सत्यमेव जयते

वर्गीय आवश्यकताओं के लिए मानक

टीईसी ४८०५०: २०२५

(सं: टीईसी ४८०५०:२०२४ को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS

TEC 48050:2025

(Supersedes No.TEC 48050:2024)

एम पी एल एस आधारित ट्रांसपोर्ट नेटवर्क के लिए राउटर

Router for MPLS Based Transport Network

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलालभवन, जनपथ, नई दिल्ली-११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 04 : Dec, 2025

FOREWORD

Telecommunication Engineering Centre(TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This Standard for Generic Requirements is for Router for MPLS based Transport Network to be deployed by the service providers in their Routing and aggregation layers.

CONTENTS

HISTORY SHEET

Sl.No.	Standard/document *No.*	*Title*	*Remarks*
1.	TEC/GR/IT/TCP-004/01 FEB-14	GR for Router for MPLS Based Transport Network	1st issue
2.	Standard Number TEC 48050:2022	Standard for Generic Requirements for Router for MPLS Based Transport Network	2nd issue Non-Chassis Routers Categories included
3.	Standard Number TEC 48050:2024	Standard for Generic Requirements for Router for MPLS Based Transport Network	3rd issue
4.	Standard for GR Number TEC 48050:2025	Standard for Generic Requirements for Router for MPLS Based Transport Network	4th issue

REFERENCES

S.No.	*Document No.*	*Title/Document Name*
[1]	ITU-T G.8031	Ethernet SNC based protection
[2]	ITU-T G.8032	EoMPLS ring protection for both S-VID and B-VID
[3]	ITU-T G.8110.1v2	Architecture of MPLS-TP Layer Network
[4]	ITU-t G.8112	Interfaces for the MPLS-TP Hierarchy
[5]	ITU-T G.8121v2	Characteristics of MPLS-TP Network Equipment Functional Blocks
[6]	ITU-T G.8131v2	MPLS SNC
[7]	ITU-T G.8132	MPLS ring protection for non MPLS-TP traffic with 16 nodes over a diameter of 1200Km
[8]	ITU-T G.8151/ T.1734	Management aspects of the T-MPLS network element
[9]	IEEE 802.1ab	Link-layer discovery protocol
[10]	IEEE 802.1d	Spanning Tree Protocol
[11]	IEEE 802.2	Logical Link Control (LLC)
[12]	IEEE 802.3	Ethernet Interface Standards by IEEE
[13]	IEEE 802.3ah, IEEE 802.1ag	Ethernet OAM, Connectivity Fault Management (CFM)
[14]	IEEE 802.3ba	40G, 100G interface
[15]	Qm 118, qm 205,qm 206,	Quality Manuals issued by QA Circle of BSNL

	qm 210, qm 301, qm 333, qm 324	
[16]	Tec/emi/tel-001	EMI / EMC Requirements
[17]	RFC 1075	Distance Vector Multicast Routing Protocol
[18]	RFC 1112	Host Extensions for IP Multicasting
[19]	RFC 1142	OSI ISIS Intra-domain Routing Protocol
[20]	RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
[21]	RFC 1215	A Convention for Defining Traps for use with the SNMP
[22]	RFC 1370	Applicability Statement for OSPF
[23]	RFC 1403	BGP-OSPF interaction
[24]	RFC 1661	The Point-to-Point Protocol (PPP)
[25]	RFC 1662	PPP in HDLC-like Framing
[26]	RFC 1745	BGP4/IDRP IP -- OSPF interaction
[27]	RFC 1772	Application of the Border Gateway Protocol in the Internet
[28]	RFC 1812	Requirements for IP Version 4 Routers
[29]	RFC 1918	Address Allocation for Private Internets (Private and overlapping IP addressing)
[30]	RFC 1930	Guidelines for creation, selection, and registration of an Autonomous System (AS) (Private and overlapping Autonomous System Numbers)
[31]	RFC 1990	The PPP Multilink Protocol (MP)
[32]	RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
[33]	RFC 1997	BGP Communities Attribute
[34]	RFC 2015	MIME Security with Pretty Good Privacy (PGP)
[35]	RFC 2080	RIPng for IPv6
[36]	RFC 2104	HMAC keypad hashing for Message Authentication and three way handshakes for IS-IS protocol

[37]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels.
[38]	RFC 2178	Security Mechanisms for the Internet
[39]	RFC 2205	Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification.
[40]	RFC 2236	Internet Group Management Protocol, Version 2.
[41]	RFC 2236	IGMPv2
[42]	RFC 2270	Using a Dedicated AS for Sites Homed to a Single Provider
[43]		
[44]	RFC 2328	OSPF Version 2
[45]	RFC 2365	Administratively Scoped IP Multicast.
[46]	RFC 2375	IPv6 Multicast Address Assignments.
[47]	RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
[48]	RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
[49]	RFC 2405	The ESP DES-CBC Cipher Algorithm with Explicit IV
[50]	RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
[51]	RFC 2427	Multiprotocol Interconnect over Frame Relay
[52]	RFC 2439	BGP Route Flap Damping
[53]	RFC 2451	The ESP CBC-Mode Cipher Algorithms
[54]	RFC 2453	RIP v2
[55]	RFC 2464	Transmission of IPv6 Packets over Ethernet Networks.
[56]	RFC 2473	Generic Packet Tunneling in IPv6 Specification.
[57]	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
[58]	RFC 2475	Architecture for Differentiated Services
[59]	RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
[60]	RFC 2597	Assured Forwarding PHB Group
[61]	RFC 2685	Virtual Private Networks Identifier
[62]	RFC 2697	Single rate three colour marking
[63]	RFC 2698	Two rate three colour metering

[64]	RFC 2702	Requirements for Traffic Engineering Over MPLS
[65]	RFC 2710	Multicast Listener Discovery (MLD) for IPv6.
[66]	RFC 2711	IPv6 Router Alert Option.
[67]	RFC 2784	Generic Routing Encapsulation (GRE)
[68]	RFC 2918	Route Refresh Capability for BGP-4
[69]	RFC 2961	RSVP Refresh Reduction Extensions
[70]	RFC 2973	IS-IS Mesh Groups
[71]	RFC 2992	Equal Cost Multi Path (ECMP) routing for load-balancing
[72]	RFC 2993	Architectural Implications of NAT.
[73]	RFC 3015	Multiprotocol Extensions for BGP-4.
[74]	RFC 3022	Network Address Translation
[75]	RFC 3031	Multi Protocol Label Switching Architecture
[76]	RFC 3032	MPLS Label Stack Encoding
[77]	RFC 3037	LDP Applicability
[78]	RFC 3056	Connection of IPv6 Domains via IPv4 Clouds.
[79]	RFC 3101	OSPF Not So Stubby Area (NSSA)
[80]		
[81]	RFC 3140	Per Hop Behavior Identification Codes
[82]	RFC 3209	RSVP and RSVP-TE Extensions to RSVP for LSP Tunnels
[83]	RFC 3210	Applicability Statement for Extensions to RSVP for LSP-Tunnels
[84]	RFC 3210	MPLS Support of Differentiated Services
[85]	RFC 3246	An Expedited Forwarding PHB (Per-Hop Behavior)
[86]	RFC 3260	Diff-Serve
[87]	RFC 3270	Multi-Protocol Label Switching (MPLS): Support of Differentiated Services
[88]	RFC 3289	MIB for Diff-Serv
[89]	RFC 3376	Internet Group Management Protocol, Version 3
[90]	RFC 3443	Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks

[91]	RFC 3446	Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
[92]	RFC 3469	Framework for Multi-Protocol Label Switching (MPLS)-based Recovery
[93]	RFC 3478	Graceful Restart Mechanism for Label Distribution Protocol
[94]	RFC 3564	Support of Differentiated Services-aware MPLS Traffic Engineering
[95]	RFC 3569	PIM Source Specific Multicast (PIM-SSM)
[96]	RFC 3587	IPv6 Global Unicast Address Format.
[97]	RFC 3618	Multicast Source Discovery Protocol (MSDP)
[98]	RFC 3623	Hitless OSPF Restart (link state redundancy) Or OSPF graceful restart
[99]	RFC 3630	Traffic Engineering (TE) extensions to OSPF v2 (OSPF-TE)
[100]	RFC 3630	Traffic Engineering Extensions to OSPF Version 2
[101]	RFC 3631	Security Mechanisms for the Internet
[102]	RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements
[103]	RFC 3813	Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
[104]	RFC 3883	Detecting Inactive Neighbors over OSPF Demand Circuits (DC)
[105]	RFC 3916	Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
[106]	RFC 3948	UDP Encapsulation of IPsec ESP Packets
[107]	RFC 3985	Pseudo-Wire Emulation Edge-to-Edge (PWE3) Architecture
[108]	RFC 4007	IPv6 Scoped Address Architecture.
[109]	RFC 4031	Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks
[110]	RFC 4090	Fast Reroute Extensions to RSVP-TE for LSP Tunnels

[111]	RFC 4110	A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)
[112]	RFC 4115	Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic
[113]	RFC 4124	Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
[114]	RFC 4125	Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
[115]	RFC 4127	Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering.
[116]	RFC 4193	Unique Local IPv6 Unicast Addresses.
[117]	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers.
[118]	RFC 4271	A Border Gateway Protocol 4 (BGP-4).
[119]	RFC 4291	IP Version 6 Addressing Architecture.
[120]	RFC 4292	IP Forwarding Table MIB.
[121]	RFC 4293	Management Information Base for the Internet Protocol (IP).
[122]	RFC 4301	Security Architecture for the Internet Protocol
[123]	RFC 4302	IP Authentication Header
[124]	RFC 4303	IP Encapsulating Security Payload (ESP)
[125]	RFC 4360	BGP Extended Communities Attribute
[126]	RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)
[127]	RFC 4377	Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks.
[128]	RFC 4378	A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM).
[129]	RFC 4382	MPLS/BGP Layer 3 Virtual Private Network (VPN) Manage Information Base.
[130]	RFC 4385	PWE3 Control Word for Use over an MPLS PSN
[131]	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet

		Protocol Version 6 (IPv6) Specification.
[132]	RFC 4447	Pseudo wire Setup and Maintenance using LDP
[133]	RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks
[134]	RFC 4456	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
[135]	RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.
[136]	RFC 4552	Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite.
[137]	RFC 4553	Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
[138]	RFC 4562	MAC-Forced Forwarding
[139]	RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification
[140]	RFC 4604	IGMPv3
[141]	RFC 4607	Source-Specific Multicast for IP
[142]	RFC 4623	Pseudowire Emulation Edge-to-Edge (PWE3) Fragmentation and Reassembly.
[143]	RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN.
[144]	RFC 4664	Framework for Layer 2 Virtual Private Networks (L2VPNs)
[145]	RFC 4665	Provider-Provisioned Virtual Private Networks
[146]	RFC 4750	OSPF Version 2 Management Information Base
[147]	RFC 4760	Multi Protocol Extensions for BGP4
[148]	RFC 4762	Virtual Private LAN Service (VPLS) Using & Label Distribution Protocol (LDP) Signaling
[149]	RFC 4786	Operation of Anycast Services
[150]	RFC 4842	Synchronous Optical Network/Synchronous Digital Hierarchy

		(SONET/SDH Circuit Emulation over Packet (CEP)
[151]	RFC 4862	IPv6 Stateless Address Autoconfiguration.
[152]	RFC 4875	Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs)
[153]	RFC 4906	MPLS-based point-to-point VPN: Transport of Layer 2 Frames Over MPLS
[154]	RFC 4966	Network Address Translation - Protocol Translation (NAT-PT).
[155]	RFC 5015	Bidirectional PIM (Bdir-PIM)
[156]	RFC 5036	LDP specification
[157]	RFC 5059	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
[158]	RFC 5060	Protocol Independent Multicast MIB
[159]	RFC 5065	Autonomous System Confederations for BGP
[160]	RFC 5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes.
[161]	RFC 5082	The Generalized TTL Security Mechanism (GTSM)
[162]	RFC 5086	Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
[163]	RFC 5095	Deprecation of Type 0 Routing Headers in IPv6.
[164]	RFC 5120	M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)
[165]	RFC 5172	IP Version 6 over PPP.
[166]	RFC 5187	OSPFv3 Graceful Restart.
[167]	RFC 5240	Protocol Independent Multicast (PIM) Bootstrap Router MIB
[168]	RFC 5246	The Transport Layer Security (TLS) Protocol version 2
[169]	RFC 5250	OSPF Opaque LSA option
[170]	RFC 5292	Address-Prefix-Based Outbound Route Filter for BGP-4.
[171]	RFC 5294	Host Threats to Protocol Independent Multicast (PIM)

[172]	RFC 5301	Dynamic Hostname Exchange Mechanism for IS-IS
[173]	RFC 5305	IS-IS Extensions for Traffic Engineering
[174]		
[175]	RFC 5308	Routing IPv6 with IS-IS.
[176]	RFC 5340	OSPF for IPv6
[177]	RFC 5382	NAT Behavioral Requirements for TCP.
[178]	RFC 5462	Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field
[179]	RFC 5492	Capabilities Advertisement with BGP-4
[180]	RFC 5508	NAT Behavioral Requirements for ICMP.
[181]	RFC 5586	MPLS Generic Associated Channel.
[182]	RFC 5596	MPLS Generic Associated Channel (GAL/G-ACH)
[183]	RFC 5601	Pseudowire (PW) Management Information Base (MIB)
[184]	RFC 5654	MPLS-TP requirements
[185]	RFC 5718	An In-Band Data Communication Network For the MPLS Transport Profile
[186]	RFC 5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
[187]	RFC 5860	MPLS-TP OAM requirements
[188]	RFC 5860	Requirements for Operations, Administration, and Maintenance(OAM) in MPLS Transport Networks.
[189]	RFC 5881	Bidirectional Forwarding Detection (BFD)
[190]	RFC 5883	Bidirectional Forwarding Detection (BFD) for Multihop Paths
[191]	RFC 5884	Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs).
[192]	RFC 5885	BFD for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)
[193]	RFC 5921	MPLS-TP General Framework
[194]	RFC 5925	The TCP Authentication Option
[195]	RFC 5950	MPLS-TP Network Management Framework

[196]	RFC 5950	Network Management Framework for MPLS-based Transport Networks.
[197]	RFC 5951	MPLS-TP Network Management requirements
[198]	RFC 5951	Network Management Requirements for MPLS-based Transport Networks.
[199]	RFC 5960	MPLS-TP Data plane Architecture
[200]	RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)
[201]	RFC 6073	Segmented Pseudowire.
[202]	RFC 6091	Using OpenPGP Keys for Transport Layer Security (TLS) Authentication.
[203]	RFC 6127	IPv4 Run-Out and IPv4-IPv6 Co-Existence Scenarios.
[204]	RFC 6145	IP/ICMP Translation Algorithm.
[205]	RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers.
[206]	RFC 6371	MPLS-TP OAM Framework
[207]	RFC 6372	MPLS-TP survivability framework
[208]	RFC 6373	MPLS-TP control plane framework
[209]	RFC 6378	MPLS-TP Linear Protection
[210]	RFC 6426	MPLS On-Demand Connectivity Verification and Route Tracing.
[211]	RFC 6427	MPLS Fault Management Operations, Administration, and Maintenance (OAM)
[212]	RFC 6428	Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile.
[213]	RFC 6478	Pseudowire Status for Static Pseudowires.
[214]	RFC 6513	Multicast in MPLS/BGP IP VPNs.
[215]	RFC 8200	Internet Protocol, Version 6 (IPv6) Specification.
[216]	RFC 8277	Carrying Label Information in BGP-4
[217]	RFC 8706	Restart Signaling for IS-IS

Table of Figures

CHAPTER-1

1.0 Introduction

IP Networks are becoming the key technology for all the data, voice and video communications. With the standardization of 4th Generation Mobile/LTE even mobile network started using the IP networks in its core. Increasing use of multimedia services like IP TV and Video-on-Demand also necessitates high bandwidth requirements and IP network with QoS guarantees. So, the bandwidth requirement for the core network has been enhanced by manifolds. Few hundred gigabits per second speed, which used to be sufficient for the earlier core networks, have become insufficient for the multi-service all-IP based packet switched optical internet. To address the current and future needs of new generation IP networks, the routers deployed in the core network and metro aggregation must be able to handle data of the order of terabits per second. Accordingly the Aggregation network, access aggregation shall handle traffic in the order of 100Gbps and in cell site aggregation in the order of 10Gbps.

1.1 This document addresses the generic requirements for the Routers to be deployed in the MPLS based transport network to be deployed by the service providers in their Routing and aggregation layers. The hardware and software requirements are categorized in this document for giving the complete flexibility to the procuring authorities.

1.2 Section-2 of this document gives a brief description of the typical network architecture and various applications / services supported in the network. The network architecture describes the four layer hierarchial architecture in general and the IP/MPLS Routing Layer and Aggregation Layer in particular where the MPLS Routers are being deployed. This section also

classifies various categories of routers to be deployed in the routing and aggregation layers of the network.

Section-3 gives the hardware, software and eMS functionality requirements for the routers and associated eMS.

The interface requirements, interface specifications and interoperability requirements are described in section-4.

The security and associated protocols are discussed in section-8. The guidelines for the tendering authority as well as recommended feature mapping for various categories of routers is given in section-10

1.3 This document covers the technical requirements for the following category of Routers

a. **Routers in the IP/MPLS Core of the Network also called Core Routers:**

These are high capacity Routers deployed by Service Providers in major cities. These routers support virtualization where in same router can function as both core and edge router. They can also act as Internet Gateway routers for connectivity to International bandwidth providers or other service providers i.e. to different autonomous system networks.

b. **Routers in the IP/MPLS Edge of the Network also called Edge Routers:**

The functionality of Edge Routers in an IP/MPLS Network is for creation of labels for the packets of data. Moreover these routers enforce the required quality policy for various services to be given to the customers. The entire network intelligence resides with the Edge Routers. These Routers also acts as an information exchange between the Aggregation and Core Routers.

c. **Routers in the MPLS aggregation Network also called Aggregation Routers**

These are converged aggregation routers which can handle both IP and TDM traffic. As there is substantial growth in the IP traffic and the TDM traffic is going down, service providers are looking at deploying converged platform for the transport of both TDM and IP traffic. These platforms by default are becoming IP/MPLS based systems as the IP traffic is in the exponential growth path. These routers aggregate the TDM and IP traffic from various access systems like DSLAM's, 3G/2G BTS etc and hand over the traffic at the Access Gateway Routers.

d. Routers in the Enterprise Customers / Remote offices also called Customer Edge Routers

Remote offices / Enterprise customers require Edge Routers to connect to Internet and/or Intranet or their application servers. These routers are connected to the Service Provider Aggregation or Edge Router over TDM or Ethernet Leased line.

1.4 The RFC documents of the IETF are subject to periodic revision. Hence where ever RFC's are mentioned in this document, the offered product shall meet either the referred RFC or its previous version or its previous draft or its updated version. Wherever a feature of the RFC is mentioned, product shall comply with the part of the RFC specifying the feature.

1.5 The interpretation of the clauses of the RFC's shall be as per RFC 2119.

2.0 Description

This section describes a typical Network Architecture, Applications / Services supported, different category of routers referred in this GR and its element management system.

Part I – Network Architecture

2.1 Four Layer Hierarchical Architecture

The IP/MPLS network is a **multi-layer centrally managed IP backbone network** designed to provide reliable routes to cover all possible destinations. It shall primarily consist of MPLS enabled Provider and Provider edge Routers interconnected in such a way as to ensure no single point of failure. It will facilitate the convergence of voice, data and video networks into a single unified packet-based multi-service network capable of providing all the current and futuristic services. The network is envisaged to support the QoS features with four different classes of traffic along with MPLS-Traffic Engineering, Fast Reroute, multi-casting. The network will provide support for multiple access technologies.

The network architecture is a collection of logical and physical functions distributed in four levels of hierarchies. These four levels of network hierarchies are Application layer, IP/MPLS routing layer, Aggregation layer, Access layer.

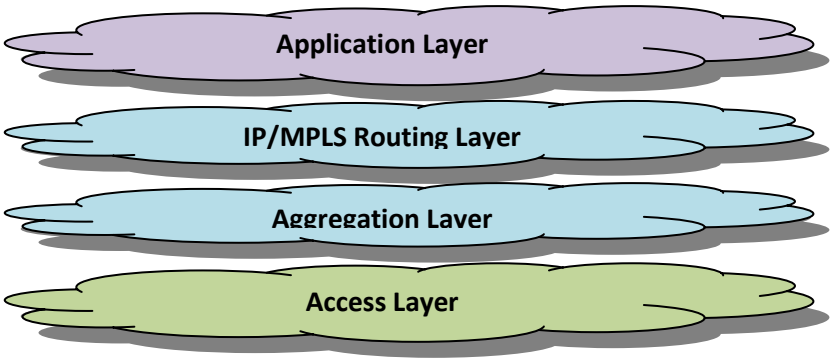

Figure 1: Network with four level of hierarchical architecture

2.2 Application Layer

The application layer contains application servers which provide service logic for delivery of various services such as data, video, voice, multi-media contents etc to end users. Typical applications are VOIP, IPTV/VOD, Audio/Video content, Gaming, E-commerce, Tele-education, Tele-medicine, etc.

2.3 IP/MPLS Routing Layer

This layer consist of high capacity, carrier class Core and Edge routers providing a unified IP/MPLS backbone for higher data forwarding/routing capability to support multiple services with multiple QoS levels and interoperating with existing technology and protocols. It supports scalability, resilience, ease of operation and reduced operational cost. The edge Router network provides information exchange between core and aggregation Routers.

2.4 Aggregation Layer

The aggregation layer, also called the metropolitan network, provides traffic aggregation from the access network and connection to the core IP/MPLS network. Ethernet technology, which was primarily used in enterprise networks in a LAN environment, has made significant deployment inroads in carrier grade networks in the WAN environment, primarily due cost effectiveness and simplicity. It is further divided into three levels, i.e., Tier-I (Metro aggregation), Tier-II (Edge aggregation) and Tier-III (Cell site aggregation). Tier-I aggregates IP Traffic from multiple Tier-II Nodes over the Tier-II Ring configuration. Tier-II aggregates the IP traffic from multiple Access Nodes which are connected

directly or from Tier-III Nodes over Tier-III Rings. Tier-III Nodes aggregate the IP traffic from multiple Access Nodes which are connected directly.

2.5 Access Layer

The access network provides broadband connection in last mile. Broadband Access technologies provide high speed, always on Internet connection for homes and businesses. Broadband access technologies enable data, voice, video and other multimedia applications for home and business use. The choice of what access technologies to deploy depends mainly on its commercially viability and which access technology can best serve the current and future consumer demands. The network is expected to use various access technologies - from xDSL technology for copper access using IP DSLAM/LMG, GPON/FTTH (Fiber to the Home) technology for Fiber Access, Wireless Access over Wi-Fi / Wi-MAX, 3G/4G Networks, etc.

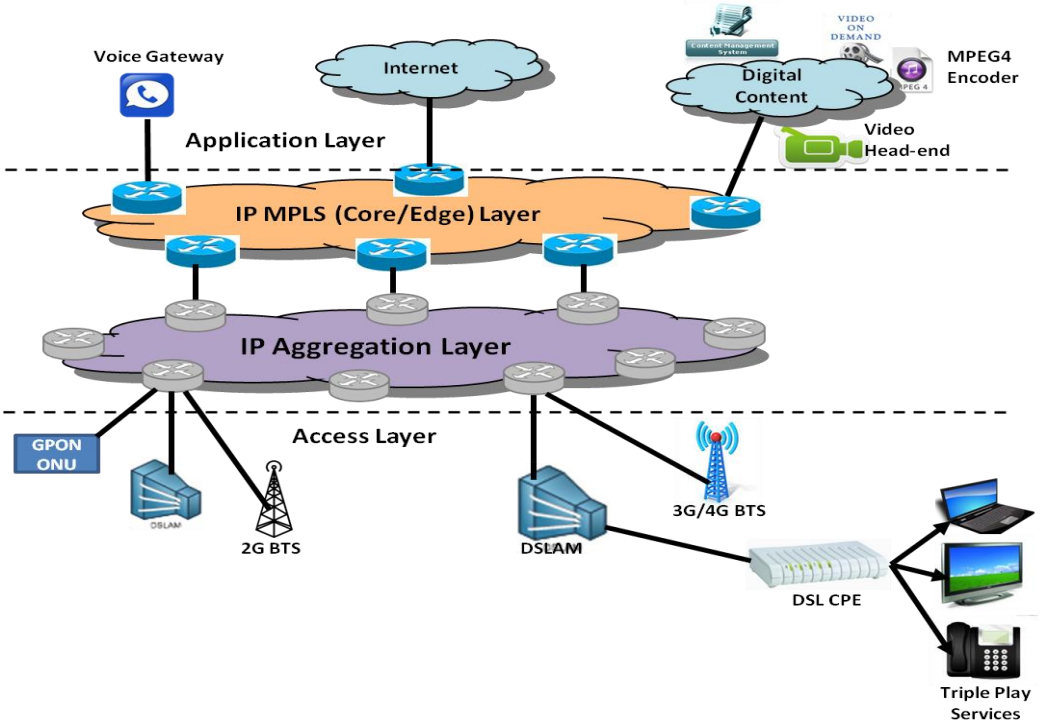

Figure 2: Overall Network View

2.6 Core Routing Architecture

The Core Network constitutes an integrated IP and MPLS network. The network constitutes high speed Backbone comprising of Core routers running modular operating system with built-in redundancies supporting both TCP-IP and MPLS protocols and whose function is primarily be limited to high-speed packet forwarding.

These nodes are connected in a mesh configuration over multiple 10G (LANPhy / WAN Phy) /40G/100G interfaces over the National DWDM Network.

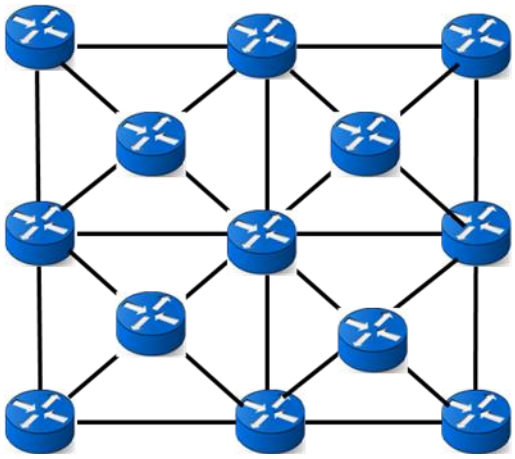

Figure 3: A Typical Core Router Architecture

In cases where large Telecom Services Providers deploying pan India based, IP-MPLS Networks, these Routers can be part of multi OSPF Areas / ISIS system with one area / system being part of National Core network and other area / system being part of Area core Network. The Area Core Network aggregates the traffic originating from edge routers deployed.

2.7 Edge Routing Architecture

The Edge routers are connected to the Core network either locally through the 10G (LANPhy / WAN Phy) (1+1) or remotely through dual homed 10G (LANPhy / WAN Phy) / STM-16. The Edge network

architecture provides for dual homing links from the Edge router to the nearest Core routers. The edge node are connected on 10G(LANPhy / WAN Phy) interfaces to both the collocated Core Router and to the Remote Core Router in the same city. The edge Router in these cities are dual homed to National Core Router on 10G (LANPhy / WAN Phy) / STM-16 interfaces. The Edge Routers so deployed acts as a multi-service edge and aggregates traffic coming from PSTN (through media Gateway), GSM (through Media Gateway and GGSN), CDMA (through Media Gateway and PDSN), Broadband (through BRAS / BNG), Wi-Max, etc. The logical relation between various network components such as Core Network and Edge Routers is depicted in figure below:

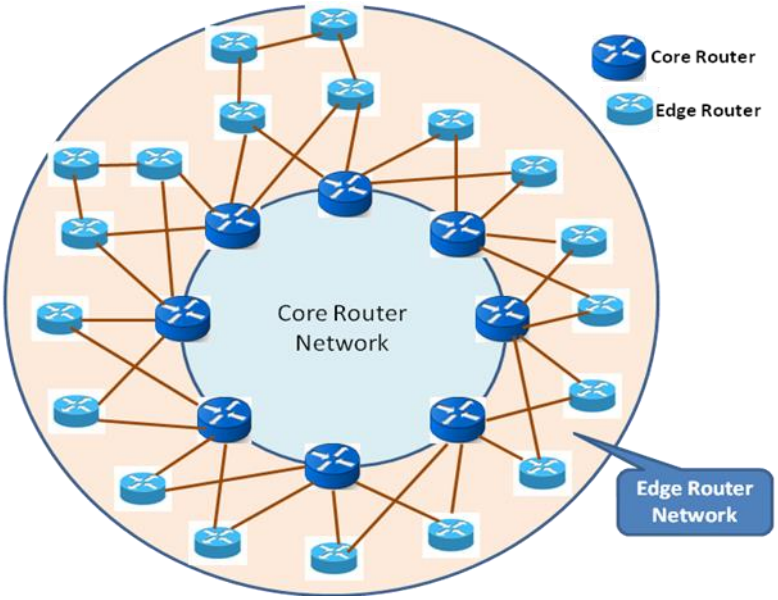

Figure 4: A Typical Edge Router Architecture with dual homing & Cascading

2.8 Aggregation Layer Architecture

A typical aggregation layer architecture which aggregates the traffic from various access nodes is given in the figure below. Here 3 Tiered aggregation architecture is shown. However the Service providers shall decide the number of layers of aggregation network required. The Aggregation routers deployed shall not pose any limitation for the same.

