall have CPU Filtering to protect the CPU from Broadcast / Multicast / Unicast flooding & protocol control packets attacks | | |
| **1.1** | Management | | |
| **(a)** | The LAN switch shall have CLI support to provide a common user interface and command set with all routers and switches of the same vendor. | | |

| | | | |
|---|---|---|---|
| **(b)** | It shall have Remote Monitoring (RMON) software agent to support four RMON groups (history, statistics, alarms and events) for enhanced traffic management, monitoring and analysis. | | |
| **(c)** | It shall support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location. | | |
| **(d)** | It shall support Network Timing Protocol (NTP/SNTP) to provide an accurate and consistent timestamp to all intranet switches. | | |
| **(e)** | It shall support SNMPv1, SNMPv2c, and SNMPv3 and Telnet interface to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management | | |
| **(f)** | It shall provide management functions for network segments (access links and individual circuits), monitors individual links. | | |
| **(g)** | It shall have traffic monitoring for all network ports effective at gigabit speed or higher, shall not impact the network performance while providing the real time & historical data of all devices from Layer 2 to Layer 7. | | |
| **(h)** | It shall support configuration rollback to replace current configuration with any saved configuration file.<br>Switch shall be capable to store multiple image file and configuration | | |
| **(i)** | Switch shall consume less power through auto-detection of link status and cable length. | | |
| **1.11** | **Certification** | | |
| **(a)** | Switch should be CE,FCC,UL,VCCI, ERTL certified | | |
| **(b)** | Switch should be functionally test and verified from ERTL and vendor need to present complete functional test report from ERTL. | | |
| | | | |

| **Switch 28 Port** | | | |
|---|---|---|---|
| **Sr No** | **Desired Specification/Qualitative Requirement** | **Compliance (Yes/No)** | **Remark** |
| **1** | **Core / Distribution Switches-28 port (Layer 3)** | | |

| | | | |
|---|---|---|---|
| **1.1** | Architecture | | |
| **(a)** | Switch should have 20 10/100/1000Base-T ports + 4 Combo 10/100/1000Base-T/SFP ports + 4 10GE SFP+ ports for uplink to Switch or Servers for Stacking. | | |
| **(b)** | Switch should provide option of Redundant power supply | | |
| **(c)** | Switch shall have Min. 256 MB SD RAM & 128 MB Flash Memory | | |
| **(d)** | Switch shall have SD Card slot for easy file store & restoration like firmware, configuration file, boot image, syslog etc. | | |
| **(e)** | Switch shall provide digital I/O design through external alarm port to have better security protection. | | |
| | | | |
| **(f)** | Switch shall be able to receive events detected by external sensors (e.g. temperature, smoking or anti-theft sensor). The switch shall be able to send a trap/log out to report the issue. | | |
| **(g)** | Switch shall be able to activate external air-conditioner/fan or ring the bell based on the condition defined by the user | | |
| **1.2** | Network Media | | |
| **(a)** | SFP's 1000BaseSX,1000BaseLX,1000BaseTX,1000Base Lx WDM | | |
| **1.3** | Performance | | |
| **(a)** | The Switch shall have Non-blocking wire speed switch fabric | | |
| **(b)** | The Switch shall have Minimum 128 Gbps Back plane or more | | |
| **(c)** | The Switch shall have Minimum 95 million pps or more | | |
| **(d)** | The Switch shall support Min. 32K Mac address or more | | |
| **(e)** | The Switch shall support Min. 4000 VLANs | | |
| **(f)** | The Switch shall support IPv4/IPv6 Routing including IPv6 Tunnel, ICMPv6, IPv6 Neighbour Discovery(ND), DHCPv6, RIPng and OSPFv3 | | |
| **(g)** | The Switch shall have 40 Gigabit Stacking Backplane | | |
| **(h)** | The Switch shall be able to do Physical Stack up to 10 units per stack or more | | |
| **(i)** | The Switch shall be able to do IP Stacking up to 30 units per IP | | |
| **(j)** | The Switch Should support Jumbo Frame (up to 9216 Bytes) | | |
| **1.4** | Layer 3 Features | | |

