

iv. Router shall support NTP (Network Time Protocol) or SNTP (Simple Network Time Protocol) for date & time synchronization from NTP Server. The router shall also be configured as NTP Server for serving the time.

v. Support for both TCP and UDP at layer 4

vi. Sub networking

vii. Classless Inter Domain Routing (CIDR)

viii. Variable Length Subnet Masking (VLSM)

ix. IEEE 802.1Q based VLAN tagging

x. VRRP

The router shall support following WAN protocols:

i. PPP

ii. Multi-link PPP

iii. HDLC

The router shall support static as well as dynamic routing with following IP routing protocols:

i. OSPF Version 3

ii. BGP Version 4

iii. Multi-Protocol BGP Version 4

The Router shall have following IP Routing features:

i. Bidirectional Forwarding Detection (BFD) for Static and OSPF Routing.

ii. Option to define a Router as Designated Router (DR) in OSPF Domain.

iii. Option to define "Point to Point" and "Point to Multi-point" links in OSPF Domain.

iv. Option to change the LSA and SPF timers as well as other timers / counters in OSPF.

v. Router shall support tracking the reachability to remote destination which is not directly connected and thereby deciding the validity of static routes etc.

Router shall support following quality of service (QoS) features:

i. Weighted Fair Queuing (WFQ)/Weighted Round Robin (WRR) or equivalent queuing mechanism

ii. IP Precedence i.e. Priority based on TOS field of IPv4 and IPv6

iii. Differentiated Services (Diff Serve) i.e. Priority based on DS Field of the IPv4 and IPv6.

iv. Weighted Random Early Detection for congestion avoidance.

The router shall have minimum eight hardware queues per port feature for assignment of bandwidth/priority to a group(s) of applications.

The router shall support forwarding of traffic in load-balancing mode on links with equal metric based on Per session or Per destination-based load balancing.

The router shall support following Security features:

i. PAP and CHAP

ii. Data Encryption as per DES, 3DES and AES Standards

iii. Generic Routing Encapsulation

iv. Hardware Accelerated IPsec based Point to Point secure tunnels for minimum 100 IPsec tunnels and minimum IPsec throughput of 200 kbps.

v. Access lists based on Network Address, Mask, Protocol Type and Socket Type

vi. Access list violation Logging & Accounting

vii. MD5 Route Authentication

viii. Controlled SNMP Access through the use of SNMP with MD5 Authentication.

ix. Multiple Privilege levels to provide different levels of access

x. Remote Authentication Dial in User Service (RADIUS)

The Router shall support authentication, authorization and accounting through RADIUS / TACACS+.