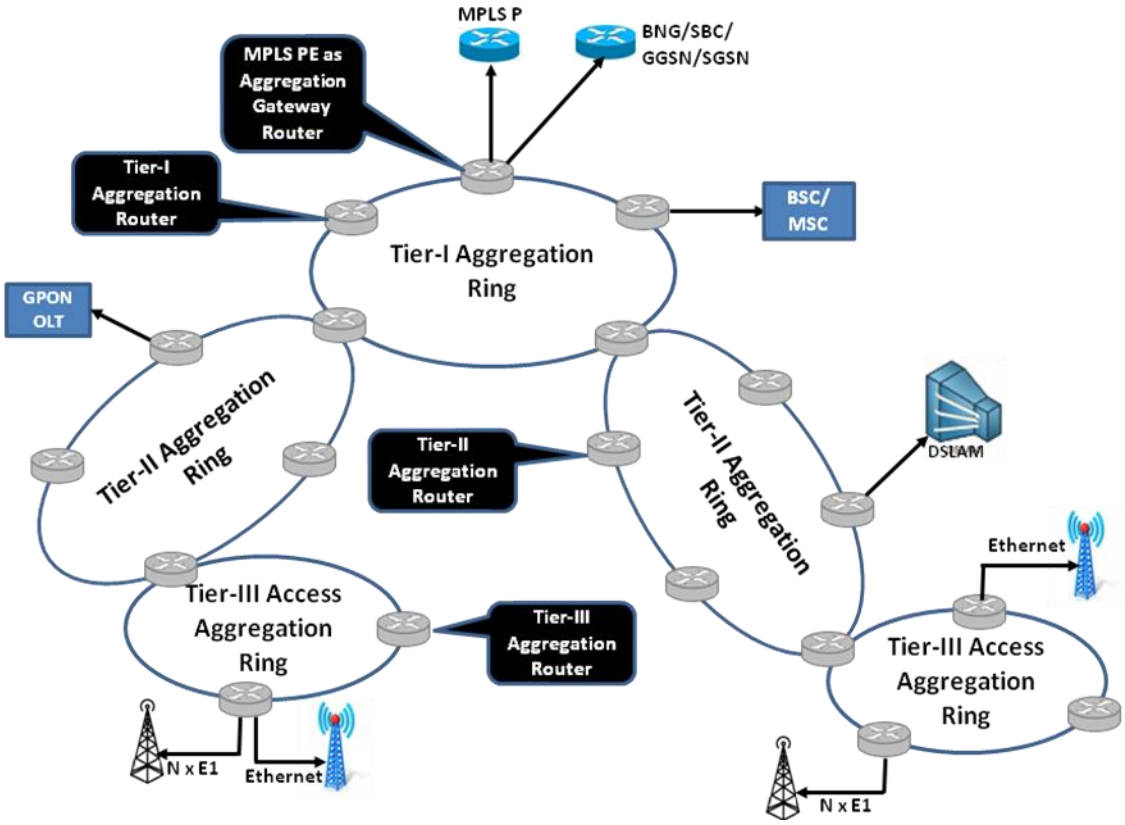

Figure 5: 3-Tier Aggregation Layer Architecture

2.9 Edge Router as Aggregation Gateway Router:

The Edge or PE Router typically acts as a Aggregation Gateway Router. The Aggregation Gateway Router terminates multiple Tier-I Rings which aggregate the traffic from multiple Tier-II Rings. The Tier-I Rings can aggregate the Metro traffic or can be used for inter-city traffic aggregation. This router can provide downlink connectivity to GPON OLTs over 10G links, FE/GE interfaces to DSLAMs and 3G/Wi-MAX base stations. The uplink Ethernet traffic could be forwarded to BNG / ASN Gateway etc, L3PE etc. The Aggregation Gateway Router shall have STM-1 interfaces for hand-off to legacy TDM equipment such as BSC. MSC etc.

2.10 Tier-I Aggregation Router

The Tier-I aggregation Router located typically in a city aggregates the traffic from multiple Tier-II Rings and sends it to the Tier-I Aggregation Gateway Router over the Tier-I Ring. Thus multiple Tier-II Rings are terminated on a Tier-I Aggregation Router. In addition, a Tier-I Node terminates GPON OLTs over 10G links, should have FE/GE interfaces to DSLAMs and 3G/Wi-MAX base stations. It has STM-1 interfaces for hand-off to legacy TDM equipment.

2.11 Tier-II Aggregation Router:

Tier-II Aggregation Routers aggregate the IP traffic from multiple Access Nodes which are connected directly or from Tier-III Aggregation Routers over Tier-III Rings and uplinks the Traffic over the Tier-II Ring. The Tier-II Ring can provide Intra City or Metro Edge Aggregation of Traffic. A Tier-II Aggregation Router can terminate multiple Tier-III rings, terminate GPON OLTs over 10G links and provide FE/GE interfaces to DSLAMs and 3G/Wi-MAX base stations. It has STM-1 interfaces for hand-off to legacy TDM equipment.

2.12 Tier-III Aggregation Router:

Tier-III Aggregation Routers aggregate the IP traffic from multiple Access Nodes which are connected directly like 2G/3G/LTE BTS, DSLAM, TDM leased circuits etc. The Tier-III Aggregation Routers are part of the Tier-III Ring which uplinks the IP/TDM traffic to the Tier-II Aggregation Router. The Tier-III Ring does the Access or Cell Site Aggregation.

2.13 Termination of the Rings:

Service providers can achieve node level redundancy by terminating the Ring in two aggregation nodes. The aggregation Routers shall not pose any limitation for the same.

2.14 Nodes per Ring:

The Architecture shall supports upto 8 Nodes per Ring

PART II – APPLICATIONS / SERVICES TO BE SUPPORTED

Based on the Requirement and availability of the various application servers and end devices, the Router Transport Network shall facilitate the following Services to the end customers.

2.15 Basic Internet Access Service

The Router Transport Network shall facilitate basic internet cccess over dial-up / Broadband or leased line Access.

2.16 TV Over IP Service

The Router Transport Network shall facilitate distribution of broadcast TV channels in digital mode (MPEG2/MPEG4/H.264) on the broadband network to the customer and is converted back to an analog format in the home for reception on a standard television set.

2.17 Video On Demand Service

The Router Transport Network shall provide users with the ability to select video content (MPEG2/MPEG4/H.264) (usually a movie from a library) and view it at their convenience. The user can pause, go backward, forward and repeat the content as per their desire. It is similar to a video tape being played from VCR except that the content is delivered via a content server which can be located at any point of the network, instead of from a VCR.

2.18 Audio On Demand Service

The mechanism is simillar to the Video On Demand Service. In place of video, it is the audio file which the user selects.

2.19 Bandwidth on Demand Service

The Router Transport Network shall provide User configurable and Service configurable bandwidth on demand.

2.20 Video Conferencing

The Router Transport Network shall permit users to establish point-to-point or point-to-multipoint connections between their PCs/H.323/SIP terminals and allow them to see and hear each other as well as share PC data / applications.

2.21 Remote Education

This Service combines both Video conferencing and the 2-way interactive data capabilities of the broadband network to create a virtual classroom where students participate remotely with an instructor in a way that mimics a regular class.

2.22 Voice and Video Over IP

The Router Transport Network shall allow H.323/ SIP terminals to set up point to point connections under control of centrally located soft switches.

2.23 Interactive Gaming Service

The Router Transport Network shall support both single user and multi user Interactive gaming

2.24 Circuit Emulation Service

The traffic from the E1 or channelised E1 interfaces are converted into packets and given the necessary Quality of Service class assignments for sending through the IP Network to the remote end. In the remote end, the

E1 interface is retrieved back. This service is for carrying E1 channel having TDM voice.

2.25 E1/STM-1 Leased Line Service

Leased line services shall be terminated in either E1 interfaces or channelized STM interfaces or STM-1 interface in Tier-II, Tier-III switches. Such interfaces may be carrying IP or TDM traffic. IP over SDH uses the POS methodology. In case of TDM traffic, circuit emulation functionality is carried out for carrying the traffic over the IP Transport Network.

2.26 Ethernet Services

These services include Point-to-Point, Point-to-Multi-Point and Multi-Point-to-Multi-Point Ethernet Services. Ethernet Private Line (EPL), Ethernet Virtual Private Line (EVPL) [E-LINE], Ethernet LAN (E-LAN) and E-TREE support shall be as per Technical Specification MEF-6 of Metro Ethernet Forum (MEF).

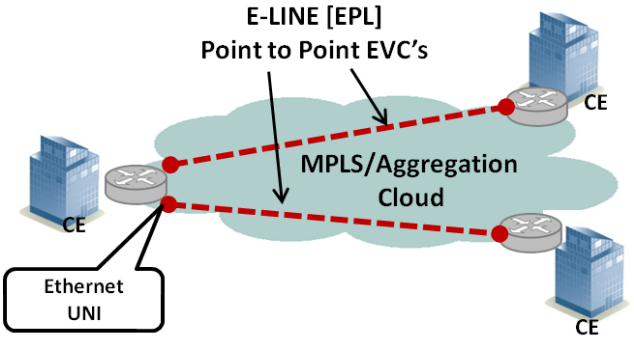

Figure 6: E-LINE Point to Point EVC's

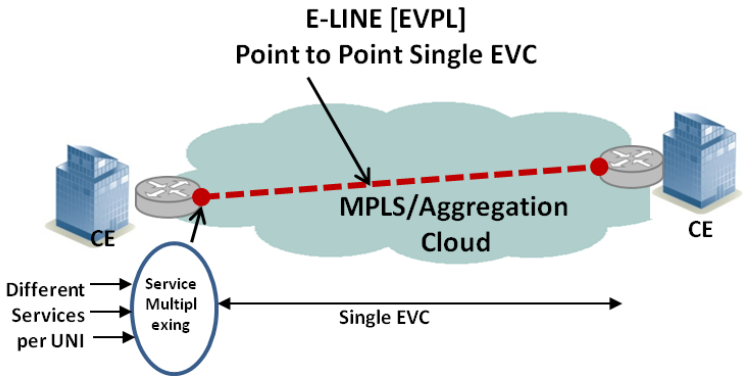

Figure 7: E-LINE EVPL Point to Point EVC

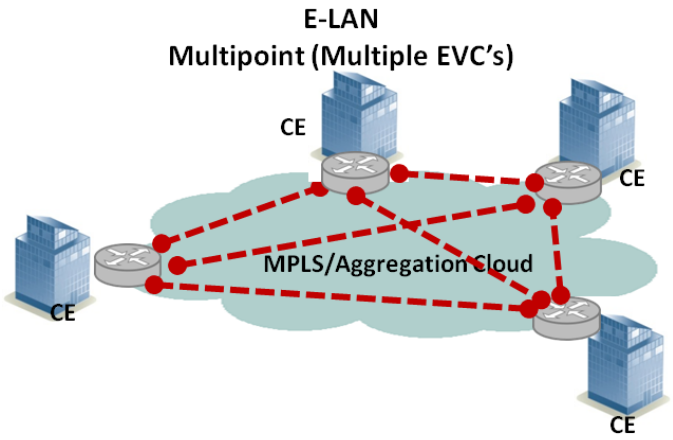

Figure 8: E-LAN Multi-Point Model

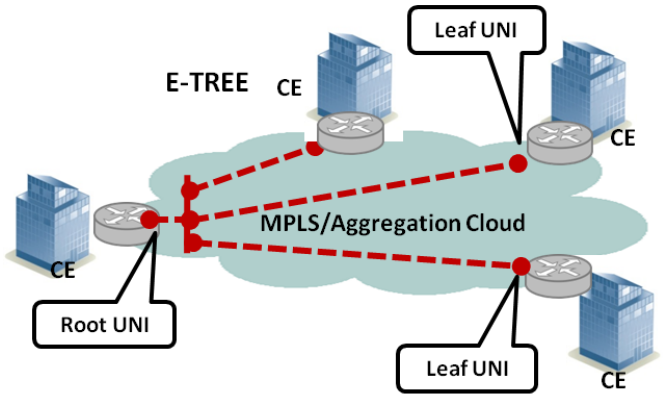

Figure 9: E-TREE Root and Leaf Model

2.27 Layer-2 Service

This service is same as E-LINE Service. E-LINE is a designation of MEF and Layer-2 VPN is a designation of IETF. Layer-2 VPN Service includes

access over E1/SDH Iso in addition to ethernet in E-LINE service. It is a pseudowire emulated point to point connection. For layer 2 VPN services, aggregator switch encapsulates the Ethernet traffic and sends it to the Edge Router. The Edge Router will send it to other Core/Edge Router which connects to destination aggregator Router.

2.28 Layer-3 VPN Service

The Service Provider MPLS network takes a routing decision for the customer traffic based on the destination IP address. The customer network becomes simpler as the routing decisions are taken by the Service Provider Network. For layer 3 VPN services, aggregation router shall take a Layer 2 decision and send the traffic to the Edge Router. Traffic belonging to different VPN shall be in different VLANs.

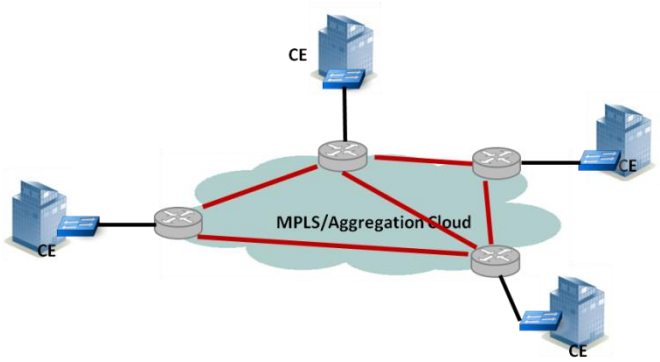

Figure 10: Layer-3 VPN from customer sites

2.29 E1/SDH/Ethernet Backhaul Services

The Router Transport Network backhauls E1 lines from 2G BTS or from last mile PDH microwave equipment and STM-1 traffic from SDH Microwave equipment to 2G BSC. System also backhauls Ethernet traffic from 3G NodeB, last mile Ethernet microwave equipment, Wi-Max base stations and LTE eNodeB to 3G RNC, Wi-Max ASN GW and 4G AGW and S-GW at Remote Access Nodes and DSLAMs, PON and OLTE at Remote Access Nodes.

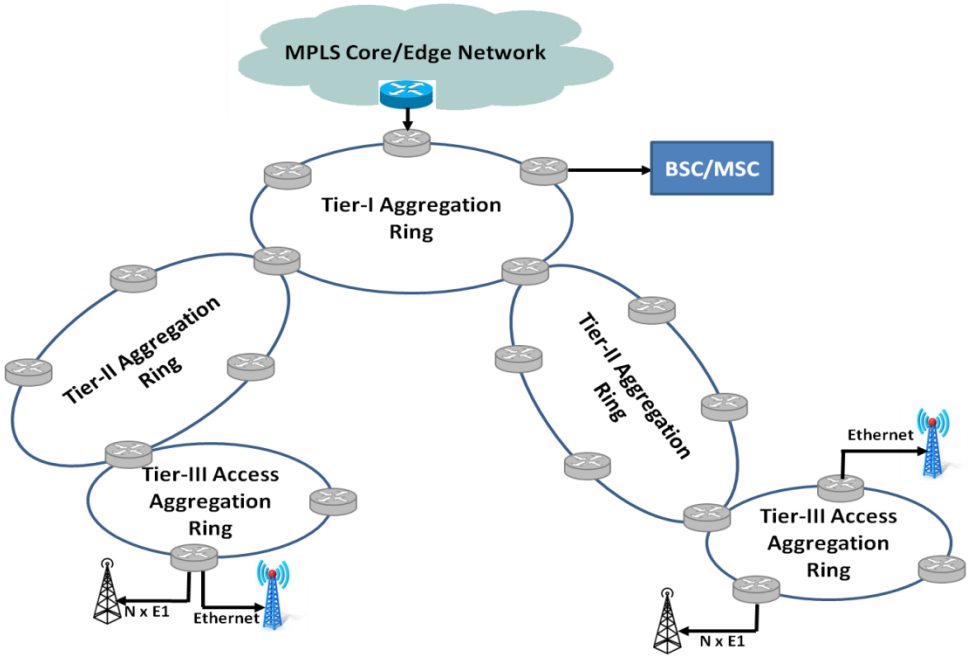

Figure 11: Mobile Backhauling Service

PART III – CATEGORY OF ROUTERS

2.30 Category of Routers

The various category of Routers in the IP/MPLS layer and aggregation layer for delivering the services as given in Part-II of this section are listed below.

Router Type	Router Category	Application
CE Router	I	Enterprise Customer Edge Router – Low Capacity
	II	Enterprise Customer Edge Router – Medium

		Capacity
	III	Enterprise Customer Edge Router – High Capacity
Aggregation Router	IV	Service Provider Access Traffic Aggregation Router – Low Capacity
	V	Service Provider Access Traffic Aggregation Router – Medium Capacity
	VI	Service Provider Access Traffic Aggregation Router – High Capacity
Edge Router	VII	Service Provider Edge Router – Low Capacity
	VIII	Service Provider Edge Router – Medium Capacity
	IX	Service Provider Edge Router – High Capacity
Core Router	X	Service Provider Core Router – Low Capacity
	XI	Service Provider Core Router – Medium Capacity
	XII	Service Provider Core Router – High Capacity

Non-Chassis based Router (Fixed Form Factor)

Router Type	**Router Category**	**Application**
CE Router	XIII	Enterprise Branch Router
	XIV	Enterprise Customer Edge Router – High Capacity
Aggregation Router	XV	Service Provider Access Traffic Aggregation Router
Core Router	XVI	Service Provider Core Router – Medium Capacity
	XVII	Service Provider Core Router –High Capacity

PART IV – ELEMENT MANAGEMENT SYSTEM

2.31 Architecture of eMS equipments

The role of element Management System (eMS) is to control and manage all aspects of the domain such as Fault, Configuration, Accounting, Performance and Security (FCAPS) as defined by ITU-T and to ensure maximum usage of the devices resources. The eMS performs the following functions:

2.31.1 Service Delivery:

2.31.1.1 Inventory Management Support: It involves maintaining a record of all the NE resources that are installed in the sub network to support the provisioning of services; it includes collection of locations, quantities of equipment, model numbers, serial numbers, versions, installation dates, etc. To ensure ongoing operational integrity, the eMS periodically resynchronizes its database with the NE using the auto discovery mechanism. It also auto discovers equipment-provisioning parameters that are stored in the eMS database for use in other service-provisioning, service-assurance operations.

2.31.1.2 Configuration Management Support: It involves complete control of sub network resources, topologies, and redundancies and includes the installation and turn-up of new equipment resources; it may include the assignment of resources to trunk routes or service areas, the control of equipment, and network protection switching.

2.31.1.3 Provisioning Support: It involves the creation of specific connections or the enabling of specific sub network features and the assignment of these to a specific subscriber for an extended period; the connections and features may take into account or be determined by a QoS level that is guaranteed to the subscriber.

2.31.1.4 Service Usage Support: It involves the measurement of the usage of the sub network resources by the various subscribers; this is the basis for billing.

2.31.2 Service Assurance:

2.31.2.1 Fault Management Support: It involves the monitoring of the network resources to detect malfunction, preempt failures, and detect faults. After faults are discovered, the user/operator can troubleshoot, repair, and restore the network as quickly as possible. Fault management ensures that service remains available.

2.31.2.2 Performance Data Collection Support: It involves the periodic collection of quality metrics that characterize the performance of the network resources over service intervals. It also facilitates the visualization of trends that can indicate periodic or gradual degradation of physical resources.

2.31.2.3 Resource Utilization data Collection Support: It involves the collection of data on the level of utilization of network resources assigned to subscribers. This data can be used to determine whether the service product is appropriately matched to the subscribers' usage characteristics. It can also be used to forecast demand and suggest service upgrades before QoS suffers.

2.31.2.4 QoS Assurance Support: It involves ensuring that the quality metrics characterizing network performance remain within the agreed limits. It requires proactive monitoring of the network fault, performance, and utilization parameters to preempt any degradation in service quality.

2.31.2.5 The eMS provides the North bound interface to integrate NMS.

2.31.2.6 The System allows to assign following categories of users

a. Helpdesk User
b. Operation and Maintenance User
c. System Administrator

2.31.2.7 The application provides the control of access right of users in respect of function menu and geographical area of interest.

3.0 FUNCTIONAL REQUIREMENTS

This section describes the varous functional requirements like Hardware requirements and features requirements for the Routers. This section also describes the functional requirements for the eMS.

PART-I HARDWARE REQUIREMENTS

3.1 Capacity of Routers

The capacity of routers is calculated based on the addition of interface slot capacity of the router. The capacity of different interface slots may not be same. The interface slot capacity of the router may depend upon the interface card (full rate) available for the product as well as the control / switching fabric card used.

The various categories of Routers shall meet the capacity requirements as listed below.

	Router Category	Minimum Slot Capacity (Full Duplex)	Minimum Chassis Capacity(*) [Full duplex]
CE Router	I	-	1 Gbps
	II	-	4 Gbps
	III	-	10 Gbps
Aggregation Router	IV	-	10 Gbps
	V	8 Gbps	40 Gbps
	VI	20 Gbps	200 Gbps
Edge Router	VII	40 Gbps	240 Gbps
	VIII	100 Gbps	800 Gbps
	IX	200 Gbps	1.6 Tbps
Core Router	X	200 Gbps	1.6 Tbps
	XI	400 Gbps	4 Tbps
	XII	400 Gbps	6Tbps [Multi-Chassis optional in case not supported in Single chassis]

* Except for Category XII Router where 6Tbps can be through Multi-chassis as well. The CE Router throughput is for the large packets

Non-Chassis based Router (Fixed Form Factor)

Router Type	**Router Category**	**Minimum Capacity [Full duplex]**
CE Router	XIII	4 Gbps
	XIV	25 Gbps
Aggregation Router	XV	300 Gbps
Core Router	XVI	3 Tbps
	XVII	12 Tbps

3.2 Router Latency

The maximum permissible Router latency for all types of Routers shall be less than 10µsec

3.3 Packet Processing Capacity

Router Category	Minimum Packet Processing and forwarding rate for a packet size of 64 bytes.(In pps)	Minimum No. of VRF	Minimum No of Routes per VRF
I	300 kpps	-	-
II	750 kpps	-	-
III	3 mpps	64	1K
IV	14 mpps	-	-
V	59 mpps	-	-
VI	297 mpps	-	-
VII	357 mpps	4K	20K
VIII	1190 mpps	4K	20K
IX	2380 mpps	4K	20K
X	2380mpps	4K	20K
XI	5952mpps	4K	20K
XII	8928 mpps	4K	20K

Non-Chassis based Router (Fixed Form Factor)

Router Category	Minimum Packet Processing and forwarding rate for a packet size of 64 bytes.(In pps)	Minimum No. of VRF	Minimum No of Routes per VRF
XIII	1 mpps	-	-
XIV	20 mpps	20	1K
XV	300 mpps	10	700
XVI	4760 mpps	200	1K
XVII	5600 mpps	200	1K

3.4 Routes to be Supported

The router shall support the following IPv4 and IPv6 FIB routes simultaneously.

Router Category	Ipv4 Routes to be supported	Ipv6 Routes to be supported
I	1K	1K
II	2K	1K
III	8K	4K
IV	8K (*)	1K (*)
V	20K (*)	5K (*)
VI	100K (*)	25K (*)
VII	2M	500K
VIII	2M	500K
IX	2M	500K
X	2M/256K	500K/128K
XI	2M/256K	500K/128K
XII	2M/256K	500K/128K

Note: * indicates NIL in case of MPLS_TP option for Aggregation Network

Non-Chassis based Router (Fixed Form Factor)

Router Category	Ipv4 Routes to be supported	Ipv6 Routes to be supported
XIII	2K	1K
XIV	10K	2K
XV	6K	1.5K
XVI	160K	40K
XVII	160K	40K

3.5 Scalability Figures

3.5.1 Ethernet Scalability figures

a. The Router shall support 4095 VLAN ID's per port

b. The Router shall support 1,488,100 packets per second (pps) on Gigabit Ethernet in Full Duplex; 148,810 pps on 100 Mbps Full Duplex Ethernet; 14,881 pps on 10 Mbps Full Duplex Ethernet at minimum frame size of 64 Bytes on Ethernet.

3.5.2 Routing Scalability figures

Router Category	MAC Address Support	SVL / LSP Entries	Static routing	RIP	OSPF	IS-IS
I	2K	-	2K	5K	-	-
II	4K	-	5K	10K	-	-
III	8K	1K	10K	15K	15K	-
IV	10K	1K	5K	5K	5K	5K
V	24K	16K	10K	15K	15K	15K
VI	80K	32K	10K	25K	25K	25K
VII	512K	192K	10K	25K	25K	25K
VIII	512K	256K	10K	25K	25K	25K
IX	512K	256K	10K	25K	25K	25K
X	512K	256K	10K	25K	25K	25K
XI	512K	256K	10K	25K	25K	25K
XII	512K	256K	10K	25K	25K	25K

Non-Chassis based Router (Non-Chassis Based)

Router Category	MAC Address Support	LSP Entries	Static routing	RIP	OSPF	IS-IS
XIII	4K	-	5K	-	10K	
XIV	16K	1K	4K	4K	6K	6K
XV	16K	512	5K	5K	5K	5K
XVI	24K	3K	10K	10K	10K	10K

XVII	24K	3K	10K	10K	10K	10K

3.5.3 VPLS / Multicase Scalability Figures

Router Category	VPLS instances	TE Tunnels	Pseudowire (VLL) services	Multicast routes	Multicast groups	BGP Peers
I	-	-	-	-	-	-
II	-	-	-	-	-	-
III	128	128	1K	256	128	64
IV	128	128	1K	1K	64	64
V	1K	1K	8K	1K	1K	64
VI	2K	2K	32K	1K	2K	64
VII	8K	8K	64K	16K	2K	4K
VIII	8K	16K	64K	16K	2K	4K
IX	8K	16K	64K	16K	2K	4K
X	8K	16K	64K	16K	2K	4K
XI	8K	16K	64K	16K	2K	4K
XII	8K	16K	64K	16K	2K	4K

Non-Chassis based Router (Fixed Form Factor)

Router Category	TE Tunnels	Multicast routes	Multicast groups	BGP Peers
XIII	-	-	-	-
XIV	10K	1K	1K	64
XV	512	1K	64	64
XVI	2K	8K	1K	200
XVII	2K	8K	1K	200

3.5.4 QoS Scalability figures

Router Category	QoS Traffic Policers	ACL Entries
I	1K	1K
II	1K	1K
III	1K	1K
IV	1K	1K
V	16K	16K
VI	32K	32K
VII	32K	32K
VIII	32K	32K
IX	32K	32K
X	16K	32K

XI	16K	32K
XII	16K	32K

Non-Chassis based Router (Fixed Form Factor)

Router Category	QoS Traffic Policers	ACL Entries
XIII	100	1K
XIV	100	4K
XV	1K	1K
XIV	1K	4K
XVII	1K	4K

3.6 Redundancy Requirements:

The routers shall supports four levels of redundancy architecture.

3.6.1 Module Level Redundancy

The requirement of module level redundancy for various types of routers is given in the following table. In certain types of critical routers, the interfaces are required to be distributed in different cards such that the failure of one card will not affect the complete traffic being handled by that type of interface. In cases where Power supply, Control and Switch Fabric redundancy has been specified, there shall not be any degradation of performance in case of Failure of the redundant module.

3.6.1.1 All categories of

Router Category	Control and Switch Fabric Cards Redundancy	Interfaces distributed in different cards
I	No	No
II	No	No
III	Optional	Yes
IV	No	No
V	Optional	Yes
VI	Yes	Yes
VII	Yes	Yes
VIII	Yes	Yes
IX	Yes	Yes
X	Yes	Yes
XI	Yes	Yes
XII	Yes	Yes
Non-Chassis based Routers		
XIII	No	No
XIV	No	No
XV	No	No
XVI	No	No
XVII	No	No

Router shall support hot-swappable/pluggable redundant (1+1 or N+1) hot standby power supplies

3.6.1.2 All categories of Router shall support hot-swappable/pluggable redundant (1+1 or N+1) hot standby fans/fan units.

3.6.2 Node Level Redundancy

Two Aggregation/Edge Routers (Type VI,VII, VIII & IX) can be dual homed to two Edge/Core Routers. The Aggregation/Edge Routers shall support such dual homed topology and provide connectivity to both Edge/Core routers, so that the subscriber's CE router will have connectivity to both Edge/Core Routers, and protect against Edge/Core Router failure

3.6.3 Path Level Redundancy

The Service providers achieve Path level redundancy by providing connectivity between routers over 1 + 1 redundant links. In such situations, the redundant paths are taken through different OF cables so as to achieve the redundancy in case of fiber cuts. The Routers shall support such path level redundancy.

3.6.4 Network Redundancy

In order to achieve very high levels of network redundancy, Core routers in 1 + 1 architecture are connected over a layered architecture as shown in the following figure. Routers shall support such layered network redundancy.

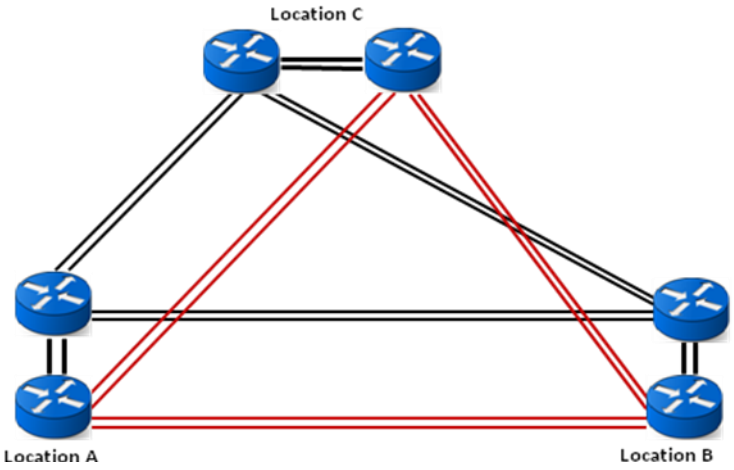

Figure 12: Layered Network Redundancy Architecture

PART-II FUNCTIONAL SPECIFICATIONS

3.7 General Functional Requirements

3.7.1 The Router shall support use of any of the optical Ethernet interfaces as Client or Aggregate interfaces.

3.7.2 The Router shall support dynamic online configuration.

3.7.3 The Router shall support jumbo frame of 9000 bytes. The MTU shall be configurable from 68 to 9000 Bytes. (XIV type router may support a minimum of 4000 bytes)

3.7.4 The Router shall support MDI-X based auto-uplink feature.

3.7.5 The Routers under Core Router category shall have support for both P and PE router functionality for MPLS on the same router simultaneously and on all the interfaces. However, this shall be an optional requirement based on the Purchaser's network requirements.

3.7.6 The Router shall support Fast convergence on the backbone links and uplinks.

3.7.7 The Router shall support egress buffering of 100 ms (it's 30 ms for non-Chasis Router) to take care of momentary congestion and link failures.

