Comments on Revision of Test Guide for “Router for MPLS based Transport Network”

(Draft Test Guide No. TEC 48051:2026)

Name of Manufacturer/Stakeholder:

Organization:

Contact Details:

Clause No.	Clause	Comments	Justification

Note: The comments on the revision of Test Guide for “Router for MPLS based Transport Network” may be provided in the above format vide Email to adic1.tec@gov.in , adit2.tec-dot@gov.in , diri.tec@nic.in

सत्यमेव जयते

अनंतिम टेस्ट गाइड

टीईसी ४८०५१: २०२६

(सं२०२ :४८०५१ :४ को अधिक्रधित करता ह)

PROVISIONAL TEST GUIDE

TEC 48051:2026

(Supersedes No. : 48051:2024)

for

एम पी एल एस आधारित ट्रांसपोर्ट नेटवर्क के लिए राऊटर

Router for MPLS based Transport Network

(जीआर सं: टीईसी ४८०५०: २०२५)

(Standard No.: TEC 48050:2025)

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: January, 2026

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 Test Guide pertains to detailed test schedule and procedure as required for evaluating conformance / functionality / requirements / performance of Router for MPLS based Transport Network as per Standard for GR 48050:2025.

CONTENTS

A. HISTORY SHEET

Sl.No.	Standard / document No.	Title	Remarks
1.	TEC/TG/IT/TCP-004/01 Feb-14	TSTP for Router for MPLS based Transport Network	
2.	TEC 48051:2022	Test Guide for Router for MPLS based Transport Network	1. Revision of Standard for GR for Router for MPLS based Transport Network 2. Conversion of TSTP to Test Guide
3.	TEC 48051:2024	Test Guide for Router for MPLS based Transport Network	Incorporating the latest updations in TEC GR 48050:2024 and Compendium document is appended as Annexure-I.
4.	TEC 48051:2026	Test Guide for Router for MPLS based Transport Network	

B. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Router for MPLS based Transport Network as per TEC Standard. No TEC 48050:2025.

It is to be noted that tests would be applicable for a router under test as per Table "Feature mapping for various Category of Routers" of Clause 10.5 of TEC 48050:2025.

C. General Information:

Sn.	General Information	Details (to be filled by testing team)	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of TEC Standard /Applicant’s Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information:-		

D. Testing team: (to be filled by testing team)

S. no.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

S.no.	Name of the test instrument	Make /Model (to be filled by testing team)	Validity of calibration (to be filled by testing team)
1			dd/mm/yyy
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: (to be filled by testing team)

(a) <Equipment/product name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

(b) <Other equipment name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals: (to be filled by testing team)

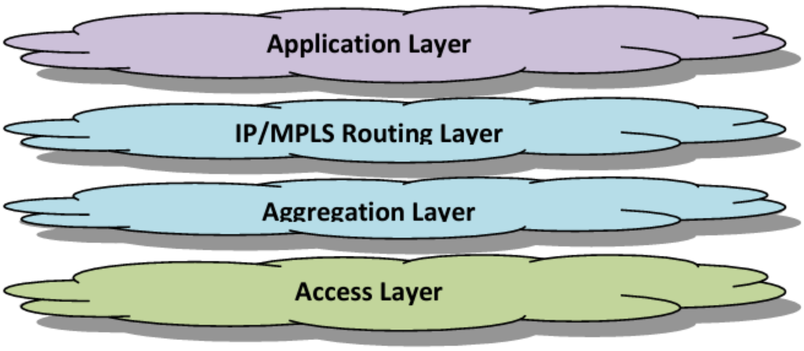
Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. (Y/N)

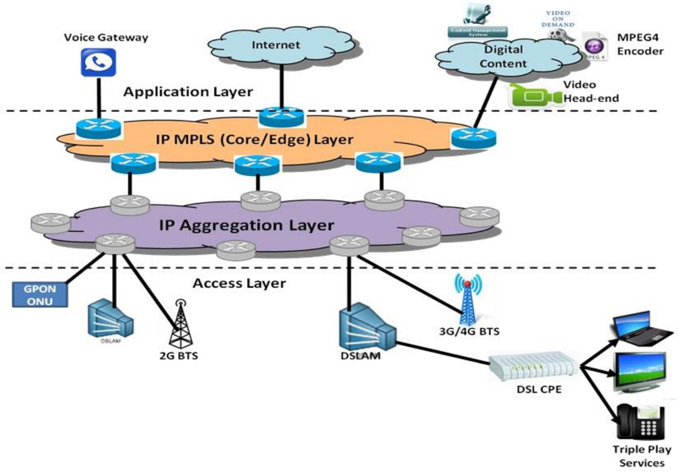
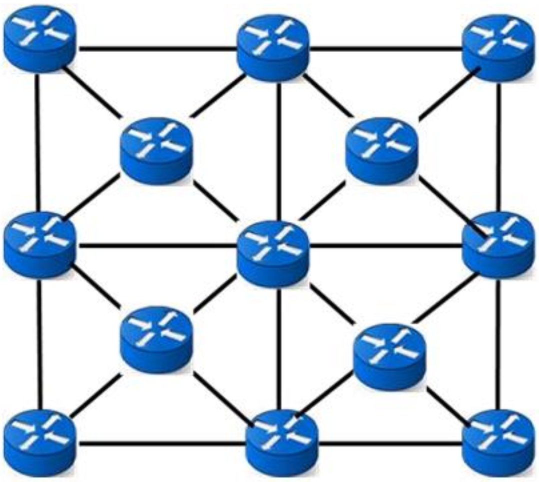
H. Clause-wise Test Type and Test No.:

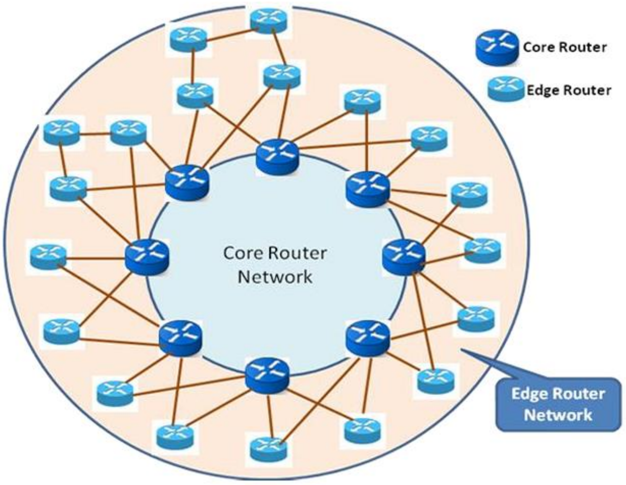
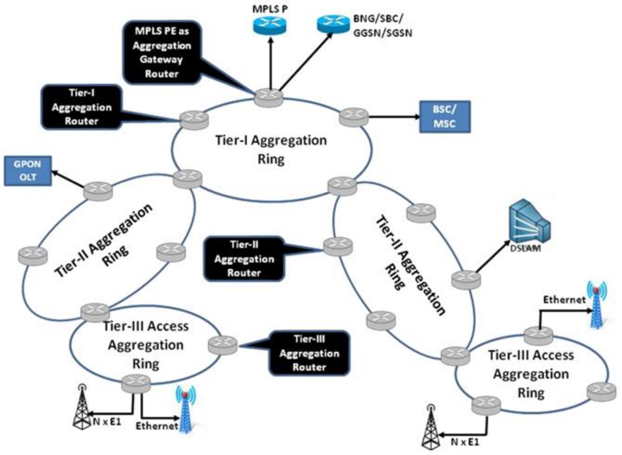
*: Please note that Compendium document is appended as Annexure-I at the end of this Test-Guide

Clause No.		Clause	*Physical Check / Declaration / Documentation / Report from Accredited Test Lab / Functional verification / Information / Lab Test (Test Reference)*
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.	Information
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.	Information
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 chapter 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 chapter-8. The guidelines for the tendering authority as well as recommended feature mapping for various categories of routers is given in section-10	Information
1.3		This document covers the technical requirements for the following category of Routers	Information
	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.	Information

	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.	Information
	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.	Information
	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.	Information
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.	Information
1.5		The interpretation of the clauses of the RFC's shall be as per RFC 2119.	Information
2.0		**DESCRIPTION**	
		This chapter describes a typical Network Architecture, Applications / Services supported, different category of routers referred in this GR and its element management system.	Information
		Part I – Network Architecture	Information
2.1		**Four Layer Hierarchical Architecture**	Information
		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.	

