

DOCUMENT DATA SHEET		
Specification RDSO/SPN/TC/83 /2014		Revision 1.0
Title of Document RDSO Specification for LAN Switch		
Author Director/ Telecom-II/ RDSO		
Approved by Executive Director/ Telecom/ RDSO		
<p style="text-align: center;">Abstract</p> <p>This document specifies technical specification of LAN Switch for IT applications in Indian Railways.</p>		

DOCUMENT CONTROL SHEET

NAME	ORGANIZATION	FUNCTION	LEVEL
Director/ Telecom-II	RDSO	Member	Prepare
Executive Director/ Telecom	RDSO	-	Approve

REVISIONS:

Version	Chapter/ Annexure	Revision	Effective Month/Year
RDSO/SPN/TC/ 83/2008	-	FIRST ISSUE	August 2008
RDSO/SPN/TC/ 83/2014, Rev. 1.0	-	SECOND ISSUE	March 2014

TABLE OF CONTENTS

Sr. No.	Item	Page No.
1.	Introduction	6
2.	General Requirements	6
3.	LAN Switch Layer 3 type suitable for Central & Divisional Hubs	8
4.	LAN Switch Layer 2 type suitable for Sub Divisional Hubs	14
5.	LAN Switch Suitable for End Locations (24 Ports)	19
6.	LAN Switch Suitable for End Locations (8 Ports)	23
7.	Regulatory Compliance of LAN Switches	26
8.	Marking & Packing	27
9.	Documentation	27

I. SUMMARY:

This document covers the technical requirements of LAN Switches for IT applications specifically for UTS & PRS applications for Indian Railways.

II. SOURCE:

1. Draft specification RDSO/ SPN/ TC/ 83 /2008, Rev 0.0 have been prepared by RDSO, Lucknow as per Railway Board letter No. 2006/Tele/TC/1 dated 28/07/2008.
2. Revision 1.0 of the Draft specification RDSO/ SPN/ TC/ 83 /2014, Rev 1.0 have been prepared by RDSO, Lucknow as per Railway Board letter No. 2010/Tele/9(3)/1, dated 15.03.2012

III. FOREWORD:

RDSO/ SPN specification is issued as draft specification. This specification is circulated to customers/ Railways and field inspection units for comments.

In the absence of IRS specification, procurement may be made as per RDSO/ SPN specification.

Wherever, reference to any specifications appears in this document, it shall be taken as a reference to the latest version of that specification unless the year of issue of the specification is specifically stated.

**RESEARCH DESIGNS & STANDARDS ORGANIZATION
MINISTRY OF RAILWAYS
MANAK NAGAR, LUCKNOW**

Draft Specification of LAN Switch

Draft Specification No: RDSO/SPN/TC/83 /2014 (Revision 1.0)

1.0 INTRODUCTION:

- 1.1 This specification lays down the technical requirements for the Local Area Network (LAN) Switches used for LAN connection applications in the Indian Railways network. The LAN switch shall be used in Internet / Intranet as mechanism for allowing interconnection of servers, clients, RAS, Routers and other devices used in the Internet, Intranet, PRS, UTS, FOIS, COIS and other applications environments in Indian Railways.
- 1.2 A LAN switch is a local area networking device operating at Layer 1 through Layer 2 and Layer 3 of the seven layer ISO-OSI model. The basic function of a LAN switch is to forward packets from one port to another.
- 1.3 In the path determination function, a switch creates dynamic tables based on addresses learnt on the network. The creation and dynamic update of this switching table is part of the intelligence of the switch. Since the switching occurs in the hardware using Application Specific Integrated Circuits (ASICs), the latency of a switch shall be very low as compared to shared media repeaters.

2.0 GENERAL REQUIREMENTS:

- 2.1 The LAN switch shall be fully solid state and adopt state of the art technology.
- 2.2 The LAN switch shall be compact, composite construction and lightweight. The actual dimension and weight of the equipment shall be furnished by the manufactures.
- 2.3 All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.
- 2.4 All cables shall be of Gigabit Ethernet ready standards.
- 2.5 The LAN switch shall have adequate cooling arrangements.