3.7.8 The Router shall support both Ipv4 and Ipv6 functionalities

3.7.9 The Router shall support built-in storage of command logs using SYSLOG. The Routers shall support a minimum log file size of 10MB. In case of Edge/Core Routers, the Routers shall support one or more such log files so as to store the log information for atleast one month. The log files shall be read only from the LCT/eMS/external terminal and it shall be possible to copy these files on an external media directly or through eMS/LCT.

3.8 Operating System related features

3.8.1 Modular Operating System

3.8.1.1 The Router shall have carrier grade, modular distributed architecture with Control Plane and Data Plane separation.

3.8.1.2 The Router shall have decoupled Forwarding and Management Planes.

3.8.1.3 The modular operating system shall provide ability to restart different modules (routing, firewall, SNMP, class of service) individually. This provides better availability of system, since a failure or restart of one module does not affect the whole system.

3.8.1.4 Modular OS shall allow the user to upgrade an OS module without rebooting the system, and shall allow upgrading the software.

3.8.1.5 The Router shall support individual restart of most modules and processes without affecting other processes or rebooting the entire operating system.

3.8.1.6 The modular OS shall support the routing protocols, interface management, chassis management, and SNMP/Netconf management each execute as independent processes.

3.8.1.7 Any disruption in the Control Plane (for Routing & Connection Management), which shall cause a switch-over to a standby Control Card, shall not affect the forwarding of data in the line cards.

3.8.1.8 During the switchover of Switch Card or Control Card, all active LSPs and the underlying Martini circuits shall be protected, remain operative and not lost.

3.8.1.9 Forwarding entries on the line cards, such as IP prefixes or MPLS labels and outgoing encapsulations shall not be affected by the loss of the active switch card.

3.8.1.10 The Router shall support forwarding and control plane separation.

3.8.2 Non-Stop Forwarding (NSF) & Non-Stop Routing (NSR)

Router shall support Non Stop forwarding (NSF) supported by graceful restart extensions (e.g. helper mode) and Non Stop Routing (NSR) supported to facilitate nonstop services for the following:

i. BGP
ii. Graceful restart for OSPF as per RFC 3623 and RFC 5187
iii. ISIS
iv. Graceful Restart Mechanism for Label Distribution Protocol as per RFC 3478
v. BGP/MPLS
vi. RSVP LSP
vii. Graceful PIM restart
viii. Graceful Restart Mechanism for BGP as per RFC4724
ix. Graceful Restart Mechanism for BGP with MPLS

3.8.3 ISSU

3.8.3.1 The Router shall support in service software upgrade to eliminate network/control plane downtime during software image upgrades from one release to another.

3.8.3.2 The Router shall support Non Service Affecting Upgrades

3.8.3.3 The Router shall support fast boot and non-disruptive expansion of flash memory to ensure that software upgrades do not disrupt the normal router operation.

3.8.3.4 The Router shall have protection of memory address space for all running processes

3.8.3.5 The Router shall support Dynamic Bandwidth upgrade for LSP and Circuits without restart

3.8.3.6 The Router shall support LSP shared implicit/explicit mode for make before break operations

3.9 Layer-2 Switching Features

3.9.1 General:

3.9.1.1 The Router shall support ingress and egress bandwidth profile per User to Network Interface (UNI).

3.9.1.2 Service multiplexing: A single Router port shall support multiple Ethernet Services

3.9.1.3 Router shall support transmission of a path join message from a receiver towards a source on a primary path, while also transmitting a secondary multicast join message from the receiver towards the source on a backup path to minimize convergence times in the event of node or link failures on the primary path.

3.9.1.4 Router shall support Layer 2 protocol transport for Ethernet and PPP.

3.9.2 Forwarding Support

3.9.2.1 The Router shall support hardware assisted Layer 2 forwarding.

3.9.2.2 The Router shall have hard-coded and unique MAC address.

3.9.2.3 The Router shall support to override Router port MAC address.

3.9.2.4 The Router shall support to set per port static MAC configuration.

3.9.3 MAC Address Learning / Limiting:

3.9.3.1 The Router shall support L2 Learning parameters: Sources learning per Port/VLAN/Source address.

3.9.3.2 The Router shall support to set per port dynamic MAC learning limit.

3.9.3.3 The Router shall support to limit the number of source MAC addresses learnt from bridge port in order to prevent MAC address flooding DoS attack. This limit is configurable per bridged port.

3.9.3.4 The Router shall support dropping of Frames with new source MAC-addresses exceeding the configured value.

3.9.3.5 The Router shall support per VLAN MAC learning to ensure MAC addresses are learnt only from a VLAN perspective and automatic/manual disabling of MAC addresses learning for the VLAN where there are less than two ports in that VLAN.

3.9.3.6 The Router shall support MAC limiting per Ethernet flow point (EFP) or bridge domain

3.9.3.7 The Router shall support MAC address limitation and aging

3.9.3.8 All static entries shall NOT be aged.

3.9.3.9 The Router shall support Hardware based aging of MAC Address Table entries.

3.9.3.10 The Router shall support to enable L2 Aging on every port.

3.9.3.11 The Router shall support MAC address learning disabling

3.9.3.12 The Router shall support to filter and discard all Ethernet frames received on bridged ports in the upstream direction with a specific MAC destination address (DA)

3.9.3.13 The Router shall support list of allowable MAC destination address

3.9.3.14 The Router shall not learn MAC address from bridge port X if the same MAC address appears in the learning table pointing to bridge port Y (port X and port Y on the same LSW and same VLAN), except in the cases where the aggregation network forwards according to MAC Learning table.

3.9.3.15 The Router shall support unique MAC address per device to prevent spoofing and provide traceability.

3.9.4 Spanning Tree Protocol

3.9.4.1 The Router shall support Spanning Tree Protocol as per IEEE 802.1d

3.9.4.2 The Router shall have the capability to prioritize BPDUs in the data plane (by providing dedicated queues) and in the control plane (by providing dedicated CPU queues for BPDUs).

3.9.4.3 The Router shall have the capability to drop BPDUs if those BPDUs have a root bridge identifier which is lower (better) than the current Spanning Tree root. This function is configurable on a per port basis.

3.9.4.4 The Router shall have the capability to drop BPDUs regardless of the BPDU content. This function is configurable on a per port basis.

3.9.5 Rapid Spanning Tree Protocol (RSTP)

3.9.5.1 The Router shall support Rapid Spanning Tree Protocol as per IEEE 802.1w

3.9.6 Multiple Spanning Tree Protocol (MSTP)

3.9.6.1 The Router shall support Multiple Spanning Tree Protocol as per IEEE 802.1s

3.9.6.2 The Router shall support minimum two instances of MST.

3.9.7 Link-layer discovery protocol

3.9.7.1 The Router shall support Link Layer Discovery Protocol as per IEEE 802.1ab

3.9.8 Logical Link Control

3.9.8.1 The Router shall support Logical Link control as per IEEE 802.2

3.9.9 Flow Control

3.9.9.1 The Router shall support Flow control as per IEEE 802.3x

3.9.10 Port trunking / Link Aggregation

3.9.10.1 The router shall allow Link Aggregation as per IEEE 802.3 ad to allow link resilience.

3.9.10.2 The Router shall support load balancing over Aggregated Links.

3.9.10.3 The Router shall allow configurations of static/LACP LAG on client ports.

3.9.11 Internet Group Management Protocol Version 2 and 3 (IGMPv2 and v3)

3.9.11.1 The Router shall support IGMP v2 as per RFC 2236

3.9.11.2 The Router shall support IGMP v3 as per RFC 3376

3.9.11.3 The Router shall support Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping as per RFC 4541

3.9.12 VLAN Features

3.9.12.1 The Router shall support creation of VLAN among ports of different types as well as on all ports of the interface cards.

3.9.12.2 Router shall support VLAN bridging (for outer tag only) as per IEEE 802.1ad

3.9.12.3 Router shall support user isolation per outer VLAN tag. This behavior shall be configurable on a per port basis.

3.9.12.4 Router shall support VLAN ingress filtering to prevent VLAN leakage.

3.9.12.5 Router shall support VLAN tag overlapping allowing some ports to be member of more than one VLAN.

3.9.12.6 The Router shall support IEEE 802.1Q Tagging in the following manner:

a. Tagged only, which is an IEEE 802.1Q trunk.
b. Untagged.
c. Hybrid, tagged and untagged frames.

3.9.12.7 The Type IV, V and VI Routers shall support the following additional IEEE 802.1Q features

a. Tag insertion, removal and swapping.
b. Capability of insertion and removal of second tag.
c. Encapsulation translation and rewrites Push, Pop and translate for IEEE 802.1Q or QinQ/IEEE 802.1ad tags.
d. Local VLAN and ports cross-connect and multipoint or point-to-multipoint with Hierarchical Virtual Private LAN service (H-VPLS bridge topologies with pseudo-wires) or locally defined bridge domains.

3.10 Routing Protocols

3.10.1 Static Routing

3.10.1.1 The Router shall support requirements for IP Version 4 Routing as per RFC 1812

3.10.1.2 The Router shall support policy based routing based on source and destination IPv4 address and TCP/UDP Port.

3.10.1.3 The Router shall support IPv6 static Routing

3.10.2 RIP

3.10.2.1 The Router shall support RIP v2 as per RFC 2453

3.10.2.2 The Router shall support RIPng for IPv6 as per RFC 2080

3.10.2.3 The Router shall support IPv6 policy-based routing

3.10.2.4 The Router shall support IPv6 route redistribution

3.10.2.5 Router shall support RIPv2 authentication as per RFC 4822

3.10.3 ECMP

3.10.3.1 The Router shall support Equal Cost Multi Path (ECMP) routing for load-balancing

3.10.4 IS-IS routing protocol

3.10.4.1 The Router shall support OSI ISIS Intra-domain Routing Protocol

3.10.4.2 The Router shall support use of OSI ISIS for Routing in TCP/IP and Dual Environments as per RFC 1195

3.10.4.3 The Router shall support definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers as per RFC 2474

3.10.4.4 The Router shall support Dynamic Hostname Exchange Mechanism for IS-IS as per RFC 5301

3.10.4.5 The Router shall support ISIS routes

3.10.4.6 The Router shall support IS-IS Extensions for Traffic Engineering as per RFC 5305

3.10.4.7 The Router shall support Restart Signaling for IS-IS as per RFC 5306

3.10.4.8 The Router shall support two levels of hierarchy.

3.10.4.9 The Router shall support IS-IS Mesh Groups (Default metric, LSA updates, graceful restart, TE extensions, mesh groups.)

3.10.4.10 The Router shall support HMAC keypad hashing for Message Authentication and three way handshakes for IS-IS protocol support as per as per RFC 2403/2404

3.10.4.11 The Router shall support Routing Ipv6 with ISIS as per RFC 5308

3.10.5 Virtual Router Redundancy Protocol (VRRP)

3.10.5.1 The Router shall support Virtual Router Redundancy Protocol (VRRP) as per RFC 3768

3.10.5.2 The Router shall support Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 as per RFC 5798

3.10.6 OSPF V2/V3

3.10.6.1 The Router shall support OSPF Version 2 as per RFC 1583 & RFC 2328

3.10.6.2 The Router shall support OSPF database overflow support

3.10.6.3 The Router shall support OSPF Version 2 Management Information Base as per RFC 4750

3.10.6.4 The Router shall support Applicability Statement for OSPF as per RFC 1370

3.10.6.5 The Router shall support BGP-OSPF interaction

3.10.6.6 The Router shall support OSPF Not So Stubby Area (NSSA) as per RFC 3101

3.10.6.7 The Router shall support OSPF Opaque LSA option as per RFC 5250

3.10.6.8 The Router shall support OSPF for IPv6 as per RFC5340

3.10.6.9 The Router shall support OSPF Stub Area

3.10.6.10 The Router shall support Hitless OSPF Restart (link state redundancy) Or OSPF graceful restart as per RFC 3623

3.10.6.11 The Router shall support Traffic Engineering (TE) extensions to OSPF v2 (OSPF-TE) as per RFC 3630

3.10.6.12 The Router shall support OSPF Sham Links

3.10.6.13 The Router shall support Variable length sub-netting

3.10.6.14 The Router shall support setting of Administrative costs, virtual links, area route aggregation, inter area route aggregation, route leaking

3.10.6.15 The Router shall support Route filtering based on administrative costs.

3.10.6.16 The Router shall support OSPFv3 RFC 2740 (OSPF for IPv6)

3.10.6.17 The Router shall support Authentication/Confidentiality for OSPFv3 as per RFC 4552

3.10.6.18 The Router shall support OSPF IPv6 (OSPFv3) IPSec ESP Encryption and Authentication (applicable for type III to XII Routers)

3.10.6.19 The Router shall support OSPFv3 dynamic interface cost support (applicable for type III to XII Routers)
3.10.6.20 The Router shall support OSPFv3 Fast Convergence - LSA and SPF throttling
3.10.6.21 The Router shall support OSPFv3 graceful restart

3.10.7 FRR & BFD

3.10.7.1 The Router shall support Fast Reroute Extensions to RSVP-TE for LSP Tunnels as per RFC 4090.
3.10.7.2 The Router shall support 1:N Protection, Upto 1K simultaneous LSP's
3.10.7.3 The Router shall support Bidirectional Forwarding Detection (BFD) as per RFC 5880, 5881
3.10.7.4 The Router shall support Bidirectional Forwarding Detection (BFD) for Multihop Paths as per RFC 5883
3.10.7.5 The Router shall support OSPFv3 for BFD
3.10.7.6 The Router shall support Static Route support for BFD over IPv6

3.10.8 BGP (v4 / v6)

3.10.8.1 The Router shall support BGPv4 as per RFC 4271, RFC 2283
3.10.8.2 The Router shall support for the application of the Border Gateway Protocol in the Internet shall be as per RFC 1772
3.10.8.3 The Router shall support matching and assignments of communities and extended communities.
3.10.8.4 The Router shall support BGP Communities Attribute as per RFC1997
3.10.8.5 The Router shall support BGP Extended Communities Attribute as per RFC4360
3.10.8.6 The Router shall support Using a Dedicated AS for Sites Homed to a Single Provider as per RFC 2270
3.10.8.7 The Router shall support BGP Route Flap Damping as per RFC 2439
3.10.8.8 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing shall be as per RFC 2545
3.10.8.9 The Router shall support Route Refresh Capability for BGP-4 as per RFC 2918
3.10.8.10 The Router shall support Carrying Label Information in BGP-4 as per RFC 3107
3.10.8.11 The Router shall support Autonomous System Confederations for BGP shall be as per RFC 5065
3.10.8.12 The Router shall support Capabilities Advertisement with BGP-4 as per RFC 5492
3.10.8.13 The Router shall support TCP Authentication Option as per RFC 5925
3.10.8.14 The Router shall support Address-Prefix-Based Outbound Route Filter for BGP-4 as per RFC 5292
3.10.8.15 The Router shall support transparent LAN using BGP
3.10.8.16 Shall support encryption of BGP peering session.
3.10.8.17 The Router shall support default route to individual BGP peers.
3.10.8.18 The Router shall support Soft Reset of BGP session on any or all peers.
3.10.8.19 The Router shall support Policy Routing to enable flexibility in making changes to the normal routing process based on the characteristics of the traffic.
3.10.8.20 The Router shall support Multiple BGP sessions.
3.10.8.21 The Router shall support ingress and egress route filtering which includes filtering on prefix, AS path and route maps.

3.10.8.22 The Router shall support Weight metric, Local Pref metric and Multi Exit Discriminator (MED) metric

3.10.8.23 The Router shall support Matching and assignments of MED values.

3.10.8.24 The Router shall support comparison of MED values between different sources.

3.10.8.25 The Router shall support the following BGP properties:

a. Route Target
b. Site of Origin
c. Route Refresh
d. ASN Override
e. Outbound Route Filters (ORF)
f. VPNv4 routes filtering based on route target
g. Inter-AS MPLS VPN model

3.10.8.26 The Router shall support Multiprotocol Extensions for BGP-4 as per RFC 2858

3.10.8.27 The Router shall support Capabilities Advertisement with BGP-4 as per RFC 3392

3.10.8.28 The Router shall support Graceful Restart Mechanism for BGP as per RFC 4724

3.10.8.29 The Router shall support IPv6 multiprotocol BGP link-local address peering

3.10.8.30 The Router shall support outbound route filtering for BGP4 as per RFC 5291

3.10.9 iBGP / eBGP

3.10.9.1 The Router shall support Interior BGP (iBGP) peering sessions.

3.10.9.2 The Router shall support Exterior BGP multi-path to support load balancing between two EBGP peers connected by two or more links.

3.10.9.3 The Router shall support setting the next hop to self between peering sessions on a per route, per peer, per AS basis regardless of if it is a eBGP, iBGP or Confederated peering session.

3.10.9.4 The Router shall support next hop tracking & Control to enable network administrators to control peering requirements with exterior BGP peers.

3.10.10 MP-BGP

3.10.10.1 The Router shall support Multi Protocol BGP (MP BGP) with the following extensionsn as per RFC 4760:

a. Multi-protocol Reachable Network Layer Reachability Information
b. Multi-protocol Non-Reachable Network Layer Reachability Information
c. Extended Community Attribute

3.10.10.2 The Router shall support Next Generation Multicast VPN features (MVPN using MP-BGP) as per RFC6513 and RFC 6516 (Ipv6)

3.10.11 Load balancing

3.10.11.1 The Router shall support Load balancing on bearer pin-hole assignment if multiple paths exist between two end points.

3.10.11.2 The Router shall support BGP4 Multi path to enable load balancing between multiple exterior BGP peers from the same downstream router.

3.10.11.3 The Router shall support Load balancing across WAN links.

3.10.12 Route Reflector

3.10.12.1 RRs are deployed in a hierarchical network to reduce the direct peering among the routers. The Router shall support BGP Route Reflection.

3.10.12.2 The Router shall support Route Reflector client and non-Route Reflector client peering sessions as per RFC4456

3.10.12.3 Different RR deployment scenarios in Service Provider networks shall be as follows:

a. RR for IPv4 and VPNv4 routes
b. RR for IPv6 and VPNv6 routes
c. Service Specific RR
d. Location redundancy

3.11 Multicast Features

General:

3.11.1.1 The Router shall support Prioritization of multicast traffic

3.11.1.2 The Router shall support to maintain static multicast entries in a separate multicast table.

3.11.1.3 The Router shall support Multicast ACL to ensure security

3.11.1.4 The Router shall support Multicast Load Balancing traffic across multiple interfaces

3.11.1.5 The Router shall support administratively Scoped IP Multicast (IPv4 Multicast address space) as per RFC 2365

3.11.1.6 The Router shall provide statistics on all active groups, sources on a per VLAN or port basis.

3.11.1.7 The Router shall support Multicast VPN based on (Draft-ietf-l3vpn-2547bis-mcast-01.txt & Draft-raggarwa-l3vpn-2547-mcast-bgp) & mVPN (draft-rosen-vpn-mcast with min 20Gbps throughput)

3.11.2 IGMP

3.11.2.1 The Router shall support Internet Group Management Protocol, Version 3 as per RFC 3376

3.11.2.2 The Router shall support Host Extensions for IP Multicasting as per RFC 1112 ()

3.11.2.3 The Router shall support Source based and shared distribution trees

3.11.3 PIM

3.11.3.1 The Router shall support Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) as per RFC 3446 ()

3.11.3.2 The Router shall support Protocol Independent Multicast MIB as per RFC 5060

3.11.3.3 The Router shall support Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) as per RFC 5059

3.11.3.4 The Router shall support Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification as per RFC 4601

3.11.3.5 The Router shall support Rendezvous Point (RP) on both leaf and non-leaf nodes – ability to be configured as an RP

3.11.3.6 The Router shall support Automatic route processing (AutoRP) ()

3.11.3.7 The Router shall support Multicast Source Discovery Protocol (MSDP) as per RFC 3618 ()

3.11.3.8 The Router shall support Bootstrap Router Mechanism for PIM Sparse Mode

3.11.3.9 The Router shall support PIM Source Specific Multicast (PIM-SSM) as per RFC 3569

3.11.3.10 The Router shall support Source-Specific Multicast for IP as per RFC4607

3.11.4 Anycast

3.11.4.1 The Router shall support operation of Anycast Services

3.11.4.2 The Router shall support Dynamic broadcast Source Failover using Anycast routing

3.11.5 IPv6 Multicast

The router shall support the following IPv6 Multicast features

3.11.5.1 IPv6 Multicast Address Assignments as per RFC 2375
3.11.5.2 IPv6 multicast Address Group Range Support
3.11.5.3 IPv6 Multicast Listener Discovery (MLD) protocol, versions 1 and 2 as per RFC 2710
3.11.5.4 MLDv2 for IPv6 as per RFC 3810
3.11.5.5 IPv6 multicast MLD group limits
3.11.5.6 IPv6 multicast SSM mapping for MLDv1 SSM
3.11.5.7 IPv6 Router Alert Option as per RFC 2711
3.11.5.8 Transmission of IPv6 Packets over Ethernet as per RFC 2464
3.11.5.9 IPv6 PIM sparse mode (PIM-SM)
3.11.5.10 IPv6 PIM Source Specific Multicast (PIM-SSM)
3.11.5.11 IPv6 multicast PIM accept register
3.11.5.12 IPv6 multicast PIM embedded RP support
3.11.5.13 IPv6 multicast scope boundaries
3.11.5.14 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
3.11.5.15 IPv6 multicast MLD access group
3.11.5.16 IPv6 multicast RPF flooding of bootstrap router (BSR) packets
3.11.5.17 IPv6 multicast routable address hello option
3.11.5.18 IPv6 multicast static multicast routing (mroute)
3.11.5.19 IPv6 multicast address family support for Multiprotocol Border Gateway Protocol (MBGP)
3.11.5.20 IPv6 multicast Explicit tracking of receivers
3.11.5.21 IPv6 multicast IPv6 BSR scoped-zone support
3.11.5.22 IPv6 multicast IPv6 BSR—ability to configure RP mapping

3.12 MPLS Requirements

3.12.1 Multi-protocol Label Switching (MPLS)

3.12.1.1 The Router shall support Multi Protocol Label Switching Architecture as per RFC 3031
3.12.1.2 The Router shall support MPLS Label Stack Encoding as per RFC 3032
3.12.1.3 The Router shall support Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks as per RFC 3443
3.12.1.4 The Router shall support the Generalized TTL Security Mechanism (GTSM) as per RFC5082
3.12.1.5 The Router shall support Framework for Multi-Protocol Label Switching (MPLS)-based Recovery as per RFC 3469
3.12.1.6 The Router shall support Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) as per RFC 3813
3.12.1.7 The Router shall support MPLS Label Switch Router/Label Switch Controller software (LSR)
3.12.1.8 The Router shall support MPLS Label Edge Router(LER) functionality.

3.12.1.9 The Router shall support Dynamic MPLS LSP setup with signaling protocol on all the router interfaces.

3.12.1.10 The Router shall support LSP path optimization. When new LSPs are added, LSP re-optimization is performed to reroute LSPs to follow a lower cost path with no data loss to existing traffic.

3.12.1.11 The Router shall support MPLS class of service.

3.12.1.12 The Router shall support ICMP Extensions for Multi Protocol Label Switching

3.12.1.13 The Router shall limit the number of routes per VRF.

3.12.1.14 The Router shall set Thresholds to provide traps and alarms when a certain number of routes are exceeded.

3.12.1.15 The Router shall support Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field shall be as per RFC 5462

3.12.1.16 The Router shall support Bidirectional Forwarding Detection (BFD) for MPLS LSPs as per RFC 5880 and RFC 5884.

3.12.2 LDP

3.12.2.1 The Router shall support LDP specification as per RFC5036

3.12.2.2 The Router shall support LDP Applicability as per RFC 3037

3.12.2.3 Graceful Restart Mechanism for Label Distribution Protocol shall be as per RFC 3478

3.12.3 MPLS VPN

3.12.3.1 The Router shall advertise both VPN routes and public internet routes in the same BGP routing instance.

3.12.3.2 The Router shall support Internet Access from the same VPN and internet Access from the global routing instance.

3.12.3.3 The Router shall support Extranet functionality

3.12.4 MPLS Layer-2 VPN

3.12.4.1 The Router shall support Framework for Layer 2 Virtual Private Networks (L2VPN) as per RFC 4664

3.12.4.2 The Router shall support Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks as per RFC 4665

3.12.4.3 The Router shall support MPLS-based point-to-point VPN: Transport of Layer 2 Frames Over MPLS as per RFC 4906

3.12.4.4 The Router shall support Address Allocation for Private Internets (Private and overlapping IP addressing) as per RFC 1918

3.12.5 MPLS Layer-3 VPN

3.12.5.1 The Router shall support BGP/MPLS IP Virtual Private Networks (VPNs) as per RFC 4364

3.12.6 VPLS:

3.12.6.1 The Router shall support Virtual Private LAN Services (VPLS), Hierarchical VPLS (H-VPLS), Virtual Private Wire Services (VPWS), Ethernet over MPLS (EoMPLS) and multi-segment pseudo-wire stitching.

3.12.6.2 The Router shall support VPLS with pseudo wire redundancy.

3.12.6.3 The Router shall support Active/standby pseudo wire.

3.12.6.4 The Router shall support PW redundancy with MAC withdrawal.

3.12.6.5 The Router shall support disable learning for providing the capability to effectively manage when addresses are added to a FIB in VPLS services.

3.12.6.6 The Router shall support FIB size limit for providing the ability to configure a maximum FIB size on a per VPLS service basis.

3.12.6.7 The Router shall support VPLS service on all the interfaces.

3.12.6.8 The Router shall support Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling as per RFC 4762

3.12.7 Autonomous System

3.12.7.1 The Router shall support Guidelines for creation, selection, and registration of an Autonomous System (AS) (Private and overlapping Autonomous System Numbers) as per RFC1930

3.12.7.2 The Router shall support Inter AS IPVPN

3.12.7.3 The Router shall support Inter Area Autonomous System (InterAS)

3.12.8 MPLS-TP

3.12.8.1 The Router shall support MPLS-TP requirements as per RFC 5654 or ITU Y.SUP4

3.12.8.2 The Router shall support Architecture of MPLS-TP Layer Network as per ITU-T G.8110.1v2 or equivalent IETF standards

3.12.8.3 The Router shall support Interfaces for the MPLS-TP Hierarchy as per ITU-T G.8112 or equivalent IETF standards

3.12.8.4 The Router shall support Characteristics of MPLS-TP Network Equipment Functional Blocks as per ITU-T G.8121v2 or equivalent IETF standards

3.12.8.5 The Router shall support MPLS-TP General Framework as per RFC 5921 or ITU G.8110.1

3.12.8.6 The Router shall support MPLS-TP survivability framework as per RFC 6372 or ITU G.8131/G.8132

3.12.8.7 The Router shall support MPLS-TP Data plane Architecture as per RFC5960 or ITU Y.SUP4

3.12.8.8 The Router shall support MPLS Generic Associated Channel (GAL/G-ACH) as per RFC 5586 or ITU G.8113.1/G.8113.2

3.12.8.9 The Router shall support Definition of ACH TLV Structure as per draft-ietf-mpls-tp-ach-tlv-02 or ITU G.8113.1/G.8113.2

3.12.8.10 The Router shall support enable/disable IEEE 802.1ag on a per port basis or BFD on a per tunnel / pseudowire basis for non MPLS-TP tunnels for the purpose of monitoring the traffic along a link / tunnel / pseudowire as the case may be.

3.12.8.11 The Router shall support Pseudowire Status for Static Pseudowires as per RFC 6478

3.12.8.12 The Router shall support MPLS On-Demand Connectivity Verification and Route Tracing as per RFC 6426 or ITU G.8113.1/G.8113.2

3.12.8.13 The Router shall support Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile as per RFC 6428 or ITU G.8113.1/G.8113.2

3.13 General IPv6 Features

3.13.1 General Support

3.13.1.1 The Router shall support IPv6 Specification as per RFC 8200

3.13.1.2 The Router shall support Path MTU Discovery for IPv6 as per RFC 8201

3.13.1.3 The Router shall support ICMPv6 for IPv6 Specification as per RFC 4443

3.13.1.4 The Router shall support ICMPv6 redirect
3.13.1.5 The Router shall support ICMPv6 rate limiting
3.13.1.6 The Router shall support Neighbor Discovery for IP version 6 (IPv6) as per RFC 4861
3.13.1.7 The Router shall support IPv6 neighbor discovery duplicate address detection
3.13.1.8 The Router shall support IPv6 Stateless Address Autoconfiguration as per RFC 4862
3.13.1.9 The Router shall support IPv6 addressing architecture as per RFC 4291
3.13.1.10 The Router shall support deprecation of Type 0 Routing Headers in IPv6 as per RFC 5095
3.13.1.11 The Router shall support IPv6 global unicast address format as per RFC 3587
3.13.1.12 The Router shall support IPv6 jumbograms.

3.13.2 Additional IPv6 Support Features

3.13.2.1 The Router shall support IPv6 Scoped Address Architecture as per RFC 4007
3.13.2.2 The Router shall support Unique Local IPv6 Unicast Addresses as per RFC 4193
3.13.2.3 The Router shall support Management Information Base for the Internet Protocol as per RFC 4293
3.13.2.4 The Router shall support SNMP over IPv6
3.13.2.5 The Router shall support IPv6 ping
3.13.2.6 The Router shall support Syslog over IPv6
3.13.2.7 The Router shall support IPv6 over PPP as per RFC 2472
3.13.2.8 The Router shall support IP Forwarding Table MIB as per RFC 4292
3.13.2.9 The Router shall support NETCONF with YANG over IPv6

3.14 Advanced IPv6 Features

3.14.1 Carrier Grade NAT

3.14.1.1 The Router shall support Network Address Translation-Protocol Translation (NAT-PT) as per RFC 2766

3.14.1.2 The Router shall support overload (PAT)

3.14.1.3 The Router shall support source-based NAT

3.14.1.4 The Router shall support to enable/disable NAT & NAPT for group of source/destination pools using any transport protocol

3.14.1.5 The Router shall support Architectural Implications of NAT as per RFC 2993

3.14.1.6 The Router shall support fragmented packets and allow such packets to pass through

3.14.1.7 The Router shall support translating (modify) IP datagrams passing between two IPv4 domains

3.14.1.8 The Router shall support for IP Network Address Translator (NAT) Terminology and Considerations

3.14.1.9 The Router shall support fragmentation

3.14.1.10 The Router shall support basic NAT-44

3.14.1.11 The Router shall support NAPT44

3.14.1.12 The Router shall support NAT64 as per RFC 6146

3.14.1.13 The Router shall support NAT444 as per RFC 6127

3.14.1.14 The Router shall support Dynamic NAT44

3.14.1.15 The Router Performance should not be impacted by running multiple concurrent translation methods

3.14.1.16 The Router Throughput performance should not be impacted more than 5% if NAT/NAPT are activated for all subscribers

3.14.1.17 The Router shall support load balancing process to handle incoming traffic between several instances on several cards simultaneously

3.14.1.18 The Router shall support enabling/disabling NAT capabilities at different levels of the NAT components hierarchy : interface, card, inside IP pool or outside IP pool.