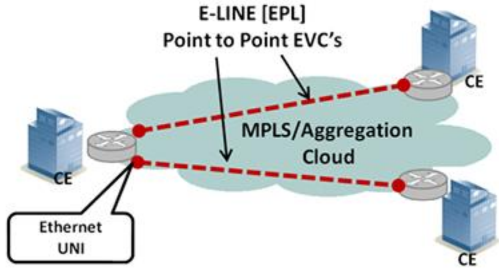
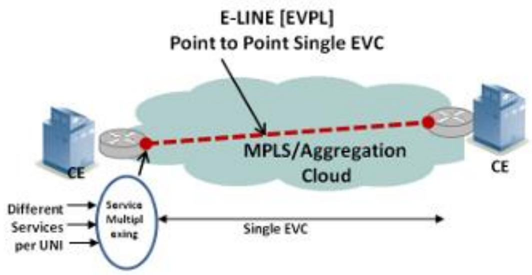
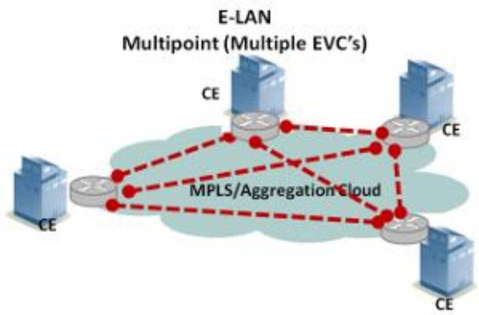
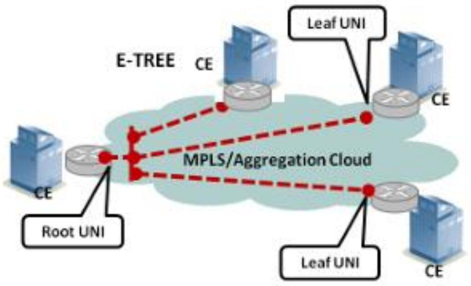
		 Application Layer IP/MPLS Routing Layer Aggregation Layer Access Layer Figure 1: Network with four level of hierarchical architecture	Information
2.2		**Application Layer:** The application layer contains application servers which provide service logic for delivery of various services such as data, video, 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.	Information
2.3		**IP/MPLS Routing Layer:** This layer consists 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.	Information
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.	Information
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.	Information

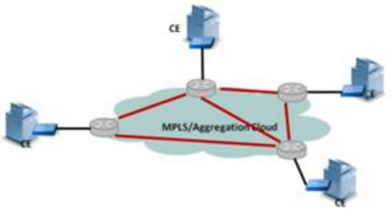
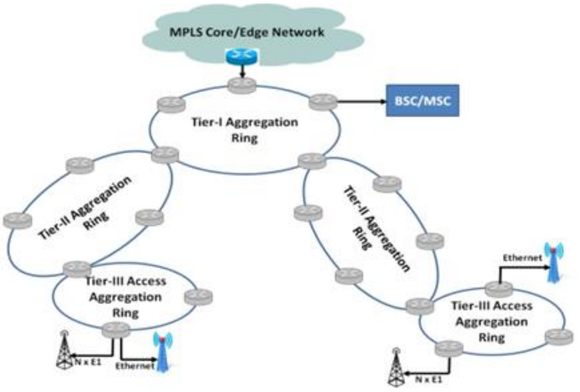
		 Voice Gateway Internet Content Management System VIDEO ON DEMAND Digital Content MPEG4 Encoder MPEG 4 Application Layer Video Head-end IP MPLS (Core/Edge) Layer IP Aggregation Layer Access Layer GPON ONU DSLAM 2G BTS DSLAM 3G/4G BTS DSL CPE Triple Play Services **Figure 2:** Overall Network View	
2.6		**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. 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.	Information
		 Figure 3: A Typical Core Router Architecture	Information

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:	Information
		 Core Router Edge Router Core Router Network Edge Router Network Figure 4: A Typical Edge Router Architecture with dual homing & Cascading	Information
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.	Information
		 MPLS P BNG/SBC/ GGSN/SGSN MPLS PE as Aggregation Gateway Router Tier-I Aggregation Router BSC/ MSC Tier-I Aggregation Ring GPON OLT Tier-II Aggregation Ring Tier-II Aggregation Router Tier-II Aggregation Ring DSLAM Ethernet Tier-III Access Aggregation Ring Tier-III Aggregation Router Tier-III Access Aggregation Ring N x E1 Ethernet N x E1 Figure 5: 3-Tier Aggregation Layer Architecture	Information

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.	Information
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.	Information
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.	Information
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.	Information
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.	Information
2.14		.**Nodes per Ring:** The Architecture shall supports upto 8 Nodes per Ring	Information
2.15		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 **Basic Internet Access Service:** The Router Transport Network shall facilitate basic internet access over dial-up / Broadband or leased line Access.	Declaration
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.	Declaration
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.	Declaration
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.	Declaration
2.19		**Bandwidth on Demand Service:** The Router Transport Network shall provide User configurable and Service configurable bandwidth on demand.	Declaration

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.	Declaration
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.	Declaration
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.	Declaration
2.23		**Interactive Gaming Service:** The Router Transport Network shall support both single user and multi user Interactive gaming	Declaration
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.	Declaration
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.	Declaration
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).	Declaration

		 E-LINE [EPL] Point to Point EVC's CE MPLS/Aggregation Cloud CE Ethernet UNI CE Figure 6: E-LINE Point to Point EVC's  E-LINE [EVPL] Point to Point Single EVC CE MPLS/Aggregation Cloud CE Different Services per UNI Service Multipl exing Single EVC Figure 7: E-LINE EVPL Point to Point EVC  E-LAN Multipoint (Multiple EVC's) CE CE MPLS/Aggregation Cloud CE CE Figure 8: E-LAN Multi-Point Model  Leaf UNI E-TREE CE CE MPLS/Aggregation Cloud CE Root UNI Leaf UNI CE Figure 9: E-TREE Root and Leaf Model	Information
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 also 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.	Declaration

<table>
<tr><td>2.28</td><td></td><td><b>Layer-3 VPN Service</b>: 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.</td><td>Declaration</td></tr>
<tr><td></td><td></td><td>
Figure 10: Layer-3 VPN from customer sites</td><td>Information</td></tr>
<tr><td>2.29</td><td></td><td><b>E1/SDH/Ethernet Backhaul Services:</b> The Router Transport Network backhaul 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 backhaul 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.</td><td>Declaration</td></tr>
<tr><td></td><td></td><td>

MPLS Core/Edge Network
BSC/MSC
Tier-I Aggregation Ring
Tier-II Aggregation Ring
Tier-II Aggregation Ring
Tier-III Access Aggregation Ring
Tier-III Access Aggregation Ring
Ethernet
N x E1
Ethernet
N x E1

Figure 11: Mobile Backhauling Service

PART III – CATEGORY OF ROUTERS</td><td>Information</td></tr>
<tr><td>2.30</td><td></td><td><b>Category of Routers:</b> 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.
<table>
<tr><th>Router Type</th><th>Router Category</th><th>Application</th></tr>
<tr><td rowspan="3">CE Router</td><td>I</td><td>Enterprise Customer Edge Router – Low Capacity</td></tr>
<tr><td>II</td><td>Enterprise Customer Edge Router – Medium Capacity</td></tr>
<tr><td>III</td><td>Enterprise Customer Edge Router – High Capacity</td></tr>
<tr><td></td><td>IV</td><td>Service Provider Access Traffic Aggregation Router – Low Capacity</td></tr>
</table></td><td>Information</td></tr>
</table>

<table>
<tr><td></td><td></td><td>Aggregation Router</td><td>V</td><td>Service Provider Access Traffic Aggregation Router – Medium Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>VI</td><td>Service Provider Access Traffic Aggregation Router – High Capacity</td><td></td></tr>
<tr><td></td><td></td><td>Edge Router</td><td>VII</td><td>Service Provider Edge Router – Low Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>VIII</td><td>Service Provider Edge Router – Medium Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>IX</td><td>Service Provider Edge Router – High Capacity</td><td></td></tr>
<tr><td></td><td></td><td>Core Router</td><td>X</td><td>Service Provider Core Router – Low Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>XI</td><td>Service Provider Core Router – Medium Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>XII</td><td>Service Provider Core Router – High Capacity</td><td></td></tr>
<tr><td></td><td></td><td colspan="3">Non-Chassis based Router (Fixed Form Factor)</td><td>Information</td></tr>
<tr><td></td><td></td><td>Router Type</td><td>Router Category</td><td>Application</td><td></td></tr>
<tr><td></td><td></td><td>CE Router</td><td>XIII</td><td>Enterprise Branch Router</td><td></td></tr>
<tr><td></td><td></td><td></td><td>XIV</td><td>Enterprise Customer Edge Router – High Capacity</td><td></td></tr>
<tr><td></td><td></td><td>Aggregation Router</td><td>XV</td><td>Service Provider Access Traffic Aggregation Router</td><td></td></tr>
<tr><td></td><td></td><td>Core Router</td><td>XVI</td><td>Service Provider Core Router – Medium Capacity</td><td></td></tr>
<tr><td></td><td></td><td></td><td>XVII</td><td>Service Provider Core Router –High Capacity</td><td></td></tr>
<tr><td></td><td></td><td colspan="3"><b>PART IV – ELEMENT MANAGEMENT SYSTEM</b></td><td>Information</td></tr>
<tr><td><b>2.31</b></td><td></td><td colspan="3"><b>Architecture of eMS equipments:</b> 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:</td><td>Information</td></tr>
<tr><td>2.31.1</td><td></td><td colspan="3"><b>Service Delivery:</b></td><td></td></tr>
<tr><td>2.31.1.1</td><td></td><td colspan="3"><b>Inventory Management Support:</b> 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.</td><td>Declaration</td></tr>
<tr><td>2.31.1.2</td><td></td><td colspan="3"><b>Configuration Management Support:</b> 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.</td><td>Declaration</td></tr>
<tr><td>2.31.1.3</td><td></td><td colspan="3"><b>Provisioning Support:</b> 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.</td><td>Declaration</td></tr>
<tr><td>2.31.1.4</td><td></td><td colspan="3"><b>Service Usage Support:</b> It involves the measurement of the usage of the sub network resources by the various subscribers; this is the basis for billing.</td><td>Declaration</td></tr>
<tr><td>2.31.2</td><td></td><td colspan="3"><b>Service Assurance:</b></td><td></td></tr>
</table>