| | | | |
|---|---|---|---|
| **(a)** | The Switch should have RIPv1(RFC1058)/RIPv2(RFC2453),RIPng,OSPFv2, OSPFv3, MPLS,MPLS VPN, VPLS | | |
| **(b)** | The Switch should have Policy Based Routing ,BGP 4 & VRRP | | |
| **(c)** | The Switch should have DVMRP v3, PIM-DM/SM/SDM for IPv4 | | |
| **(d)** | The Switch should have IPv6 Tunnelling | | |
| **(e)** | The Switch should have Up to 256 IP Interfaces & 10K route entries or more | | |
| **(f)** | The Switch should have Multi Path Routing support for Equal cost & Weighted Cost | | |
| **(g)** | The Switch should have Per port Limit IP Multicast Address Range for Control Packet | | |
| **1.5** | Layer 2 Features | | |
| **(a)** | The Switch should have IGMP Snooping v1,v2,v3 & MLD Snooping | | |
| **(b)** | The Switch should have Spanning tree 802.1d,802.1w,802.1s | | |
| **(c)** | The Switch should have 802.3ad Link Aggregation Up to 30 groups per device | | |
| **(d)** | The Switch should have Port Mirroring One to one/Many to One & RSPAN | | |
| **(e)** | The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment | | |
| **(f)** | The Switch shall have the capability to build the trunk across stack | | |
| **(g)** | The Switch shall support IEEE 802.3ah, IEEE 802.1ag, 802.1AX & ITU-T Y.1731 | | |
| **(h)** | It shall support LLDP and LLDP-MED including client location information. It shall exchange link and device information in multi-vendor networks | | |
| **1.6** | VLAN | | |
| **(a)** | The LAN switch shall have IEEE 802.1Q VLAN encapsulation. Up to 255 VLANs per switch and up to 4000 VLAN IDs. | | |
| **(b)** | It shall have Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors. | | |

| | | | |
|---|---|---|---|
| **(c)** | It shall have centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the others switches automatically, thus reducing the overhead of creating/modifying/deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting. | | |
| **(d)** | It shall have support for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops | | |
| **(e)** | It shall support 802.1v & Q-in-Q Vlan | | |
| **1.7** | Quality of Service | | |
| **(a)** | It shall support 802.1p Priority Queues (8 Queues) | | |
| **(b)** | Queue Handling mode: WRR & Strict Mode | | |
| **(c)** | Granular Rate Limiting functions on per port & flow based to guarantee bandwidth in increments shall be as low as 64 Kilobits per Second. | | |
| **d)** | Switch shall support three color marker with CIR/PIR minimum granularity of 1 kbps | | |
| **(e)** | Class of service shall be based on Switch port, DSCP, Vlan ID,TCP/UDP port, Protocol type,802.1p queues, IPv4/v6 address, IPv6 flow label & User defined packet content | | |
| **1.8** | Access Control List | | |
| **(a)** | The Lan Switch shall have the capability to apply access list control based on IPv4/v6 address, Protocol type,IPv6 flow label, Time based ACL, Vlan-ID, MAC-ID, DSCP, IPv6 traffic class, TCP/UDP Port, Switch port & user defined packet content | | |
| **(b)** | The Switch shall support up to 1600 Access Control Entries minimum | | |
| **1.9** | Network Security | | |
| **(a)** | The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication. | | |

| | | | |
|---|---|---|---|
| **(b)** | The LAN switch shall support for Admission Control features 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 such as Microsoft for security-policy compliance and enforcement before a host is permitted to access the network | | |
| **(c)** | It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions. | | |
| **(d)** | It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration. | | |
| **(e)** | It shall support 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. | | |
| **(f)** | It shall support DHCP Interface Tracker (Option 82) to augment a host IP address request with the switch port ID. | | |
| **(g)** | It shall support that each end node can be isolated from each other and they should be able to connect to shared ports such as Internet and servers | | |
| **(h)** | It shall support port security to secure the access to an access or trunk port based on MAC address. After a specific timeframe, the aging feature should remove the MAC address from the switch to allow another device to connect to the same port.(up to 14 MAC-ID per port) | | |
| **(i)** | It shall have MAC-IP-Port binding up with support for ACL mode to 475 Entries per device | | |
| **(j)** | It shall have Web & MAC Based Access Control | | |
| **(k)** | It shall have CPU Filtering to protect the CPU from Broadcast / Multicast / Unicast flooding & protocol control packets attacks | | |
| **1.1** | Management | | |
| **(a)** | The LAN switch shall have CLI support to provide a common user interface and command set with all routers and switches of the same vendor. | | |