3.14.1.19 The Router shall support various filtering techniques such as endpoint independent filtering, and address dependent filtering

3.14.1.20 The Router shall support static allocation of IPv4 and IPv6 and port binding to configurable set/all users

3.14.1.21 The Router shall support NAT outside pool to be made up of contiguous IPv4 subnets, non-contiguous IPv4 subnets and/or a combination of both

3.14.1.22 The Router shall support Port Block Allocation and log reduction

3.14.1.23 The Router shall support Dual-Stack lite broadband deployments post IPv4 address exhaustion as per draft-ietf-softwire-dual-stack-lite

3.14.1.24 The Router shall support DS-Lite AFTR (Address Family Transition Router) function

3.14.1.25 The Router shall support NAT/NAPT from one IP-VPN context to the global/default routing context

3.14.1.26 The Router shall support NAT/NAPT from one IP-VPN context to another IP-VPN context

3.14.1.27 The Router shall support NAT behavioral Requirements for TCP as per RFC 5382

3.14.1.28 The Router shall support NAT behavioral Requirements for UDP as per RFC 4787

3.14.1.29 The Router shall support NAT behavioral Requirements for ICMP as per RFC 5508

3.14.1.30 The Router shall support adjusting checksum values of all IP, UDP, TCP and ICMP headers

3.14.1.31 The Router shall support all TCP and UDP based applications in NAT64 environment

3.14.1.32 The Router shall support mapping table between Inside IP (private IPs) and Outside IP (public Ips) and ports

3.14.1.33 The Router shall support mapping table generate log message per day with time stamp, inside prefix, outside prefix, outside mask, reserved ports, dynamic address pool factor, maximum ports per user etc.

3.14.1.34 The Router shall support prohibition of mapping of the previliged/well-known TCP and UDP ports

3.14.1.35 The Router shall support allocation of the same public IP address for a customer as detected on the source IPv6 address in DS-Lite and NAT64 or IPv4 in NAT44

3.14.1.36 The Router shall support Bypass within NAT rule for certain traffic

3.14.1.37 The Router shall support hairpinning when both source and destination are managed by same CGNAT device

3.14.1.38 The NAT function of Router shall interpret the IPv4 TOS and IP Precedence field in accordance to the RFC2474 DiffServe (DS) interpretation and meanings

3.14.1.39 The Router shall support requirements for IP Version 4 Routers as per RFC 1812

3.14.1.40 The Router shall support different translation and tunnelling techniques such as NAT/NAPT 44, NAT/NAPT 64, DS-Lite and Static NAT technique on same blade

3.14.1.41 The Router shall support Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers as per RFC 6146

3.14.2 IPv6 Tunneling

3.14.2.1 The Router shall support generic packet tunneling in Ipv6 as per RFC 2473

3.14.2.2 The Router shall support connection of IPv6 Domains via IPv4 Clouds as per RFC 3056

3.14.2.3 The Router shall support an Anycast Prefix for 6to4 Relay Routers

3.14.2.4 The Router shall support Basic Transition Mechanisms for IPv6 Hosts and Routers as per RFC 4213

3.14.2.5 The Router shall support MPLS/BGP Layer 3 VPN MIB as per RFC 4382

3.14.2.6 The Router shall support BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN as per RFC 4659

3.14.2.7 The Router shall support connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) as per RFC 4798

3.14.2.8 The Router shall support Automatic IPv4-compatible tunnels

3.14.2.9 The Router shall support manually configured IPv6 over IPv4 tunnels

3.14.2.10 The Router shall support IPv6 over IPv4 tunnels

3.14.2.11 The Router shall support IP over IPv6 tunnels

3.14.2.12 The Router shall support IPv6 VPN over MPLS

3.14.2.13 The Router shall support IP SLAs (Service Level Agreements) for IPv6

3.14.2.14 The Router shall support IP/ICMP transition as per RFC 6145

3.14.2.15 The Router shall support dual stack transition mechanism

3.15 Traffic Engineering Requirements

The metrics involved in routing algorithms and Spanning Tree calculations often leads to certain paths being selected more often than others. As network utilization increases, certain links can be overloaded, while others sit idle. Traffic engineering solves this problem by providing the control required to balance the use of precious network resources. Additionally, traffic engineering enables the service provider to create route diversity, which minimizes the risk of a single link or device failure causing a simultaneous interruption to both the primary and backup path through a network.

3.15.1 General Traffic Engineering Requirements:

3.15.1.1 The Router shall support manual configuration and provisioning functionality of end-to-end traffic tunnels through eMS.

3.15.1.2 The Router shall support traffic tunnels of minimum 2Mbps granularity.

3.15.1.3 The Router shall support protection to a TE tunnel through two explicit paths configured through the network by the administrator.

3.15.1.4 The Router shall support capability of re-optimizing the TE tunnel path based on the network status. The network manager shall also re-optimize the TE tunnel through CLI during troubleshooting/management.

3.15.1.5 The Router shall support options for automatic and manual selection of TE path.

3.15.1.6 The Router shall support to establish routing adjacencies between two routers over the TE tunnel.

3.15.1.7 The Router shall support bandwidth management features.

3.15.2 MPLS Traffic Engineering

3.15.2.1 The Router shall support requirements for Traffic Engineering Over MPLS as per RFC 2702

3.15.2.2 The Router shall support dynamic MPLS Traffic Engineering

3.15.2.3 The Router shall support Traffic Engineering Extensions to OSPF Version 2 as per RFC 3630

3.15.2.4 The Router shall support IS-IS Extensions for Traffic Engineering shall be as per RFC 5305

3.15.2.5 The Router shall support OSPF inter area MPLS Traffic Engineering

3.15.2.6 The Router shall support automatic bandwidth adjustment for TE tunnels.

3.15.2.7 The Router shall support linkages to the IGP Traffic Engineering database to enable Constraint Based Shortest Path First (CSPF) calculations for tunneling.

3.15.2.8 The Router shall support IGP (OSPF and IS-IS) traffic engineering LSAs flooding of bandwidth constraints across local areas.

3.15.2.9 The Router shall support each interface carry multiple MPLS TE tunnels for various traffics of different priority. Different levels of priority shall be assigned to various TE tunnels.

3.15.3 RSVP .

3.15.3.1 Resource Reservation protocol shall provide the label distribution. The Router shall have the capability to do CSPF signaling based on the IGP link state database.

3.15.3.2 The Router shall support Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification as per RFC 2205

3.15.3.3 The Router shall support Applicability Statement for Extensions to RSVP for LSP-Tunnels

3.15.3.4 The Router shall support IGP Area tunneling for RSVP

3.15.3.5 The Router shall support Aggregation of Martini circuits within an RSVP–TE tunneled LSP

3.15.3.6 All interfaces and sub-interfaces of the Router shall support RSVP-TE signaling.

3.15.3.7 The Router shall support RSVP and RSVP-TE Extensions to RSVP for LSP Tunnels as per RFC 3209 with support of

a. Create one or more explicit paths with bandwidth assurances for each traffic trunk.
b. Takes into consideration the policy constraints associated with trunks, as well as the physical network resources and network topology.
c. Packet routes are based not only on destination address, but also on resource availability and policy.
d. MPLS Fast Reroute Extensions to RSVP-TE for LSP Tunnels, both link protection and Node protection shall be as per RFC 4090. The re-route shall be completed within 50 ms for up to 8K simultaneous LSP.
e. RSVP Refresh Reduction Extensions shall be as per RFC 2961
f. Shall provide the mechanism to setup an explicitly routed LSP that could differ from the normal path calculated by the IGP.
g. Shall perform 'downstream on demand' label allocation, distribution, and binding among LSRs in the path, thus establishing path state in network nodes.
h. LSP pre-emption based on administrative policy control or QOS based congestion management for LSP.
i. Loop detection and avoidance during the initial LSP set-up and rerouting an existing LSP.
j. Monitor and maintain the state of an explicitly routed LSP
k. Pre-emption and defending priority settings.

3.15.4 Pseudo-Wire Emulation

3.15.4.1 The Router shall support Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3) as per RFC 3916

3.15.4.2 The Router shall support Pseudo-Wire Emulation Edge-to-Edge (PWE3) Architecture as per RFC 3985

3.15.4.3 The Router shall support PWE3 Control Word for Use over an MPLS PSN as per RFC 4385

3.15.4.4 The Router shall support Encapsulation Methods for Transport of Ethernet over MPLS Networks as per RFC 4448

3.15.4.5 The Router shall support Pseudowire (PW) Management Information Base (MIB) as per RFC 5601

3.15.4.6 The Router shall support Pseudo wire Setup and Maintenance using LDP as per RFC 4447

3.15.4.7 The Router shall support PWE3 fragmentation and reassembly as per RFC 4623

3.15.4.8 The Router shall support segmented Pseudowires as per RFC 6073

3.15.5 Multicast Traffic Engineering

3.15.5.1 The Router shall support Point-to-Multipoint (P2MP) LSP: Establishing Point-to-Multipoint MPLS TE LSPs.

3.15.5.2 The Router shall support Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs) as per RFC 4875 for Core/Edge Routers

3.15.5.3 M-ISIS: The Router shall support Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs) as per RFC 5120

3.15.6 DS-TE

3.15.6.1 Diffserv TE: The Router shall support traffic prioritization into 8 class types. Class types shall be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints shall be assigned to individual hardware queues.

3.15.6.2 The Router shall support MPLS Support of Differentiated Services as per RFC 3270

3.15.6.3 The Router shall support Differentiated Services-aware MPLS Traffic Engineering as per RFC 3564

3.15.6.4 The Router shall support Protocol Extensions for Diffserv-aware MPLS Traffic Engineering as per RFC 4124

3.15.6.5 The Router shall support Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering.

3.15.6.6 The Router shall support Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering as per RFC 4127

3.15.6.7 The Router shall support MPLS-TP tunnels with support of per LSP queuing/scheduling i.e. the ability to assign and guarantee per class bandwidth profiles (CIR, EIR, CBS, and EBS) for each LSP.

3.15.6.8 The Routers shall support both the MPLS LSP Link and node-link protection to help reduce the amount of time taken to reroute LSP traffic in case of failure scenario.

3.16 Quality of Service Requirements

3.16.1 General:

3.16.1.1 The Router shall support QoS in all Types of interfaces.

3.16.1.2 The Router shall support the QoS features per port and per VLAN

3.16.1.3 The Router shall support VLAN CoS preservation.

3.16.1.4 The Router shall support VLAN CoS differentiation: It shall be possible to configure the classification of the traffic according to the port, VLAN, IEEE 802.1p bits or TOS/DSCP bits.

3.16.1.5 The Router shall support creation of VLAN or Flow with TCP/IP parameters per service for data, video and O&M traffic for service differentiation.

3.16.1.6 The Router shall support prediction of performance bounds for each flow in terms of throughput, loss, delay and delay variation, according to their respective defined service classes.

3.16.1.7 The Router shall support 16, 32, 64, 128, 256 and 512 k Bytes burst sizes

3.16.1.8 The Router shall support wire speed forwarding on all interfaces and all packet sizes even with classification and QoS activated on all interfaces.

3.16.1.9 The Router shall support bandwidth management reports and statistics.

3.16.2 Diff-Serv

3.16.2.1 The Router shall support Diff-Serv as per RFC3260.

3.16.2.2 The Router shall support IEEE 802.1Q DEI and IEEE 802.1p PCP including support for untagged as well as tagged priority frames.

3.16.2.3 The Router shall support Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers as per RFC 2474

3.16.2.4 The Router shall support Architecture for Differentiated Services as per RFC 2475

3.16.2.5 The Router shall support MIB for Diff-Serv as per RFC 3289

3.16.2.6 The Router shall support IP Precedence (TOS-IPP)

3.16.2.7 The Router shall support Per Hop Behavior Identification Codes as per RFC 3140

3.16.2.8 The Router shall support Assured Forwarding PHB Group as per RFC 2597

3.16.2.9 The Router shall support Expedited Forwarding PHB (Per-Hop Behavior) as per RFC 3246

3.16.3 Classification/Prioritization:

3.16.3.1 The Router shall support Policy based bandwidth classification

3.16.3.2 The Router shall support Service QoS flow identification.

3.16.3.3 The Router shall support classification of ingress traffic for a specific service based on the following mapping:

a. IEEE 802.1P Mapping - it shall be possible to reserve parts of the link bandwidth for frames with particular IEEE 802.1p values.
b. Customer IEEE 802.1p priority
c. IP DSCP Mapping as per RFC 5462
d. Multiprotocol Label Switching (MPLS) Label Stack Entry:"EXP" Field Renamed to "Traffic Class" Field as per RFC 5462
e. Ethernet L2 Based Conversation and protocol Mapping.
f. Source MAC address
g. Destination MAC address
h. Ether Type or Protocol Type
i. Incoming port (Logical and Physical)
j. Incoming/Destination IP address and mask
k. Source/Destination TCP/UDP Port
l. Type of Service (ToS) Precedence bits.
m. UDP/TCP socket
n. VLAN ID
o. IEEE 802.1Q
p. Default queue for non-matching traffic

3.16.3.4 The Router shall aggregate incoming traffic into Traffic Classes by following characteristics:

a. Incoming port (Logical and Physical)
b. Incoming/Destination IP address
c. Source/Destination TCP/UDP Port
d. Type of Service (ToS) Precedence bits.
e. Source/ destination MAC
f. Type of Protocol
g. UDP/TCP socket
h. Link layer priority information as per IEEE 802.1p

3.16.3.5 The Router shall support classification based on.

a. Layer-4 information
b. Source and Destination port/range numbers

3.16.3.6 The Router shall support traffic prioritization.

3.16.3.7 The Router shall give all network base keep alives (PPP keep alives, OSPF LSAs, BGP, SNMP etc.) highest priority and route before any traffic type.

3.16.4 Mapping:

3.16.4.1 The Router shall support mapping of DSCP to VLAN or other traffic engineering capabilities in the Regional Network.

3.16.4.2 The Router shall aggregate incoming traffic into Traffic Classes by MPLS Label EXP bits (E-LSP)

3.16.4.3 The Router shall support mapping of IEEE 802.1p and IP TOS bits into MPLS EXP bits.

3.16.4.4 The Router shall support mapping of IEEE 802.1q VLAN tags into MPLS labels

3.16.5 Marking/Policing/Shaping:

The Router shall support the following Marking/Policing/Shaping requirements

a. 8 level Priority marking as per IEEE 802.1p
b. Filtering
c. Broadcast/Multicast suppression
d. Bandwidth management policies.
e. Single rate three colour marking (srTCM) RFC 2697
f. Two rate three colour metering (trTCM) RFC 2698
g. Colour aware srTCM and trTCM based metering
h. Trust the colour of the incoming packet.
i. Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic
j. 4K ingress policing instances with 10 entries in each
k. Ingress and egress policing based on Layer 3-4 information.
l. Shaping of Burst Traffic

3.16.6 Rate Limiting:

3.16.6.1 The Router shall support Rate limiting of bandwidth per Port and per class (or flow)

3.16.6.2 The Router shall support configuration of user bandwidth in steps of

- 64kbps for less than 1 Mbps
- 1 Mbps for 1-1000Mbps
- 100 Mbps granularity for 1-100 Gbps.

/ The Router shall support configuration of user bandwidth in Percentage.

3.16.6.3 The Router shall support defining Committed Information Rate (CIR) and an Excess Information Rate (EIR) for each flow in steps of 1Mbps

3.16.6.4 The Router shall support flow based rate limiting method based on per source address, destination address or both.

3.16.7 Queuing:

3.16.7.1 The Router shall support the following queuing

a. SPQ – Strict Priority Queuing
b. WFQ – Weighted fair Queuing (This feature is not mandatory for Routers [Type I/II/III/XIII/XIV/XV/XVI/XVII])
c. Diff-Serv queuing for the Assured forwarding (AF) and Expedited forwarding.
d. No of queues per flow treatment of traffic.
e. Setting the maximum size/depth of all queues.
f. Intelligent queuing based on IP ToS bits for scalability.
g. Per service ingress queues are defined on the basis of Maximum burst Size (MBS), Committed Burst Size (CBS), Peak Information Base (PIB) and committed Information rate (CIR).
h. Per service egress queues have distinct parameters defining its operations like Maximum burst Size (MBS), Committed Burst Size (CBS), Peak Information Base (PIB) and committed Information rate (CIR).

i. Alternate priority routing traffic necessary to keep from starving other priority queues.
j. Service Level Accounting:
k. Counters for queues for billing and accounting.

3.16.7.2 The Router shall support each queue with the following counters:

a. Counters for packets and octets accepted into the queue.
b. Counters for packets and octets rejected at the queue.
c. Counters for packets and octets transmitted in-profile.
d. Counters for packets and octets transmitted out-of-profile.

3.16.8 Scheduling:

3.16.8.1 The Router shall support scheduling of queues to strict priority with 2 or more priority levels

3.16.8.2 The CE Routers [Type I/II/III] shall support the following congestion avoidance mechanisms

a. Tail Drop
b. WTD (Weighted Tail Drop)
c. Selective Packet Discard
d. Longest Queue Drop for extreme or sudden congestion
e. Deficit Round Robin (DRR)
f. Weighted Round Robin (WRR)
g. DWRR(Deficit Weighted Round Robin)
h. WRED
i. Modified Deficit Round Robin (MDRR)
j. Strict Priority (SP)
k. SP + Weighted Round Robin (SP + WRR)

3.16.8.3 The Aggregation/Edge/Core Routers [Type IV to XII] shall support the following congestion avoidance mechanisms

a. Tail Drop
b. Selective Packet Discard
c. WRED
d. Weighted Fair Queuing
e. Strict Priority (SP)

3.16.8.4 The Router shall support configuring the scheduling as per the

a. Per Hop Behaviour (PHB).
b. Physical port or logical port basis.
c. 100ms ingress buffering and 100ms egress buffering at line-rate.
d. Upto 8 forwarding class queues can be configured on a per service basis each with its own CIR, PIR, CBS, MBS and Forwarding Class attribute.
e. At least three level dropping precedence levels in each queue.

3.16.8.5 The Non-Chasis Routers shall support the following congestion avoidance mechanisms

l. Tail Drop
m. Weighted Round Robin (WRR)
n. WRED (applicable for type XIV Routers)
o. Strict Priority (SP)
p. SP + Weighted Round Robin (SP + WRR)

3.16.8.6 The Router shall support Scheduling/ queuing for 4/8 classes that provide configurable minimum bandwidth allocation to each class, based on IEEE 802.1p and IP TOS bits.

3.16.9 Hierarchical QOS

3.16.9.1 The Router shall support hierarchical QoS at egress at CoS, Flow, EVC Tunnel and MPLS-TP/Egress UNI level.

3.16.9.2 The Router shall support at least 500 EVC level queues.

3.16.9.3 The Router shall support traffic buffering and shaping capability with at least 32 MB buffering.

3.16.9.4 The Router shall support traffic shaping at egress is done on per MPLS-TP Tunnel basis.

3.16.9.5 The Router shall support upto 3 levels of QoS.

3.16.10 IPv6 QoS features

3.16.10.1 The Router shall support packet classification

3.16.10.2 The Router shall support traffic shaping

3.16.10.3 The Router shall support traffic policing

3.16.10.4 The Router shall support packet marking/re-marking

3.16.10.5 The Router shall support IPv6 QoS queuing

3.16.10.6 The Router shall support weighted random early detection (WRED)- based drop

3.16.10.7 The Router shall support NSF and graceful restart for MP-BGP IPv6 address family

3.17 Circuit Emulation Protocols

The legacy TDM traffic shall be carried over the Router Transport network using circuit emulation methods. Payloads shall be encapsulated by the terminating Router over the following standards. The Service Provider shall specify the type of circuit emulation protocol required.

3.17.1.1 The Router shall support PW using Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP). It is possible to change the VCID and tunnel label from UI so as to allow integration to third party MPLS network as per RFC 4553

3.17.1.2 The Router shall support Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN) as per RFC 5086

3.18 Network Synchronization Requirements

3.18.1 General

3.18.1.1 The router shall be able to synchronize with an external reference clock.

3.18.1.2 The Router shall support Synchronous clock selection algorithm based on the following parameters:

a. Quality of Signal
b. Signal fail
c. Priority
d. External Commands

3.18.2 NTP Support:

The Router shall support Network Time Protocol (NTP) for synchronizing with a central NTP server. Network Time Protocol Version 4: Protocol and Algorithms Specification shall be as per RFC 5905

3.18.3 PTP Support:

The Router shall support Precision Time Protocol (PTP) which enables precise synchronization of clocks via packet networks shall be as per IEEE 1588v2. The Router shall support Boundary Clock and Transparent clock functionality of PTP as per IEEE 1588v2.

3.18.4 SyncE Support:

The Router shall support timing and synchronization aspects of Packet Networks based on SyncE as per G.8261. The Router shall support timing characteristics of a synchronization slave clock as per G.8262.

3.18.5 Synchronization reference

3.18.5.1 The Router shall support the external synchronization through BITS interface (2Mbps or 2MHz).

3.18.5.2 Frequency accuracy, hold-over mode accuracy, clock bandwidth and frequency pull-in and pull-out range shall be as per ITU-T Recommendations.

3.18.6 Timing output interface

The Router shall support provide a timing-output interface at 2048 KHz for external synchronization. The output shall conform to ITU-T Rec. G.812, as applicable.

3.19 Protection Switching Requirements

3.19.1 Protection Switching Time:

3.19.1.1 For all the modes of protection, the Router shall support automatic switching within 50ms of expiration of any manually selected hold-off time (with both SF/SD scenario) and shall support all operator commands (Forced Switching[FS], manual Switching [MS], lockout of protection).

3.19.2 Protection Switching Modes for SDH Interfaces:

3.19.2.1 The Router shall support automatic switching and Forced switching as analogous to SDH systems.

3.19.2.2 The Router shall support automatic switching triggered by fault detection, such as loss of signal, loss of frame, signal degrade (BER becomes worse than the predetermined threshold), and so on.

3.19.2.3 The Router shall support Forced switching activated by administrative events, such as fibre rerouting, fibre replacement, etc.

3.19.3 Ring Protection Mechanism:

3.19.3.1 The Router shall support EoMPLS ring protection for both S-VID and B-VID as per G.8032

3.19.4 Linear protection mechanisms:

3.19.4.1 The Router shall support MPLS-TP Linear Protection support as per IETF standards

OR

Ethernet/MPLS SNC based protection as per ITU-T standards.

3.19.4.2 The Router shall support customer ELAN/multicast traffic transported over a co-routed bidirectional P2MP MPLS-TP tunnel or VPLS to allow Traffic Engineered ELAN circuits provisioning.

3.19.5 OAM Requirements:

3.19.5.1 The switching mechanism is generally realized by the OAM function; therefore, the required OAM information field is reserved in the OAM frame

3.20 Scalability Requirements

3.20.1 The Router has UNI (User Network Interface) and NNI (Network Node Interfaces). The Router shall support UNI or NNI mode of operation on all the ports.

3.20.2 Single tagged or IEEE 802.1Q Mode

3.20.2.1 The Router shall allows configuring all 4094 VID on all ports and at the same time supporting all 4094 VLANs simultaneously. The user/operator shall be able to reuse the same VLAN-ID on a different port on the same router and terminate it into a different PW/VLAN.

3.20.2.2 The Router shall accept untagged, priority tagged and C-tagged frames through a IEEE 802.1Q port.

3.20.3 Q-in-Q or IEEE 802.1ad mode Requirements

3.20.3.1 The Routers shall perform classification and service delineation based on outer Q tag and outer IEEE 802.1p bits. (i.e. ignore inner tag).

a. It shall support VLAN stacking as per IEEE 802.1ad
b. It shall have minimum of 4094 S-VIDs. VIDs “0” and “FFFF” is reserved.
c. It shall allow only S-tagged frame in .1ad ingress ports. It shall be possible to map the traffic to any PW based on SVLAN tag. It shall be possible to keep or pop the SVLAN tag before forwarding it to the PW.
d. It shall be possible to set the priority bits in the S-VLAN priority based on the PCP bits of C-tag of the incoming packet in .1ad mode.

3.20.4 LSP Mode Requirements

3.20.4.1 The Router shall support LSP Mode Scalability Options i.e. Virtual Private LAN Service (VPLS) using Label Distribution Protocol (LDP) Signaling as per RFC 4762

a. Shall support Packet Transport Network solution by using PW service tunnel.
b. TDM and Ethernet traffic shall be emulated into Pseudo-wires and PW label is added for service identification.

c. End-to-end transport path LSP shall be created based on MPLS-TP standard (ongoing) and multiple PWs are transported over the same LSP end-to-end in both directions.
d. The traffic tunnels shall support per LSP queuing/scheduling i.e. the ability to assign and guarantee per LSP per class bandwidth profiles (CIR, EIR, CBS, and EBS)

3.21 Operation, Administration and Management Protocols

3.21.1 General

3.21.1.1 The Router shall support debugging of control plane including OSPF, IS-IS, RIP, BGP, Route Table Manager (RTM), VRRP, RSVP, LDP, MPLS, VPN services.

3.21.1.2 The Router shall support analysis of network traffic for network profiling, accounting, network planning, security, Denial of Service monitoring and network monitoring. Information on network users, applications, peak usage times and traffic routing is provided.

3.21.1.3 The Router shall support management aspects of the T-MPLS network element as per ITU-T G.8151/ T.1734 or equivalent IETF standards

3.21.2 OAM Framework

3.21.2.1 The Router shall support MPLS-TP OAM Framework as per RFC 6371 or ITU G.8113.1 / G.8113.2

3.21.2.2 The Router shall support MPLS-TP OAM requirements as per RFC 5860 or ITU G.8113.1 / G.8113.2

3.21.2.3 The Router shall support MPLS-TP Network Management Framework as per RFC 5950 or ITU G.8113.1 / G.8113.2

3.21.2.4 The Router shall support MPLS-TP Network Management requirements as per RFC 5951 or ITU G.8113.1 / G.8113.2

3.21.3 Configuration:

3.21.3.1 The Router shall support manual configuration of end-to-end MPLS-TP tunnels through eMS. It shall be possible for creation of co-routed bidirectional path from eMS, through eMS or through distributed control plane.: (A Thesaurus for the Terminology used in Multiprotocol Label Switching Transport Profile (MPLS-TP) drafts/RFCs and ITU-T's Transport Network Recommendations as per draft-ietf-mpls-tp-rosetta-stone)

3.21.4 Performance monitoring:

3.21.4.1 The router shall support MPLS-TP OAM based on BFD or Y.1731. The eMS shall show the packet counts, byte counts, packet drops and packet errors as per draft-bhh-mpls-tp-oam-y1731

3.21.4.2 The router shall support measurement of delay, Jitter, Ethernet alarm signal and Ethernet test signal function.

3.21.4.3 The router shall allow setting end-to-end performance bounds for Frame Delay, Frame Delay Variation, and Frame Loss for each flow

3.21.5 Fault Management:

3.21.5.1 The Router shall support MPLS-TP Fault management OAM as per RFC 6427 or ITU G.8113.1 / G.8113.2

3.21.5.2 The Router shall support Ethernet OAM, Connectivity Fault Management (CFM) as per IEEE 802.3ah and IEEE 802.1ag

3.21.5.3 The router shall support Ethernet OAM Connectivity Checks. The provisioning of all expected MEP IDs shall be automated via the eMS as per ITU-T Y.1731 and Y.1711 or BFD as per IETF RFC 5885

3.21.5.4 The Router shall support connection verification for MPLS Transport Profile LSP shall be as per RFC 6428.

3.21.5.5 The Router shall support alarms shall in the eMS. If any performance bounds (Frame Delay, Frame Delay Variation, and Frame Loss) are exceeded, the alarm shall be raised.

3.21.5.6 The Router shall support MPLS fault management as per RFC4377 and RFC4378

3.21.5.7 The Router shall support MPLS Connectivity verification and route tracing as per RFC 6426

3.21.5.8 The Router shall support MPLS BFD for LSP as per RFC5884

3.21.6 Non Ethernet OAM features:

3.21.6.1 Telnet, FTP/TFTP support: The Router shall support Telnet access to the console and FTP/TFTP access to its configuration/ boot files. Provision shall exist for remote reboot.

3.21.6.2 The Router shall support Service Ping, IP Ping, IP Trace Route

3.21.7 MPLS Non Ethernet OAM Features

3.21.7.1 The Router shall support MPLS traceroute, IP-VPN Ping, IP-VPN trace route, LSP Ping and trace route, BFD, Trace for P2MP LSPs , Virtual Circuit Connectivity Verification [VCCV], MPLS TE LSP trace and MPLS TE SNMP notification.

3.21.8 SNMP Manageability:

3.21.8.1 The Router shall support SNMP v2 & SNMP v3

3.21.8.2 The Router shall support RMON (Remote Monitoring) MIB I, II

3.21.8.3 Console or Out-of-Band Management: The Router shall have console management access, with the provision for remote out-of-band management capability using asynchronous serial interface

PART-III eMS/NMS REQUIREMENTS

The role of element Management System (eMS) is to control and manage all aspects of the domain such as Fault, Configuration, -Administration, Performance and Security (FCAPS) as defined by ITU-T and to ensure maximum usage of the devices resources. The eMS shall performs the following functions:

3.22 General operational and functional requirements

3.22.1 The eMS shall generate reports for various types of faults, performance history, security management etc. It should also be possible to generate up time-reports to facilitate monitoring performance statistics.