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.	Declaration
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.	Declaration
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.	Declaration
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.	Declaration
2.31.2 .5		The eMS provides the North bound interface to integrate NMS.	Declaration
2.31.2 .6		The System allows to assign following categories of users	
	a.	Helpdesk User	Declaration
	b.	Operation and Maintenance User	Declaration
	c.	System Administrator	Declaration
2.31.2 .7		The application provides the control of access right of users in respect of function menu and geographical area of interest.	Declaration
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.	Information

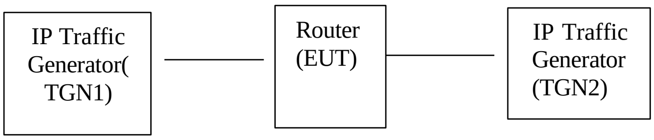
	Router Category	Minimum Slot Capacity (Full Duplex)	Minimum Chassis Capacity(*) [Full duplex]
CE Router	I		1 Gbps
	II		4 Gbps
	III		10 Gbps
	IV		10 Gbps

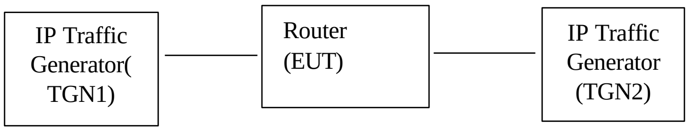
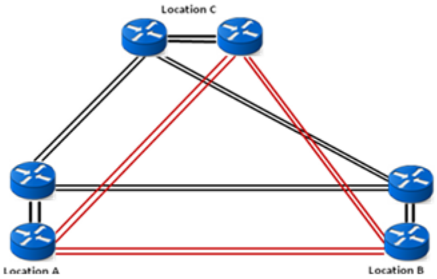
		on Router	V	8 Gbps	40 Gbps	
			VI	20 Gbps	200 Gbps	
		Edge Router	VII	40 Gbps	240 Gbps	
			VIII	100 Gbps	800 Gbps	
			IX	200 Gbps	1.6 Tbps	
		Core Router	X	200 Gbps	1.6 Tbps	
			XI	400 Gbps	4 Tbps	
			XII	400 Gbps	6Tbps [Multi-Chassis optional in case not supported in Single chassis]	
		* Except for Category XII Router where 6Tbps can be through Multi-chassis as well.				
		The CE Router throughput is for the large packet				
		Non-Chassis based Router (Fixed Form Factor)				Information
		Router Type	Router Category	Minimum Chassis 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				Declaration
3.3		**Packet Processing Capacity**				Declaration
		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)							Declaration
		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.							Declaration
		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)							Declaration
		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**							
		Ethernet Scalability figures							
3.5.1	a.	The Router shall support 4095 VLAN ID’s per port							Declaration
	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)							Declaration
		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	5K	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)			Declaration
		Router Category	QoS Traffic Policers	ACL Entries	
		XIII	100	1K	
		XIV	100	4K	
		XV	1K	1K	
		XVI	1K	4K	
		XVII	1K	4K	
3.6		**Redundancy Requirements:** The routers shall support four levels of redundancy architecture.			Information
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.			Functional Verification
		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 Router			
		Router Category			Functional Verification
		XIII	No	No	
		XIV	No	No	
		XV	No	No	
		XVI	No	No	
		XVII	No	No	

<table>
<tr>
<td>3.6.1.1</td>
<td></td>
<td>
Router shall support hot-swappable/pluggable redundant (1+1 or N+1) hot standby power supplies.
<table>
<tr><td><b>Test Details</b></td><td>Test for Hot-swappable/pluggable redundant (1+1 or N+1) hot standby Power supplies</td></tr>
<tr><td><b>Test Instruments Required</b></td><td>1. Router
2. IP Traffic generator
3. Fiber cable</td></tr>
<tr><td><b>Test Setup</b></td><td>
</td></tr>
<tr><td><b>Test Limits</b></td><td>NA</td></tr>
<tr><td><b>Test Procedure</b></td><td>1. Router should have redundant power supply
2. Power up the Router and Traffic Generators
3. Create a topology using physical links as shown above, and run bidirectional IP traffic between TGN1 and TGN2. No packet drop should be observed
4. Remove power supply module1 from Router. No Packet loss should be observed at TGN1 or TGN2
5. Insert the power supply module1 in Router. No Packet loss should be observed at TGN1 or TGN2
6. Repeat steps 4 and 5 for all the power supply modules in the system, one by one.</td></tr>
<tr><td><b>Expected Results</b></td><td>Power module redundancy should pass without any packet loss.
Enclose the Test Results</td></tr>
</table>
</td>
<td>Functional Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>
All categories of Router shall support hot-swappable/pluggable redundant (1+1 or N+1) hot standby fans/fan units.
<table>
<tr><td><b>Test Details</b></td><td>Test for Hot-swappable/pluggable redundant (1+1 or N+1) hot standby Fans/Fan-units</td></tr>
<tr><td><b>Test Instruments Required</b></td><td>1. Router
2. IP Traffic generator
3. Fiber cable</td></tr>
<tr><td><b>Test Setup</b></td><td></td></tr>
</table>
</td>
<td></td>
</tr>
</table>

3.6.1.2		 IP Traffic Generator(TGN1) Router (EUT) IP Traffic Generator (TGN2) **Test Limits** NA **Test Procedure** 1. Router should have redundant Fans/Fan units 2. Power up the Router and Traffic Generators 3. Create a topology using physical links as shown above, and run bidirectional IP traffic between TGN1 and TGN2. No packet drop should be observed 4. Remove Fan1/Fan unit1 from Router. No Packet loss should be observed at TGN1 or TGN2 5. Insert the Fan1/Fan unit1 in Router. No Packet loss should be observed at TGN1 or TGN2 6. Repeat steps 4 and 5 for all the Fans/Fan units in the system, one by one. **Expected Results** Fans/Fan units redundancy should pass without any packet loss. Enclose the Test Results	Functional Verification
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	Declaration
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.	Declaration
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	Declaration
		 Figure 12: Layered Network Redundancy Architecture	Information
		PART-II FUNCTIONAL SPECIFICATIONS	
3.7		**General Functional Requirements**	

3.7.1		It shall be possible to use any of the optical Ethernet interfaces as Client or Aggregate interfaces.	Declaration
3.7.2		The Router shall support dynamic online configuration.	Functional Verification
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)	Functional Verification
3.7.4		The Router shall support MDI-X based auto-uplink feature.	Declaration
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.	Declaration
3.7.6		The Router shall support Fast convergence on the backbone links and uplinks.	Declaration
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.	Declaration
3.7.8		The Router shall support both Ipv4 and Ipv6 functionalities	Declaration
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.	Functional Verification & Declaration
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.	Functional Verification
3.8.1.2		The Router shall have decoupled Forwarding and Management Planes.	Declaration
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.	Functional Verification
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.	Declaration
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.	Declaration
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.	Declaration
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.	Declaration
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.	Declaration
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.	Declaration
3.8.1.10		The Router shall support forwarding and control plane separation.	Declaration
3.8.2		**Non-Stop Forwarding (NSF) & Non-Stop Routing (NSR)**	Information