| | | | |
|---|---|---|---|
| **(b)** | It shall have Remote Monitoring (RMON) software agent to support four RMON groups (history, statistics, alarms and events) for enhanced traffic management, monitoring and analysis. | | |
| **(c)** | It shall support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location. | | |
| **(d)** | It shall support Network Timing Protocol (NTP/SNTP) to provide an accurate and consistent timestamp to all intranet switches. | | |
| **(e)** | It shall support SNMPv1, SNMPv2c, and SNMPv3 and Telnet interface to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management | | |
| **(f)** | It shall provide management functions for network segments (access links and individual circuits), monitors individual links. | | |
| **(g)** | It shall have traffic monitoring for all network ports effective at gigabit speed or higher, shall not impact the network performance while providing the real time & historical data of all devices from Layer 2 to Layer 7. | | |
| **(h)** | It shall support configuration rollback to replace current configuration with any saved configuration file. | | |
| | Switch shall be capable to store multiple image file and configuration | | |
| **(i)** | Switch shall consume less power through auto-detection of link status and cable length. | | |
| **1.11** | **Certification** | | |
| **(a)** | Switch should be CE,FCC,UL,VCCI, ERTL certified | | |
| **(b)** | Switch should be functionally test and verified from ERTL and vendor need to present complete functional test report from ERTL. | | |
| | | | |

| **Switch POE 28 Port** | | | |
|---|---|---|---|
| **Sr No** | **Desired Specification/Qualitative Requirement** | **Compliance (Yes/No)** | **Remark** |
| **1** | **PoE Managed 28 port Switches** | | |
| **1.1** | Architecture | | |

| | | | |
|---|---|---|---|
| **(a)** | Switch should have 20 10/100/1000Base-T PoE+ ports + 4 Combo 10/100/1000Base-T PoE+/SFP ports + 4 10GE SFP+ ports for uplink to Switch or Servers for Stacking. | | |
| **(b)** | Switch should provide option of Redundant power supply | | |
| **(c)** | Switch shall have Min. 256 MB SD RAM & 128 MB Flash Memory | | |
| **(d)** | Switch shall have SD Card slot for easy file store & restoration like firmware, configuration file, boot image, syslog etc. | | |
| **(e)** | Switch shall provide digital I/O design through external alarm port to have better security protection. | | |
| | | | |
| **(f)** | Switch shall be able to receive events detected by external sensors (e.g. temperature, smoking or anti-theft sensor). The switch shall be able to send a trap/log out to report the issue. | | |
| **(g)** | Switch shall be able to activate external air-conditioner/fan or ring the bell based on the condition defined by the user | | |
| **1.2** | Network Media | | |
| **(a)** | SFP's 1000BaseSX,1000BaseLX,1000BaseTX,1000Base Lx WDM | | |
| **1.3** | Performance | | |
| **(a)** | The Switch shall have Non-blocking wire speed switch fabric | | |
| **(b)** | The Switch shall have Minimum 128 Gbps Back plane or more | | |
| **(c)** | The Switch shall have Minimum 95 million pps or more | | |
| **(d)** | The Switch shall support Min. 32K Mac address or more | | |
| **(e)** | The Switch shall support Min. 4000 VLANs | | |
| **(f)** | The Switch shall support IPv4/IPv6 Routing including IPv6 Tunnel, ICMPv6, IPv6 Neighbour Discovery(ND), DHCPv6, RIPng and OSPFv3 | | |
| **(g)** | The Switch shall have 40 Gigabit Stacking Backplane | | |
| **(h)** | The Switch shall be able to do Physical Stack up to 10 units per stack or more | | |
| **(i)** | The Switch shall be able to do IP Stacking up to 30 units per IP | | |
| **(j)** | The Switch Should support Jumbo Frame (up to 9216 Bytes) | | |
| **(k)** | The Switch Should support 802.3af and 802.3at standard | | |
| **1.4** | Layer 3 Features | | |