3.22.2 The eMS shall have a view of selected network controlled by the Element Management System as per requirement. By zooming—in, it shall be possible to drill-down upto module—level in each NE for configuration and fault management.

3.22.3 The eMS shall provide the ability to drill down to the individual element, then to subsystem, then to card and then to port level configuration template from the domain-map by clicking on the icon of the network element.

3.22.4 The eMS shall shall have suitable system level backup mechanism for taking backup of eMS data of at least one month.

3.22.5 The eMS shall provide the visual presentation of the Network Element's status and the alarms.

3.22.6 The eMS shall supportto take any Network Element out-of-service & in-service through the eMS. It shall be possible to restart the Network Element from eMS

3.22.7 The eMS shall carry out the systematic Health Monitoring of the elements of the Network. Check on the health of the card of any element of the Network shall be possible through command with settable periodicity - @ 24 hrs, l week, and 1 month

3.22.8 The configuration of the various network elements like creating, viewing, and editing shall be possible from the eMS. The configurations of the network elements shall also be stored at a suitable place in eMS from where it can be retrieved in case of failure

3.22.9 The eMS shall support to execute any schedulable administrative command i.e.- NE backup software download, performance etc., at any time by attaching a time tag to the command and it shall be executed when the Network real time matches the time tag. It shall be possible to define both time and date.

3.22.10 Messaging system: The eMS shall have a messaging system which will generate and send alert messages on e-mail to the designated personnel depending upon the location of NE, on generation of alarms.

3.22.11 The response time for query/command on any operator terminal, local or remote shall be 10 seconds or less.

3.22.12 The eMS shall manage upto 5000 nodes

3.23 Fault Management

3.23.1 Fault & Alarms management

3.23.1.1 Fault and troubleshooting capabilities includes Fault aggregation/consolidation, fault-severity indications, extensive list of fault filters, fault-forwarding, fault event-driven actions such as email, paging, scripts, forwarding etc.

3.23.1.2 The eMS shall provide Service Level view that shows VPN Topologies and end customer to customer paths and traces.

3.23.1.3 The eMS shall provide network topological view at Layer 2 and Layer 3 using hierarchical viewing methods. The views are customizable to manageable hierarchy. The view can be configured in either graphical forms or in linked-list form.

3.23.1.4 The eMS shall support SNMP as per RFC 1215, 'A Convention for Defining Traps for use with the SNMP' / gRPC/gNMI/Netconf

3.23.1.5 The eMS shall provide total alarm visibility of all NEs under its management:

a. Real time alarm monitoring and collection
b. Alarm display with audible and visual alert signal
c. Alarm graphical representation on network map
d. Alarm storage
e. Alarm reports
f. Alarm attributes and colour coded

g. Archiving and exporting
h. Alarm acknowledgement and alarm clear
i. Alarm filtering

3.23.1.6 The eMS shall support to customize according to user requirement.

3.23.1.7 The eMS shall support to send critical alarm alerts through SMS or e-mail and the same shall be configurable.

3.23.1.8 The eMS shall support alarm reduction through correlation & suppression based on object modeling.

3.23.1.9 The eMS shall support turn on or off the correlation rule.

3.23.1.10 The eMS shall support pre-defined correlation rule support.

3.23.1.11 The eMS shall support accessibility of affected alarm details from a single point.

3.23.1.12 The eMS shall provide information about all suppressed alarms.

3.23.1.13 The eMS shall provide information about all affected objects.

3.23.1.14 The eMS shall provide following topology views:

a. Physical Topology e.g. Location, Nodes, Interface
b. Logical Topology e.g. VLAN, LSP
c. Routing Topology e.g. OSPF, BGP, Multicast
d. Addressing Topology e.g. IPv4, IPv6
e. VPN Topology e.g. L2 VPN, L3 VPN
f. Services Topology e.g. Unicast, Multicast

3.23.1.15 Users shall be able to view overall Network topology as well as drill down to customer-specific VPN view if required. Users shall be able to launch troubleshooting applications eg. Ping, Trace Route, VPN Continuity Tests and from the view. The user manual provides a detailed list of such trouble shooting applications supported from the eMS.

3.23.1.16 The fault management system shall support the following functions:

a. Network and service fault alarms with severity level indicators.
b. Archive log for historical alarms and events.
c. Threshold alarms
d. End-to-end logical connection view of service components.

3.23.1.17 The fault management shall provide root cause analysis and correlate the physical failures with:

a. Physical network infrastructure
b. Logical network infrastructure
c. Routing / Signaling protocol alarms
d. Customer profile
e. Customer Services
f. Access Infrastructure

3.23.2 Discovery

3.23.2.1 The eMS system shall automatically discover manageable elements connected to the network and map the connectivity between them.

3.23.2.2 The eMS system shall support multiple types of discovery including following:

a. IP range discovery-including support for both IPv4/IPv6.
b. Import data- from pre-formatted files (IPs, ranges, strings or ports).

c. Discovery using route tables and SNMP MIBs or gRPC telemetry or NETCONF (RFC 6241) and YANG-based models (RFC 6020/7950) to retrieve device configuration, capabilities, and topology information.
d. Trap-based Discovery- whenever new devices are added with capability to exclude specific devices based on IP addresses/ IP address range.

3.23.2.3 The eMS system shall support discovery and inventory of heterogeneous physical network devices like Layer 2 & Layer 3 switches, routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual port level.

3.23.2.4 The eMS system shall support for SNMP v3 based discovery and management of supported devices to provide added security.

3.23.2.5 The eMS system shall support mapping and modeling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments.

3.23.2.6 Discovery shall identify and model router redundancy so that alarms generated from these virtual addresses are automatically excluded.

3.23.2.7 The eMS system shall support map grouped by network topology, geographical locations of the equipments and user group/departments.

3.23.2.8 The eMS system shall support manual modeling adjustments to allow administrators to customize the structure, the layout and relationship between modeled elements.

3.23.2.9 The eMS system shall support user-configurable discovery control to manage the frequency and scope network discovery.

3.23.2.10 The eMS system shall support user-configurable event to alarm mapping system that sets a differentiation that events do not necessarily need an alarm to be generated.

3.24 Configuration Management

3.24.1 The eMS shall discovers network elements based on SNMP, IP Address, manual or as batch entry using CSV or similar format.

3.24.2 The eMS shall do configuration changes for network devices from a central location.

3.24.3 The eMS shall capture and keep record of any configuration change happening on a network device.

3.24.4 The eMS shall keep a record of who does what change for auditing purpose.

3.24.5 The eMS shall support bare metal configuration of network devices.

3.24.6 The eMS shall show the difference between 2 configuration in color coded text format so that changes are visually identified.

3.24.7 The eMS shall provide configuration roll back option, so that a device can be brought to a good state configuration.

3.24.8 The eMS shall provide capability to follow an approval workflow before some or all changes can be implemented.

3.24.9 The eMS shall perform ACL updates on selected or all network devices.

3.24.10 The eMS shall generate compliance reports for management.

3.24.11 The eMS shall provide easy custom report generation capability.

3.24.12 The eMS shall detect and report vulnerabilities which exist on the network devices in the environment.

3.24.13 The eMS shall administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:

a. Capture running configuration
b. Capture startup configuration
c. Compare configurations
d. Upload configuration
e. Write startup configuration
f. Upload firmware

3.25 Administrative Management

3.25.1 Inventory Management

3.25.1.1 The eMS shall indicate the absence or presence of any physical module hardware elements. It shall also indicate the usage of module i.e., how many ports are in use, which interface is in use and which are free to be used etc

3.25.1.2 The eMS shall be able to discover and keep the device information.

3.25.1.3 The eMS shall be able to keep track on any change in the network inventory reporter chronologically.

3.25.1.4 The eMS shall provide the inventory information to the Network Management Layer (NML)/ Service Management Layer (SML) so that SML is able to create and activate a service to the customer automatically. This shall also assist SML in providing the network inventory to which the SML shall add the customer identification and maintain this information in the database.

3.25.1.5 The eMS shall provide the complete view of the network elements and the interconnecting links

3.25.1.6 The eMS shall be easy to use, flexible, customizable integrated solution to address:

a. Discovery of infrastructure
b. Maintaining an accurate inventory of the Routers.
c. Configuring and patching the NE's.

3.25.1.7 The eMS shall identify software and hardware configurations from a central location. Provide complete hardware and software information from all the NE's.

3.25.1.8 The eMS shall have the capability to scan and retrieve basic inventory information without the installation and ongoing overhead of an installed agent. At the same time should also provide the agent to collect deep inventory information from NE's.

3.25.1.9 The eMS shall provide patch management to keep computers up-to-date and complaint with our security requirements..

3.25.1.10 The eMS shall be capable to verify installation status of patches.

3.25.1.11 The software distribution function shall provide flexible and scalable delivery, installation, and configuration of software.

3.25.1.12 The eMS shall allow administrators to configure the software distribution such that if required management server can distribute and install the software immediately or can be scheduled.

3.25.1.13 The eMS shall schedule reports to run at a later time including repeating intervals.

3.25.1.14 The eMS shall support PDF & CSV as report formats.

3.25.1.15 The eMS shall provide facility to administrators to easily customize reports or create new reports.

3.25.2 Software Management

3.25.2.1 The eMS shall support to carry out the following tasks under the software management function.

a. Loading of new system software
b. Manage different versions of software
c. Shall have the capability of managing multiple versions of software for individual elements. In this case, one software version shall remain active and other versions shall be passive.

d. Installation of software patches.
e. At the time of downloading the software, the message shall be displayed that the software has been downloaded successfully or failed and at what stage.
f. The eMS shall support FTP/TFTP for downloading of Software, configuration, patches etc., to the Network Element
g. The operator terminals (local & remote) shall not allow loading of any software without the terminal administrator's authorization
h. The eMS shall enable operations like changing the system configuration, reconfiguration of input and output devices, loading a new software package, etc. Both automatic and manual reconfiguration capabilities shall be available.

3.25.2.2 **Software download:** Local & remote software download via management system to NEs and LCT shall be possible, including the means of identification of software module versions. No loss of data/traffic & connection-map shall take place during the software down-loading process

3.25.3 Helpdesk Management

3.25.3.1 The eMS shall provide flexibility of logging, viewing, updating and closing incidents manually

3.25.3.2 The eMS shall support to associate each incident with multiple activity logs entries via manual update or automatically update from other security tools or system management tools.

3.25.3.3 The eMS shall provide flexibility of incident assignment based on the workload, category or location.

3.25.3.4 The eMS shall support each escalation policy which shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.

3.25.3.5 The eMS shall support escalation policy which shall allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.

3.25.3.6 The eMS shall support web-base knowledge database to store useful history incident resolution.

3.25.3.7 The eMS shall have access on different knowledge articles for different users.

3.25.3.8 The eMS shall be able to log and escalate user interactions and requests.

3.25.3.9 The eMS shall provide status of registered calls to end-users over email and through web.

3.25.3.10 The eMS shall support updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

3.25.3.11 The eMS shall have the capability to track work history of calls to facilitate troubleshooting.

3.25.3.12 The eMS shall support tracking of SLAs for call requests within the help desk through service types.

3.25.3.13 The eMS shall support request management, problem management, configuration management and change management.

3.25.3.14 The eMS shall have the capability of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web, etc.

3.25.3.15 The eMS shall provide knowledge tools as an integral part of Service Desk and these tools should be accessible from the same login window.

3.25.3.16 The eMS shall have executive dashboard for viewing the service desk KPIs in graph & chart format.

3.25.3.17 The eMS shall provide seamless integration to log incident automatically via system and network management.

3.26 Performance Management

3.26.1 The eMS shall have ability to generate SLA reports based on monitoring performance parameter MIBs in the NEs. It also shall support threshold violation alarms.

3.26.2 The eMS shall be able to retrieve, generate and print reports and graphs on Performance Management data based on real time, time intervals, daily, weekly, monthly, annually or specific period, for all NEs and its resources by using the built-in report capabilities of the System.

3.26.3 The eMS shall support provision of performance measurements (e.g. QoS/CoS) for the following:

a. Interface/ Port level
b. Logical interface level
c. Service type

3.26.4 The eMS shall enable correlation of Service Performance Measurement is linked and featured in the fault management module with the following:

a. Customer profile
b. Customer services
c. Logical network infrastructure
d. Physical network infrastructure
e. Class of Service / Type of Service

3.26.5 The eMS shall provide detail and summary information for the following to be used as an accounting trigger in terms of GUI or web based

a. Subscriber profile
b. Service Type
c. Bandwidth Utilization and subscription (Total, New Subscription, Upgrade, etc)
d. Traffic originating and terminating points
e. Traffic Statistics
f. Connectivity Time (Average, Total, Peak, etc)

3.26.6 The eMS shall provide the monitoring and tracking tool for services with Service Level Agreement (SLA) for Service Assurance Management.

3.26.7 The eMS shall also provides automated calculation of service achievement, management and operational report for SLA and Non-SLA services.

3.26.8 The user manual shall describe in detail how the System Administrator can control, configure, diagnose, query, set thresholds and monitor the eMS locally and remotely.

3.26.9 The eMS shall support the following reports

a. Statistics/Network Performance
b. Performance statistics for troubleshooting & monitoring
c. Interface & LSP label status collection.
d. Service Performance Statistics
e. Seamless solution to address scalability.
f. Real-Time & Historical graphing support for statistics.

3.26.10 The eMS shall support response time agents to perform network performance tests to identify network performance bottlenecks.

3.26.11 The eMS shall monitor QoS parameters configured to provide traffic classification and prioritization for reliable VoIP transport. Discover and model configured QoS classes, policies and behaviors.

3.26.12 The eMS shall provide network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization, etc.) for network infrastructure.

3.26.13 The eMS shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.

3.26.14 The eMS shall give performance of Network devices like CPU, memory & buffers, etc, LAN and Wan interfaces and network segments.

3.26.15 The eMS shall provide availability, service levels, response time and throughput of various Internet/web services, e.g., DNS, HTTP, SMTP, etc.

3.26.16 The eMS shall give the comprehensive health reporting to identify infrastructure in need of upgrades and immediate attention. The eMS shall support capacity planning reports to identify traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. It also shall support capacity planning to enable understanding the effect of growth on available network resources.

3.26.17 The eMS shall the following performance reports:

a. Executive summary report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.
b. Capacity planning report which provides a view of under-and-over utilized elements.
c. Service Level report that shows the elements with the worst availability and worst response time – the two leading metrics used to monitor SLAs.

3.26.18 The eMS shall have a built-in report authoring tool to customize performance reports.

3.26.19 The eMS shall have integrated performance view for all managed systems and networks along with the various threshold violation alarms in them. It is possible to drill-down into the performance view to execute context specific reports.

3.26.20 The eMS shall be capabe to auto-calculate resource utilization baseline for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

3.26.21 The eMS shall provide Latency (both one way and round trip times) report for critical devices and links.

3.27 Router Specific eMS Requirements

3.27.1 Switching Parameters

3.27.1.1 The eMS shall support Configuration of the following Switching Parameters.

a. Ingress and egress bandwidth profile per User to Network Interface (UNI).
b. Ethernet services supported on each port.
c. Layer 2 protocol transport for Ethernet and PPP.
d. Hardware assisted Layer 2 forwarding.
e. MAC address for each port.
f. L2 Learning parameters: Sources learning per Port/VLAN/Source address
g. Dynamic MAC learning limit on each port.

h. The no. of source MAC addresses learnt from bridge port.
i. Automatic/manual disabling of MAC addresses learning for the VLAN.
j. MAC address limit.
k. Aging time (Aging Time or No Aging) for MAC addresses.
l. L2 Aging on every port.
m. Disable MAC address learning.
n. Policy to discard all Ethernet frames based on MAC destination address.
o. Allowable MAC destination address.
p. Spanning Tree Protocol as per IEEE 802.1d
q. Queues to prioritize BPDUs.
r. Each port to drop BPDU if those BPDUs have a root bridge identifier which is lower (better) than the current Spanning Tree root.
s. Each port to drop BPDU regardless of the BPDU content.
t. RSTP as per IEEE 802.1w
u. MSTP as per IEEE 802.1s
v. Link-layer discovery protocol as per IEEE 802.1ab
w. Logical Link Control (LLC) as per IEEE 802.2
x. Flow Control as per IEEE 802.3x
y. Link aggregation as per IEEE 802.3ad
z. Static/LACP Link Aggregation Groups (LAG) on client ports
aa. IGMPv2 and v3 as per RFC 2236 and 4604 respectively. (applicable for type Ito XII Routers)
bb. PAT
cc. NAT as per RFC 3022

3.27.1.2 The eMS shall support configuration of the following VLAN Parameters.

a. VLAN creation among ports of different types as well as on all ports of the interface cards. The IEEE 802.1Q Tagging creation based on Tagged only i.e. which is an IEEE 802.1Q trunk, Untagged, Hybrid, Tag insertion, removal and swapping,
b. Configuration of VLAN bridging as per IEEE 802.1ad
c. Configuration of user isolation per outer VLAN tag on a per port basis.
d. Enable/Disable VLAN ingress filtering, VLAN tag overlapping
e. Insertion and removal of second tag.
f. Encapsulation translation and rewrites Push, Pop and translate for IEEE 802.1Q or Q-in-Q/IEEE 802.1ad tags.
g. Local VLAN and ports cross-connect and multipoint or point-to-multipoint with Hierarchical Virtual Private LAN service (H-VPLS bridge topologies with pseudo-wires) or locally defined bridge domains.
h. VLAN stacking
i. S-VLAN tags and priority.
j. Q-in-Q as per IEEE 802.1Q

3.27.2 Routing Parameters

3.27.2.1 The eMS shall support configuration any of the optical Ethernet interfaces as Client or Aggregate interfaces.

3.27.2.2 The eMS shall support configuration of the following OSPF Features

a. OSPF v2 parameters as per RFC 1370, 1583, 2328, 4750
b. OSPF routes, adjacencies and areas.
c. Filtering route based on administrative costs.

d. Setting of Administrative costs, virtual links, area route aggregation, inter area route aggregation, route leaking.
e. BGP-OSPF interaction
f. OSPF Not So Stubby Area (NSSA) as per RFC 3101
g. OSPF Opaque LSA option as per RFC 5250
h. OSPF for IPv6 as per RFC 5340
i. OSPF Stub Area
j. OSPF graceful restart as per RFC 3630
k. OSPF Sham Links

3.27.2.3 The eMS shall support configuration of the following FRR & BFD features
a. Fast Reroute Extensions to RSVP-TE for LSP Tunnels as per RFC 4090.
b. Bidirectional Forwarding Detection (BFD) as per RFC5880, 5881, 5883.

3.27.2.4 The eMS shall support configuration of the following BGP features
a. BGPv4 as per RFC 4271, RFC 2283
b. Border Gateway Protocol features as per RFC 1772, RFC 1997, RFC 4360, RFC 2270, RFC 2439, RFC 2545, RFC 2918, RFC 3107, RFC 5065,RFC 5492, RFC 5925
c. Transparent LAN using BGP
d. Encryption of BGP peering session.
e. Default route to individual BGP peers.
f. Soft reset the BGP session on any or all peers.
g. Policy Routing to enable flexibility in making changes to the normal routing process based on the characteristics of the traffic.
h. Multiple BGP sessions.
i. Ingress and egress route filtering
j. Weight metric, Local Pref metric and Multi Exit Discriminator (MED) metric.
k. BGP properties like, Route Target, Site of Origin, Route Refresh, ASN Override , Outbound Route Filters (ORF), VPNv4 routes filtering based on route target, Inter-AS MPLS VPN model
l. Interior BGP (iBGP) peering with other border routers.
m. Exterior BGP multi-path support-to-support load balancing.
n. Multi Protocol BGP (MP BGP) as per RFC4760
o. Next Generation Multicast VPN features (MVPN using MP-BGP)
p. BGP for Load balancing.
q. BGP Route Reflection (RR) as per RFC 4456

3.27.2.5 The eMS shall support configuration of the following Multicast features
a. Prioritization of multicast traffic.
b. Multicast table.
c. Multicast ACL.
d. Multicast Load Balancing traffic across multiple interfaces
e. Administratively Scoped IP Multicast
f. IPv4 Multicast address space as per RFC 2365
g. Internet Group Management Protocol, Version 3 as per RFC 3376.
h. Source based and shared distribution trees
i. Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) as per RFC 3446
j. Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) as per RFC 5059
k. Protocol Independent Multicast - Sparse Mode (PIM-SM): as per RFC 4601

l. Rendezvous Point (RP) on both leaf and non-leaf nodes.
m. Multicast Source Discovery Protocol (MSDP) as per RFC 3618
n. Bootstrap Router Mechanism for PIM Sparse Mode
o. PIM Source Specific Multicast (PIM-SSM) as per RFC 3569
p. Source-Specific Multicast for IP as per RFC 4607
q. Operation of Anycast Services
r. Dynamic broadcast Source Failover using Anycast routing.

3.27.3 MPLS Parameters

3.27.3.1 The eMS shall support the following MPLS Configuration features. However the Customer related functions are handled through the VPN Management Function

a. Various MPLS Configurations as per RFC3813, RFC 3031, 3032, 3443
b. Static & dynamic MPLS LSP Configurations & LSP Path optimizations
c. Generalized TTL Security Mechanism (GTSM) as per RFC5082
d. Configuration / mappings of MPLS class of service.
e. Limiting the number of routes per VRF.
f. Set Thresholds to provide traps and alarms when a certain number of routes are exceeded.
g. LDP attributes as per RFC5036, 3037, 3478
h. Generic Virtual Private Networks Configurations as per RFC 4364.
i. L2VPN Configurations as per RFC 4664, 4665, 4906
j. VPLS, H-VPLS, VPWS, EoMPLS, multi-segment PWS and Pseudo wire redundancy
k. Disable learning, FIB size limit on a per VPLS service basis
l. Creation, selection, and registration of an Autonomous System (AS) (Private and overlapping Autonomous System Numbers) as per RFC1930
m. Inter AS/Inter VPN configurations as per RFC4364
n. Enable cRTP as per RFC2508
o. MPLS Auto-bandwidth
p. LSP Mode Scalability Options through VPLS using LDP as per RFC4762.
q. MPLS-TP configurations as per G.8110, G.8112, RFC6371, 5860, 5950, 5951
r. MPLS-TP survivability framework configurations as per RFC 6372 or ITU-T G.8131/G.8132
s. Manual configuration of end-to-end MPLS-TP tunnels through eMS. It is possible to create co-routed bidirectional path from eMS, through eMS or through distributed control plane as per draft-helvoort-mpls-tp-rosetta-stone

3.27.3.2 The eMS shall support Fault Management features of MPLS

a. MPLS based Recovery as per RFC 3469
b. MPLS-TP fault management parameters as per RFC 5884 and 4379 or G.8121
c. MPLS-TP fault management parameters as per RFC 5860 or ITU Y.SUP4
d. MPLS-TP fault management parameters RFC 5586 or ITU G.8113.1
e. MPLS-TP Fault OAM as per RFC 6427 or ITU G.8113.1 / G.8113.2
f. Ethernet OAM, Connectivity Fault Management (CFM) as per IEEE 802.3ah, IEEE 802.1ag
g. Ethernet OAM Connectivity Checks. The provisioning of all expected MEP IDs is automated via the eMS as per ITU-T Y.1731, ITU-T Y.1711 or BFD RFC 5885
h. Connection verification for MPLS Transport Profile LSP as per RFC 6428
i. If any performance bounds (Frame Delay, Frame Delay Variation, and Frame Loss) are exceeded, the alarm shall be raised in the eMS.

3.27.3.3 The eMS shall support Performance Management features of MPLS

a. MPLS-TP performance management parameters as per RFC 5860 or ITU Y.SUP4

b. MPLS-TP OAM based on Y.1731
c. Measurement of delay, Jitter, Ethernet alarm signal and Ethernet test signal function.
d. Set end-to-end performance bounds for Frame Delay, Frame Delay Variation, and Frame Loss for each flow
e. Enable/disable IEEE 802.1ag or BFD on a per port basis for non MPLS-TP tunnels for the purpose of monitoring the traffic along a link.

3.27.4 Traffic Engineering & QoS Parameters

3.27.4.1 The eMS shall support the following QoS Configuration management features

i) Define Traffic Classes
ii) Create traffic classes based on their property, such as, voice, video, data, priority.
iii) Define Committed Information Rate (CIR), Excess Information Rate (EIR), Committed Burst Size (CBS) and Excess Burst Size (EBS) groups using a template. (16, 32, 64, 128, 256 and 512 k Bytes burst sizes)
iv) Assign traffic classes to each customer (VLAN ID).
v) Assign CIR, EIR, CBS, and EBS template to each customer (VLAN ID).
vi) Define CIR, EIR, CBS and EBS for storm suppression (Broadcast/Multicast).
vii) Assign storm suppression control on each port.
viii) CIR/EIR to be configured in steps of 1Mbps
ix) User bandwidth is to be configured in steps of
- 64kbps for less than 1 Mbps
- 1 Mbps for 1-1000Mbps
- 100 Mbps granularity for 1-100 Gbps.

x) Create Diff-Serve boundary in the network.
xi) Define trust boundary by trusting the interfaces in the network.
xii) Classify the incoming packet based on DSCP value.
xiii) Assign traffic class QoS profiles to the interfaces.
xiv) Define Policy Control List. Configure rule and corresponding action for the following:
- IEEE 802.1p values (0 to 7)
- VLAN ID
- Source MAC address
- Destination MAC address
- Ether Type or Protocol
- Incoming/Destination IP address and mask
- Source/Destination TCP/UDP Port
- Type of Service (ToS) Precedence bits.
- UDP/TCP socket
- Default queue for non-matching traffic

xv) Configure Metering Table [Index, SrTCM-CIR/CBS/EBS, TrTCM-CIR/CBS/PIR/PBS, Color Aware/Blind, Action for Yellow and Red, Re-marking (Modify DSCP/UP) , Forward, Drop]
xvi) Modify QoS profile mapping (DSCP, COS/User Priority, EXP, Drop Precedence, Traffic Class)
xvii) Configure marking/shaping scheme, such as, Single Rate Two Color or Two Rate Three Color marking scheme.
xviii) Configure meter as Color blind or color aware.
xix) Define congestion avoidance management – Configure dropping mechanism, such as, Tail Drop, WRTD (Weighted Random Tail Drop), WRED, Selective Packet Discard etc.

xx) WRTD-Configure No of masking bits.
xxi) WRED-Configure Thresholds for Dropping the traffic (Minimum threshold, Maximum threshold)
xxii) Define queues on each port, queue buffer size and their priority group (Strict Priority, DRR, SDWRR).
xxiii) Configure queuing mechanism on each port, such as, SPQ – Strict Priority Queuing, WFQ – Weighted fair Queuing.
xxiv) Configure scheduling mechanisms for each queue, such as, Deficit Round Robin (DRR), Weighted Round Robin (WRR), SDWRR(Shaped Deficit Weighted Round Robin), Modified Deficit Round Robin (MDRR), Weighted Fair Queuing, Strict Priority (SP), SP + Weighted Round Robin (SP + WRR), etc.
xxv) Configure weights for the WRR/SDWRR/MDRR/WFQ queues.
xxvi) Configure Shapping Rate on port wise or queue wise.
xxvii) Define customer profile for Hierarchical QOS based on
- VLAN ID
- Category – Gold, Silver, Bronze
- Type of service – Voice, Video, Data
- Rate- CIR/EIR, CBS/EBS

xxviii) Define bandwidth profile for different types of services – Voice, Video and Data
xxix) Define bandwidth profile for different types of Category – Gold, Silver, Bronze

3.27.4.2 The eMS shall support the following Traffic Engineering configuration management features

i) End-to-End traffic tunnels with 2Mbps granularity.
ii) Multiple paths for a TE tunnel to provide protection.
iii) Modify/re-optimize TE tunnels.
iv) Options for automatic and manual selection of TE path.
v) LSP based Traffic Engineering as per RFC 5654
vi) VLAN Tunnel based Traffic Engineering as per IEEE 802.1Qay
vii) Bandwidth management feature both for Compression and Filtering
viii) Traffic Engineering Over MPLS as per RFC 2702
ix) Traffic parameter attributes (peak rates, average rates, permissible burst size, etc.)
x) Generic path selection and management attributes
- Administratively Specified Explicit Paths
- Hierarchy of Preference Rules For Multi-Paths
- Resource Class Affinity Attributes
- Adaptivity Attribute (permit re-optimization, disable re-optimization)
- Load Distribution Across Parallel Traffic Trunks

xi) Priority attribute
xii) Preemption attribute (preemptor enabled, non-preemptor, preemptable, and non-preemptable)
xiii) Resilience Attribute
xiv) Policing attribute
xv) Resource Attributes
xvi) Maximum Allocation Multiplier
xvii) Resource Class Attribute
xviii) Dynamic MPLS Traffic Engineering

xix)Traffic Engineering Extensions to OSPF Version 2 as per RFC 3630
xx) Router Address TLV
xxi)Configure Link TLV
- Link type (Point-to-Point, Multi-access)
- Link ID
- Local interface IP address
- Remote interface IP address
- Traffic engineering metric
- Maximum bandwidth
- Maximum reservable bandwidth
- Unreserved bandwidth
- Administrative group

xxii) for IS-IS Extensions for Traffic Engineering as per RFC 5305
xxiii) Extended IS Reachability TLV
- Administrative Group (color, resource class)
- IPv4 Interface Address
- IPv4 Neighbor Address
- Maximum Link Bandwidth
- Maximum Reservable Link Bandwidth
- Unreserved Bandwidth
- Traffic Engineering Default Metric

xxiv) Extended IP Reachability TLV
xxv) OSPF inter area MPLS Traffic Engineering
xxvi) IGP Traffic Engineering database for Constraint Based Shortest Path First (CSPF) calculations for tunneling.
xxvii) Priorities for TE tunnels.
xxviii) RSVP as per RFC 2205
xxix) RSVP to provide the label distribution and capability to do CSPF signaling based on the IGP link state database.
xxx) IGP Area tunneling for RSVP.
xxxi) Traffic control and policy control parameters.
xxxii) Interfaces to support RSVP-TE signaling.
xxxiii) Aggregation of Martini circuits within an RSVP – TE tunneled LSP.
xxxiv) RSVP and RSVP-TE Extensions to RSVP for LSP Tunnels as per RFC 3209
xxxv) Configure reservation styles
- Fixed Filter (FF) Style
- Wildcard Filter (WF) Style
- Shared Explicit (SE) Style

xxxvi) Define administrative policy to Rerouting Traffic Engineered Tunnels
xxxvii) MPLS Fast Reroute Extensions to RSVP-TE for LSP Tunnels, as per RFC 4090
xxxviii) RSVP Refresh Reduction Extensions as per RFC 2961
xxxix) Pseudo-Wire Emulation
xl) Pseudo-Wire Emulation Edge-to-Edge (PWE3) as per RFC 3916, 3985
xli) PWE3 Control Word for Use over an MPLS PSN as per RFC 4385
xlii) Encapsulation Methods for Transport of Ethernet over MPLS Networks as per RFC 4448
xliii) Pseudo wire Setup and Maintenance using LDP as per RFC 4447
xliv) Pseudowire (PW) Management Information Base (MIB) as per RFC 5601
xlv) Point-to-Multipoint (P2MP) LSP.
xlvi) Point to Multipoint MPLS TE LSPs

xlvii) Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs) as per RFC 5601
xlviii) M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs) as per RFC 5120
xlix) MPLS Support of Differentiated Services as per RFC 3270
l) Support of Differentiated Services-aware MPLS Traffic Engineering as per RFC 3564
li) Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering as per RFC 4124
lii) Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
liii) Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering as per RFC 4127
liv) Bandwidth profiles (CIR, EIR, CBS, and EBS) for each LSP.