		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:	Information
	i.	BGP	Declaration
	ii.	Graceful restart for OSPF as per RFC 3623 and RFC 5187	Declaration
	iii.	ISIS	Declaration
	iv.	Graceful Restart Mechanism for Label Distribution Protocol as per RFC 3478	Declaration
	v.	BGP/MPLS	Declaration
	vi.	RSVP LSP	Declaration
	vii.	Graceful PIM restart	Declaration
	viii.	Graceful Restart Mechanism for BGP as per RFC 4724	Declaration
	ix.	Graceful Restart Mechanism for BGP with MPLS	Declaration
3.8.3		**ISSU**	Information
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.	Functional Verification
3.8.3.2		The Router shall support Non Service Affecting Upgrades	Declaration
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.	Declaration
3.8.3.4		The Router shall have protection of memory address space for all running processes	Declaration
3.8.3.5		The Router shall support Dynamic Bandwidth upgrade for LSP and Circuits without restart	Functional Verification
3.8.3.6		The Router shall support LSP shared implicit/explicit mode for make before break operations	Declaration
3.9		**Layer-2 Switching Features**	Information
3.9.1		**General:**	
3.9.1.1		The Router shall support ingress and egress bandwidth profile per User to Network Interface (UNI).	Declaration
3.9.1.2		Service multiplexing: A single Router port shall support multiple Ethernet Services	Functional Verification
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.	Declaration
3.9.1.4		Router shall support Layer 2 protocol transport for Ethernet and PPP.	Functional Verification
3.9.2		**Forwarding Support**	
3.9.2.1		The Router shall support hardware assisted Layer 2 forwarding.	Declaration
3.9.2.2		The Router shall have hard-coded and unique MAC address.	Declaration
3.9.2.3		The Router shall support to override Router port MAC address.	Functional Verification
3.9.2.		The Router shall support to set per port static MAC configuration.	Declaration
4			
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.	Functional Verification
3.9.3.2		The Router shall support to set per port dynamic MAC learning limit.	Declaration

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.	Declaration
3.9.3.4		The Router shall support dropping of Frames with new source MAC-addresses exceeding the configured value.	Declaration
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.	Declaration
3.9.3.6		The Router shall support MAC limiting per Ethernet flow point (EFP) or bridge domain	Functional Verification
3.9.3.7		The Router shall support MAC address limitation and aging	Declaration
3.9.3.8		All static entries shall NOT be aged.	Declaration
3.9.3.9		The Router shall support Hardware based aging of MAC Address Table entries.	Declaration
3.9.3.10		The Router shall support to enable L2 Aging on every port.	Declaration
3.9.3.11		The Router shall support MAC address learning disabling	Functional Verification
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)	Declaration
3.9.3.13		The Router shall support list of allowable MAC destination address	Declaration
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.	Declaration
3.9.3.15		The Router shall support unique MAC address per device to prevent spoofing and provide traceability.	Declaration
3.9.4		**Spanning Tree Protocol**	
3.9.4.1		The Router shall support Spanning Tree Protocol as per IEEE 802.1d	Lab Test-Refer Test No. 16 of Compendium
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).	Declaration
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.	Declaration
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.	Declaration
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	Functional Verification
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	Functional Verification
3.9.6.2		The Router shall support minimum two instances of MST.	Declaration
3.9.7		**Link-layer discovery protocol**	

3.9.7.1		The Router shall support Link Layer Discovery Protocol as per IEEE 802.1ab	Lab Test-Refer Test No. 16 of Compendium
3.9.8		**Logical Link Control**	
3.9.8.1		The Router shall support Logical Link control as per IEEE 802.2	Functional Verification
3.9.9		**Flow Control**	
3.9.9.1		The Router shall support Flow control as per IEEE802.3x	Functional Verification
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.	Functional Verification
3.9.10.2		The Router shall support load balancing over Aggregated Links.	Functional Verification
3.9.10.3		The Router shall allow configurations of static/LACP LAG on client ports.	Declaration
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	Lab Test-Refer Test No. 16 of Compendium
3.9.11.2		The Router shall support IGMP v3 as per RFC 3376	Lab Test-Refer Test No. 16 of Compendium
3.9.11.3		The Router shall support Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping as per RFC 4541	Declaration
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.	Declaration
3.9.12.2		Router shall support VLAN bridging (for outer tag only) as per IEEE 802.1ad	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.9.12.3		Router shall support user isolation per outer VLAN tag. This behavior shall be configurable on a per port basis.	Declaration
3.9.12.4		Router shall support VLAN ingress filtering to prevent VLAN leakage.	Declaration
3.9.12.5		Router shall support VLAN tag overlapping allowing some ports to be member of more than one VLAN.	Declaration
3.9.12.6		The Router shall support IEEE 802.1Q Tagging in the following manner:	Lab Test-Refer Test No. 16 of Compendium
	a.	Tagged only, which is an IEEE 802.1Q trunk.	Lab Test-Refer Test No. 16 of Compendium
	b.	Untagged.	Lab Test-Refer Test No. 16 of Compendium
	c.	Hybrid, tagged and untagged frames.	Lab Test-Refer Test No. 16 of Compendium
3.9.12.7		The Type IV, V and VI Routers shall support the following additional IEEE 802.1Q features	Information
	a.	Tag insertion, removal and swapping.	Declaration
	b.	Capability of insertion and removal of second tag.	Declaration

	c.	Encapsulation translation and rewrites Push, Pop and translate for IEEE 802.1Q or QinQ/IEEE 802.1ad tags.	Declaration
	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.	Declaration
3.10		**Routing Protocols**	Information
3.10.1		**Static Routing**	Information
3.10.1 .1		The Router shall support requirements for IP Version 4 Routing as per RFC 1812	Declaration
3.10.1 .2		The Router shall support policy based routing based on source and destination IPv4 address and TCP/UDP Port.	Declaration
3.10.1 .3		The Router shall support IPv6 static Routing	Functional Verification
3.10.2		**RIP**	
3.10.2 .1		The Router shall support RIP v2 as per RFC 2453	Lab Test-Refer Test No. 16 of Compendium
3.10.2 .2		The Router shall support RIPng for IPv6 as per RFC 2080	Lab Test-Refer Test No. 16 of Compendium
3.10.2 .3		The Router shall support IPv6 policy-based routing	Declaration
3.10.2 .4		The Router shall support IPv6 route redistribution	Declaration
3.10.2 .5		Router shall support RIPv2 authentication as per RFC 4822	Declaration
3.10.3		**ECMP**	
3.10.3 .1		The Router shall support Equal Cost Multi Path (ECMP) routing for load-balancing	Declaration
3.10.4		**IS-IS routing protocol**	
3.10.4 .1		The Router shall support OSI ISIS Intra-domain Routing Protocol	Declaration
3.10.4 .2		The Router shall support use of OSI ISIS for Routing in TCP/IP and Dual Environments as per RFC 1195	Lab Test-Refer Test No. 16 of Compendium
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	Declaration
3.10.4 .4		The Router shall support Dynamic Hostname Exchange Mechanism for IS-IS as per RFC 5301	Declaration
3.10.4 .5		The Router shall support ISIS routes	Functional Verification
3.10.4 .6		The Router shall support IS-IS Extensions for Traffic Engineering as per RFC 5305	Declaration
3.10.4 .7		The Router shall support Restart Signaling for IS-IS as per RFC 5306	Declaration
3.10.4 .8		The Router shall support two levels of hierarchy.	Declaration
3.10.4 .9		The Router shall support IS-IS Mesh Groups (Default metric, LSA updates, graceful restart, TE extensions, mesh groups.)	Declaration
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	Declaration
3.10.4 .11		The Router shall support Routing Ipv6 with ISIS as per RFC 5308	Lab Test-Refer Test No. 16 of Compendium
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	Functional Verification
3.10.5 .2		The Router shall support Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 as per RFC 5798	Declaration
3.10.6		**OSPF V2/V3**	
3.10.6 .1		The Router shall support OSPF Version 2 as per RFC 1583 & RFC 2328	Check functionality as per RFC 2328 (lab test No. 16 of Compendium) and Declaration for 2178
3.10.6 .2		The Router shall support OSPF database overflow support	Declaration
3.10.6 .3		The Router shall support OSPF Version 2 Management Information Base as per RFC 4750	Declaration
3.10.6 .4		The Router shall support Applicability Statement for OSPF as per RFC 1370	Declaration
3.10.6 .5		The Router shall support BGP-OSPF interaction	Declaration
3.10.6 .6		The Router shall support OSPF Not So Stubby Area (NSSA) as per RFC 3101	Check functionality as per Lab Test-Refer Test No.16 of Compendium
3.10.6 .7		The Router shall support OSPF Opaque LSA option as per RFC 5250	Declaration
3.10.6 .8		The Router shall support OSPF for IPv6 as per RFC5340	Declaration
3.10.6 .9		The Router shall support OSPF Stub Area	Declaration
3.10.6 .10		The Router shall support Hitless OSPF Restart (link state redundancy) Or OSPF graceful restart as per RFC 3623	Declaration
3.10.6 .11		The Router shall support Traffic Engineering (TE) extensions to OSPF v2 (OSPF-TE) as per RFC 3630	Declaration
3.10.6 .12		The Router shall support OSPF Sham Links	Declaration
3.10.6 .13		The Router shall support Variable length sub-netting	Declaration
3.10.6 .14		The Router shall support setting of Administrative costs, virtual links, area route aggregation, inter area route aggregation, route leaking	Declaration
3.10.6 .15		The Router shall support Route filtering based on administrative costs.	Declaration
3.10.6 .16		The Router shall support OSPFv3 RFC 2740 (OSPF for IPv6)	Lab Test-Refer Test No. 16 of Compendium
3.10.6 .17		The Router shall support Authentication/Confidentiality for OSPFv3 as per RFC 4552	Declaration
3.10.6 .18		The Router shall support OSPF IPv6 (OSPFv3) IPSec ESP Encryption and Authentication (applicable for type III to XII Routers)	Declaration
3.10.6 .19		The Router shall support OSPFv3 dynamic interface cost support (applicable for type III to XII Routers)	Declaration
3.10.6 .20		The Router shall support OSPFv3 Fast Convergence - LSA and SPF throttling	Declaration