- 2.6 Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.
- 2.7 Each terminal block and individual tags shall be numbered suitably with clear identification code and shall correspond to the associated wiring their circuit diagrams and functions.
- 2.8 The LAN switch shall be designed for continuous operation. The manufacturer shall furnish the MTBF (Mean Time Between Failure) and MTRR (Mean Time to Restore) predicted and observed values along with calculations.
- 2.9 Suitable visual indications for healthy, unhealthy conditions and for non-urgent alarms shall be provided.
- 2.10 The design of the equipment shall not allow plugging of a module in a wrong slot or upside down.
- 2.11 The removal or addition of any interface cards shall not disrupt traffic on other cards.
- 2.12 In the event of a nig found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.
- 2.13 In the event of a full systems failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.
- 2.14 Necessary alarms (indicators) for indication of faults at various levels of hardware shall be provided on the individual modules.
- 2.15 A power down condition shall not cause loss of connection configuration data storage.
- 2.16 The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with Indian Railways network for voice, data and transmission systems, as the case shall be.
- 2.17 The system hardware / software shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium / century, leap year etc., in the normal functioning of the system.
- 2.18 The LAN switch shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.

3.0 LAN SWITCH LAYER 3 TYPE SUITABLE FOR CENTRAL & DIVISIONAL HUBS:

3.1 Physical Specification:

3.1.1 The LAN switch shall be rack mountable with 24 Nos. 10/100/1000 Base-T ports with 4 Nos. 10/100/ 1000 Base-T/1000 Base-X ports.

3.2 General Specification:

3.2.1 The LAN switch shall be available with minimum 56 Gbps Switch Fabric.

3.2.2 The LAN switch shall have minimum packet forwarding rate of 41 million packets per second at 64-byte packet length.

3.2.3 The LAN switch shall support minimum 12000 MAC address.

3.2.4 The LAN switch shall support 11000 Unicast routes, 1000 IGMP and multicast groups.

3.2.5 The switch should be stackable with a minimum stacking bandwidth of atleast 64Gbps, through dedicated stack ports. It should support stacking of atleast 4 units high.

3.2.6 The switch shall have dual hot-pluggable redundant power supply (RPS) module. The switch should not undergo reboot (no downtime) while adding/removing of redundant power supply.

3.2.7 The switch shall be able to work on both IPv4 and IPv6 (dual stack) from day one.

3.2.8 All ports in the switch shall operate at wire-speed / line-rate.

3.2.9 The switch shall be capable of working with AC Power Supply with a voltage varying from 170-240Volts at 50 +/-2 Hz.

3.2.10 It shall have hot swappable fan tray.

3.2.11 The switch shall support 19 inch rack mounting.

3.2.12 The LAN Switch should be PoE compliant as per IEEE802.3af / IEEE802.3at.

3.3 Layer-2 Features:

3.3.1 The LAN switch shall support IEEE 802.1Q VLAN up to 1000 VLANs.

- 3.3.2 It shall support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.
- 3.3.3 It shall support centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the other switches automatically, thus reducing the overhead of creating / modifying / deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting. It shall support GVRP or any other industry standard protocol for VLAN pruning and management.
- 3.3.4 It shall support spanning-tree Port Fast and Port Fast guard for fast convergence.
- 3.3.5 It shall support Port-spanning functionality for measurements using a network analyzer.
- 3.3.6 It shall support 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad.
- 3.3.7 It shall support spanning-tree root guard to prevent other edge switches becoming the root bridge.
- 3.3.8 It shall support IGMP v1, v2 & v3 as well as IGMP v1, v2 & v3 snooping.
- 3.3.9 It shall support Link Aggregation Protocol (LACP).
- 3.3.10 It shall support 802.3ah for Detection of Unidirectional Links and to disable them to avoid problems such as spanning-tree loops and shall support UDLD or any other industry equivalent protocol for unidirectional link detection.
- 3.3.11 It shall support configurable Maximum Transmission Unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes (Jumbo frames) for bridging on Gigabit Ethernet ports
- 3.3.12 It shall 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. It shall support LLDP or LLDP-MED for network discovery.
- 3.3.13 It shall support Multicast VLAN registration.
- 3.3.14 It shall support for switch port auto recovery (err disable) to automatically re-enable a link that is disabled because of a network error.

