संयुक्त निदेशक का कार्यालय,
बाढ़ प्रबंधन सुधार सहायक केन्द्र,
जल संसाधन विभाग, अनिसाबाद, पटना

कोटेशन आमंत्रण सूचना

पत्रांक:-बा०प्र०सु०स०के०-30/2013-722 पटना, दिनांक:- 07/12/2015

बाढ़ प्रबंधन सुधार सहायक केन्द्र, द्वितीय तल, जल संसाधन भवन, अनिसाबाद, पटना-2 में निम्न सामग्रियो के आपूर्ति हेतु मुहरबंद लिफाफे में मान्यताप्राप्त/निबंधित आपूर्तिकर्ता/फर्मो से कोटेशन दिनांक-24/12/2015 को 3.00 बजे अपराह्न तक आमंत्रित किये ,जाते हैं । कोटेशन उसी दिन अपरहन 3.30 में खोला जायेगा । जिसमें कोटेशनदाता अथवा उनके प्राधिकृत प्रतिनिधि उपस्थित रह सकते हैं ।

विवरण:-

क्रमांक	सामग्रियों के नाम	मात्रा	प्रति इकाई दर (सभी करों सहित) रू० में	अभ्युक्ति
1	2	3	4	5
1.	Firewall (UTM) (with five year support, installation, commissioning etc. all complete.)	1 No		
2.	L-3 Switch, 24 port (with five year support, installation, commissioning etc. all complete.)	1 No		
3.	Router & Load balancer (with five year support, installation, commissioning etc. all complete.)	1 No		
4.	Network Attached Storage (NAS) (2TB) (with installation, commissioning etc. all complete.)	6 Nos		
5.	32 GB Pen Drive (Good Quality)	20 Nos		

O/C

शर्तें:-

1. बिना कारण बताये किसी कोटेशन या सारे कोटेशन को रद्द करने तथा एक से अधिक कोटेशनदाताओं के बीच कार्य बटवारे का अधिकार अधोहस्ताक्षरी को सुरक्षित रहेगा ।
2. कोटेशन के साथ कोटेशनदाता को अपने फर्म का निबंधन प्रमाणपत्र, आयकर सफाया प्रमाणपत्र, वैट क्लियरेंस प्रमाणपत्र एवं बिक्रीकर क्लियरेंस प्रमाणपत्र की स्व अभिप्रमाणित छाया प्रति सलंग्न करना होगा ।
3. सशर्त कोटेशन स्वीकार नही किया जायेगा ।
4. सामग्रियो की विशष्टियों एवं कोटेशन संबंधी विशेष जानकारी हेतु अधोहस्ताक्षरी के कार्यालय से संपर्क किया जा सकता है ।
5. सामग्रियो की आपूर्ति के साथ-साथ अघिष्ठापन एवं कमीशनिंग इत्यादि आपूतिकर्त्ता को करना होगा।
6. कोटेशन प्राप्ति की तिथि को अवकाश घोषित होने की स्थिति में अगले कार्य दिवस तक कोटेशन प्राप्त किया जाएगा एवं उसी दिन खोला जाएगा ।

विश्वासभाजन

7/12/15

(गणेश प्रसाद)

संयुक्त निदेशक

Technical Specification of the proposed components :

L3 Managed Switch		
Hardware Features		
	Description	**Compliance (Yes/No)**
1	Fixed configuration stackable managed switch	
2	Stackable up to 4 units	
3	24 x 10/100/1000 Base-T from day 1	
4	Should support 4 x 10 Gigabit Ethernet Uplink ports (should not be shared with fixed ports)	
5	Switching Fabric - 125 Gbps or more	
6	Forwarding Rate - 92 Mpps or more	
General Features		
1	Modular Operating System with resource separation	
2	Restart process independently	
3	Configurable up to 16000 MAC addresses	
4	Should have 1 GB or more Flash memory	
5	Should have at least 512 MB DRAM	
6	Support for 6,000 unicast routes	
7	Support for 9216 bytes (Jumbo frames)	
8	Should have 8 hardware queues per port	
9	Should support RPS	
Layer 2 Features		
1	Support for IEEE 802.1w Rapid Spanning Tree Protocol	
2	VLAN / Spanning Tree Support	
3	Support IEEE 802.1Q VLAN, Voice VLAN with 1000 VLAN’s.	
4	Port based VLAN, MAC based VLAN	
5	Link Aggregation Control Protocol with 32 groups	
6	Multiple instances of Spanning Tree Protocol (MSTP)	
Routing Services		
1	Basic IP routing protocols (static, Routing Information Protocol Version 1 [RIPv1], and RIPv2) from Day 1	
2	Support for OSPF v1/v2, IGMP v1/v2/v3, PIM by license upgrade.	
3	Support for Proxy ARP	
4	Support for IPv6 static routing	
Protocol Support		
1	IEEE 802.1Q, 802.1p, 802.1D, 802.3x, 802.3ad, 802.1w, 802.1s.	
2	IEEE 802.3u 100BASE-TX specification.	
3	IEEE 802.3ab 1000BASE-T specification.	
5	RMON I and II standards.	
6	SNMPv1, SNMPv2c, SNMPv3.	