3.10.6 .21		The Router shall support OSPFv3 graceful restart	Declaration
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.	Functional Verification
3.10.7 .2		The Router shall support 1:N Protection, Upto 1K simultaneous LSP's	Declaration
3.10.7 .3		The Router shall support Bidirectional Forwarding Detection (BFD) as per RFC 5880, 5881	Declaration
3.10.7 .4		The Router shall support Bidirectional Forwarding Detection (BFD) for Multihop Paths as per RFC 5883	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.10.7 .5		The Router shall support OSPFv3 for BFD	Declaration
3.10.7 .6		The Router shall support Static Route support for BFD over IPv6	Declaration
3.10.8		**BGP (v4 / v6)**	
3.10.8 .1		The Router shall support BGPv4 as per RFC 4271, RFC 2283	Check functionality as per RFC 4271, Declaration as per 2858
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	Declaration
3.10.8 .3		The Router shall support matching and assignments of communities and extended communities.	Declaration
3.10.8 .4		The Router shall support BGP Communities Attribute as per RFC1997	Declaration
3.10.8 .5		The Router shall support BGP Extended Communities Attribute as per RFC4360	check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.10.8 .6		The Router shall support Using a Dedicated AS for Sites Homed to a Single Provider as per RFC 2270	Declaration
3.10.8 .7		The Router shall support BGP Route Flap Damping as per RFC 2439	Declaration
3.10.8 .8		Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing shall be as per RFC 2545	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.10.8 .9		The Router shall support Route Refresh Capability for BGP-4 as per RFC 2918	Check functionality as per Lab Test-
			Refer Test No. 16 of Compendium
3.10.8 .10		The Router shall support Carrying Label Information in BGP-4 as per RFC 3107	Declaration
3.10.8 .11		The Router shall support Autonomous System Confederations for BGP shall be as per RFC 5492	Declaration
3.10.8 .12		The Router shall support Capabilities Advertisement with BGP-4 as per RFC 5492	Declaration

3.10.8.13		The Router shall support TCP Authentication Option as per RFC 5925	Declaration
3.10.8.14		The Router shall support Address-Prefix-Based Outbound Route Filter for BGP-4 as per RFC 5292	Declaration
3.10.8.15		The Router shall support transparent LAN using BGP	Declaration
3.10.8.16		Shall support encryption of BGP peering session.	Declaration
3.10.8.17		The Router shall support default route to individual BGP peers.	Declaration
3.10.8.18		The Router shall support Soft Reset of BGP session on any or all peers.	Declaration
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.	Declaration
3.10.8.20		The Router shall support Multiple BGP sessions.	Declaration
3.10.8.21		The Router shall support ingress and egress route filtering which includes filtering on prefix, AS path and route maps.	Declaration
3.10.8.22		The Router shall support Weight metric, Local Pref metric and Multi Exit Discriminator (MED) metric	Declaration
3.10.8.23		The Router shall support Matching and assignments of MED values.	Declaration
3.10.8.24		The Router shall support comparison of MED values between different sources.	Declaration
3.10.8.25		The Router shall support the following BGP properties:	Functional Verification
	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	Declaration
3.10.8.27		The Router shall support Capabilities Advertisement with BGP-4 as per RFC 3392	Declaration
3.10.8.28		The Router shall support Graceful Restart Mechanism for BGP as per RFC 4724	Declaration
3.10.8.29		The Router shall support IPv6 multiprotocol BGP link-local address peering	Declaration
3.10.8.30		The Router shall support outbound route filtering for BGP4 as per RFC 5291	Declaration
3.10.9		**iBGP / eBGP**	
3.10.9.1		The Router shall support Interior BGP (iBGP) peering sessions.	Functional Verification
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.	Functional Verification
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.	Declaration
3.10.9.4		The Router shall support next hop tracking & Control to enable network administrators to control peering requirements with exterior BGP peers.	Declaration

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:	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
	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)	Declaration
3.10.11		**Load balancing**	Information
3.10.11.1		The Router shall support Load balancing on bearer pin-hole assignment if multiple paths exist between two end points.	Declaration
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.	Declaration
3.10.11.3		The Router shall support Load balancing across WAN links.	Declaration
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.	Declaration
3.10.12.2		The Router shall support Route Reflector client and non-Route Reflector client peering sessions as per RFC4456	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.10.12.3		Different RR deployment scenarios in Service Provider networks shall be as follows:	Declaration
	a.	RR for IPv4 and VPNv4 routes	Declaration
	b.	RR for IPv6 and VPNv6 routes	Declaration
	c.	Service Specific RR	Declaration
	d.	Location redundancy	Declaration
3.11		**Multicast Features**	
3.11.1		**General:**	
3.11.1.1		The Router shall support Prioritization of multicast traffic	Functional Verification
3.11.1.2		The Router shall support to maintain static multicast entries in a separate multicast table.	Functional Verification
3.11.1.3		The Router shall support Multicast ACL to ensure security	Declaration
3.11.1.4		The Router shall support Multicast Load Balancing traffic across multiple interfaces	Functional Verification
3.11.1.5		The Router shall support administratively Scoped IP Multicast (IPv4 Multicast address space) as per RFC 2365	Declaration
3.11.1.6		The Router shall provide statistics on all active groups, sources on a per VLAN or port basis.	Declaration
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)	Declaration
3.11.2		**IGMP**	

3.11.2.1		The Router shall support Internet Group Management Protocol, Version 3 as per RFC 3376	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.11.2.2		The Router shall support Host Extensions for IP Multicasting as per RFC 1112	Declaration
3.11.2.3		The Router shall support Source based and shared distribution trees	Declaration
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	Declaration
3.11.3.2		The Router shall support Protocol Independent Multicast MIB as per RFC 5060	Declaration
3.11.3.3		The Router shall support Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) as per RFC 5059	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.11.3.4		The Router shall support Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification as per RFC 4601	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
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	Functional Verification
3.11.3.6		The Router shall support Automatic route processing (AutoRP)	Declaration
3.11.3.7		The Router shall support Multicast Source Discovery Protocol (MSDP) as per RFC 3618	Declaration
3.11.3.8		The Router shall support Bootstrap Router Mechanism for PIM Sparse Mode	Declaration
3.11.3.9		The Router shall support PIM Source Specific Multicast (PIM-SSM) as per RFC 3569	Functional Verification
3.11.3.10		The Router shall support Source-Specific Multicast for IP as per RFC4607	Declaration
3.11.4		**Anycast**	Information
3.11.4.1		The Router shall support operation of Anycast Services	Declaration
3.11.4.2		The Router shall support Dynamic broadcast Source Failover using Anycast routing	Declaration
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	Functional Verification
3.11.5.2		IPv6 multicast Address Group Range Support	Declaration
3.11.5.3		IPv6 Multicast Listener Discovery (MLD) protocol, versions 1 and 2 as per RFC 2710	Declaration
3.11.5.4		MLDv2 for IPv6 as per RFC 3810	Check functionality as per Lab Test-Refer Test No. 16 of Compendium

3.11.5 .5		IPv6 multicast MLD group limits	Declaration
3.11.5 .6		IPv6 multicast SSM mapping for MLDv1 SSM	Declaration
3.11.5 .7		IPv6 Router Alert Option as per RFC 2711	Declaration
3.11.5 .8		Transmission of IPv6 Packets over Ethernet as per RFC 2464	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.11.5 .9		IPv6 PIM sparse mode (PIM-SM)	Functional Verification
3.11.5 .10		IPv6 PIM Source Specific Multicast (PIM-SSM)	Declaration
3.11.5 .11		IPv6 multicast PIM accept register	Declaration
3.11.5 .12		IPv6 multicast PIM embedded RP support	Declaration
3.11.5 .13		IPv6 multicast scope boundaries	Declaration
3.11.5 .14		Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	Declaration
3.11.5 .15		IPv6 multicast MLD access group	Declaration
3.11.5 .16		IPv6 multicast RPF flooding of bootstrap router (BSR) packets	Declaration
3.11.5 .17		IPv6 multicast routable address hello option	Declaration
3.11.5 .18		IPv6 multicast static multicast routing (mroute)	Declaration
3.11.5 .19		IPv6 multicast address family support for Multiprotocol Border Gateway Protocol (MBGP)	Declaration
3.11.5 .20		IPv6 multicast Explicit tracking of receivers	Declaration
3.11.5 .21		IPv6 multicast IPv6 BSR scoped-zone support	Declaration
3.11.5 .22		IPv6 multicast IPv6 BSR—ability to configure RP mapping	Declaration
3.12		**MPLS Requirements**	Information
3.12.1		**Multi-protocol Label Switching (MPLS)**	Information
3.12.1 .1		The Router shall support Multi Protocol Label Switching Architecture as per RFC 3031	Declaration
3.12.1 .2		The Router shall support MPLS Label Stack Encoding as per RFC 3032	Declaration
3.12.1		The Router shall support Time To Live (TTL) Processing in Multi-Protocol Label	Declaration
.3		Switching (MPLS) Networks as per RFC 3443	
3.12.1 .4		The Router shall support the Generalized TTL Security Mechanism (GTSM) as per RFC5082	Declaration
3.12.1 .5		The Router shall support Framework for Multi-Protocol Label Switching (MPLS)-based Recovery as per RFC 3469	Declaration
3.12.1 .6		The Router shall support Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) as per RFC 3813	Declaration