| | | | |
|---|---|---|---|
| **(a)** | The Switch should have RIPv1(RFC1058)/RIPv2(RFC2453),RIPng,OSPFv2, OSPFv3, MPLS,MPLS VPN, VPLS | | |
| **(b)** | The Switch should have Policy Based Routing ,BGP 4 & VRRP | | |
| **(c)** | The Switch should have DVMRP v3, PIM-DM/SM/SDM for IPv4 | | |
| **(d)** | The Switch should have IPv6 Tunnelling | | |
| **(e)** | The Switch should have Up to 256 IP Interfaces & 10K route entries or more | | |
| **(f)** | The Switch should have Multi Path Routing support for Equal cost & Weighted Cost | | |
| **(g)** | The Switch should have Per port Limit IP Multicast Address Range for Control Packet | | |
| **1.5** | Layer 2 Features | | |
| **(a)** | The Switch should have IGMP Snooping v1,v2,v3 & MLD Snooping | | |
| **(b)** | The Switch should have Spanning tree 802.1d,802.1w,802.1s | | |
| **(c)** | The Switch should have 802.3ad Link Aggregation Up to 30 groups per device | | |
| **(d)** | The Switch should have Port Mirroring One to one/Many to One & RSPAN | | |
| **(e)** | The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment | | |
| **(f)** | The Switch shall have the capability to build the trunk across stack | | |
| **(g)** | The Switch shall support IEEE 802.3ah, IEEE 802.1ag, 802.1AX & ITU-T Y.1731 | | |
| **(h)** | It shall support LLDP and LLDP-MED including client location information. It shall exchange link and device information in multi-vendor networks | | |
| **1.6** | VLAN | | |
| **(a)** | The LAN switch shall have IEEE 802.1Q VLAN encapsulation. Up to 255 VLANs per switch and up to 4000 VLAN IDs. | | |
| **(b)** | It shall have Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors. | | |

| | | | |
|---|---|---|---|
| **(c)** | It shall have centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the others switches automatically, thus reducing the overhead of creating/modifying/deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting. | | |
| **(d)** | It shall have support for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops | | |
| **(e)** | It shall support 802.1v & Q-in-Q Vlan | | |
| **1.7** | Quality of Service | | |
| **(a)** | It shall support 802.1p Priority Queues (8 Queues) | | |
| **(b)** | Queue Handling mode: WRR & Strict Mode | | |
| **(c)** | Granular Rate Limiting functions on per port & flow based to guarantee bandwidth in increments shall be as low as 64 Kilobits per Second. | | |
| **d)** | Switch shall support three color marker with CIR/PIR minimum granularity of 1 kbps | | |
| **(e)** | Class of service shall be based on Switch port, DSCP, Vlan ID,TCP/UDP port, Protocol type,802.1p queues, IPv4/v6 address, IPv6 flow label & User defined packet content | | |
| **1.8** | Access Control List | | |
| **(a)** | The Lan Switch shall have the capability to apply access list control based on IPv4/v6 address, Protocol type,IPv6 flow label, Time based ACL, Vlan-ID, MAC-ID, DSCP, IPv6 traffic class, TCP/UDP Port, Switch port & user defined packet content | | |
| **(b)** | The Switch shall support up to 1600 Access Control Entries minimum | | |
| **1.9** | Network Security | | |
| **(a)** | The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication. | | |

| | | | |
|---|---|---|---|
| **(b)** | The LAN switch shall support for Admission Control features 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 such as Microsoft for security-policy compliance and enforcement before a host is permitted to access the network | | |
| **(c)** | It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions. | | |
| **(d)** | It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration. | | |
| **(e)** | It shall support 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. | | |
| **(f)** | It shall support DHCP Interface Tracker (Option 82) to augment a host IP address request with the switch port ID. | | |
| **(g)** | It shall support that each end node can be isolated from each other and they should be able to connect to shared ports such as Internet and servers | | |
| **(h)** | It shall support port security to secure the access to an access or trunk port based on MAC address. After a specific timeframe, the aging feature should remove the MAC address from the switch to allow another device to connect to the same port.(up to 14 MAC-ID per port) | | |
| **(i)** | It shall have MAC-IP-Port binding up with support for ACL mode to 475 Entries per device | | |
| **(j)** | It shall have Web & MAC Based Access Control | | |
| **(k)** | It shall have CPU Filtering to protect the CPU from Broadcast / Multicast / Unicast flooding & protocol control packets attacks | | |
| **1.1** | Management | | |
| **(a)** | The LAN switch shall have CLI support to provide a common user interface and command set with all routers and switches of the same vendor. | | |