3.3.15 It shall support for Cross Stack Uplink Fast or equivalent technology to provide for sub second failover.

3.3.16 The switch shall support at least 128 STP instances.

3.4 Layer-3 Features:

3.4.1 The LAN switch shall have HSRP/VRRP.

3.4.2 The LAN switch shall support IP unicast routing protocols (static, RIPv1, and OSPF). It shall support IP unicast routing for full layer3 routing between 2 or more VLANs.

3.4.3 It shall support for advanced routing protocol Border Gateway Protocol Version 4 [BGPv4]) for load balancing and constructing scalable LANs. It shall support BGP+, BGP (support multi-address family).

3.4.4 It shall support Policy-Based Routing (PBR).

3.4.5 It shall support for IP unicast routing capability (static, RIPv1, RIPv2 and OSPFv3 protocols) to forward IP traffic through configured interfaces.

3.4.6 It shall support for Protocol Independent Multicast (PIM) for IP Multicast routing, including PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode.

3.4.7 It shall support for 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.

3.4.8 The switch should support IPv6 routing in hardware including RIPng, and RFC2740 for OSPF for IPv6.

3.5 Quality of Service (QoS) Features:

3.5.1 The LAN switch shall support classification and scheduling as per IEEE 802.1P on all ports. It shall support classification and marking based on IP type of Service (TOS) and DSCP.

3.5.2 It shall have Control- and Data-plane QoS ACLs.

3.5.3 There shall be no performance penalty for highly granular QoS functions.

3.5.4 There shall be four egress queues per port to enable differentiated management of up to four traffic types across the stack.

- 3.5.5 There shall be weighted tail drop (WTD) to provide congestion avoidance or other industry standard protocol.
- 3.5.6 It shall support strict priority queuing mechanisms.
- 3.5.7 Granular Rate Limiting function to guarantee bandwidth in increments shall be as low as 64 kbps.
- 3.5.8 The LAN switch shall provide traffic shaping and rate limiting features (for egress as well as ingress traffic) for specified Host, network, applications etc.
- 3.5.9 Rate limiting support 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 shall be available.
- 3.5.10 There shall be support for Asynchronous data flows upstream and downstream from the end station or on the uplink using ingress policing and egress shaping.
- 3.5.11 Up to 64 aggregate or individual policers for per Fast Ethernet or Gigabit Ethernet port shall be available.
- 3.5.12 There shall be support for Automatic Quality of Service for easy configuration of QoS features for critical applications.
- 3.5.13 It shall support QoS configuration on per switch port basis.

3.6 Network Security Features:

- 3.6.1 The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.
- 3.6.2 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 solutions for security-policy compliance and enforcement before a host is permitted to access the network.
- 3.6.3 It shall support VLAN ACLs (VACLs) on all VLANs to prevent unauthorized data flows from being bridged within VLANs. It shall also support port-based ACLs (PACLs) for Layer 2 interfaces to allow application of security policies on individual switch ports.
- 3.6.4 It shall support MAC Address based filters / Access Control Lists (ACLs) on all switch ports. Shall support Filters/ACLs based on Network Address, Mask, Protocol Type & Socket Type on all switch ports.

- 3.6.5 It shall support unicast MAC filtering to prevent the forwarding of any type of packet with a matching MAC address. Switch shall support per port broadcast, multicast & unicast storm control to prevent degradation of overall system performance occurred due to faulty end equipment.
- 3.6.6 It shall support unknown unicast and multicast port blocking to allow tight control by filtering packets that the switch has not already learned how to forward.
- 3.6.7 It shall have support for SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
- 3.6.8 It shall support private VLAN to provide security and isolation between switch ports to ensure that users cannot snoop on other users' traffic.
- 3.6.9 It shall support Port Mirroring based on port basis / VLAN basis to support intrusion prevention system deployment in different VLANs.
- 3.6.10 It shall support dynamic Arp and 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.
- 3.6.11 IP source guard shall be available to prevent a malicious user from spoofing or taking over another user's IP address by creating a binding table between client's IP and MAC address, port, and VLAN.
- 3.6.12 It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.
- 3.6.13 It shall support MAC address notification to allow administrators to be notified of users added to or removed from the network.
- 3.6.14 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.
- 3.6.15 It shall support DHCP Interface Tracker (Option 82) to augment a host IP address request with the switch port ID.
- 3.6.16 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. It shall support minimum 6 multi-link trunks with 4 multi-link groups.

