

NATIONAL PAYMENTS CORPORATION OF INDIA

C-9, 8th Floor, RBI Premises ,Bandra-Kurla Complex Bandra (E), Mumbai-400 051

Requirement for L3 Switches

NPCI requires the following

1. L3 switch with (48*10/100/1000 ports auto negotiating) – 2 no's
2. SFP ports – 4
3. Fiber Cable to connect from 2nd floor to 8th floor
 - A. Fiber cable per meter
 - B. Cabling charges per meter

The detailed specification for L3 Switch is as under.

Specifications for L3 SWITCH – 2 Nos. of 48 ports

L3 Switches should meet the following specifications:-

GENERAL FEATURES

1. The switch should have minimum 48 x 10/100/1000 Ports auto negotiating with four SFP and two redundant power systems (RPS)
2. The Switch should be Stackable and should be able to stack up to 8 switches in a single stack
3. The stacking ports should be separate from the normal uplink ports

PERFORMANCE

4. Should support 32-Gbps switching fabric capacity
5. Forwarding rate – 38.7 mpps.
6. Support for up to 12,000 MAC addresses, up to 20,000 unicast routes & 1000 IGMP groups and multicast routes.
7. Configurable MTU of upto 9000 bytes with the maximum Ethernet frame size of 9018 bytes for bridging on Gigabit Ethernet ports and upto 1546 bytes for bridging and routing on Fast Ethernet ports

ADDITIONAL FEATURES

8. Ether Channeling - IEEE 802.3ad or port aggregation technologies

9. Unidirectional Link Detection Protocol on fibre ports
10. Cross-Stack EtherChannel
11. IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP), Per-VLAN Rapid Spanning Tree (PVRST+)

LAYER-2 FEATURES

12. IEEE 802.1Q VLAN encapsulation. Up to 1005 VLANs per switch or stack and upto 4000 VLAN IDs
13. Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.
14. Centralized VLAN Management. VLANs created on the Core Switches should 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.
15. Spanning-tree PortFast and PortFast guard for fast convergence
16. 802.1d, 802.1s, 802.1w, 802.3ad
17. Spanning-tree root guard to prevent other edge switches becoming the root bridge.
18. IGMP snooping v1, v2 and v3
19. Support for Detection of Unidirectional Links and to disable them to avoid problems such as spanning-tree loops.
20. 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.
21. Support for Switch port autorecovery (errdisable) to automatically reenale a link that is disabled because of a network error.
22. Support for CrossStack UplinkFast to provide increased redundancy and network resiliency through fast spanning-tree convergence (less than 2 seconds) across a switch stack

LAYER-3 FEATURES

23. Basic IP unicast routing protocols (static, RIPv1, and RIPv2)
24. Support for IPv6 unicast routing capability (static, RIP, and OSPF protocols) to forward IPv6 traffic through configured interfaces in hardware
25. Support for Advanced IP unicast routing protocols (OSPF, , and Border Gateway Protocol Version 4 [BGPv4]) for load balancing and constructing scalable LANs. Policy-Based Routing (PBR)

26. 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.
27. Support for Distance Vector Multicast Routing Protocol (DVMRP) tunneling to interconnect two multicast-enabled networks across nonmulticast networks.
28. 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.

QoS FEATURES

29. Standard 802.1p CoS and DSCP
30. Control- and Data-plane QoS ACLs
31. Four egress queues per port to enable differentiated management of up to four traffic types across the stack.
32. Weighted tail drop (WTD) to provide congestion avoidance
33. Strict priority queuing mechanisms
34. Granular Rate Limiting function to guarantee bandwidth in increments as low as 8 kbps.
35. 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.
36. Support for Asynchronous data flows upstream and downstream from the end station or on the uplink using ingress policing and egress shaping.
37. Up to 64 aggregate or individual policers for per Fast Ethernet or Gigabit Ethernet port.
38. Support for Automatic Quality of Service for easy configuration of QoS features for critical applications.

NETWORK SECURITY FEATURES:-

39. IEEE 802.1x to allow dynamic, port-based security, providing user authentication.
40. VLAN ACLs (VACLs) on all VLANs to prevent unauthorized data flows from being bridged within VLANs. Port-based ACLs (PACLs) for Layer 2 interfaces to allow application of security policies on individual switch ports.
41. Standard and Extended IP security router ACLs (RACLs) to define security policies on routed interfaces for control- and data-plane traffic.

42. Unicast MAC filtering to prevent the forwarding of any type of packet with a matching MAC address.
43. Unknown unicast and multicast port blocking to allow tight control by filtering packets that the switch has not already learned how to forward.
44. Support for SSHv2, Kerberos, and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
45. Private VLAN to provide security and isolation between switch ports, helping ensure that users cannot snoop on other users' traffic.
46. The switch should support Port Mirroring based on port basis / vlan basis to support intrusion prevention system deployment in different VLANs.
47. AAA authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.
48. MAC address notification to allow administrators to be notified of users added to or removed from the network.
49. 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.
50. 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.
51. Multilevel security on console access to prevent unauthorized users from altering the switch configuration.
52. BPDU Guard feature, to shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
53. Spanning-Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
54. Support for up to One thousand access control entries (ACEs).

MANAGEMENT:-

55. CLI support to provide a common user interface and command set with all routers and switches of the same vendor
56. For enhanced traffic management, monitoring, and analysis, the Embedded Remote Monitoring (RMON) software agent should support four RMON groups (history, statistics, alarms, and

events). All nine RMON groups should be supported through a SPAN port, which permits traffic monitoring of a single port, a group of ports, or the entire stack from a single network analyzer or RMON probe.

57. Layer 2 trace route of ease troubleshooting by identifying the physical path that a packet takes from source to destination.
58. Network Timing Protocol (NTP) to provide an accurate and consistent timestamp to all intranet switches.
59. RMON I and II standards
60. SNMPv1, SNMPv2c, and SNMPv3
61. Out-of-band Ethernet management port along with RS-232 console port

Terms and Conditions:

Payment terms:

- 1.90% on delivery and successful installation
- 2.10% against Bank Guarantee or end of the year.
3. Delivery should be within 5 working days from the date of release of PO
4. Onsite support for one year (24*7) with 4 hours response and resolution time.

Interested bidders may send the sealed quotations on or before 28th June 2010 by 3 PM.

To the following address:

Chief Executive Officer

National Payments Corporation of India

C-9, 8th Floor,

RBI premises,

Bandra Kurla Complex,

Bandra (East)

Mumbai- 400051

Tel: 022- 2657 3150.

Contact Person:

Satish Gantayat-8108108638

Email: satish.gantayat@npci.org.in