| | | | |
|---|---|---|---|
| **(b)** | It shall have Remote Monitoring (RMON) software agent to support four RMON groups (history, statistics, alarms and events) for enhanced traffic management, monitoring and analysis. | | |
| **(c)** | It shall support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location. | | |
| **(d)** | It shall support Network Timing Protocol (NTP/SNTP) to provide an accurate and consistent timestamp to all intranet switches. | | |
| **(e)** | It shall support SNMPv1, SNMPv2c, and SNMPv3 and Telnet interface to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management | | |
| **(f)** | It shall provide management functions for network segments (access links and individual circuits), monitors individual links. | | |
| **(g)** | It shall have traffic monitoring for all network ports effective at gigabit speed or higher, shall not impact the network performance while providing the real time & historical data of all devices from Layer 2 to Layer 7. | | |
| **(h)** | It shall support configuration rollback to replace current configuration with any saved configuration file.<br>Switch shall be capable to store multiple image file and configuration | | |
| **(i)** | Switch shall consume less power through auto-detection of link status and cable length. | | |
| **1.11** | **Certification** | | |
| **(a)** | Switch should be CE,FCC,UL,VCCI, ERTL certified | | |
| **(b)** | Switch should be functionally test and verified from ERTL and vendor need to present complete functional test report from ERTL. | | |
| | | | |

| **Technical Specification for POE Wireless Access Point 802.11a/b/g/n with Internal Antenna** | | | |
|---|---|---|---|
| **Sr No** | **Technical Specification for POE Wireless Access Point 802.11a/b/g/n with Internal Antenna** | **Compliance (Yes/No)** | **Remarks** |

| | | | |
|---|---|---|---|
| 1 | Provide Ethernet to Wireless LAN bridge fully IEEE 802.3 compatible on the Ethernet side and fully interoperable with IEEE 802.11a/b/g/n compliant equipment. | | |
| 2 | Operation at 2.4GHz and 5GHz band to meet worldwide regulations | | |
| 3 | AP should support have soft reboot button and factory reset button. | | |
| 4 | Allows auto fallback data rate for reliability, optimized throughput and transmission range. | | |
| 5 | Supports IEEE 802.11 a/b/g/n wireless data encryption with 64/128-bit WEP for security. | | |
| 6 | Supports enhanced security – WPA2-Personal & WPA2-Enterprise,PSK, TKIP and AES, Pre-authentication for WPA2 Enterprise, Key caching for WPA2 Enterprise | | |
| 7 | Supports PoE (Class 3) | | |
| 8 | Supports one 10/100/1000 Ethernet port with Auto-sensing MDI/-MDI-X | | |
| 9 | Up to 16 Virtual APs (VAP) per radio and Allows up to 200 wireless clients connected | | |
| 10 | Supports WDS in both of standalone and managed mode | | |
| 11 | Supports AP Clustering, enabling APs to form a cluster for simple management and configuration | | |
| 12 | Can be managed via Web GUI, CLI or SNMP. | | |
| 13 | Supports IPv6 management function on both of standalone and managed mode. | | |
| 14 | Firmware upgradeable using TFTP and HTTP | | |
| 15 | EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAP-GTC, PEAP-TLS, PEAP-MS-CHAPv2 | | |
| 16 | Configure client access based on AP utilization level | | |
| 17 | Neighbouring AP detection (Rogue AP) using continuous channel scanning | | |
| 18 | Supports authentication with RADIUS, Can configure up to 4 external RADIUS server for failover | | |

| | | | |
|---|---|---|---|
| 19 | Supports 802.1p Quality of Service (QoS) for enhanced throughput and better performance of time-sensitive traffic like VoIP and streaming and DSCP | | |
| 20 | Allows up to 200 wireless clients connected to AP | | |
| 21 | Supports 802.1Q VLAN Tagging, Maximum of 64 Dynamic VLAN | | |
| 22 | AP should have built in utility for packet capture. | | |
| 23 | Access point should have 2.4GHz and 5GHz PIFA antenna, 2x2 2.4GHz 5 dBi Omni-directional antennas & 2x2 5GHz 6 dBi Omni-directional antennas with 4 reserved external antenna connectors. | | |
| 24 | Should have RJ 45 Console port | | |
| 25 | CE, FCC, C-Tick, IC, VCCI, NCC, WiFi, TELEC, CE/ LVD, UL/CSA 60950-1, UL2043 | | |