3.6.17 It shall support multilevel security on console access to prevent unauthorized users from altering the switch configuration.

3.6.18 It shall support BPDU Guard feature, to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.

3.6.19 It shall support spanning-Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes or any other industry standard method/protocol.

3.6.20 It shall have support for min. 2000 access control entries (ACEs).

3.7 Management:

3.7.1 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.

3.7.2 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. The LAN switch shall have support for all nine RMON groups through the use of a mirrored port, which permits traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe.

3.7.3 It shall have Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.

3.7.4 It shall have Domain Name System (DNS) to provide IP address resolution with user-defined device names.

3.7.5 It shall support Trivial File Transfer Protocol (TFTP) and File Transfers Protocol (FTP) to reduce the cost of administering software upgrades by downloading from a centralized location.

3.7.6 It shall support Simple Network Timing Protocol (SNTP) / Network Timing Protocol (NTP) to provide an accurate and consistent time stamp to all intranet switches.

3.7.7 It shall support RMON v1 and v2 standards.

3.7.8 It shall support SNMPv1, SNMPv2, and SNMPv3 and Telnet interface to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management.

- 3.7.9 It shall have a console port with RS-232/RJ-45 interface for configuration & diagnostic purpose.
- 3.7.10 It shall support all the standard MIBs (MIB-I & II).
- 3.7.11 It shall support Telnet & SSH V-2 for command line management.
- 3.7.12 It shall support System & Event logging function as well as forwarding these logs onto a separate server for log management.
- 3.7.13 The LAN switch shall support online software reconfiguration to implement changes without rebooting. For any changes in configuration of switches related to L-2 & 3 functions, VLAN, STP, Security, QoS or firmware, rebooting the switch may be allowed.
- 3.7.14 It shall have comprehensive debugging features required for software & hardware fault diagnosis.
- 3.7.15 It shall support multiple privilege levels to provide different levels of access on console port & telnet sessions.
- 3.7.16 It shall support following user level access, i.e. the user with minimum privileges: PING, TELNET, TRACEROUTE, Display of preconfigured description/label on each interface, Display of Input & output error statistics on all interfaces, Display of Dynamic ARP table, Display of MAC Address table & Display of Routing Table.

4.0 LAN SWITCH LAYER 2 TYPE SUITABLE FOR SUB DIVISIONAL HUBS:

4.1 Physical Specification:

- 4.1.1 The LAN switch shall be rack mountable with 24 Nos. 10/100/1000 Base-T ports with 4 Nos. 10/100/ 1000 Base-T/1000 Base-X ports.

4.2 General Specification:

- 4.2.1 The LAN switch shall be available with minimum 56 Gbps Switching Fabric.
- 4.2.2 The LAN switch shall have minimum packet forwarding rate of 41 million packets per second at 64 byte packet length.
- 4.2.3 The LAN switch shall support minimum 12000 MAC addresses.
- 4.2.4 There shall be 255 IGMP groups.

4.2.5 The switch should be stackable with a minimum stacking bandwidth of at least 40 Gbps stacking for a minimum of 4 units.

4.2.6 The switch should support external redundant power supply (RPS).

4.2.7 The switch shall be able to work on both IPv4 and IPv6 (dual stack) from day one.

4.2.8 All ports in the switch shall operate at wire-speed / line-rate.

4.2.9 The switch shall be capable of working with AC Power Supply with a voltage varying from 170-240Volts at 50 +/-2 Hz.