3.12.1.7		The Router shall support MPLS Label Switch Router/Label Switch Controller software (LSR)	Functional Verification
3.12.1.8		The Router shall support MPLS Label Edge Router (LER) functionality.	Functional Verification
3.12.1.9		The Router shall support Dynamic MPLS LSP setup with signaling protocol on all the router interfaces.	Declaration
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.	Declaration
3.12.1.11		The Router shall support MPLS class of service.	Functional Verification
3.12.1.12		The Router shall support ICMP Extensions for Multi Protocol Label Switching	Declaration
3.12.1.13		The Router shall limit the number of routes per VRF.	Declaration
3.12.1.14		The Router shall set Thresholds to provide traps and alarms when a certain number of routes are exceeded.	Declaration
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	Declaration
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**	Information
3.12.2.1		The Router shall support LDP specification as per RFC5036	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.12.2.2		The Router shall support LDP Applicability as per RFC 3037	Declaration
3.12.2.3		Graceful Restart Mechanism for Label Distribution Protocol shall be as per RFC 3478	Declaration
3.12.3		**MPLS VPN**	Information
3.12.3.1		The Router shall advertise both VPN routes and public internet routes in the same BGP routing instance.	Declaration
3.12.3.2		The Router shall support Internet Access from the same VPN and internet Access from the global routing instance.	Declaration
3.12.3.3		The Router shall support Extranet functionality	Declaration
3.12.4		**MPLS Layer-2 VPN**	Information
3.12.4.1		The Router shall support Framework for Layer 2 Virtual Private Networks (L2VPN) as per RFC 4664	Declaration
3.12.4.2		The Router shall support Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks as per RFC 4665	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
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	Declaration
3.12.4.4		The Router shall support Address Allocation for Private Internets (Private and overlapping IP addressing) as per RFC 1918	Declaration
3.12.5		**MPLS Layer-3 VPN**	Information

3.12.5 .1		The Router shall support BGP/MPLS IP Virtual Private Networks (VPNs) as per RFC 4364	Functional Verification
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.	Functional Verification
3.12.6 .2		The Router shall support VPLS with pseudo wire redundancy.	Functional Verification
3.12.6 .3		The Router shall support Active/standby pseudo wire.	Declaration
3.12.6 .4		The Router shall support PW redundancy with MAC withdrawal.	Declaration
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.	Declaration
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.	Declaration
3.12.6 .7		The Router shall support VPLS service on all the interfaces.	Declaration
3.12.6 .8		The Router shall support Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling as per RFC 4762	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.12.7		**Autonomous System**	Information
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	Functional Verification
3.12.7 .2		The Router shall support Inter AS IPVPN	Declaration
3.12.7 .3		The Router shall support Inter Area Autonomous System (InterAS)	Declaration
3.12.8		**MPLS-TP**	
3.12.8 .1		The Router shall support MPLS-TP requirements as per RFC 5654 or ITU Y.SUP4	Functional Verification
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	Functional Verification
3.12.8 .3		The Router shall support Interfaces for the MPLS-TP Hierarchy as per ITU-T G.8112 or equivalent IETF standards	Functional Verification
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	Functional Verification
3.12.8 .5		The Router shall support MPLS-TP General Framework as per RFC 5921 or ITU G.8110.1	Declaration
3.12.8 .6		The Router shall support MPLS-TP survivability framework as per RFC 6372 or ITU G.8131/G.8132	Declaration
3.12.8		The Router shall support MPLS-TP Data plane Architecture as per RFC5960 or ITU	Declaration
.7		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	Declaration
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	Declaration

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.	Declaration
3.12.8 .11		The Router shall support Pseudowire Status for Static Pseudowires as per RFC 6478	Declaration
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	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
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	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.13		**General IPv6 Features**	Information
3.13.1		**General Support**	Information
3.13.1 .1		The Router shall support IPv6 Specification as per RFC 8200	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.13.1 .2		The Router shall support Path MTU Discovery for IPv6 as per RFC 8201	Declaration
3.13.1 .3		The Router shall support ICMPv6 for IPv6 Specification as per RFC 4443	Functional Verification
3.13.1 .4		The Router shall support ICMPv6 redirect	Declaration
3.13.1 .5		The Router shall support ICMPv6 rate limiting	Declaration
3.13.1 .6		The Router shall support Neighbor Discovery for IP version 6 (IPv6) as per RFC 4861	Declaration
3.13.1 .7		The Router shall support IPv6 neighbor discovery duplicate address detection	Declaration
3.13.1 .8		The Router shall support IPv6 Stateless Address Autoconfiguration as per RFC 4862	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.13.1 .9		The Router shall support IPv6 addressing architecture as per RFC 4291	Declaration
3.13.1 .10		The Router shall support deprecation of Type 0 Routing Headers in IPv6 as per RFC 5095	Declaration
3.13.1 .11		The Router shall support IPv6 global unicast address format as per RFC 3587	Declaration
3.13.1 .12		The Router shall support IPv6 jumbograms.	Declaration
3.13.2		**Additional Ipv6 Support Features**	Information
3.13.2		The Router shall support IPv6 Scoped Address Architecture as per RFC 4007	Declaration
.1			
3.13.2 .2		The Router shall support Unique Local IPv6 Unicast Addresses as per RFC 4193	Declaration
3.13.2 .3		The Router shall support Management Information Base for the Internet Protocol as per RFC 4293	Declaration

3.13.2.4		The Router shall support SNMP over IPv6	Functional Verification
3.13.2.5		The Router shall support IPv6 ping	Functional Verification
3.13.2.6		The Router shall support Syslog over IPv6	Functional Verification
3.13.2.7		The Router shall support IPv6 over PPP as per RFC 2472	Declaration
3.13.2.8		The Router shall support IP Forwarding Table MIB as per RFC 4292	Declaration
3.13.2.9		The Router shall support NETCONF with YANG over IPv6	
3.14		**Advanced IPv6 Features**	
3.14.1		**Carrier Grade NAT**	Information
3.14.1.1		The Router shall support Network Address Translation-Protocol Translation (NAT-PT) as per RFC 2766	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.14.1.2		The Router shall support overload (PAT)	Functional Verification
3.14.1.3		The Router shall support source-based NAT	Functional Verification
3.14.1.4		The Router shall support to enable/disable NAT & NAPT for group of source/destination pools using any transport protocol	Declaration
3.14.1.5		The Router shall support Architectural Implications of NAT as per RFC 2993	Declaration
3.14.1.6		The Router shall support fragmented packets and allow such packets to pass through	Declaration
3.14.1.7		The Router shall support translating (modify) IP datagrams passing between two IPv4 domains	Declaration
3.14.1.8		The Router shall support for IP Network Address Translator (NAT) Terminology and Considerations	Declaration
3.14.1.9		The Router shall support fragmentation	Declaration
3.14.1.10		The Router shall support basic NAT-44	Functional Verification
3.14.1.11		The Router shall support NAPT44	Functional Verification
3.14.1.12		The Router shall support NAT64 as per RFC 6146	Functional Verification
3.14.1.13		The Router shall support NAT444 as per RFC 6127	Functional Verification
3.14.1.14		The Router shall support Dynamic NAT44	Functional Verification
3.14.1.15		The Router Performance should not be impacted by running multiple concurrent translation methods	Declaration
3.14.1.16		The Router Throughput performance should not be impacted more than 5% if NAT/NAPT are activated for all subscribers	Declaration
3.14.1.17		The Router shall support load balancing process to handle incoming traffic between several instances on several cards simultaneously	Declaration