| | **Module (Multi-Mode Fiber Transceiver)** | | |
|---|---|---|---|
| **Feature** | **Specification** | **Compliance (Yes/No)** | **Remarks** |
| 1 | 1000 Base-SX port (IEEE 802.3z standard) | | |
| 2 | Duplex LC connector | | |
| 3 | Full Duplex operation | | |
| 4 | 802.3x flow control support | | |
| 5 | Fiber type: 50um or 62.5um multi-mode fiber up to 550m | | |
| 6 | Wave length: 850nm | | |
| 7 | Power support: 3.3V | | |
| 8 | Hot Pluggable | | |
| 9 | Class 1 laser product complies with EN 60825-1 | | |
| 10 | TTL signal detect indicator | | |
| 11 | Metal enclosure for lower EMI | | |
| | | | |

**Network Management System Software**

| S.N | **Specifications** | **Compliance (Yes/No)** | **Remarks** |
|---|---|---|---|
| **1** | **Topology Map** | | |

| | | | |
|---|---|---|---|
| **2** | **Topology Import / Export** | | |
| **3** | **Domain Manager** | | |
| | It should be able to create and modify the domain parameters, such as the domain name, the legal host which is allowed to access, monitor and manage the domain | | |
| | It should be able to configure which workstation (user) is allowed to access which domain | | |
| **4** | **Link Manager** | | |
| | It should be able to maintain the link relationship between 2 devices when create the devices manually. | | |
| | It should Add/ delete/ modify feature supported | | |
| 5 | **Web Client** | | |
| | It should allow the access and essential configuration via Web | | |
| | It should be able to discover the topology by subnet or IP address range. | | |
| 6 | **Topology Discovery** | | |
| | It should allow automatically and periodically polling the network and adding the new discovered device into the topology | | |
| **7** | **Separated Polling Interval** | | |
| | It should be able to configure the different polling interval for device groups | | |
| 8 | **Trap Editor** | | |
| | It should have the support to Add trap's OID definition into NMS with associated message description. When NMS receives the trap, the message board will display the trap's information which was defined in the trap editor. | | |
| 9 | **Trap Filter** | | |
| | Normally, when NMS receives a trap, NMS will launch associated notification procedure which was defined in NMS. When enable the trap filter, NMS will ignore the trap's associated notification action. | | |
| 10 | **Event Configuration** | | |
| | It should configure the notification method for each event/trap as following:- | | |

| | | | |
|---|---|---|---|
| | The notification methods include | | |
| | 2-1. Sound | | |
| | 2-2. Keep a log | | |
| | 2-3 Flash | | |
| | 2-4 Send an E-Mail | | |
| 11 | **Polling Configuration** | | |
| | It should be able to define the polling protocol, polling interval and determine which device will be monitored. | | |
| 12 | **System Log** | | |
| | It should save and maintain the administrators' operation log and the system's log | | |
| | | | |
| 13 | **Syslog Server** | | |
| | It should act as a syslog server to collect all the syslog message sent from each devices | | |
| 14 | **Batch Configuration** | | |
| | It should be able to simultaneously configure several devices at the same time | | |
| | It should be enable to support functions such as Save file, Enable/Disable RMON, Enable/Disable Safeguard Engine, Enable/Disable Spanning Tree, Firmware updates, Device Resource information update, Configuration file update, Port Status check, Reboot the selected device, VLAN creation | | |
| | It should have the support to configure 3rd parties' device OID information into NMS's database. When NMS polling the network and found the same OID, NMS will identify the device and display the name you entered in the topology map. | | |
| 15 | **Device Customization** | | |
| | If 3rd parties' device is not defined first over here, the device will displayed as a "GenSNMP Device" in topology map. | | |
| | 3rd parties' devices on Netmap can be changed with selected Icons for customized presentation to keep some basic information of devices to help administrator's management. | | |