4.2.10 The switch shall support 19 inch rack mounting.

4.2.11 The LAN Switch should be PoE compliant as per IEEE802.3af / IEEE802.3at.

4.3 Layer - 2 Features:

4.3.1 The LAN switch shall support IEEE 802.1Q VLAN encapsulation. Minimum 255 VLANs per switch and up to 4000 VLAN IDs.

4.3.2 It shall support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.

4.3.3 It shall support centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the other switches automatically, thus reducing the overhead of creating / modifying / deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting.

4.3.4 It shall support spanning-tree Port Fast for fast convergence or any other industry standard protocol.

4.3.5 It shall support 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad.

4.3.6 It shall support spanning-tree root guard or any other industry standard protocol to prevent other edge switches becoming the root bridge.

4.3.7 It shall support IGMP snooping v1, v2 and v3.

4.3.8 It shall support Link Aggregation Protocol (LACP).

- 4.3.9 It shall Support 802.3ah Ethernet Link OAM for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops and support Unidirectional Link Detection (UDLD) or equivalent.
- 4.3.10 It shall 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.
- 4.3.11 It shall support for Switch port auto recovery (err disable) to automatically re-enable a link that is disabled because of a network error.
- 4.3.12 It shall support Multicast VLAN registration.
- 4.3.13 It shall support Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.
- 4.3.14 It shall support LLDP / LLDP-MED including client location information. It shall exchange link and device information in multi vendor networks.
- 4.3.15 It shall support configuration rollback to replace current configuration with any saved configuration file.
- 4.3.16 It shall support link state tracking which provides layer 2 redundancy in the network when used in conjunction with server teaming.
- 4.3.17 It shall support configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes (Jumbo frames) for bridging on Gigabit Ethernet ports.
- 4.3.18 It shall support auto sensing speed on 10/100/1000 ports, auto negotiating half/full-duplex on all ports and Auto-MDIX.

4.4 QoS Features:

- 4.4.1 The LAN switch shall have per-port broadcast, multicast, and unicast storm control.
- 4.4.2 It shall have standard 802.1p CoS and DSCP classification using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number.
- 4.4.3 It shall have Control- and Data-plane QoS ACLs.
- 4.4.4 It shall have no performance penalty for highly granular QoS functions.

- 4.4.5 There shall be four egress queues per port to enable differentiated management of up to four traffic types.
- 4.4.6 There shall be weighted tail drop (WTD) or any other industry standard protocol to provide congestion avoidance.
- 4.4.7 There shall be strict priority queuing mechanisms.
- 4.4.8 Granular Rate Limiting functions to guarantee bandwidth in increments shall be as low as 64 Kbps.
- 4.4.9 Rate limiting support 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 (IPv4 and IPv6) or MAC ACLs), class maps, and policy maps shall be available. ACL should be based on user defined packet content (Max. 6bytes length user defined).
- 4.4.10 There shall be support for Asynchronous data flows upstream and downstream from the end station or on the uplink using ingress policing and egress shaping.
- 4.4.11 There shall be support for Automatic Quality of Service for easy configuration of QoS features for critical applications.

4.5 Network Security Features:

- 4.5.1 The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.
- 4.5.2 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 solutions for security-policy compliance and enforcement before a host is permitted to access the network.
- 4.5.3 It shall support port-based ACLs (PACLs) for Layer 2 interfaces to allow application of security policies on individual switch ports. It shall also support VLAN based filters.
- 4.5.4 It shall support unicast MAC filtering to prevent the forwarding of any type of packet with a matching MAC address. It shall support Unicast and Multicast MAC addresses and associated VLANs.
- 4.5.5 It shall support unknown unicast and multicast port blocking to allow tight control by filtering packets that the switch has not already learned how to forward.

- 4.5.6 It shall support IGMP filtering which shall provide multicast authentication by filtering out no subscribers and limits the number of concurrent multicast streams available per port.
- 4.5.7 It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
- 4.5.8 The switch shall support 2 session of Port Mirroring based on port basis / VLAN basis to support intrusion prevention system deployment in different VLANs. It shall support bidirectional data on mirror port which allows IDS to take action when an intruder is detected.
- 4.5.9 It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.
- 4.5.10 It shall support MAC address notification to allow administrators to be notified of users added to or removed from the network / It shall support SNMP Trap for new MAC notification.
- 4.5.11 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.
- 4.5.12 It shall support DHCP Interface Tracker (Option 82) to augment a host IP address request with the switch port ID.
- 4.5.13 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.
- 4.5.14 It shall support multilevel security on console access to prevent unauthorized users from altering the switch configuration.
- 4.5.15 It shall support BPDU Guard feature, to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- 4.5.16 It shall support Spanning-Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
- 4.5.17 It shall support for up to 512 access control entries (ACEs).