3.27.4.3 The eMS shall support the following Traffic Engineering and QoS performance management features
a. No of packets conforming or non-conforming to policy (Green, Yellow, Red) for each class of service.
b. No of packets dropped for each class of service.
c. Bandwidth utilization of each link.
d. Bandwidth Management Report

3.27.5 Circuit Emulation

3.27.5.1 The eMS shall support the following Circuit Emulation configuration management features
i) Selection of Interface and applicable CE Standard (SAToP /CESoPSN)
ii) Grooming of SDH under CESoPSN options from multiple interfaces including combining fractional E1
iii) Change of Parameters of SAToP interface like VCID, Tunnel Label etc
iv) Change of Parameters of CESoPSN interfaces
v) View of the configuration of all the interfaces

3.27.5.2 The eMS shall support the following Circuit Emulation fault management features
i) Test Loop back at different granularities at different interfaces from different locations like near end, far end, intermediate locations
ii) Detection of various types of defects in SAToP interfaces like Stray Packets, Malformed Packets, Excessive Packet Loss rate, Buffer Overrun, Remote Packet Loss
iii) Detection of various types of defects in CESoPSN interfaces like misconnection, mistype, loss of packets, loss of synchronisation etc

3.27.5.3 The eMS shall support Circuit Emulation performance management features w.r.t. BER measurements for the interfaces and related statistics & alarms

3.27.6 Synchronisation

3.27.6.1 The eMS shall support the following Synchronisation configuration management features
i) Selection of I, II, III, IVth frequency synchronisation reference
ii) (External, TDM Interface, IP Interface (SyncE), Holdover mode etc)
iii) Manual change of Frequency synchronisation reference
iv) PTP reference assignment (Primary, Secondary etc) for 1588v2 Phase sync

v) NTP Server (Primary/Secondary) Assignment

3.27.6.2 The eMS shall support the following Synchronisation fault management features

i) Set limits for Frequency synchronisation accuracy
ii) Frequency Synchronisation Alarm: When the synchronisation exceeds the limits, Signal fail etc
iii) PTP Error Message
iv) NTP Error Message

3.27.7 Protection Switching

The eMS shall support the following Protection Switching configuration management features

i) Selection of Protection Switching Mode for SDH interfaces[Automatic, Forced, Manual, Disable Protection Switching]
ii) G.8032 Ring protection configuration
iii) MPLS-TP Linear Protection configuration requirements as per IETF standards OR Ethernet/MPLS SNC based protection as per ITU-T standards

3.28 VPN Management

3.28.1 The eMS shall support efficient provisioning of VPN services across the network with the following functions:

a. VPN Provisioning.
b. VPN Data Collection.
c. VPN Management Tool.

3.28.2 VPN Provisioning:

The eMS shall support Provide comprehensive and integrated offering of operations management functions covering the management of MPLS VPN services throughout the service life cycle. The eMS shall support following VPNMS functions:

3.28.2.1 The VPNMS (eMS) shall support Step-by-step information-assisted population of templates.

3.28.2.2 The VPNMS (eMS) shall support operators who shall add, delete, or modify customer VPNs. They shall set up extranet relationships.

3.28.2.3 The VPNMS (eMS) shall support templates which shall be converted into appropriate commands and shall be downloaded to the network.

3.28.2.4 The VPNMS (eMS) shall support scheduling like when a new service or service change is entered, users shall have the ability to make arrangements for hardware delivery or for other steps required prior to activation of the service. Following shall be supported:

a. Scheduling of tasks at creation time.
b. Scheduling of tasks after creation time.
c. Scheduling of tasks once, hourly, daily, weekly, monthly, yearly.

3.28.2.5 The VPNMS (eMS) shall support service changes in the network through reliable delivery of commands to the appropriate network elements.

3.28.2.6 The VPNMS (eMS) shall support Post-activation testing so that services can be tested to ensure reliable delivery of the service. E.g., a site-to-site ping test ensures correct activation of a new site to an existing VPN service.

3.28.2.7 The VPNMS (eMS) shall support smart collection whereby the VPNMS collects only changed configuration files from the Routers.

3.28.2.8 The VPNMS (eMS) shall support display of VPN topology with following:

a. Circular Layout to portray interconnected ring and star topologies.
b. Hierarchical Layout to organize the topology into distinct levels.
c. Symmetric Layout to expose the natural symmetry inherent in many networks.
d. Orthogonal Layout to draw graphs in which links run horizontally or vertically along a grid.
e. Facility to expand and collapse views.

3.28.2.9 The VPNMS (eMS) shall support configuration of the Service Level Agreement (SLA) monitoring parameters in the CE Router.

3.28.2.10 The VPNMS (eMS) shall support generation of SLA reports with annually, monthly, weekly, hourly time-scales. Following reports can be generated:

a. Summary Report
b. Jitter Report
c. Customer Packet Drop (CE-CE) Report
d. Customer Round Trip Delay (CE-CE) Report
e. SLA Definition Report

3.28.2.11 The VPNMS (eMS) shall support Committed Rate Monitoring Reports with annually, monthly, weekly, hourly time-scales.

3.28.2.12 The VPNMS (eMS) shall support Accounting by collecting data to provide end-to-end usage information on VPN-based network traffic from the VPN Data Collection Server.

3.28.2.13 The VPNMS (eMS) shall support generation of the following accounting reports:

a. Traffic Summary Report – To display total packets and total KB for traffic that can be mapped to the VPN (VPN Traffic) and otherwise to Unmappable traffic.
b. Application Type Summary Report – To provide total packets and total K bytes for each application type.
c. Customer Summary Report – To provide total packets and total KB for each customer plus additional reports for customer site and application type.
d. PE to PE Traffic Summary Report – Reports on all traffic between PE to PE, plus additional reports for the following:
    x. PE to connected CE,
    xi. PE to remote CE,
    xii. PE traffic and
    xiii. PE to CE.
e. CE to CE Traffic Summary Report-Reports on all traffic between CE to CE.
f. Type of Service Summary Report-Provides total packets and total KB for each type of service.
g. Customer Traffic Volume (CE-CE) Report-Provides information on all traffic volume for a specific customer between CE to CE in packets or KB (by type of service).
h. Network Traffic Volume (PE-PE) Report-Provides information on all traffic volume between PE to PE in packets or KB (by type of service).
i. Traffic Volume (PE-CE) Report-Provides information on all traffic between PE to (by type of service).

3.28.2.14 The VPNMS (eMS) API shall support third party tools for the following:

a. Defining VPN objects & constructing service requests to implement a VPN service.
b. Transferring configuration data to and from VPN routers.
c. Collecting VPN-usage data and VPN performance.

3.28.3 VPN Data Collection

3.28.3.1 The eMS shall collect VPN Flow data, aggregates (or summarises) that data, and filters specified data from supported PE Routers and shall support following:

a. Data Collection shall be done at each Provider Edge location.
b. Import of traffic flow data from the PE Router which consist of following attributes:
    i. Source & Destination IP Address.
    ii. Source & Destination TCP/UDP Port.
    iii. Type of Service (TOS).
    iv. Flow Timestamp.
    v. Interface.
c. Filtering and aggregation of the traffic flow data for VPN supporting following:
    i. Raw Flows
    ii. Source Node
    iii. Destination Node
    iv. Host Matrix (Source, Destination Node)
    v. Source Port
    vi. Destination Port
    vii. Protocol
    viii. Autonomous System Matrix (Source, Destination AS)
    ix. Detailed Call Record (Source Node, Destination Node, Source Port, Destination Port, Protocol, Type of Service, Source Interface, and Destination Interface).
d. Does not accept packets from any unspecified sources.
e. Support for script files to be invoked for further processing.
f. Shall support unsolicited event notification to generate messages on encountering errors.
g. Export of data to the VPN Provisioning function.

3.28.4 VPN Management Tool

It is an element-level provisioning system for rapidly deploying high-quality configurations to Customer Edge (CE) & Provider Edge (PE) routers. It shall support following:

3.28.4.1 Template based automatic configuration generation to enable configuration and provisioning of any managed network services like MPLS VPN.

3.28.4.2 Multiple discrete customer networks that use the same unregistered IP address ranges.

3.28.4.3 Telnet Gateway Server to allow download of configuration files to CE & PE Routers.

3.28.4.4 The system administration function allows user-based authentication.

3.28.4.5 GUI based operation to support following tools:

a. Element Manager - creates and manages domains and elements (including uploading of configurations generated in the template manager).
b. Template Manager - Creates and manages templates and template data, and for generation of configurations.
c. Log Viewer - views records of system activity, allowing sorting on various criteria.
d. Archive Manager - archives the configuration file on each network element and template, and maintains a history of configuration file changes on each network element.
e. Permission Manager - creates and manages permission group (the means by which users are given access rights).
f. User Manager – manages individual users.

3.28.5 VPNMS management functions:

3.28.5.1 The eMS shall support to map and manage enterprise MPLS-VPNs by automating the provider connection resolution and monitoring the service health with an option to auto-provision service assurance testes to proactively calculate the availability of remote sites.

3.28.5.2 The eMS shall support export of traffic flow data to the eMS Server through SNMP / XML to the NMS. This shall be supported using one of the following methods:

a. Autonomous System Matrix: One flow record is exported for every unique set of source autonomous system (AS), destination AS, input interface index, and output interface index.
b. Protocol Port Matrix: One flow record is exported for every unique set of source application port number, destination application port number, and IP protocol
c. Source Prefix Matrix: One flow record is exported for every unique set of source IP prefix, source prefix mask, source AS, and source interface index.
d. Destination Prefix Matrix: One flow record is exported for every unique set of destination IP prefix, destination prefix mask, destination AS, and output interface index.
e. Prefix Matrix : One flow record is exported for every unique set of source IP prefix, source prefix mask, destination IP prefix, destination prefix mask, source AS, destination AS, input interface index, and output interface index.

3.28.5.3 The router shall be able to collect the following statistics. These statistics shall be transported using SNMP commands or FTP/TFTP commands to eMS.

a. Source IP address/ subnet
b. Destination IP address/ subnet
c. Source TCP and UDP port
d. Destination TCP and UDP port
e. ICMP per interface basis
f. IGMP per interface basis

3.29 SLA Management

3.29.1 The SLA Management system shall provide a web interface for the customers to login and verify their SLA related parameters.

3.29.2 The SLA Management system shall provide visibility of the service quality delivered across the Network (indicated in the figure above) together with the ability to manage end customer SLAs.

3.29.3 Features: The SLA Management system shall support the following features:

a. Dynamic service monitoring overview
b. Service problem investigation
c. Service quality impact analysis
d. Real-time status views.
e. Generates SLA violation alarms and notifications.
f. Service quality trend reporting - historical reports on how key parameters have varied over user defined reporting periods.
g. Produces periodic service level conformance reports

3.29.4 The SLA Management system shall provide the capability to model services and report the overall Quality of Service and Service Level Agreement and SLA fulfillment.

3.29.5 The SLA Management system shall be capable of extending support to additional services required in the future.

3.29.6 The SLA Management system shall provide service metrics to be defined using Key Quality Indicators (KQIs).

3.29.7 The SLA Management system shall provide resource metrics to be defined using Key Performance Indicators (KPIs).

3.29.8 The SLA Management system shall provide a GUI that allows KQIs and KPIs to be configured easily using point-and-click techniques.

3.29.9 The SLA Management system shall have the capability to use various mathematical and logical operations for calculating KQI and KPI metrics

3.29.10 The SLA Management system shall allow the configuration of a variety of data sources including:

a. Performance data source for key network measures
b. Fault data sources for relevant alarms
c. Operational data sources like trouble tickets

3.29.11 The SLA Management system shall allow defining thresholds to detect SLA violations.

3.29.12 The SLA Management system shall generate service quality alerts when anomalies are detected based on a comparison to historical KQI trends.

3.29.13 The SLA Management system shall allow different thresholds to be configured for different times of day.

3.29.14 The SLA Management system shall have configurable interfaces to collect data from various data sources (NEs, trouble-ticketing, fault management systems, performance management systems).

3.29.15 The SLA Management system shall collect data via standards-based, open interfaces.

3.29.16 The SLA Management system shall allow privileged user to specify the list of resources from which to collect data, the list of measurements to collect, and the collection interval.

3.29.17 The SLA Management system shall use trouble ticket data to compute key KQIs like the MTTR.

3.29.18 The SLA Management system shall compute availability KQIs using the fault data source.

3.29.19 The SLA Management system shall calculate availability KQIs to monitor for SLA violations.

3.29.20 The SLA Management system shall generate SLA violation information in real time when a KQI/KPI threshold is violated so the Network Operation Center can be alerted to this condition.

3.29.21 The SLA Management system shall forward service quality alarms to other systems via SNMP.

3.29.22 The SLA Management system shall aggregate Service Quality Records over time on a per customer/service basis.

3.29.23 The SLA Management system shall create historical trends based on quality parameters.

3.29.24 In response to a threshold violation, the SLA Management system shall provide following automatic task:

a. Generate an alert.
b. Forward an email/SMS.

c. Execute a customized script.

3.29.25 The SLA Management system shall provide viewing and editing displays of Service Definitions.

3.29.26 The SLA Management system shall provide a dashboard view on a browser front-end. The dashboard view can be configured so that it can be personalized for different users

3.29.27 The SLA Management system's dashboard shall provide instant visibility to potential alerts in the services.

3.29.28 The SLA Management system's dashboard view shall allow a user to view detailed service quality metrics on a per customer basis upon seeing an alert.

3.29.29 The SLA Management system shall provide user-configurable reports indicating SLA compliance on a per-customer basis.

3.29.30 The SLA Management system shall provide option for the scheduling of reports.

3.29.31 The SLA Management system shall provide reports to users via a web-based interface.

3.29.32 The SLA Management system shall generate management reports providing information on customer network configuration and changes, faults and achievement against the SLAs.

3.29.33 The SLA Management system shall deliver network management reports via a secure Web site.

3.29.34 The SLA Reports include latency, packet loss, jitter, error apart from the availability and the link utilization reports.

3.29.35 It shall generate detailed and summary reports for all the above parameters. The reports are customer friendly.

3.29.36 The SLA Management system shall provide customer his network topology as well as alarms on his network in a user friendly format.

3.29.37 The SLA Management system shall allow customer to view reports pertaining to different queues in case QoS is implemented for the customer.

3.29.38 The SLA Management system shall store all collected service quality data with a timestamp including the date and time received.

3.29.39 The SLA Management system shall store both raw service quality data for a period of 3 months and normalized data in a historical log for a period of one year.

3.29.40 The SLA Management system shall support the computation and aggregation of KPI and KQI metrics indicative of the quality of service (QoS) for various services and applications delivered over the network infrastructure.

3.29.41 The SLA Management system shall support root cause analysis of QoS violations through 'drill down' analysis of KQI and KPI metric data. Root cause analysis includes the presentation of failure modes / cause codes and identification of failure distribution by location, service/device type, subscriber type or other dimensions as appropriate to the monitored services.

3.29.42 The SLA Management system shall monitor the service from both its internal perspective i.e. how the service is coping across the network as well as that of its customers and partners.

3.29.43 The SLA Management system shall provide a real-time availability based service management view.

3.29.44 The SLA Management system shall allow building service models, integrating business service status from data sources or event sources, and display customized business service views, scorecards, and dashboards in real time.

3.29.45 The SLA Management system shall provide service visualization capability, by integrating data from event sources or data sources to show the status of various services and the impact of outages.

3.29.46 The SLA Management system shall allow creating custom business service views. The module provides a graphical user interface (GUI) that allows to logically linking services and business requirements within the service model.

3.29.47 The SLA Management system shall provide dynamic visualization of key performance indicators to show the health and performance of critical business services.

3.29.48 The SLA Management system shall display a dependency view which depicts the relationship models and the status of its building blocks as it relates to each model.

3.30 Provisioning Management System [Service Provisioning]

3.30.1 The provisioning management system shall support single GUI based provisioning system which provisions network and end user services from a single screen.

3.30.2 The provisioning management system shall support consistent and simplified service activation methodology across services.

3.30.3 The provisioning management system shall allows one touch network / service provisioning for all the services as mentioned in the earlier sections.

3.30.4 Provisioning tool shall maintain a complete inventory of end customers being served along with contact information and automatically associate services against customers in this list.

3.30.5 For each of these services deployed, Provisioning tool shall maintain a detailed association of the resources (e.g. ports, Customer VLAN ids, Bandwidth Profiles, QoS mapping, VPN ID and so on)

3.30.6 The provisioning management system shall maintain a real-time database of the existing customer / services / resources.

3.30.7 The provisioning management system shall support remote software and configuration upgrades/ downgrades for large number of NEs.

3.30.8 The provisioning management system shall automatically capture all the configurations from the existing network and make an inventory of end subscribers out of it.

3.30.9 In case of any NE failure and replacement, the provisioning management system shall put the latest database stored configuration in the element.

3.30.10 The provisioning management system shall handle end-to-end service provisioning (across the Core, aggregation and access) from one single point of provisioning platform regardless of whether the system manages a single family or different family products.

3.30.11 The provisioning management System shall provide GUI-based features for all applications such as system configuration, service provisioning etc.

3.30.12 The provisioning management System shall be configurable from the GUI for all services like L3VPN, L2VPN, E-line, ELAN (Point to point service, Point to

Multipoint, multipoint to multipoint) and Triple play services (voice/video/data) etc.

3.30.13 The provisioning management System shall configure the physical and logical connections of the core, aggregation and access.

3.30.14 The provisioning management System shall perform auto discovery features as following

a. Underlying Transmission Technology
b. IP Device Type (Layer 2 and Layer 3)
c. Routing / Signaling /MPLS Protocols
d. Device information e.g. Cards, Ports, Interfaces, IP addresses, MAC addresses, etc.
e. Device Physical and Logical Connectivity

3.31 NMS Requirements

The northbound interface of the eMS towards NMS layer shall be SNMPv2, SNMPv3 and XML complaint. The southbound interface towards NEs shall be SNMPv2 [or later interface] implemented on UDP/IP stack or XML/SOAP. It shall be possible to verify SNMP MIBs during their testing.

3.32 Local Management Interface

3.32.1 The router shall provide at least one remote management interface and one Local Management Interface (LMI) at each Network Element as conforming to SNMP version2 [or later interface] with standard MIBs Browser. It shall be implemented on UDP/IP stack.

3.32.2 The complete details of the management interface and the protocols, as pertaining to each layer of the protocol-stack implemented in the management system, shall be made available, for the purpose of integrating the local management capabilities with the centralized NMS at a later date. The minimum requirements shall be:

a. Protocol details at all layers of TCP/IP stack
b. PHY I/F at each layer
c. Database structures
d. Number formats
e. Node addressing system
f. Complete application software details etc
g. eMS software check-sum

3.33 eMS Hardware Requirements

3.33.1 eMS Network Requirements

A typical eMS network architecture of the NOC [Network Operating Center] is given below. The requirement of the eMS network or the redundancy of the eMS network elements shall be decided by the purchaser. Purchaser can procure the eMS servers alone also with or without the SAN Switch and Storage components

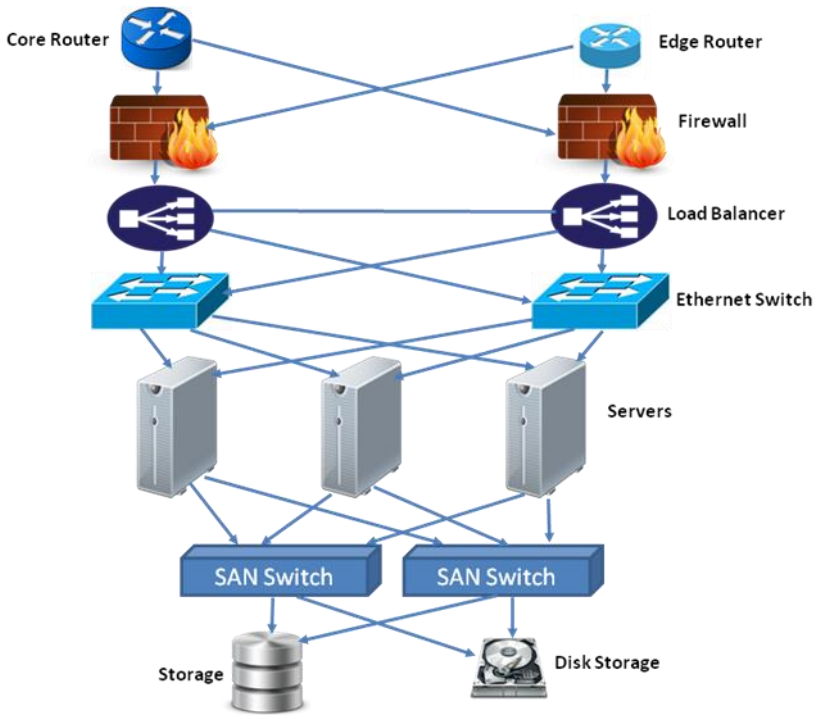

Figure 13: Typical Redundant eMS Network Architecture

3.33.1.1 The Core/Edge router shown in figure is the existing or the being deployed MPLS Network of the Service Provider.

3.33.1.2 The tendering authority shall indicate the redundancy requirement for Firewall, Load Balancer, Ethernet switch, SAN Switch etc as shown in the figure.

3.33.1.3 The tendering authority shall indicate whether separate Storage is required as shown in the figure or the Storage in the Server is adequate.

3.33.1.4 The Firewall shall be as per TEC/GR/IT/FWS-001/04 MAR 2014. The type of firewall required shall be specified by the purchaser.

3.33.1.5 The Load Balancer shall be as per TEC/GR/IT/LSW-002/03 MAR 2015. The Category of Load Balancer required shall be specified by the purchaser.

3.33.1.6 The Ethernet Switch shall be as per TEC/GR/IT/LSW-001/05 MAR 2014. The Category of Switch required shall be specified by the purchaser.

3.33.1.7 The eMS Server hardware shall be as per TEC/GR/IT/SRV-001/02 MAR 2018. The Category of Server required shall be specified by the purchaser.

3.33.1.8 The Type of server required shall be specified by the purchaser.

3.33.1.9 The Storage hardware shall be as per TEC/GR /IT/DSI-001/04 DEC 15. The type of Storage hardware required shall be specified by the purchaser.

3.33.1.10 The eMS solution runs in high availability mode with redundancy i.e. N+1 (Active or Passive) configuration

3.33.1.11 All SW applications shall run in a redundant active – standby pair of hosts with automatic switchover in case active server or its applications have any failure.

3.33.1.12 Hardware Sizing Guidelines: Hardware sizing is based on the following CPU utilization metric (CPU Utilization = 100 – CPU Idle)%. Peak CPU Utilization shall not exceed 75% at any time, on 24x7 basis. Average CPU Utilization over any hour, measured at 5 minute intervals, shall not exceed 60%. The hardware sizing indicated is minimum and indicative.

4.0 Interconnectivity and Inter-Operability Requirements

This section describes the interface, interconnectivity and inter-operability requirements for the Routers.

4.1 Interface Requirements

The router shall be capable of supporting the following types of interfaces. However the Type & actual number of interfaces shall be decided by the purchaser.

i. 100 G Optical Interface
ii. 40 G Optical Interface
iii. 10 G Optical Interface
iv. 1 G Optical Interface
v. 10/100/1000 Base-T Electrical Interface
vi. STM-16 POS Optical Interface
vii. STM-1 POS Optical Interface
viii. STM-1 CE
ix. E1 IP Interface
x. E1 CE Interface
xi. 10/100 Base-T Electrical Interface
xii. 25 G Optical Interface
xiii. 50 G Optical Interface
xiv. 200 G Optical Interface
xv. 400 G Optical Interface
xvi. 34 Mbps-E3
xvii. 45 Mbps
xviii. Fast Ethernet Optical Interface
xix. N X 64 Kbps
xx. CDMA
xxi. WCDMA or HSPA
xxii. GSM or GPRS or EDGE
xxiii. LTE or LTE-A
xxiv. 5G NR (FR1)
xxv. 5G NR FR1 & FR2
xxvi. 5G NR FR2
xxvii. ADSLx
xxviii. SHDSL
xxix. VDSLx
xxx. ISDN BRI
xxxi. ISDN PRI
xxxii. 800 G Optical Interface
xxxiii. 2.5G BASE-T Electrical Interface
xxxiv. 5G BASE-T Electrical Interface
xxxv. 10G BASE-T Electrical Interface

4.2 Interface Specifications

4.2.1 General Requirements

a. The Router shall support to use all optical interfaces as either client interface or network interface. Each port shall be configurable for any direction of transmission.
b. The Router shall be based on commercially available pluggable (CFP/QSFP28/QSFP+/QFP/SFP/XFP) optics for all optical interfaces.
c. The Router shall support full duplex capabilities on all Ethernet ports
d. The Router shall support to monitor transmit and receive power on all optical interface ports on the Router.
e. The interface cards shall be hot pluggable on chassis based Routers

4.2.2 100G Optical Interface

4.2.2.1 Specifications

Window of operation	Around 1300 nm
Data Rate in each lane	25.78125 Gbps
Mean launch power, each Lane	-4.5 to +4.5 dBm
Distance coverage	10/40 Km

4.2.2.2 The 100G interface shall be as per IEEE 802.3ba standard

4.2.2.3 The interface shall be based on QSFP28, CFP or CPAK

4.2.3 40G Optical Interface

4.2.3.1 Specifications

Window of operation	Around 1300 nm
Data Rate in each lane	10 Gbps
Mean launch power, each Lane	-4.5 to +4.5 dBm
Distance coverage	10 Km

4.2.3.2 The 40G interface shall be as per IEEE 802.3ba standard

4.2.3.3 The interface shall be based on QSFP+/QFP or CFP

4.2.4 10G Optical Interface

4.2.4.1 Specifications

Wavelengths	850nm, 1310 nm and 1550 nm windows
Wavelength	Wideband / Narrow Band (Coloured λ interface to DWDM) (Purchaser shall specify the wavelength required)
Distance Coverage	300m/10Km/40Km/80Km
SFP Type	LAN Phy/WAN Phy/G.709 FEC SFP+/XFP The SFP Type requirement to be specified by the purchasing authority vide clause10.4.1
Buffer Type	**LQ:** Low Queue support interface with support of more than 8 Queues **HQ:** High Queue support interface with support of more than 32K Queues. However for category III

	and V Routers the interface shall support more than 8K Queues
Fiber	G.652 single mode

10G Interface Type	Distance	Wavelength	Avg. Launch Power (dBm)
10GBASE-SR/SW	300m	850 nm	-7.3 to -1.0
10GBASE-LR/LW	10 Km	1310 nm	-8.2 to 0.5
10GBASE-ER/EW	40 Km	1550 nm	-4.7 to 4.0
10GBASE-ZR	80 Km	1550 nm	0 to 4

4.2.4.2 Features

a. The Router shall support 10GBASE-SR, 10GBASE-LR and 10GBASE-ER as per IEEE 802.3ae for LAN applications.
b. The Router shall support 10 GBASE-LW and 10 GBASE-EW supporting 10 and 40 Km each over single-mode fiber for WAN applications.
c. The Router shall support Optional direct coupling to MUX input of third party DWDM system through colored λ interface.
d. The interface shall be based on SFP+ or XFP

4.2.5 1G Optical Interface

4.2.5.1 Specifications

Wavelengths	850 nm multi mode or 1310/1550 nm single mode
Buffer Type	**LQ:** Low Queue support interface with support of more than 8 Queues **HQ:** High Queue support interface with support of more than 8K Queues
Distance coverage (Multimode)	500 m
Distance coverage (Single mode)	10/40/70 Km, SFP+

1G Interface Type	Fiber	Distance	Wavelength	Avg. Launch Power (dBm)
1GBASE-SX	MM	200 - 500m	850 nm	-9 to -3
1GBASE-LX	SM	10 Km	1310 nm	-9 to -3
1GBASE-EX	SM	40 Km	1310 nm	-5 to 0
1GBASE-LX	SM	70 Km	1550 nm	-2.0 to +3.0

4.2.5.2 Features

a. The Router shall support 1000BaseSX, 1000BaseLX, 1000BaseZX as per IEEE 802.3
b. The Router shall support 1000BaseT as per IEEE 802.3ab, 1000Base SX/LX as per IEEE 802.3z.
c. The interface shall be based on SFP

4.2.6 10/100/1000 Base-T Electrical Interface

4.2.6.1 The Router shall support 10/100/1000 Base-T, 100mt, Full duplex, autosensing

4.2.6.2 The interface shall be based on SFP

4.2.7 STM-16 POS Optical Interface

4.2.7.1 Specifications

Wavelengths	1310 nm and 1550 nm windows
Distance coverage	10/40 Km depending on type of SFP+
Fiber	G.652 single mode

4.2.7.2 Features

a. The STM-16 POS interface shall support PPP, RFC 1661
b. The STM-16 POS interface shall support PPP over SONET/SDH, RFC 2015

4.2.8 STM-1 POS Optical Interface

4.2.8.1 Specifications

Wavelengths	1310 nm and 1550 nm windows
Distance coverage	10 to 40 Km depending on type of SFP+
Fiber	G.652 single mode

4.2.8.2 Features

a. The STM-1 POS interface shall support PPP, RFC 1661
b. The STM-1 POS interface shall support ML-PPP

4.2.9 Channelised STM-1 Optical Interface

4.2.9.1 Specifications

Wavelengths	1310 nm and 1550 nm windows
Distance coverage	10 to 40 Km depending on type of SFP+
Fiber	G.652 single mode

4.2.9.2 Features

a. Each Channelised STM-1 port shall support upto 63 E1 circuits.
b. The E1 circuits may carry TDM traffic to be transported over Circuit Emulation or IP traffic
c. Within the channelised STM-1 port, each logical E1 channel is configurable as unframed E1 and channelised E1.
d. The channelised STM-1 port shall support the IP protocol and the ppp encapsulation protocol .
e. The channelised STM-1 port along with all channelised E1 virtual ports shall support Multilink PPP (MLPPP) as per RFC 1990.
f. Channelized for PPP and MLPPP also.