7	IGMP, DiffServ Code Point field (DSCP), PIM.	
Security Features		
1	DHCP snooping, Access control lists, Private VLAN	
2	Multicast Filtering	
3	VLAN based ACL (VACLs) and Port-based ACLs (PACLs).	
4	Switched Port mirroring (Port, VLAN, ACL)	
5	1500 access control entries (ACEs).	
6	Control Plane DoS Protection	
7	Support for Terminal Access Controller Access Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS).	
8	Should be able to support Network Admission Control.	
9	Dynamic ARP Inspection, IP source Guard, MAC Limiting	
QoS Features		
1	Layer 2/Layer3 QoS	
2	Congestion Avoidance Mechanism	
3	802.1p class of service (CoS) and Differentiated Services Code Point (DSCP).	
4	L2/L3/L4 traffic classification.	
5	Rate Limiting for guaranteed bandwidth	
6	Queue servicing:- Shaped round robin / Shaped Deficit Weighted Round-Robin and strict priority queuing, Weighted tail drop, Ingress traffic policing, Egress traffic shaping.	
7	Congestion avoidance : Granular rate limiting & Jumbo Frames	
8	Strict Priority Scheduling	
9	Eight egress queues per port help enable differentiated management of different traffic types across the switch.	
Management Features		
1	Web / GUI based Management	
2	Telnet and TFTP access	
3	RMON - Remote Monitoring (RMON) with 4 RMON groups (history, statistics, alarms, and events).	
4	SNMP agent - SNMPv1, SNMPv2c, SNMPv3.	
5	Configuration and image rollback	
Certification		
1	EAL3 or above	

Note: - supply, install and configure at FMISC office.

Firewall (UTM)

Features	Description	Compliance
Interface (on-board)	4 x SFP + 6 10/100/1000 Copper	
Module options	8 modular slots : T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, DS3/E3, Gigabit Ethernet ports (PoE+), 10G	
Memory	DRAM : 2GB Flash : 2 GB	
Operating system	• Modular OS • Separated control & data plane • Protected memory for stability	
Firewall performance	5 Gbps	
Firewall performance (HTTP)	1.5 Gbps	
Firewall plus routing throughput	700 Kpps	
VPN performance (AES256+SHA-1/3DES+SHA-1 VPN)	1000 Mbps	
IPSec VPN tunnels	2000	
Connections per second	25,000	
Maximum concurrent sessions	350,000	
IPS performance	800 Mbps	
Layer 2 switching	• VLAN 802.1Q • Link Aggregation 802.3ad/LACP • Jumbo Frame • STP, RSTP, MSTP • Authentication 802.1x Port based and multiple supplicant	

Routing	• Static routes • RIPv2 • OSPF (700K routes, 55 instances) • BGP (700K routes, 55 instances) • ECMP (700K routes, 55 instances) • IS-IS	
MPLS	• Circuit cross-connect (CCC) • Translational cross-connect (TCC) • LDP •Multicast VPNs • Virtual private LAN service (VPLS) • RSVP • Secondary and standby label-switched paths (LSPs) • OSPF and IS-IS traffic engineering extensions	
IPv6	• OSPFv3 • RIPng • IPv6 Multicast Listener Discovery (MLD) • BGP • ISIS	
Multicast	Multicast ((Internet Group Management Protocol (IGMPv3), PIM, Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), source-specific)	
Traffic management	• Marking, policing, and shaping • Class-based queuing with prioritization • Weighted random early detection • Queuing based on VLAN, data-link connection identifier, interface, bundles, or filters	
Application Security	• Application awareness and classification	