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.	Declaration
3.14.1 .19		The Router shall support various filtering techniques such as endpoint independent filtering, and address dependent filtering	Declaration
3.14.1 .20		The Router shall support static allocation of IPv4 and IPv6 and port binding to configurable set/all users	Declaration
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	Declaration
3.14.1 .22		The Router shall support Port Block Allocation and log reduction	Declaration
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	Declaration
3.14.1 .24		The Router shall support DS-Lite AFTR (Address Family Transition Router) function	Declaration
3.14.1 .25		The Router shall support NAT/NAPT from one IP-VPN context to the global/default routing context	Declaration
3.14.1 .26		The Router Support for NAT/NAPT from one IP-VPN context to another IP-VPN context	Declaration
3.14.1 .27		The Router shall support NAT behavioral Requirements for TCP as per RFC 5382	Declaration
3.14.1 .28		The Router shall support NAT behavioral Requirements for UDP as per RFC 4787	Declaration
3.14.1 .29		The Router shall support NAT behavioral Requirements for ICMP as per RFC 5508	Declaration
3.14.1 .30		The Router shall support adjusting checksum values of all IP, UDP, TCP and ICMP headers	Declaration
3.14.1 .31		The Router shall support all TCP and UDP based applications in NAT64 environment	Declaration
3.14.1 .32		The Router shall support mapping table between Inside IP (private IPs) and Outside IP (public Ips) and ports	Declaration
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	Declaration
3.14.1 .34		The Router shall support prohibition of mapping of the previliged/well-known TCP and UDP ports	Declaration
3.141. 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	Declaration
3.14.1 .36		The Router shall support Bypass within NAT rule for certain traffic	Declaration
3.15.1 .37		The Router shall support hairpinning when both source and destination are managed by same CGNAT device	Declaration
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	Declaration
3.14.1 .39		The Router shall support requirements for IP Version 4 Routers as per RFC 1812	Declaration
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	Declaration

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	Declaration
3.14.2		**IPv6 Tunneling**	
3.14.2 .1		The Router shall support generic packet tunneling in Ipv6 shall be as per RFC 2473	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.14.2 .2		The Router shall support connection of IPv6 Domains via IPv4 Clouds as per RFC 3056	Check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.14.2 .3		The Router shall support an Anycast Prefix for 6to4 Relay Routers	Declaration
3.14.2 .4		The Router shall support Basic Transition Mechanisms for IPv6 Hosts and Routers shall be as per RFC 4213	Declaration
3.14.2 .5		The Router shall supportMPLS/BGP Layer 3 VPN MIB shall be as per RFC 4382	Declaration
3.14.2 .6		The Router shall supportBGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN shall be as per RFC 4659	Declaration
3.14.2 .7		The Router shall support connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) shall be as per RFC 4798	Declaration
3.14.2 .8		The Router shall support automatic IPv4-compatible tunnels	Declaration
3.14.2 .9		The Router shall support manually configured IPv6 over IPv4 tunnels	Declaration
3.14.2 .10		The Router shall support IPv6 over IPv4 tunnels	Functional Verification
3.14.2 .11		The Router shall support IP over IPv6 tunnels	Declaration
3.14.2 .12		The Router shall support IPv6 VPN over MPLS	Declaration
3.14.2 .13		The Router shall support IP SLAs (Service Level Agreements) for IPv6	Declaration
3.14.2 .14		The Router shall support IP/ICMP transition as per RFC 6145	Declaration
3.14.2 .15		The Router shall support dual stack transition mechanism	Declaration
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.	Information
3.15.1		**General Traffic Engineering Requirements:**	Information
3.15.1 .1		The Router shall support manual configuration and provisioning functionality of end-to-end traffic tunnels through eMS	Declaration

3.15.1 .2		The Router shall support traffic tunnels of minimum 2Mbps granularity	Declaration
3.15.1 .3		The Router shall support protection to a TE tunnel through two explicit paths configured through the network by the administrator	Declaration
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	Declaration
3.15.1 .5		The Router shall support options for automatic and manual selection of TE path	Declaration
3.15.1 .6		The Router shall support to establish routing adjacencies between two routers over the TE tunnel	Declaration
3.15.1 .7		The Router shall support the bandwidth management features	Declaration
3.15.2		**MPLS Traffic Engineering**	
3.15.2 .1		The Router shall support requirements for Traffic Engineering over MPLS as per RFC 2702	Functional Verification
3.15.2 .2		The Router shall support dynamic MPLS Traffic Engineering	Functional Verification
3.15.2 .3		The Router shall support traffic Engineering Extensions to OSPF Version 2 as per RFC 3630	Declaration
3.15.2 .4		The Router shall support IS-IS Extensions for Traffic Engineering as per RFC 5305	Declaration
3.15.2 .5		The Router shall support OSPF inter area MPLS Traffic Engineering	Declaration
3.15.2 .6		The Router shall support automatic bandwidth adjustment for TE tunnels	Declaration
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	Declaration
3.15.2 .8		The Router shall support IGP (OSPF and IS-IS) traffic engineering LSAs shall support the flooding of bandwidth constraints across local areas	Declaration
3.15.2 .9		The Router shall support each interface shall carry multiple MPLS TE tunnels for various traffics of different priority. Different levels of priority shall be assigned to various TE tunnels	Declaration
3.15.3		**RSVP**	Information
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.	Functional Verification
3.15.3 .2		The Router shall support Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification as per RFC 2205	Declaration
3.15.3 .3		The Router shall support Applicability Statement for Extensions to RSVP for LSP-Tunnels	Declaration
3.15.3 .4		The Router shall support IGP Area tunneling for RSVP	Declaration
3.15.3 .5		The Router shall support Aggregation of Martini circuits within an RSVP–TE tunneled LSP	Declaration
3.15.3 .6		All interfaces and sub-interfaces of the Router shall support RSVP-TE signaling.	Declaration
3.15.3 .7		The Router shall support RSVP and RSVP-TE Extensions to RSVP for LSP Tunnels shall be 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	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
	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	Functional Verification
3.15.4 .2		The Router shall support Pseudo-Wire Emulation Edge-to-Edge (PWE3) Architecture as per RFC 3985	Declaration
3.15.4 .3		The Router shall support PWE3 Control Word for Use over an MPLS PSN as per RFC 4385	Declaration
3.15.4 .4		The Router shall support encapsulation Methods for Transport of Ethernet over MPLS Networks as per RFC 4448	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.15.4 .5		The Router shall support Pseudowire (PW) Management Information Base (MIB) as per RFC 5601	Declaration
3.15.4 .6		The Router shall support pseudo wire Setup and Maintenance using LDP as per RFC 4447	Declaration
3.15.4 .7		The Router shall support PWE3 fragmentation and reassembly as per RFC 4623	Declaration
3.15.4 .8		The Router shall support segmented Pseudowires as per RFC 6073	Declaration
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	Functional Verification
3.15.5 .2		The Router shall support extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs) shall be as per RFC 4875 for Core/Edge Routers	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
3.15.5 .3		M-ISIS: The Router shall support Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs) shall be as per RFC 5120	Declaration
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	Functional Verification
3.15.6. 2		The Router shall support MPLS Support of Differentiated Services as per RFC 3270	Declaration
3.15.6 .3		The Router shall support Differentiated Services-aware MPLS Traffic Engineering as per RFC 3564	Declaration
3.15.6 .4		The Router shall support Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering as per RFC 4124	Declaration
3.15.6 .5		The Router shall support maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering	Functional Verification
3.15.6 .6		The Router shall support Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering as per RFC 4127	Declaration
3.15.6 .7		The Router shall support MPLS-TP tunnels shall 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	Functional Verification
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	Declaration
3.16		**Quality of Service Requirements**	Information
3.16.1		**General**	Information
3.16.1 .1		The Router shall support QoS in all Types of interfaces.	Declaration
3.16.1 .2		The Router shall support the QoS features per port and per VLAN	Functional Verification
3.16.1 .3		The Router shall support VLAN CoS preservation	Declaration
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	Functional Verification
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	Declaration
3.16.1 .6		The Router shall support prediction of performance bounds for each flow shall be predictable in terms of throughput, loss, delay and delay variation, according to their respective defined service classes	Declaration
3.16.1 .7		The Router shall support 16, 32, 64, 128, 256 and 512 k Bytes burst sizes	Declaration
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	Declaration
3.16.1 .9		The Router shall support bandwidth management reports and statistics	Declaration
3.16.2		**Diff-Serv**	Information
3.16.2 .1		The Router shall support Diff-Serv as per RFC3260	Functional Verification
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	Check functionality as per Lab Test-Refer Test No. 16 of Compendium

			for 802.1q and functional verification for 802.1p
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	Declaration
3.16.2.4		The Router shall support architecture for Differentiated Services as per RFC 2475	Declaration
3.16.2.5		The Router shall support MIB for Diff-Serv as per RFC 3289	Declaration
3.16.2.6		The Router shall support IP Precedence (TOS-IPP)	Functional Verification
3.16.2.7		The Router shall support Per Hop Behavior Identification Codes as per RFC 3140	Functional Verification
3.16.2.8		The Router shall support assured Forwarding PHB Group as per RFC 2597	Declaration
3.16.2.9		The Router shall support expedited Forwarding PHB (Per-Hop Behavior) as per RFC 3246	Functional Verification
3.16.3		**Classification/Prioritization**	Information
3.16.3.1		The Router shall support Policy based bandwidth classification	Functional Verification
3.16.3.2		The Router shall support Service QoS flow identification	Declaration
3.16.3.3		The Router shall support classification of ingress traffic for a specific service based on the following mapping:	Declaration
	a.	IEEE 802.1P Mapping - it shall be possible to reserve parts of the link bandwidth for frames with particular IEEE 802.1p values	Declaration
	b.	Customer IEEE 802.1p priority	Functional Verification
	c.	IP DSCP Mapping as per RFC 5462	Check functionality as per Lab Test-Refer Test No. 16 of Compendium
	d.	Multiprotocol Label Switching (MPLS) Label Stack Entry:"EXP" Field Renamed to "Traffic Class" Field as per RFC 5462	Functional Verification
	e.	Ethernet L2 Based Conversation and protocol Mapping	Declaration
	f.	Source MAC address	Functional Verification
	g.	Destination MAC address	Functional Verification
	h.	Ether Type or Protocol Type	Declaration
	i.	Incoming port (Logical and Physical)	Declaration
	j.	Incoming/Destination IP address and mask	Functional Verification
	k.	Source/Destination TCP/UDP Port	Declaration
	l.	Type of Service (ToS) Precedence bits	Declaration
	m.	UDP/TCP socket	Declaration
	n.	VLAN ID	Functional Verification
	o.	IEEE 802.1Q	Functional