| | | | |
|---|---|---|---|
| 16 | **Device Manager** | | |
| | It should have device informations such as device's name, vendor, model type, Device's interface information, | | |
| | It should have Device's detail information such as location, buyer, purchase date, number of modules, number of port, serial number, firmware version. | | |
| | It should have the support to configure device's SNMP community name, SNMP v3 authentication and launch 3rd parties' device management tool. | | |
| 17 | **MIB Complier/MIB Browser** | | |
| | It should be able to Compile 3rd parties' MIB file into NMS's database. | | |
| | If there's no management tool or management module to manage 3rd parties' device, the MIB files of 3rd parties' devices need to be compiled into NMS first and then use MIB browser to query the data or configure the data into devices. | | |
| 18 | **MIB Utilities** | | |
| | It should have the utilities to configure the MIB information | | |
| | It should include utilities such as Device SNMP configuration, MIB II information and statistics, IF information table, Spanning tree information and port configuration, Bridge 802.1d information and port configuration, RMON statistic, History and Event group, Transparent bridge, forwarding and static filter, tables and port, Counter, 802.1p priority configuration, L3 utilities | | |
| 19 | **Surveillance for Windows Server** | | |
| | It should manage all SNMP enabled Windows Servers | | |
| | It should be able to monitor the disk space usage, network load, memory usage | | |
| | It should set the notification level for disk space, network load and memory usage | | |
| 20 | **Inventory Management** | | |
| | It should be able to categorize the switch's model and generate the report | | |

| | | | |
|---|---|---|---|
| | It should be able to display switch's IP address, firmware version etc. | | |
| | It should be able to categorize the switches by model type and display the quantity information | | |
| 21 | **Device Locator** | | |
| | It should be able to search device by IP address and pinpoint the Netmap where the device is | | |
| 22 | **Device Statistics** | | |
| | It should be able to display some statistics information of devices | | |
| | It should support information such as Vendor statistics, the buyer statistics, the purchase date statistics | | |
| 23 | **Performance Monitor** | | |
| | It should be able to collect device's RMON information, and the device need to enable RMON first before performs the Performance Monitor. | | |
| | Performance Monitor contains 3 main reports, the Error Ratio, Data Distribution and Port Flow | | |
| | It should includes Error Ratio such as Drop Events, CRCAlignError, UndersizedPkt, OversizedPkt, Segments, Jabbers, Collisions | | |
| | It should have Data Distribution which includes 0 ~ 64 Octets, 65 ~ 127 Octets, 128 ~ 255 Octets, 256 ~ 511 Octets,512 ~ 1023 Octets, 1024 ~ 1518 Octets | | |
| 24 | **Port Packet Monitor** | | |
| | It should have Port Flow which includes Octets, Packets, Broadcast Packets, Multicast Packets | | |
| | It should support essential information collection for the devices which do not support RMON | | |
| | It should be able to collect the statistics information based on RFC1213. | | |
| 25 | **Reporting** | | |
| | It should contain 2 reports, the Utilization and Packet Info. | | |
| | It should includes Utilization such as Port utilization, Port's In Octets, Port's Out Octets | | |

| | | | |
|---|---|---|---|
| | It should have Packet Info that includes In Unicast Packets, In Non-unicast Packets, In Discards, In Errors, In Unknown Port, Out Unicast Packets, Out Non-unicast Packets | | |
| | NMS should support templates for user to generate the report | | |
| | Users should be able to pick up the parameters which NMS will collect the data and display it on the report. | | |
| | It should display not only the real-time report but also historical data which is restored in the database. | | |
| 26 | **SFlow** | | |
| | It should allow the sFlow connector to collect the sFlow datagram sending from sFlow enabled switches | | |
| 27 | **Authentication** | | |
| | It should support local and Radius authentication modes when log on | | |
| | | | |
| 28 | **Differentiated User Access Control** | | |
| | It should behave in a manner so that, when different users login into NMS, the functions in the menu is enabled accordingly | | |
| 29 | **SNMPv3 Security** | | |
| | It should support the SNMPv3 security functions such as Packet encryption/decryption, MPD (RFC 2572), TARGET (RFC 2573), USM (RFC 2574), VACM (RFC 2575) | | |
| 30 | **System Configuration** | | |
| | It should be able to configure essential information of system such as management IP station, authentication configuration. | | |
| 31 | **Administrator Manager** | | |
| | It should manage the administrators, such as adding or removing users ; create and delete the user group; configure the access right for each individual users | | |
| 32 | **Link Capacity Check** | | |
| | It should be able to check the link speed and the connection relationship between two switches. | | |
| 33 | **Device Type Check** | | |
| | It should have the control to Check the device model type | | |

| | | | |
|---|---|---|---|
| 34 | **Trace Route** | | |
| | Trace route command | | |
| 35 | **Scheduling** | | |
| | It should be able to support the ability to arrange the schedule for daily operations or to process specific functions | | |
| 36 | **Nodes Supported** | | |
| | Should support maximum of 5000 nodes | | |