4.2.10 E1 IP Interface

4.2.10.1 Specifications

a. The E1 IP interface shall be as per, ITU-T G.703 standard.
b. The E1 IP interface shall support Framed and Unframed.
c. Each logical E1 channel shall be capable of channelisation down to 64kbps and N x 64 kbps channels. Each channelised E1 port shall support 31 such channels.
d. The channelised E-1 port shall support the IP protocol and ppp encapsulation protocol.

4.2.11 E1 CE Interface

4.2.11.1 Specifications

a. The E1 CE interface shall be as per, ITU-T G.703 standard.
b. The E1 CE interface shall support Framed and Unframed.
c. Each logical E1 channel shall be capable of channelisation down to 64kbps and N x 64 kbps channels. Each channelised E1 port shall support 31 such channels.
d. Each channel shall carry TDM traffic to be carried using Circuit Emulation Protocols.

4.2.12 10/100 Base-T Electrical Interface

4.2.12.1 The Router shall support 10/100 Base-T, 100mt, Full duplex, autosensing

4.2.12.2 The interface shall be based on SFP

4.2.13 * 25 G Optical Interface

- The specifications/limits/values of the above optical Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.2.14 * 50 G Optical Interface

- The specifications/limits/values of the above optical Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.2.15 * 200 G Optical Interface

- The specifications/limits/values of the above optical Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.2.16 * 400 G Optical Interface

- The specifications/limits/values of the above optical Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.2.17 * Fast Ethernet Optical Interface

- The specifications/limits/values of the above optical Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.2.18 45 Mbps Interface

4.2.18.1 The 45 Mbps interface shall be as per ITU-T G.703, Annex-I

4.2.19 34 Mbps-E3 Interface

4.2.19.1 The 34 Mbps-E3 interface shall be as per ITU-T G.823, Annex-I

4.2.20 N X 64 Interface

4.2.20.1 The NX64 interface shall be as per ITU-T G.823, Annex-I

4.2.21 CDMA Interface

The CDMA interface shall be as per 1xS0011 or EN 301 908-04 CDMA. Annex F9, NFAP, Annex-F

4.2.22 WCDMA or HSPA Interface

4.2.22.1 The WCDMA or HSPA interface shall be as per 3GPP TS 34.121-1 or EN 301 908-2. Annex F11, NFAP, Annex-F

4.2.23 GSM or GPRS or Edge Interface

The GSM or GPRS or EDGE interface shall be as per 3GPP TS 51 010-1 or EN 301 511. Annex F10, NFAP Annex-F

4.2.24 LTE or LTE-A Interface

4.2.24.1 The LTE interface shall be as per 3GPP TS 36.521-1 or EN 301 908-13. Annex-F12, NFAP, Annex-F

4.2.25 5G NR (FR1) Interface

4.2.25.1 The 5G NR (FR1) interface shall be as per 3GPP TS 38.521-1 standard

4.2.26 5G NR FR2 Interface

4.2.26.1 The 5G NR (FR2) interface shall be as per 3GPP TS 38.521-1 & 3GPP TS 38.521-2 standard

4.2.27 5G NR FR1 & FR2 interworking with other Radios

4.2.27.1 The 5G NR (FR1 & FR2) interface shall be as per 3GPP TS 38.521-3 standard

4.2.28 ADSLx Interface

4.2.28.1 The ADSLx interface shall be as per ETSI EN 300 001. Annex-J1

4.2.29 SHDSL Interface

4.2.29.1 The SHDSL interface shall be as per G.991.2. Annex-J1

4.2.30 VDSLx Interface

4.2.30.1 The VDSLx interface shall be as per G.993.1 or G993.2. Annex-J1, ETSI EN 300 001. Annex-D

4.2.31 ISDN BRI Interface

4.2.31.1 The ISDN BRI interface shall be as per Q.931, Annex-D1

4.2.32 ISDN PRI Interface

4.2.32.1 The ISDN PRI interface shall be as per Q.931, Annex-D1, G.703 Cl. 11.1 ETSI TBR-4 Cl. 9.2.3. Annex-I , G.823 I.431 ETSI TBR-4. Annex-I

- The specifications/limits/values of the above interfaces are as per Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures

4.3 Inter-Operability Requirements

4.3.1 Ethernet Handover

4.3.1.1 The handover of IP traffic from/to the existing IP Networks shall be supported at Ethernet level (1GE or 10GE) over the UNI interfaces.

4.3.2 TDM handover:

4.3.2.1 The handover of TDM traffic from/to the existing TDM network shall be supported at STM-1 level over the UNI interfaces.

4.3.3 MPLS Interworking:

4.3.3.1 The Routers shall provide the interworking function with the IP-MPLS network using

a. LSP-Stitching
b. MSPW
c. VLAN hand over
d. MPLS-TP and IP/MPLS interworking

4.3.4 Inter ISP:

4.3.4.1 Inter ISP Operations shall be as per RFC4364.

5.0 Quality Requirements

5.1 The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.

5.2 The equipment shall be manufactured in accordance with international quality management system ISO 9001:2015 or any other equivalent ISO certificate for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted.

5.3 The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue- March, 2010}(TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipments" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case.

6.0 EMI/EMC REQUIREMENTS

GENERAL ELECTROMAGNETIC COMPATIBILITY (EMC) REQUIREMENTS:

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report from accredited test lab shall be furnished from a test agency.

a) **Conducted and radiated emission (applicable to telecom equipment):**

Name of EMC Standard: "CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits:-

i) To comply with Class B of CISPR 32 (2015) with amendments for indoor deployments and Class A of CISPR 32 (2015) with amendments with amendments for outdoor deployments.

b) **Immunity to Electrostatic discharge:**

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits:-

i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) **Immunity to radiated RF:**

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".

Limits:-

For Telecom Equipment and Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000-4-4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".

Limits:-

Test Level 2 i.e.

a) 1 kV for AC/DC power lines;

b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test".

Limits:-

i) For mains power input ports : (a) 2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling

ii) For telecom ports : (a) 2kV peak open circuit voltage for line to ground (b) 2KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) with amendments) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio-frequency fields".

Limits:-

Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests".

Limits:-

i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10s.

h) **Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):**

Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.

Limits:-

i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.

ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.

iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.

iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C.

v. Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.

Note: - For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 (TEC 11016:2016) and the referenced base standards i.e. IEC and CISPR standards and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard TEC/SD/DD/EMC-221/05/OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 32	EN55032
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

7.0 SAFETY REQUIREMENTS

The equipment shall conform to relevant safety requirements as per IS/IEC 62368-1:2018 or Latest as prescribed under Table no. 1 of the TEC document ‘SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT”: TEC10009: 2024. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.

8.0 SECURITY REQUIREMENTS

8.1 Security Requirements for the Routers

8.1.1 Port Address Translation (PAT)

The Router shall support Port Address Translation . The requirement for router with data capacity of more than 10Gbps to be specified by the purchasing authority vide clause10.4.1

8.1.2 Network Address Translation (NAT)

8.1.2.1 The Router shall support Network Address Translation as per RFC 3022. The requirement for router with data capacity of more than 10Gbps to be specified by the purchasing authority vide clause10.4.1

8.1.3 DHCP:

8.1.3.1 The Router shall support DHCP

8.1.3.2 The Router shall be able to insert option 82 when functioning as a DHCP relay. It shall be posssible to add / replace or drop the option 82 tags to the incoming DHCP packet.

8.1.3.3 The Router shall support Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

8.1.3.4 The Router shall support DHCPv6 prefix delegation

8.1.3.5 The Router shall support DHCP for IPv6 relay agent

8.1.3.6 The Router shall support DHCPv6 prefix delegation via AAA

8.1.3.7 The Router shall support DHCPv6 Server Stateless Auto Configuration

8.1.3.8 The Router shall support DHCPv6 relay - reload persistent interface ID option

8.1.3.9 The Router shall support DHCP - DHCPv6 Individual Address Assignment

8.1.3.10 The Router shall support DHCP IPv6 Prefix Delegation as per RFC 8415

8.1.3.11 The Router shall support DNS Extensions to Support IP Version 6 as per RFC 3596

8.1.3.12 The Router shall support DNS Configuration options for DHCPv6 as per RFC 3646

8.1.4 Broadcast Storm control:

8.1.4.1 The Router shall support unicast, multicast and broadcast storm control blocking on any interface or port.

8.1.4.2 The Router shall support to control multicast, broadcast, DLF traffic on per tunnel basis. Frames is dropped once the per-second counter goes beyond the configured limit

8.1.4.3 The Router shall support Unknown Unicast Flood Blocking (UUFB)

8.1.5 Proxy ARP:

8.1.5.1 All ARP requests from subscribers shall be given the MAC address of the Router that provides L3 aggregation of that VLAN. The ARP address which the Router responds shall be unique per VLAN.

8.1.6 Spoofing Attacks:

8.1.6.1 The Router shall protect ARP spoofing attacks at layer 2 by ARP inspection to prevent malicious users from impersonating other hosts.

8.1.6.2 The Router shall support Dynamic ARP Inspection (IPv4 only)
8.1.6.3 The Router shall support Neighbour Spoofing in IPv6
8.1.6.4 The Router shall support IP/MAC address anti spoofing

8.1.7 Unicast Reverse Path forwarding (URPF):

8.1.7.1 The Router shall compare the source address of a packet with its routing entries to verify if the data has been received on the legitimate interface. The packet would be forwarded only if the reverse path has been verified to be legitimate thus preventing malicious users from changing their source addresses.

8.1.8 DOS Attacks: The Router shall support Blocking IP DoS attacks from:

a. Unknown Protocol
b. UDP Short header/Flood
c. TCP Packets without flag
d. Oversized TCP packets
e. SYN attack
f. IP Spoofing
g. IP Stream Option
h. IP short header
i. Internet Control Message Protocol (ICMP) Source quench /Mask request/ Mask reply/Large
j. packet/Info Request and Reply/ Flood
k. Too many fragments
l. Call gapping

8.1.9 ICMP Rate limiting:

8.1.9.1 The router shall provide the capability to control the rate at which a user is able to ping any of its interface, logical or physical. Wire speed filtering and rate limit shall be provided.

8.1.10 Port Security:

8.1.10.1 The Router shall support Port Mirroring
8.1.10.2 The Router shall support Port level security mechanism to prevent unauthorized nodes from accessing the switch.
8.1.10.3 The Router shall not allow port to port traffic to prevent the by passing of network policy enforcement point by the users.

8.1.11 Port Binding:

8.1.11.1 The Router shall support Dynamic binding of MAC address with port

8.1.12 Access Control List (ACL):

8.1.12.1 The Router shall support ACLs to prevent unauthorized access. The Router shall support Standard Access Lists and Extended Access Lists to implement access control supervision and control. It shall be possible to deny traffic based on the following:

a. Source Interface type
b. Source/ destination MAC
c. VLAN ID
d. Protocol Type (TCP/UDP/IP etc.)

8.1.12.2 The Router shall support Access Control Lists for controlled SNMP Access only to the SNMP manager or the NMS workstation.

8.1.12.3 The Router shall support ACLs at layer 2-4 in hardware.

8.1.12.4 The Router shall support ACLs can limit telnet and SNMP access to the router.

8.1.12.5 The ACL shall be implemented in hardware and even when running at the maximum number of ACL, there shall not be any performance degradation.

8.1.12.6 The Router shall support classification capabilities at line rate.

8.1.12.7 For IP ACL classification, the Router shall support traffic templates to define service classes, traffic policies, CIR/PIR etc. These templates shall then be applied to specified IP interfaces.

8.1.12.8 The Router shall support Time based access list to control the usage of application and resource based on time parameters.

8.1.12.9 The Router shall support Standard access control lists for IPv6

8.1.12.10 The Router shall support Extended access control lists for IPv6

8.1.12.11 The Router shall support IPv6 ACL extensions for IPSec authentication header (applicable for type I to XII Routers)

8.1.12.12 The Router shall support Secure Shell (SSH) support over IPv6

8.1.13 IPSec & Encryption

8.1.13.1 The Router shall support IP Security (IPSec) for Management plane

8.1.13.2 The Router shall support site-to-site and remote access IPSec VPN & SSL VPN.

8.1.13.3 The Router shall support security Architecture for the Internet Protocol as per RFC 4301

8.1.13.4 The Router shall support IP Authentication Header as per RFC 4302

8.1.13.5 The Router shall support IP Encapsulation Security Payload as per RFC 4303

8.1.13.6 The Router shall support IKEv2 as per RFC 5996

8.1.13.7 The Router shall support Local Key Distribution Function (LKDF) for delivering Authentication Keys

8.1.13.8 The Router shall support 3DES and other strong ESP cipher algorithms as per RFC 2451 and RFC 3602

8.1.13.9 The Router shall support Transport Layer Security (TLS) Protocol Version 1.2 as per RFC 5246

8.1.13.10 The Router shall support UDP Encapsulation of IPsec ESP Packets as per RFC 3948

8.1.13.11 IPv6 IPSec VPN

8.1.14 Lawful Interception [Port Mirroring]:

8.1.14.1 The Router shall support port mirroring over L2/L3 network – both local and remote.

a. Up to 10 sessions.
b. Option to filter incoming / outgoing traffic.

8.1.14.2 It shall be possible to mirror a particular service from a particular port or on per SVLAN/PW basis to a probe port.

8.1.14.3 The Router shall support logging and forwarding the egress and ingress traffic on a per-logical channel basis to a central location in the network for Lawful Interception and Monitoring.

8.2 eMS Requirements specific to Routers Security functionalities

The eMS shall support the following Configurations, Fault and Performance management support which are specific to Routers Security

8.2.1 Broadcast Storm control:

a. Configure Unicast, multicast and broadcast storm control blocking on any interface or port
b. Configure to control/limit multicast, broadcast, DLF traffic on per tunnel basis.

8.2.2 Spoofing Attacks:

a. Configure ARP spoofing attacks prevention at layer 2, Dynamic ARP Inspection, Neighbour Spoofing in IPv6, IP/MAC address anti spoofing

8.2.3 Unicast Reverse Path forwarding (URPF):

a. Configuration of selected interfaces and users

8.2.4 DOS Attacks

8.2.5

a. Configure Blocking of IP DoS attacks from Unknown Protocol, UDP Short header/Flood, TCP Packets without flag, Oversized TCP packets, SYN attack, IP Spoofing, IP Stream Option, IP short header, Internet Control Message Protocol (ICMP) Source quench /Mask request/ Mask reply/Large, packet/Info Request and Reply/ Flood, Too many fragments, Call gapping

8.2.6 ICMP Rate limiting:

a. Configurations to control the rate at which a user is able to ping any of its interface, logical or physical.

8.2.7 Port Security:

a. Port level security mechanism control configurations
b. Configure to control port to port traffic

8.2.8 Port Binding:

a. Port binding parameters configurations

8.2.9 Access Control List (ACL):

a. Setup the ACL and configuraion based on Source Interface type, Source/ destination MAC, VLAN ID, Protocol Type (TCP/UDP/IP etc.) etc
b. Configure Access Control Lists for controlled SNMP Access only to the SNMP manager or the NMS workstation.
c. Configure ACLs to limit telnet and SNMP access to the router.
d. Configure Time based access list to control the usage of application and resource based on time parameters.

8.2.10 IPSec & Encryption

a. IP Security (IPSec), IPSec VPN & SSL VPN configurations as per RFC4301, 4302, 4303, 3715, 3948
b. Internet Security Association and Key Management Protocol (ISAKMP), Local Key Distribution Function (LKDF)configurations as per RFC5996.

c. IKE Keep alive configurations
d. TLS Protocol configurations as per RFC5246

8.2.11 Lawful Interception / Port Mirroring:

a. Configure local and remote Port mirroring over L2/L3 network with Option to filter incoming / outgoing traffic
b. Configuration to mirror a particular service from a particular port or on per SVLAN/PW basis to a probe port.
c. Configure Logging and forwarding the egress and ingress traffic on a per-logical channel basis to a central location in the network for Lawful Interception and Monitoring [LIM].

8.2.12 Fault Management

a. Protocol anomaly detection alarms
b. System response to Intrusion Prevention Service: After it detects an attack, the Router shall responds by Generate an alarm, Log the alarm event and Record the session to an IP session log

8.2.13 Performance Management

a. Report any unauthorized activity.

8.3 Security Management Requirements for the eMS

8.3.1 General

8.3.1.1 The eMS shall provide adequate security to the data and for the access to the management system as per the following details:

8.3.1.2 The eMS shall have the capability of supporting the management of Network through local and remote operators. The authorizations and the privileges of the operators (remote and local) shall depend upon the Login and Password

a. Low-level protection for read only access to faults and performance information.
b. Medium-level protection for access to configuration status and features.
c. High-level protection for control of access to change in the configuration and control parameters.

8.3.1.3 The eMS shall support operator authentication, command, menu restriction and operator privileges. The eMS shall support multi-level passwords as below-

a. eMS shall allow the System Administrator to define the level of access to the network capabilities or feature for each assigned password. It shall be desirable that the eMS shall block the access to the operator in case of unauthorized commands being tried for five consecutive times. Also it is desirable that the eMS shall also not allow the entry into the eMS in case wrong password is provided more than five consecutive times during the login
b. The system administrator shall be able to monitor and log all operator activities in the eMS.
c. The dynamic password facility shall be provided in which the operator may change his password at any time

8.3.1.4 All log-in and log-out attempts shall be logged in the security log file of the eMS system

8.3.1.5 The eMS system shall be protected against intentional or accidental abuse, unauthorized access and loss of communication.

8.3.1.6 The man-machine communication programs shall have the facility of restricting the use of certain commands or procedures to certain passwords and terminals.

8.3.1.7 It shall be mandatory for the system to have a record of all log-ins for a period of at least six months after which a back up should be _possible under system administrator command.

8.3.1.8 It shall be possible to connect eMS and the network elements to the IP-MPLS network. The eMS and components of the existing/proposed Network Management Layer (NML)/Service Management Layer (SML) of a purchaser shall be part of the common MPLS-VPN providing the inherent security required for the management information in addition to the login and password based authorization for the operators of the Network Manager.

8.3.1.9 **Back up for programs and data:** The eMS shall be able to back up and restore the data base to and from external storage media.

8.3.2 LOG Capturing/Analysis

8.3.2.1 The eMS shall support collection of logs via either of the following methods:

a. Syslog over UDP/TCP.
b. SyslogNG
c. Check Point LEA.
d. SNMP
e. ODBC (to pull events from a remote database).
f. FTP (to pull a flat file of events from a remote device that can't directly write to the network).
g. Windows Event Logging Protocol.
h. XML

8.3.2.2 The eMS shall support collection of log data during database backup, de-fragmentation and other management scenarios, without any disruption to service.

8.3.2.3 RAW logs that are send to the SIEM [Security Information and Event Management] solution if any shall be Authenticated (time-stamped), encrypted and compressed before being written to log storage.

8.3.2.4 The eMS shall support log compression capability for storage optimization (compression level at least 50%).

8.3.2.5 The solution Database shall use Write Once Read Many (WORM). Once the logs are written to the disk/database no one including database/system administrator can alter the stored RAW logs.

8.3.2.6 Purpose built object oriented database shall be used for storing IP related information and not relational databases. The storage system has flat file system to store log data.

8.3.2.7 Parting of logs or filtering of logs shall not be done at any stage of log collection or log storage.

8.3.2.8 The eMS shall support Single Global View of all the data across sites/geographies.

8.3.2.9 The eMS shall be scalable to support from 5000 devices up to 20000 devices

8.3.2.10 The eMS shall collect raw data in real-time to a Central Database from any IP device including home grown, customized and proprietary applications.

8.3.2.11 Historical records and database query done shall be within the solution. No third party tool shall be required to access the database.

8.3.2.12 The eMS shall support compliance to Regulations with data archival.

8.3.2.13 Log parsing shall use only XML and shall not use any other proprietary parsing mechanisms.

8.3.2.14 The eMS shall support two factor authentications to login to the system.

8.3.2.15 The eMS shall support watch list feature to monitor desired data like specific IP addresses, usernames and other data.

8.3.3 Altering and Viewing Requirements

8.3.3.1 The eMS shall support full playback of events that have occurred to ensure comprehensive trend and historical analysis and reporting.

8.3.3.2 The eMS shall support email alerts and integration capabilities to third party ticketing engines and forward alerts via Syslog or SNMP.

8.3.3.3 The eMS shall categorize all event collected by device into event taxonomies for easier classification and management.

8.3.3.4 The eMS shall support Distributed viewing and delegation of user rights across devices and access to individual components of the application.

8.3.3.5 The eMS shall support Alert suppression for specific events.

8.3.3.6 The eMS shall allow creating baselines of network activity and shall provide a mechanism to raise alerts when baselines are crossed.

8.3.3.7 The eMS shall support Email of scheduled reports to recipients.

8.3.3.8 Email notifications shall contain the content of the report capable of being saved as HTML and/or PDF.

8.3.3.9 The eMS shall support configurable automated actions in response to security problem, sending E-mail Notifications, SMTP notification, SYSLOG notification, SNMP Notification to operators.

8.3.3.10 The eMS shall support facility to view Summary of all Dashboard views for the entire enterprise.

8.3.3.11 The eMS shall support provision of view filter when displaying the logs related to specific IP address, specific service or specific time duration.

8.3.3.12 The eMS shall support event display Window for all alerts.

8.3.3.13 The eMS shall support web based (both http and https) user interface for device performance monitoring and analysis with SSL connectivity to backend appliances.

8.3.4 Reporting

8.3.4.1 Reports shall be available for compliance and supported devices.

8.3.4.2 The system shall allow modification of existing reports and creation of new reports (through wizard).

8.3.4.3 Reports shall be available in the following exported formats:

a. PDF
b. CSV
c. HTML

8.3.4.4 The eMS shall support capability to schedule reports. All raw log format fields shall be available for query using the solution.

8.3.4.5 The eMS shall provide process for creating ad hoc queries. This process shall use standard syntax such as wildcards and regular expressions.

8.3.4.6 The process shall allow applying filters and sorting to query results.

8.3.5 Security Features

8.3.5.1 Log transaction between Client/Agent & Engine shall support SSL/encryption.

8.3.5.2 The eMS shall have capability to gather information on real-time threats and zero day attacks through signatures issued by anti-virus or IDS vendors or audit logs and add this information as intelligence feed in to the solution via patches.

8.3.5.3 Archival information and summary information shall be provided separately.

8.3.5.4 The eMS shall maintains audit trail for the management activities of individual users accessing and using the application.

8.3.5.5 The eMS shall support capability to create and assign role-based views.

8.3.5.6 The eMS shall support mechanism for protection of unauthorized access on the Log Database.

8.3.5.7 Incident status and escalation shall be supported and a record of action taken shall be maintained.

8.3.5.8 The eMS shall support Robust & scalable architecture to handle high volume of data with high Events per second.

8.3.6 Correlation

8.3.6.1 The eMS shall support correlation of logs from all the devices within an enterprise and all security scenarios like spoofing, authentication failure, etc. Multi-device, multi-event and multi-site correlation across the enterprise.

8.3.6.2 The eMS shall support following types of correlation:

a. Rule-Based correlation
b. Vulnerability Based Correlation
c. Statistical Based
d. Historical Based

8.3.6.3 The eMS shall display summarization of events.

8.3.6.4 The eMS shall support rules for popular IDS, firewalls, antivirus, etc. The exact requirement to be specified by the purchasing authority vide clause10.4.1

8.3.6.5 The rules shall allow import/export in XML format. Provide a GUI based application for creating new correlation rules/modifying existing rules.

8.3.6.6 The eMS shall support capability to correlate all the fields in a log without normalizing the logs at collection points.

8.3.6.7 The eMS shall support wizard based interface for rule creation. The rules shall support logical operators for specifying various conditions in rules.

8.3.6.8 The eMS shall support system leverage information about enterprise assets and known vulnerability to identify false-positive IDS messages and to browse assets and vulnerabilities. The exact requirement to be specified by the purchasing authority vide clause10.4.1

8.3.7 Forensic Capabilities

8.3.7.1 The eMS shall support flexible dashboard interface customized to user preferences allowing the examination of a specific event or a holistic view of the systems within the enterprise.

8.3.7.2 The eMS shall support Quick and easy access to real-time as well as historical operational data.

8.3.7.3 The eMS shall provide tool for comprehensive trend and historical analysis of logs and their reporting.

8.3.7.4 Following categories of predefined graphs and queries shall be supported:

a. Firewall, including Top Firewall Interface, File Access through Firewall, and Login Failure Summary.
b. Database, such as Login Activity, Authorization Level and Authorization Level by User.

c. Intrusion detection, including Top Attack Signatures, Attack Type by Severity Level, and IDS Signature Summary.
d. Operations, such as Device Activity Analysis, Activity by Event Category, and Network over Time.
e. User, including Privilege Users Monitoring, Configuration Change Details and Activity by Specific Username. The exact requirement to be specified by the purchasing authority vide clause10.4.1

8.3.8 External Attached Storage Array

8.3.8.1 The eMS shall support Tiered storage strategy for the online, archival, backup and restoration of event log information. The platform shall optimally manages the storage of an event from the moment it is created to when it is no longer needed. All logs shall be managed from the time of generation to retirement of logs.

8.3.8.2 The eMS shall support integration of DAS/NAS and SAN.

8.3.8.3 The eMS shall support entire Life Cycle management solution for log retention and purging after log retention period is over.

8.3.8.4 The eMS shall support Online and offline storage of logs which is needed for log retention.

8.3.8.5 The eMS shall enable offline storage of logs with automated tools for log purging and retrieval from offline storage.

8.4 The Routers shall comply to the security guidelines issued by DoT vide letter no. 10-54/2010-CS-III (ILD) dt.31/05/2011 and subsequent amendments if any.

9.0 OTHER MANDATORY REQUIREMENTS

9.1 ENGINEERING REQUIREMENTS

The system shall meet the following engineering requirements:

9.1.1 The equipment shall adopt state of the art technology.

9.1.2 All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.

9.1.3 All cables shall be of Gigabit Ethernet ready standards.

9.1.4 The equipment shall have adequate cooling arrangements.

9.1.5 The actual dimensions and weight of the equipment shall be furnished by the manufacturers

9.2 OPERATIONAL REQUIREMENTS

The system shall meet the following maintenance & operational requirements:

9.2.1 The equipment shall be designed for continuous operation.

9.2.2 The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level.

9.2.3 Suitable visual indications shall be provided, to indicate the healthy and unhealthy conditions.

9.2.4 The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.

9.2.5 The removal or addition of any cards shall not disrupt traffic on other cards. (applicable for type Chassis based Routers)

9.2.6 In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.

9.2.7 A power down condition shall not cause loss of connection configuration data storage.

9.2.8 The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with SP's network for voice, data and transmission systems, as the case may be.

9.2.9 The system shall support built in power diagnostics system to detect hardware failures.

9.2.10 The router shall be 19"/ 23" Euro Rack Mountable.

9.2.11 The Router shall support built-in power-on diagnostics and system monitoring capabilities to detect hardware failures. All modules shall provide LED/LCD display to indicate operational status of the module

9.3 POWER SUPPLY REQUIREMENTS:

9.3.1 **AC Voltage Requirements:** The specified category of routers shall be capable of working with 220V AC ±20%

9.3.2 **DC Requirements:** The specified category of routers shall be capable of working with –48 V DC Nominal (negative 48 V DC) with a voltage variation –40 V to –57 V DC.

9.3.3 The equipment power supply shall meet the following requirements:

i. The equipment shall be able to function over the range specified in the respective sections, without any degradation in performance.

ii. The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.

iii. The derived DC voltages shall have protection against short circuit and overload.

9.3.4 The Router could be working with AC or DC input Power Supply or Both. The exact requirement of AC working or DC working or Both AC & DC working shall be specified by the purchaser.

9.4 INSTALLATION REQUIREMENTS

9.4.1 The equipment shall have:

i. Proper earthing arrangement,

ii. Protection against short circuit / open circuit

iii. Protection against accidental operations for all switches / controls provided in the front panel

iv. Protection against entry of dust, insects and lizards

9.5 OTHER REQUIREMENTS

9.5.1 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.

9.5.2 Wherever, the standardized documents like ITU-T, IEEE, QA, TEC etc. documents are referred, the latest issue and number with the amendments shall be applicable.

9.5.3 The latest issues and number shall be applicable for all referred standardized documents like ITU-T, IEEE, TEC etc

9.6 MINIMUM EQUIPMENTS FOR TYPE APPROVAL TESTING

While offering the Routers for Type Approval Certificate, the following shall be the minimum requirements and the same shall be mentioned in the Type Approval Certificate. The Type Approval certificate shall be issued for the offered category.

a. One Router of the offered category
b. Minimum two interfaces of each type as per the category of the Router
c. eMS server with eMS software including optional items (In case required for the offered category)

10.0 DESIRABLE REQUIREMENTS

This section describes the desirable requirements for the Routers and will depend upon the requirement of the purchaser. Hence the tendering authority may choose out of the clauses mentioned below as per requirement.

10.1 DOCUMENTATION

10.1.1 All technical documents shall be in English language both in CD- ROM and in hard copy.

10.1.2 The documents shall comprise of:

i. System description documents

ii. Installation, Operation and Maintenance documents

iii. Training documents

iv. Repair manual.