4.6 Management:

- 4.6.1 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.
- 4.6.2 It shall have Remote Monitoring (RMON v1 and v2) software agent to support for enhanced traffic management, monitoring, and analysis.
- 4.6.3 It shall have support for RMON groups through the use of a mirrored port, which permits traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe.
- 4.6.4 It shall have Time-Domain Reflectometer (TDR) or equivalent technology to diagnose and resolve cabling problems on copper ports.
- 4.6.5 It shall have layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination or it shall support OAM 802.3ah.
- 4.6.6 It shall support Trivial File Transfer Protocol (TFTP) and File Transfer Protocol (FTP) to reduce the cost of administering software upgrades by downloading from a centralized location.
- 4.6.7 It shall support Simple Network Time Protocol/Network Timing Protocol (SNTP/NTP) to provide an accurate and consistent timestamp to all intranet switches.
- 4.6.8 It shall support RMON v1 and v2 standards.
- 4.6.9 It shall support SNMPv1, SNMPv2, and SNMPv3 and Telnet interface to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management.
- 4.6.10 It shall support IPV6 management. ACL and QoS and IPv6 Neighbor Discovery.

5.0 LAN SWITCH SUITABLE FOR END LOCATIONS (24 Ports):

5.1 Physical Specification:

- 5.1.1 The LAN switch shall be rack mountable with 24 Nos. 10/100/1000 Base-T ports with 4 Nos. 10/100/ 1000 Base-T/1000 Base-X ports.

5.2 General Specification:

- 5.2.1 The LAN switch shall be available with 48 Gbps Switching Fabric.

5.2.2 The LAN switch shall have minimum packet forwarding rate of 35 million packets per second at 64-byte packet length.

5.2.3 The LAN switch shall support minimum 12000 MAC address.

5.2.4 The LAN switch shall have 255 IGMP groups.

5.2.5 The LAN Switch should be PoE compliant as per IEEE802.3af / IEEE802.3at.

5.2.6 The switch should be stackable with a minimum stacking bandwidth of at least 40 Gbps stacking for a minimum of 4 units.

5.3 Layer-2 Features:

5.3.1 The LAN switch shall support IEEE 802.1Q VLAN encapsulation. Up to 256 VLANs per switch and upto 4000 VLAN IDs.

5.3.2 It shall support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.

5.3.3 It shall support centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the other switches automatically, thus reducing the overhead of creating / modifying / deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting.

5.3.4 It shall support spanning-tree Port Fast guard for fast convergence.

5.3.5 It shall support 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad.

5.3.6 It shall support spanning-tree root guard to prevent other edge switches becoming the root bridge.

5.3.7 It shall support IGMP snooping v1, v2 and v3.

5.3.8 It shall support Link Aggregation Protocol (LACP) as per IEEE 802.3ad.

5.3.9 It shall support 802.3ah Ethernet Link OAM for Detection of Unidirectional Links and to disable them to avoid problems such as spanning-tree loops and support Unidirectional Link Detection (UDLD) or equivalent.

5.3.10 It shall 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.

5.3.11 It shall support for Switch port auto recovery (err disable) to automatically re-enable a link that is disabled because of a network error.

5.3.12 It shall support Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.

5.3.13 It shall support LLDP/LLDP-MED exchange link and device information in multi-vendor networks.

5.3.14 It shall support configuration rollback to any saved configuration can be managed externally via TFTP.

5.3.15 It shall support Auto sensing speed on 10/100/1000 ports, Auto negotiating half/full-duplex on all ports and Auto-MDIX.