	• Nested application support • User-role based policies • SSL inspection • Classification based on risk level, user ID, zones, source, and destination addresses, as well as volumes.	
Wireless	• Support for In-built Wireless Controller with more than 4 Access points • 3G /4G LTE Bridge support	
Unified Threat Management (Support)	• Antivirus • Antispyware • Anti-adware • Antikeylogger • Antispam • Web filtering • Content filtering	
Virtualization	• Security zone : 95 • Virtual router : 128 • VLAN : 3950	
Security	• Security policies - 7000 • Firewall, zones, screens, policies • Stateful firewall, ACL filters • DoS and DDoS protection (anomaly-based) • Prevent replay attack; Anti-Replay • Unified Access Control	
User Authentication	• Third-party user authentication RADIUS, RSA SecureID, LDAP • RADIUS accounting • XAUTH VPN, Web-based, 802.X authentication	

	• PKI certificate requests • Certificate Authorities : VeriSign, Entrust, Microsoft, RSA Keon, iPLanet, (Netscape), Baltimore, DoD PK	
VPN	• Tunnels (generic routing encapsulation, IP-in-IP, IPsec) • IPsec, DES, 3DES, AES encryption • MD5 and SHA-1 authentication	
High availability	• VRRP •Active/active—L3 mode •Active/passive—L3 mode • Stateful failover • Dual Power Supplies from Day 1	
System management	• Web UI • CLI • Configuration rollback	

Note: - supply, install and configure at FMISC office.

Link Load Balancer	
Hardware	**Compliance (Yes/No)**
should be appliance based solution with purpose built hardware for high performance.	
Minimum 4 GB RAM scalable to 8GB RAM.	
The appliance should have minimum 4 x1G copper ports scalable to 8 . It should support 2x 10 G Ports	
The appliance should have 5 Gbps of system throughput and scalable to 10 Gbps on same appliance.	
Should provide 4M concurrent connections.	
appliance should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.	

Load balancing Features	
Support for multiple internet links in Active-Active load balancing and active-standby failover mode.	
Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, target proximity and dynamic detect.	
Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity & dynamic detect.	
Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.	
IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.	
Domain name support for A-record, MX record for inbound load balancing.	
Dynamic detect (DD) based health check for intelligent traffic routing and failover	
In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.	
Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.	
Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.	
Should support persistency features including RTS (return to sender) and ip flow persistence.	
The appliance should support software based site selection feature to provide global load balancing features on same appliance	
Should support global load balancing algorithms like global round robin (grr), VIP based weighted global round robin, global connection overflow, global least connections, IP overflow, Proximity etc.,	
High Availability and Cluster	
Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.	
Stateful session failover with N+1 clustering support when deployed in HA mode	
Should support USB based FFO link to synchronize configuration at boot time of HA	
Support for multiple communication links for realtime configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc.. and heartbeat information	
should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speedup the failover	
should support for secondary communication link for backup purpose	
should support floating IP address and group for statefull failover support. Appliance must have support 256 floating ip address for a floating group	
should support built in failover decision conditions including unit failover, group failover and reboot	

should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway	
Configuration synchronization at boot time and during run time to keep consistence configuration on both units.	
Security and Application Performance	
Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.	
should support TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.	
TCP optimization option configuration must be defined on per virtual service basis not globally.	
software based compression for HTTP based application,SSL acceleration and high speed HTTP processing on same appliance.	
Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues.	
Should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols.	
Should support rate shaping for setting user defined rate limits on critical application.	
should support integrated firewall module to protect the device itself from network based DOS and DDOS attacks.	
Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation .	
Management	
The appliance should have extensive report like http squid or customized http logging with inbuilt tcpdump and log collecting functionality	
The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.	
Should support XML-RPC for integration with 3rd party management and monitoring of the devices.	
The appliance should provide detailed logs and graphs for real time and time based statistics	
Appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback	
The system should support led warning and system log alert for failure of any of the power and CPU issues	
Technical center must be available in India from last 3years.	

Note: - supply, install and configure at FMISC office.

SPECIFICATION FOR UP-GRADATION OF EXISTING DELL POWER VAULT Nx3100 (NAS)

S. NO	STORAGE SPECIFICATION		Remarks
	Storage Slots	12 Nos.	Existing
1	Occupied Slots	4 Nos	Existing
2	Free Slots	6 Nos.	Existing
3	**Required Storage**	**12 TB**	Required
4	Supply, install and configure , backup original old data and restore backup data in NAS.		

GIS Specialist Database Specialist Web Master System Manager