10.1.2.1 System description documents:

The following system description documents shall be supplied along with the system:

i. Over-all system specification and description of hardware and software

ii. Equipment layout drawings

iii. Cabling and wiring diagrams

iv. Schematic drawings of all circuits in the system with timing diagrams wherever necessary

v. Detailed specification and description of all Input / Output devices

vi. Adjustment procedures, if there are any field adjustable units.

vii. Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources

viii. Detailed description of software describing the principles, functions and interactions with hardware, structure of the program and data

ix. Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data

x. Program and data listings

xi. Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification

10.1.2.2 System operation documents:

The following system operation documents shall be available:

i. Installation manuals and testing procedures

ii. Precautions for installation, operations and maintenance

iii. Operating and Maintenance manual of the system

iv. Safety measures to be observed in handling the equipment

v. Man-machine language manual

vi. Fault location and troubleshooting instructions including fault dictionary

vii. Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.

viii. Emergency action procedures and alarm dictionary

10.1.2.3 Training Documents:

i. Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.

ii. Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.

iii. The structure and scope of each document shall be clearly described.

iv. The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

v. All diagrams, illustrations and tables shall be consistent with the relevant text

10.1.2.4 Repair Manual:

i. List of replaceable parts used .

ii. Detailed ordering information for all the replaceable parts

iii. Procedure for trouble shooting and sub-assembly replacement

iv. Test fixtures and accessories for repair

v. Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions

10.2 ADDITIONAL INSTALLATION REQUIREMENTS

10.2.1 All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR.

10.2.2 It shall be ensured that all testers, tools and support required for carrying out the stage by stage testing of the equipment before final commissioning of the network shall be supplied along with the equipment.

10.2.3 All installation materials, consumables and spare parts to be supplied.

10.2.4 All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.

10.2.5 For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations.

10.2.6 Special tools required for wiring shall be provided along with the equipment.

10.3 MAINTENANCE REQUIREMENTS:

10.3.1 All the software updates shall be provided on continuous basis for a minimum period of 7 years from the date of induction of system in the telecom network network. These updates shall include new features and services and other maintenance updates.

10.3.2 In the event of a bug 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.

10.4 GUIDELINES FOR TENDERING AUTHORITY

10.4.1 The tendering authority shall specify the following parameters:

1.	Category of Router
2.	Type & Quantity of each Type of Interface i.e. 100G, 40G, 10G, 1G etc (refer to clause 4.1)
3.	Wavelength, Distance criteria etc of each type of optical interface
4.	Wide band / Narrow band (Cλ interface for working with DWDM) optical interface for 10GE
5.	Buffer type for 1GE/10GE interfaces for the Core Routers
6.	Type of Circuit Emulation Standard required to be supported in their network
7.	Requirement of advanced Ipv6 features
8.	Requirement of optional Security features
9.	Requirement of eMS
10.	Requirement of eMS network as per clause 3.33.1
11.	Requirement of eMS network redundancy and network elements
12.	Type of Firewall Required for the eMS
13.	Type of Load Balancer Required for the eMS
14.	Type of Ethernet Switch Required for the eMS
15.	Category and Type of Server Required for the eMS
16.	Type of Storage Required for the eMS
17.	Requirement of Optional eMS features
18.	Scalability requirements for the SLA Management system like no.of business customers, maximum leads per customer etc may be provided
19.	North Bound interface required towards NMS
20.	Requirement of Optional Features
21.	Interfaces required to support SyncE features
22.	Requirement of control or switch card or both redundancy in case of categroy III and V Routers
23.	Ipv4 / Ipv6 Routes to be supported shall be specified for the aggregation and Core Routers among the options given
24.	Support of P and PE functionality on Core Routers
25.	Documentation requirements as per clause 10.1
26.	Additional Installation Requirements as per clause 10.2
27.	Maintenance Requirements as per clause 10.3
28.	The list of protocol support not required may be specified by the purchaser (refer to clause 3.10)
29.	The redundancy and hot-swappability of power supply and fans requirements may be specified by the purchaser (refer to clause 3.6.1.1 & 3.6.1.2) See Note#1 below.
30.	The requirement of SNMP/ Netconf to be specified by the purchasing authority as per clause 3.8.1.6

31.	The requirement of SNMP / gRPC/gNMI/Netconf to be specified by the purchasing authority as per clause 3.23.1.4
32.	The requirement of SNMP MIBs or gRPC telemetry or NETCONF (RFC 6241) and YANG-based models (RFC 6020/7950) to be specified by the purchasing authority as per clause 3.23.2.2
33.	Minimum value of MTBF required may be indicated (refer to clause 5.1)
34.	Applicable environmental category to be specified (refer to clause 5.3)
35.	The SFP Type requirement for 10G Optical interface as per clause 4.2.4.1
36.	Port Address Translation ferature as per clause 8.1.1.1
37.	Network Address Translation as per RFC 3022, as per clause 8.1.2.1
38.	The eMS Security requirements /features as per clause 8.3.6.4, 8.3.6.8, 8.3.7.4 e

Note#1 Suggestive Power Supply & Fan Unit Redundancy & Hot Swappable features requirement

Router Category	Power Supply redundancy (N+M), where N,M >0	Hot Swappable Power Supply	Fan Redundancy (N+M), where N, M >0	Hot Swappable Fan
Chassis Type Routers				
I	No	No	Optional	No
II	No	No	Optional	No
III	Yes	Yes	Yes	Yes
IV	Yes	Yes	Yes	Yes
V	Yes	Yes	Yes	Yes
VI	Yes	Yes	Yes	Yes
VII	Yes	Yes	Yes	Yes
VIII	Yes	Yes	Yes	Yes
IX	Yes	Yes	Yes	Yes
X	Yes	Yes	Yes	Yes
XI	Yes	Yes	Yes	Yes
XII	Yes	Yes	Yes	Yes
Non- Chassis Type Routers				
XIII	Optional	Optional	Optional	Optional
XIV	Yes	Optional	Yes	Optional
XV	Yes	Yes	Yes	Yes
XVI	Yes	Yes	Yes	Yes
XVII	Yes	Yes	Yes	Yes

While taking the decision on the above features, the purchaser or tendering authority make take into account the actual working environment conditions, network availability requirements and cost implications.

10.4.2 The following clauses are optional for Tendering Authority in respect of Non- Chassis Router:

S No.	Clause No	Salient features
1.	3.9.1.1	Ingress and egress bandwidth.
2.	3.9.1.3	transmission of a path join message
3.	3.9.1.4	Layer 2 protocol transport for Ethernet and PPP.
4.	3.9.14	aggregation network forwards according to MAC Learning table.
5.	3.9.4.4	the capability to drop BPDUs regardless of the BPDU content.
6.	3.10.6.2	OSPF database overflow support.
7.	3.10.6.10	support Hitless OSPF Restart etc.
8.	3.10.6.14	support setting of Administrative costs, virtual links, etc.
9.	3.10.6.18	support OSPF IPv6 (OSPFv3) IPSec ESP
10.	3.10.8.25 (d)	ASN Override
11.	3.10.8.28	support Graceful Restart Mechanism for BGP as per RFC 4724
12.	3.10.9.4	support next hop tracking & Control to enable network administrators
13.	3.10.10.2	Next Generation Multicast VPN features
14.	3.10.11.1	support Load balancing on bearer pin-hole assignment
15.	3.10.12.3	Different RR deployment scenarios in Service Provider networks
16.	3.11.1.5	administratively Scoped IP Multicast
17.	3.11.1.6	statistics on all active groups, sources on a per VLAN or port basis.
18.	3.11.1.7	shall support Multicast VPN based
19.	3.11.2.2	Host Extensions for IP Multicasting as per RFC 1112
20.	3.11.3.1	Anycast Rendezvous Point (RP) Mechanism using Protocol etc.
21.	3.11.3.6	Automatic route processing (AutoRP)
22.	3.11.3.7	Multicast Source Discovery Protocol (MSDP) as per RFC 3618
23.	3.12.3.2	the same VPN and internet Access from the global routing instance
24.	3.13.1.10	deprecation of Type 0 Routing Headers in IPv6 as per RFC 5095
25.	3.13.2.1	support IPv6 Scoped Address Architecture as per RFC 4007
26.	3.13.2.4	The Router shall support SNMP over IPv6
27.	3.13.2.7	support IPv6 over PPP as per RFC 2472
28.	3.13.2.8	IP Forwarding Table MIB as per RFC 4292
29.	3.14.2.2	connection of IPv6 Domains via IPv4 Clouds as per RFC 3056
30.	3.14.2.3	an Anycast Prefix for 6to4 Relay Routers
31.	3.14.2.4	Transition Mechanisms for IPv6 Hosts and Routers as per RFC 4213
32.	3.14.2.5	MPLS/BGP Layer 3 VPN MIB as per RFC 4382
33.	3.14.2.7	connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider
34.	3.15.3.7(d)	MPLS Fast Reroute Extension
35.	3.15.4.8	segmented Pseudowires as per RFC 6073
36.	3.16.1.5	creation of VLAN or Flow with TCP/IP parameters per service for data etc.
37.	3.16.1.6	prediction of performance bounds for each flow
38.	3.16.1.9	bandwidth management reports and statistics
39.	3.16.5(g)	Colour aware srTCM and trTCM based metering
40.	3.16.5(j)	4K ingress policing instances with 10 entries in each
41.	3.16.7.1(e)	Setting the maximum size/depth of all queues.
42.	3.16.7.1(g)	ingress queues are defined on the basis of Maximum burst Size (MBS) etc.
43.	3.16.7.1(h)	egress queues have distinct parameters defining its operations

44.	3.16.7.1(i)	routing traffic necessary to keep from starving other priority queues
45.	3.16.7.1(j)	Service Level Accounting
46.	3.16.7.1(k)	Counters for queues for billing and accounting.
47.	3.16.7.2	each queue with the following counters:
48.	3.16.10.6	weighted random early detection (WRED)- based drop
49.	3.16.10.7	NSF and graceful restart for MP-BGP IPv6 address family.
50.	3.21.7.1	MPLS traceroute, IP-VPN Ping, IP-VPN trace route, LSP Ping etc.
51.	4.3.3	MPLS Interworking
52.	8.1.4.2	to control multicast, broadcast, DLF traffic on per tunnel basis.
53.	8.1.8(a)	Unknown Protocol
54.	8.1.8(b)	UDP Short header/Flood
55.	8.1.8(f)	IP Spoofing
56.	8.1.8(g)	IP Stream Option
57.	8.1.8(h)	IP short header
58.	8.1.8(i)	Internet Control Message Protocol (ICMP) Source quench /Mask request
59.	8.1.8(j)	packet/Info Request and Reply/ Flood
60.	8.1.8(k)	Too many fragments etc.
61.	8.1.8(l)	Call gapping etc.
62.	8.1.12.5	there shall not be any performance degradation.
63.	8.1.12.11	IPv6 ACL extensions for IPSec authentication header etc.
64.	8.1.14.3	logging and forwarding the egress and ingress traffic etc.

10.5 Feature mapping for various Category of Routers

Functional Requirements	**Category of Routers**											
	CE Router			**Aggregation**			**Edge Router**			**Core Router**		
	I	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**	**X**	**XI**	**XII**
General functional Requirements	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Operating System Features:												
Modular operating System	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
NSF and NSR	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
ISSU	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
Layer-2 Switching features:												
General Requirements	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Forwarding Support	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MAC Address Learning / Limiting	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Spanning Tree Protocol	N	N	N	Y	Y	Y	N	N	N	N	N	N
RSTP & MSTP	N	N	N	Y	Y	Y	N	N	N	N	N	N
LLDP	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
LLC	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Flow Control	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Link Aggregation	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
IGMP	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PAT & NAT	Y	Y	Y	N	N	N	N	N	N	N	N	N
VLAN Features	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Routing:												
Static Routing	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RIP	Y	Y	Y	N	N	N	Y	Y	Y	N	N	N
ECMP	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IS-IS	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VRRP	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
OSPF	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
FRR & BFD	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BGP, iBGP, eBGP, MP-BGP, Load balancing	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Route Reflector	N	N	N	N	N	N	O	O	O	N	N	N
Multicast:												
General Multicast Features	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IGMP	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PIM	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Any cast	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Ipv6 Multicast	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS:												
MPLS General Requirements	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
LDP	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS-VPN	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS L2-VPN	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS L3-VPN	N	N	Y	N	O	O	Y	Y	Y	O	O	O
VPLS	N	N	Y	N	O	O	Y	Y	Y	Y	Y	Y
Autonomous System	N	N	Y	N	N	N	Y	Y	Y	Y	Y	Y
MPLS-TP	N	N	N	O	O	O	O	O	O	N	N	N
General Ipv6 Features												
General Support	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Additional Ipv6 support features	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Advanced Ipv6 Features	N	N	N	N	N	N	O	O	O	O	O	O
Traffic Engineering:												
General TE Requirements	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS TE	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RSVP	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Pseudo-wire Emulation	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Multicast TE	N	N	N	O	O	O	Y	Y	Y	Y	Y	Y
DS-TE	N	N	Y	O	O	O	Y	Y	Y	Y	Y	Y
Quality of Service:												
General QoS Requirements	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DiffServ	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Classification/Prioratisation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mapping	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Marking/Policing/Shaping	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

Rate Limiting	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Queueing	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Scheduling	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hierarchical QoS	N	N	N	Y	Y	Y	Y	Y	Y	O	O	O
Ipv6 QoS Features	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Circuit Emulation:	N	N	N	Y	Y	Y	O	O	O	N	N	N
Synchronisation:												
General Requirements	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NTP Support:	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PTP Support:	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N
SyncE Support	N	N	N	O	O	O	O	O	O	O	O	O
Synchronisation Reference	N	N	N	N	N	Y	Y	Y	Y	N	N	N
Timing Output Interface	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N
Protection Switching:	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N
Scalability:												
IEEE 802.1Q	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Q in Q Mode	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
LSP Mode	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
OAM Requirements:												
General	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
OAM Framework	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Configuration	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Performance Management	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Fault Management	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Security	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Non Ethernet OAM Features	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MPLS Non Ethernet OAM	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMP Manageability	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Security:												
DHCP	Y	Y	Y	N	N	N	Y	Y	Y	N	N	N
Broadcast Storm Control	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Proxy ARP	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Spoofing Attacks	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Unicast Reverse Path forwarding	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Restricted forwarding	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
DOS Attacks	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
ICMP Rate Limiting	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Port Binding	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Access Control Lists	Y	Y	Y	N	N	N	O	O	O	N	N	N
IPSec and Encryption	Y	Y	Y	N	N	N	N	N	N	N	N	N
Lawful Interception Requirements	N	N	N	N	N	N	Y	Y	Y	N	N	N
eMS Requirements:												
eMS Architecture	N	N	N	S	S	S	S	S	S	S	S	S
Fault Management	N	N	N	S	S	S	S	S	S	S	S	S
Configuration Management	N	N	N	S	S	S	S	S	S	S	S	S
Administrative												

Management:												
Inventory Management	N	N	N	S	S	S	S	S	S	S	S	S
Software Management	N	N	N	O	O	O	O	O	O	O	O	O
Helpdesk Management	N	N	N	O	O	O	O	O	O	O	O	O
Performance Management	N	N	N	S	S	S	S	S	S	S	S	S
Router Specific eMS Requirements	N	N	N	R	R	R	R	R	R	R	R	R
Security Management:												
General	N	N	N	S	S	S	S	S	S	S	S	S
Log Capturing / Analysis	N	N	N	S	S	S	S	S	S	S	S	S
Alerting & Viewing	N	N	N	S	S	S	S	S	S	S	S	S
Reporting	N	N	N	S	S	S	S	S	S	S	S	S
Security	N	N	N	O	O	O	O	O	O	O	O	O
Correlation	N	N	N	O	O	O	O	O	O	O	O	O
Forensic	N	N	N	O	O	O	O	O	O	O	O	O
External Storage	N	N	N	O	O	O	O	O	O	O	O	O
VPN Management	N	N	N	S	S	S	S	S	S	N	N	N
SLA Management	N	N	N	O	O	O	O	O	O	O	O	O
Provisioning Management	N	N	N	O	O	O	O	O	O	O	O	O
NMS Interface	N	N	N	S	S	S	S	S	S	S	S	S
Local Management Interface	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
eMS Network Requirements	N	N	N	O	O	O	O	O	O	O	O	O

Y – Yes, Required feature

O – Optional requirement, Shall be based on purchasers requirement

R – Requirement of the feature in the eMS shall be based on the availability of the feature on the Router being managed.

N – This feature is not required to be supported in the concerned category of the Router

S – This feature is required to be supported in the eMS in case the eMS is supplied

Functional Requirements	CE Router		Aggregation	Core Router	
	XIII	XIV	XV	XVI	XVII
General functional Requirements					
Operating System Features:					
Modular operating System	N	N	N	N	N
NSF and NSR	N	N	N	N	N
ISSU	N	N	N	N	N
Layer-2 Switching features:					
General Requirements	N	Y	Y	Y	Y
Forwarding Support	Y	Y	Y	Y	Y
MAC Address Learning / Limiting	Y	Y	Y	Y	Y
Spanning Tree Protocol	Y	Y	Y	Y	Y
RSTP & MSTP	Y	Y	Y	Y	Y
LLDP	N	Y	Y	Y	Y
LLC	N	N	N	N	N
Flow Control	N	O	N	Y	Y
Link Aggregation	N	Y	Y	Y	Y
IGMP	N	Y	Y	Y	Y
PAT & NAT	Y	Y	N	N	N
VLAN Features	Y	Y	Y	Y	Y
Routing:					
Static Routing	Y	Y	Y	Y	Y
RIP	N	Y	Y	Y	Y
ECMP	N	Y	Y	Y	Y
IS-IS	N	N	Y	Y	Y
VRRP	N	Y	Y	Y	Y
OSPF	Y	Y	Y	Y	Y
FRR & BFD	N	O	O	O	O
BGP, iBGP, eBGP, MP-BGP, Load balancing	N	Y	Y	Y	Y
Route Reflector	N	Y	Y	Y	Y
Multicast:					
General Multicast Features	N	Y	Y	Y	Y
IGMP	N	Y	Y	Y	Y
PIM	N	Y	Y	Y	Y
Any cast	N	N	N	N	N
Ipv6 Multicast	N	Y	Y	Y	Y
MPLS:					
MPLS General Requirements	N	Y	Y	Y	Y
LDP	N	Y	Y	Y	Y
MPLS-VPN					
MPLS L2-VPN	N	Y	Y	N	N
MPLS L3-VPN	N	Y	Y	Y	Y
VPLS	N	N	N	N	N
Autonomous System	N	O	O	O	O
MPLS-TP	N	N	N	N	N
General Ipv6 Features					
General Support	Y	Y	Y	Y	Y
Additional Ipv6 support features	Y	Y	Y	Y	Y

Advanced Ipv6 Features	**N**	**N**	**N**	**O**	**O**
Traffic Engineering:					
General TE Requirements	N	O	O	O	O
MPLS TE	N	O	O	O	O
RSVP	N	O	O	O	O
Pseudo-wire Emulation	N	N	N	N	N
Multicast TE	N	N	N	N	N
DS-TE	N	O	O	O	O
Quality of Service:					
General QoS Requirements	Y	Y	Y	Y	Y
DiffServ	Y	Y	Y	Y	Y
Classification/Prioratisation	Y	Y	Y	Y	Y
Mapping	N	Y	Y	Y	Y
Marking/Policing/Shaping	N	Y	Y	Y	Y
Rate Limiting	N	Y	Y	Y	Y
Queueing	N	Y	Y	Y	Y
Scheduling	N	Y	Y	Y	Y
Hierarchical QoS	N	N	N	N	N
Ipv6 QoS Features	N	Y	Y	Y	Y
Circuit Emulation:	N	N	N	N	N
Synchronisation:					
General Requirements	N	N	N	N	Y
NTP Support:	Y	Y	Y	Y	Y
PTP Support:	N	N	N	N	Y
SyncE Support	N	N	N	N	Y
Synchronisation Reference	N	N	N	N	N
Timing Output Interface	N	N	N	N	N
Protection Switching:	N	N	N	N	N
Scalability:					
IEEE 802.1Q	Y	Y	Y	Y	Y
Q in Q Mode	N	O	O	O	N
LSP Mode	N	Y	Y	Y	Y
OAM Requirements:					
General	Y	Y	Y	Y	Y
OAM Framework	N	N	N	N	N
Configuration	N	N	N	N	N
Performance Management	N	N	N	N	N
Fault Management	N	N	N	N	N
Security					
Non Ethernet OAM Features	N	Y	Y	Y	Y
MPLS Non Ethernet OAM	N	O	O	O	O
SNMP Manageability	Y	Y	Y	Y	Y
Security:					
DHCP	O	O	O	O	O
Broadcast Storm Control	O	Y	Y	N	N
Proxy ARP	Y	Y	Y	Y	Y
Spoofing Attacks	N	O	N	N	N
Unicast Reverse Path forwarding	N	N	N	N	N

Restricted forwarding					
DOS Attacks	N	Y	Y	Y	Y
ICMP Rate Limiting	O	Y	Y	Y	Y
Port Binding	O	O	O	O	O
Access Control Lists	Y	Y	Y	Y	Y
IPSec and Encryption	Y	Y	N	N	N
Lawful Interception Requirements	N	Y	Y	Y	Y
eMS Requirements:					
eMS Architecture	S	S	S	S	S
Fault Management	***S***	***S***	***S***	***S***	***S***
Configuration Management	***R***	***R***	***R***	***R***	***R***
Administrative Management:					
Inventory Management	Y	Y	Y	Y	Y
Software Management	Y	Y	Y	Y	Y
Helpdesk Management	O	O	O	O	O
Performance Management	***Y***	***Y***	***Y***	***Y***	***Y***
Router Specific eMS Requirements	***R***	***R***	***R***	***R***	***R***
Security Management:					
General	Y	Y	Y	Y	Y
Log Capturing / Analysis	O	O	O	O	O
Alerting & Viewing	O	O	O	O	O
Reporting	Y	Y	Y	Y	Y
Security	R	R	R	R	R
Correlation	R	R	R	R	R
Forensic	O	O	O	O	O
External Storage	O	O	O	O	O
VPN Management	R	R	R	R	R
SLA Management	R	R	R	R	R
Provisioning Management	R	R	R	R	R
NMS Interface	S	S	S	S	S
Local Management Interface	O	Y	Y	Y	Y
eMS Network Requirements	O	O	O	O	O

Abbreviation

ACH TLV	Associated Channel Header Threshold Limit Value
ACL	Access Control List
AIS	All 1's (Ones)
AN	Access Network
AS	Autonomous System
ASN	Access Service Network
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BITS	Building Integrated Timing Source
BNG	Broadband Network Gateway
BPDU	Bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSR	Bootstrap Router
BTS	Base Transceiver Station
B-VID	Backbone V-LAN Identifier
CBS	Committed Burst Size
CDMA	Code Division Multiplex Access
CD-ROM	Compact Disc Read-Only Memory
CE Router	Customer Edge Router
CEP	Circuit Emulation over Packet
CESoPSN	Circuit Emulation Service over Packet Switched Network
CFM	Connectivity Fault Management
CFP	Compact form factor pluggable
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processor Unit
CSPF	Constraint Based Shortest Path First
CSV	Comma Seperated Values
DA	Destination Address
DAS	Direct Attached Storage
DBA	Data Base Administrator
DCN	Data Communication Network
DEI	Drop Eligibility Indicator
DHCP	Dynamic Host Control Protocol
DNI	Directory Number Identification
DNS	Domain Name System
DoS	Denial of Service
DRR	Deficit Round Robin
DSAP	Destination Service Access Point
DSCP	Differential Services Code Point

DSLAM	Digital Subscriber Loop Access Multiplexer
DVD	Digital Video Disk
DVMRP	Distance Vector Multicast Routing Protocol
DWDM	Dense Wavelength Division Multiplexer
DWRR	Deficit Weighted Round Robin
EBS	Excess Burst Size
ECMP	Equicost Multipath Routing
EFP	Ethernet Flow Pouint
EIR	Excess Information Rate
E-LAN	Ethernet LAN
E-LINE	Ethernet Line
E-TREE	Ethernet Tree
EMC	General Electromagnetic Compatibility
e-MS	Element Management System
EoMPLS	Ethernet over MPLS
EPL	Ethernet Private Line
ES	Errored Seconds
EVC	Ethernet Virtual Circuit
EVPL	Ethernet Virtual Private Line
FCAPS	Fault, Configuration, Accounting, Performance and Security
FE	Fast Ethernet
FIB	Forwarding Information Base
FR	Frame Relay
FRE	Fast Reroute Extenssion
FRR	Fast Reroute
FS	Forced Switching
FTP	File Transfer Protocol
FTTH	Fibre to the Home
GAL/G-ACH	Generic Associated Channel
GGSN	Gateway GPRS Support Node
GMPLS	Generalised Multi Protocol Label Switching
GPON	Gigabit Passive Optical Network
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communication
GTSM	Generalized TTL Security Mechanism
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability
HQ	High Queue support interface
HRR	Hierarchical Round Robin
HTTP	Hyper Text Transfer Protocol
H-VPLS	Hierarchical VPLS
I/O	Input / Output
IBGP	Interior BGP
ICMP	Internet Control Message Protocol
IDRP	Inter Domain Routing Protocol
IEEE	Institute of Electrical and Electronic Engineers

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Prevention Service
IPTV	Internet Protocol Television
IPv4	IP version 4
IPv6	IP version 6
IS-IS	Intermediate System to Intermediate System
ISSU	In-Service Software Upgrade
JPEG	Joint Photographic Experts Group
KPI	Key Performance Indicator
KQI	Key Quality Indicator
L2VPN	Layer 2 Virtual Private Network
L3PE	Layer-3 Provider Edge
LAG	Link Aggregation Groups
LAN	Local Area Network
LCD	Liquid Crystel Diode
LCT	Local Craft Terminal
LDAP	Light Weight Directory Access Protocol
LDP	Label Distribution Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LMG	Line Media Gateway
LOF	Loss of Frame
LOS	Loss of Signal
LQ	Low Queue support interface
LSA	Link State Advertisement
LSR	Label Switch Controller software
LSW	LAN Switch
LTE	Long Term Evolution
MAC	Media Access Control
MBS	Maximum burst Size
MDRR	Modified Deficit Round Robin
MED	Multi Exit Discriminator
MEF	Metro Ethernet Forum
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MP BGP	Multi Protocol BGP
MPEG2	Moving Pictuire Expert Group
MPLS	Multi Protocol Label Switching
MRPS	MPLS-TP Ring Protection Switching
MS	Manual Switching
MSDP	Multicast Source Discovery Protocol
MSTP	Multiple Spanning Tree Protocol
MT	Multi Topology
MTBF	Mean Time Between Failure

MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NE	Network Element
NetBIOS	Network Basic Input Output System
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevension System
NML	Network Management Layer
NMS	Network Management System
NNI	Network Node Interfaces
NNTP	Network News Transfer Protocol
NSF	Non-Stop Forwarding
NSR	Non-Stop Routing
NTP	Network Time Protocol
OAM	Operation And Maintenance
ORF	Outbound Route Filters
OS Module	Open Source Module
OSPF	Open Shortest Path First
PAT	Port Address Translation
PC	Personal Computer
PCI	Payment Card Industry
PCP	Priority Code Point
PDF	Portable Document Format
PDH	Plesiochronous Digital Hierarchy
PDSN	Public Swithed Data Network
PE	Provider Edge
PHB	Per Hop Behaviour
PIB	Peak Information Base
PIM	Protocol Independent Multicast
PIR	Peak Information Rate
PPP	Point to Point Protocol
PPVPN	Provider Provisioned Virtual Private Network
PSTN	Public Switched Telephone Network
PTP	Precision Time Protocol
PVC	Private Virtual Circuit
PW	Pseudo-wires
PWE	Pseudo wire Emulation Edge-To-Edge
QFP	Quad Flat Pack
QoS	Quality of Service
QoSPS	QoS Provisioning Server
RDBMS	Relational Database Management System
RDI	Remote Defect Indication
RFC	Request for Comments
RIP	Routing Information Protocol
RMON	Remote Monitoring
RNC	Radio Network Controller
RP	Rendezvous Point

RR	Route Reflector
RSTP	Rapid Spanning Tree Protocol
RSVP LSP	Resource Reservation Protocol
RSVP-TE	Reservation Protocol Traffic Switching Engineering
RTM	Route Table Manager
RTP	Real Time Protocol
SAN	Storage Area Network
SAToP	Structure Agnostic TDM over Packet
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SDH	Synchronous Digital Hierarchy
SES	Severely Errored Seconds
SIP	Session Initiation Protocol
SM	Sparse Mode
SML	Service Management Layer
SMTP	Simple Mail Transfer Protocol
SNC	Sub Network Connection
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SOX	Sarbanes-Oxley
SP	Strict Priority
SPQ	Strict Priority Queuing
SQL	Structured Query Language
srTCM	Single rate three colour marking
SSAP	Source Service Access Point
SSM	Source Specific Multicast
STM	Synchronous Transfer Mode
S-VID	Service V-LAN Identifier
SVLAN	Service Provider Network VLAN
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TEC	Telecommunications Engineering Centre
TFTP	Trivial File Transfer Protocol
TLC	Transport Layer Security
TLV	Type Length Value
ToS	Type of Service
TOS-IPP	Type of Service IP Presidence
TTL	Time To Live
UAS	Unavailable Seconds
UDP	User Datagram Protocol
UNI	User Network Interface
UNIX	Uniplexed Information and Computer Systems
URPF	Unicast Reverse Path forwarding
VCID	Virtual Circuit Identifier
VID	V-LAN Identifier

VLAN	Virtual LAN
VoD	Video On Demand
VoIP	Voice Over Internet Protocol
VPE	Virtual PE
VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VPNMT	VPN Management Tool
VPWS	Virtual Private Wire Services
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted fair Queuing
Wi-Fi	Wireless Fidelity
Wi-MAX	Worldwide Interoperability for Microwave Access
WORM	Write Once Read Many
WRED	Weighted Randon Early Detection
WRR	Weighted Round Robin
WTD	Weighted Tail Drop

========= End Of Document =========