5.4 Quality of Service (QoS) Features:

5.4.1 The LAN switch shall have per-port broadcast, multicast, and unicast storm control.

5.4.2 There shall be four egress queues per port to enable differentiated management of up to four traffic types.

5.4.3 There shall be weighted tail drop (WTD) to provide congestion avoidance or any other Industry standard protocol.

5.4.4 There shall be strict priority queuing mechanisms.

5.5 Network Security Features:

5.5.1 The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.

5.5.2 It shall support unicast MAC filtering to prevent the forwarding of any type of packet with a matching MAC address.

5.5.3 It shall support unknown unicast and multicast port blocking to allow tight control by filtering packets that the switch has not already learned how to forward.

5.5.4 It shall support IGMP filtering to provide multicast authentication by filtering out no subscribers and limits the number of concurrent multicast streams available per port.

5.5.5 It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.

- 5.5.6 It shall support Port Mirroring based on port basis / VLAN basis to support intrusion prevention system deployment in different VLANs. It shall support bidirectional data on mirror port which allows IDS to take action when an intruder is detected.
- 5.5.7 It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.
- 5.5.8 It shall support MAC address notification to allow administrators to be notified of users added to or removed from the network or it shall support SNMP Trap for New MAC notification.
- 5.5.9 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.
- 5.5.10 It shall support multilevel security on console access to prevent unauthorized users from altering the switch configuration.
- 5.5.11 It shall support BPDU Guard feature, to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- 5.5.12 It shall support Spanning-Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.

5.6 Management:

- 5.6.1 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.
- 5.6.2 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.
- 5.6.3 It shall have Time-Domain Reflectometer (TDR) or equivalent technology to diagnose and resolve cabling problems on copper ports.
- 5.6.4 It shall have Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.
- 5.6.5 It shall support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location

5.6.6 It shall support Simple Network Time Protocol/Network Timing Protocol (SNTP/NTP) to provide an accurate and consistent time stamp to all intranet switches

5.6.7 It shall support RMON v1 and v2 standards.

5.6.8 It shall support SNMPv1, SNMPv2c, and SNMPv3 and Telnet interface support to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management

6.0 LAN SWITCH SUITABLE FOR END LOCATIONS (8 Ports):

6.1 Physical Specification:

6.1.1 The LAN switch shall be standalone / rack mountable with 8-port 10/100/1000 Mbps with 2 combo 10/100/1000 Base-T/SFP port.

6.2 General Specification:

6.2.1 The LAN switch shall be available with minimum 10 Gbps Switching Fabric.

6.2.2 The LAN switch shall have minimum packet forwarding rate of 13 million packets per second at 64-byte packet length.

6.2.3 The LAN switch shall support minimum 4000 MAC address.

6.2.4 The LAN switch shall have 255 IGMP groups.

6.2.5 The LAN Switch should be PoE compliant as per IEEE802.3af.

6.2.6 The switch shall be capable of working with AC Power Supply with a voltage varying from 170-240Volts at 50 +/-2 Hz.

6.3 Layer-2 Features:

6.3.1 The LAN switch shall support IEEE 802.1Q VLAN encapsulation. Minimum 64 VLANs.

6.3.2 It shall support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.

6.3.3 It shall support centralized VLAN Management. VLANs created on the Core Switches shall be propagated to all the other switches automatically, thus reducing the overhead of creating / modifying / deleting VLANs in all the switches in turn eliminating the configuration errors & troubleshooting.

- 6.3.4 It shall support spanning-tree Port Fast guard for fast convergence or any other industry standard.
- 6.3.5 It shall support 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad.
- 6.3.6 It shall support spanning-tree root guard to prevent other edge switches becoming the root bridge.
- 6.3.7 It shall support IGMP snooping v1, v2 and v3.
- 6.3.8 It shall support Link Aggregation Protocol (LACP) as per IEEE 802.3ad.
- 6.3.9 It shall support 802.3ah Ethernet Link OAM for Detection of Unidirectional Links and to disable them to avoid problems such as spanning-tree loops and support Unidirectional Link Detection (UDLD) or equivalent.
- 6.3.10 It shall 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.
- 6.3.11 It shall support for Switch port auto recovery (err disable) to automatically re-enable a link that is disabled because of a network error.
- 6.3.12 It shall support Local Proxy Address Resolution Protocol (ARP) to work in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth
- 6.3.13 It shall support LLDP / LLDP-MED exchange link and device information in multi vendor networks.
- 6.3.14 It shall support configuration rollback to replace current configuration with any saved configuration file.
- 6.3.15 It shall support Auto sensing speed on 10/100/1000 ports, Auto negotiating half/full-duplex on all ports and Auto-MDIX.

6.4 Quality of Service (QoS) Features:

- 6.4.1 The LAN switch shall have per-port broadcast, multicast, and unicast storm control.
- 6.4.2 There shall be four egress queues per port to enable differentiated management of up to four traffic types.

6.4.3 There shall be weighted tail drop (WTD) to provide congestion avoidance or any other Industry standard protocol.

6.4.4 There shall be strict priority queuing mechanisms.

6.5 Network Security Features:

6.5.1 The LAN switch shall support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.

6.5.2 It shall support unicast MAC filtering to prevent the forwarding of any type of packet with a matching MAC address.

6.5.3 It shall support unknown unicast and multicast port blocking to allow tight control by filtering packets that the switch has not already learned how to forward.

6.5.4 It shall support IGMP filtering to provide multicast authentication by filtering out no subscribers and limits the number of concurrent multicast streams available per port.

6.5.5 It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.

6.5.6 It shall support Port Mirroring based on port basis / VLAN basis to support intrusion prevention system deployment in different VLANs. It shall support bidirectional data on mirror port which allows IDS to take action when an intruder is detected.

6.5.7 It shall support RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.

6.5.8 It shall support MAC address notification to allow administrators to be notified of users added to or removed from the network.

6.5.9 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.

6.5.10 It shall support multilevel security on console access to prevent unauthorized users from altering the switch configuration.

6.5.11 It shall support BPDU Guard feature, to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.

6.5.12 It shall support Spanning-Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.

6.6 Management:

6.6.1 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.

6.6.2 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.

6.6.3 It shall have Time-Domain Reflectometer (TDR) or equivalent technology to diagnose and resolve cabling problems on copper ports.

6.6.4 It shall have Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.

6.6.5 It shall support Trivial File Transfer Protocol (TFTP) and File Transfer Protocol (FTP) to reduce the cost of administering software upgrades by downloading from a centralized location

6.6.6 It shall support Simple Network Time Protocol/Network Timing Protocol (SNTP/NTP) to provide an accurate and consistent time stamp to all intranet switches

6.6.7 It shall support RMON v1 and v2 standards.

6.6.8 It shall support SNMPv1, SNMPv2c, and SNMPv3 and Telnet interface support to deliver comprehensive in-band management, and a CLI-based management console to provide detailed out-of-band management

7.0 REGULATORY COMPLIANCE OF LAN SWITCHES:

7.1 The LAN switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards.

7.2 The LAN switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC.

7.3 The LAN switch shall conform to the Electromagnetic Compatibility (EMC) requirement as per the following standards and limits indicated therein:

- EN55022 class A, FCC class A, VCCI class A Immunity: EN55024, EN61000-3- levels 2.

7.4 The operating personnel shall be protected against shock hazards as per IS 8473 (1993) – Guide on the effects of current passing through the human body (equivalent to IEC publications 479 – 1984).

7.5 The switch shall be manufactured in accordance with international quality standards ISO9001:2008 for which manufacturer should be duly accredited.

8.0 MARKING & PACKING:

8.1 The following information shall be clearly marked at a suitable place on each equipment:

- i) Name and Address of the manufacturer.
- ii) Month & Year of the manufacturing.
- iii) Serial number of Equipment.

8.2 The equipment and its sub assemblies shall be packed in thermocole boxes and the empty spaces shall be filled with suitable filling material. Before keeping in the thermocole box, the equipment shall be wrapped with bubble sheet. The equipment shall be finally packed in a wooden case of sufficient strength so that it can withstand bumps and jerks encountered in a road/rail journey.

9.0 DOCUMENTATION:

The supplier shall provide the complete operation, maintenance and installation manuals in English for the product under procurement.