			Verification
	p.	Default queue for non-matching traffic	Declaration
3.16.3.4		The Router shall aggregate incoming traffic into Traffic Classes by following characteristics	Information
	a.	Incoming port (Logical and Physical)	Functional Verification
	b.	Incoming/Destination IP address	Functional Verification
	c.	Source/Destination TCP/UDP Port	Declaration
	d.	Type of Service (ToS) Precedence bits	Functional Verification
	e.	Source/ destination MAC	Functional Verification
	f.	Type of Protocol	Functional Verification
	g.	UDP/TCP socket	Declaration
	h.	Link layer priority Information as per IEEE 802.1p	Declaration
3.16.3.5		The Router shall support classification based on	Information
	a.	Layer-4 Information	Declaration
	b.	Source and Destination port/range numbers	Functional Verification
3.16.3.6		The Router shall support traffic prioritization	Functional Verification
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.	Declaration
3.16.4		**Mapping:**	Declaration
3.16.4.1		The Router shall support mapping of DSCP to VLAN or other traffic engineering capabilities in the Regional Network	Declaration
3.16.4.2		The Router shall aggregate incoming traffic into Traffic Classes by MPLS Label EXP bits (E-LSP)	Declaration
3.16.4.3		The Router shall support mapping of IEEE 802.1p and IP TOS bits into MPLS EXP bits	Functional Verification
3.16.4.4		The Router shall support mapping of IEEE 802.1q VLAN tags into MPLS labels	Functional Verification
3.16.5		**Marking/Policing/Shaping:**	Declaration
		The Router shall support the following Marking/Policing/Shaping requirements	
	a.	8 level Priority marking as per IEEE 802.1p	Functional Verification
	b.	Filtering	Functional Verification
	c.	Broadcast/Multicast suppression	Functional Verification
	d.	Bandwidth management policies	Functional Verification
	e.	Single rate three colour marking (srTCM) RFC 2697	Functional Verification
	f.	Two rate three colour metering (trTCM) RFC 2698	Functional Verification
	g.	Colour aware srTCM and trTCM based metering	Functional Verification
	h.	Trust the colour of the incoming packet	Declaration
	i.	Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic	Declaration

	j.	4K ingress policing instances with 10 entries in each	Declaration
	k.	Ingress and egress policing based on Layer 3-4 Information	Declaration
	l.	Shaping of Burst Traffic	Functional Verification
3.16.6		**Rate Limiting**	
3.16.6 .1		The Router shall support Rate limiting of bandwidth per Port and per class (or flow)	Declaration
3.16.6 .2		The Router shall support configuration of user bandwidth in steps of	Functional Verification
		· 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	Declaration
3.116. 6.4		The Router shall support flow based rate limiting method based on per source address, destination address or both	Declaration
3.16.7		**Queuing**	Information
3.16.7 .1		The Router shall support the following queuing	Information
	a.	SPQ – Strict Priority Queuing	Functional Verification
	b.	WFQ – Weighted fair Queuing (This feature is not mandatory for Routers [Type I/II/III/XIII/XIV/XV/XVI/XVII])	Functional Verification
	c.	Diff-Serv queuing for the Assured forwarding (AF) and Expedited forwarding	Functional Verification
	d.	No of queues per flow treatment of traffic	Declaration
	e.	Setting the maximum size/depth of all queues	Declaration
	f.	Intelligent queuing based on IP ToS bits for scalability	Declaration
	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)	Declaration
	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).	Declaration
	i.	Alternate priority routing traffic necessary to keep from starving other priority queues	Declaration
	j.	Service Level Accounting	Declaration
	k.	Counters for queues for billing and accounting	Declaration
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**	Information
3.16.8 .1		The Router shall support scheduling of queues to strict priority with 2 or more priority levels	Functional Verification
3.16.8 .2		The CE Routers [Type I/II/III] shall support the following congestion avoidance mechanisms	Declaration
	a.	Tail Drop	Declaration

	b.	WTD (Weighted Tail Drop)	Declaration
	c.	Selective Packet Discard	Declaration
	d.	Longest Queue Drop for extreme or sudden congestion	Declaration
	e.	Deficit Round Robin (DRR)	Declaration
	f.	Weighted Round Robin (WRR)	Functional Verification
	g.	DWRR(Deficit Weighted Round Robin)	Declaration
	h.	WRED	Functional Verification
	i.	Modified Deficit Round Robin (MDRR)	Declaration
	j.	Strict Priority (SP)	Declaration
	k.	SP + Weighted Round Robin (SP + WRR)	Functional Verification
3.16.8 .3		The Aggregation/Edge/Core Routers [Type IV to XII] shall support the following congestion avoidance mechanisms	Information
	a.	Tail Drop	Declaration
	b.	Selective Packet Discard	Declaration
	c.	WRED	Functional Verification
	d.	Weighted Fair Queuing	Functional Verification
	e.	Strict Priority (SP)	Functional Verification
3.16.8 .4		The Router shall support configuring the scheduling as per the	Declaration
	a.	Per Hop Behaviour (PHB)	Functional Verification
	b.	Physical port or logical port basis	Declaration
	c.	100ms ingress buffering and 100ms egress buffering at line-rate	Declaration
	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	Declaration
	e.	At least three level dropping precedence levels in each queue	Declaration
3.16.8 .5		The Non-Chasis Routers shall support the following congestion avoidance mechanisms	
	a.	Tail Drop	Declaration
	b.	Weighted Round Robin (WRR)	Functional Verification
	c.	WRED (applicable for type XIV Routers)	Functional Verification
	d.	Strict Priority (SP)	Functional Verification
	e.	SP + Weighted Round Robin (SP + WRR)	Declaration
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.	Declaration
3.16.9		**Hierarchical QOS**	Declaration
3.16.9 .1		The Router shall support hierarchical QoS at egress at CoS, Flow, EVC Tunnel and MPLS-TP/Egress UNI level	Functional Verification
3.16.9 .2		The Router shall support at least 500 EVC level queues	Declaration
3.16.9 .3		The Router shall support traffic buffering and shaping capability with at least 32 MB buffering	Declaration

3.16.9.4		The Router shall support traffic shaping at egress is done on per MPLS-TP Tunnel basis	Declaration
3.16.9.5		The Router shall support upto 3 levels of QoS	Functional Verification
3.16.10		**IPv6 QoS features**	Declaration
3.16.10.1		The Router shall support packet classification	Declaration
3.16.10.2		The Router shall support traffic shaping	Declaration
3.16.10.3		The Router shall support traffic policing	Declaration
3.16.10.4		The Router shall support packet marking/re-marking	Declaration
3.16.10.5		The Router shall support IPv6 QoS queuing	Declaration
3.16.10.6		The Router shall support weighted random early detection (WRED)- based drop	Declaration
3.16.10.7		The Router shall support NSF and graceful restart for MP-BGP IPv6 address family	Declaration
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	Declaration
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	Functional Verification
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	Functional Verification
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	Lab Test - Refer Test No. 20 of Compendium
3.18.1.2		The Router shall support Synchronous clock selection algorithm shall be based on the following parameters	Declaration
	a.	Quality of Signal	Declaration
	b.	Signal fail	Declaration
	c.	Priority	Declaration
	d.	External Commands	Declaration
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	Lab Test - Refer Test No. 21 of Compendium
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	Check functionality as per Lab Test-Refer Test No. 16 of Compendium

3.18.4		**SyncE Support:** The Router shall support the timing and synchronization aspects of Packet Networks based on SyncE shall be as per G.8261. The router shall support timing characteristics of a synchronization slave clock. as per G.8262	Functional Verification
3.18.5		**Synchronization reference**	
3.18.5 .1		The Router shall support the external synchronization through BITS interface (2Mbps or 2MHz)	Lab Test - Refer Test No. 20 of Compendium
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	Declaration
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	Functional Verification
3.19		**Protection Switching Requirements**	
3.19.1		**Protection Switching Time**	Declaration
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).	Functional Verification
3.19.2		**Protection Switching Modes for SDH Interfaces**	Declaration
3.19.2 .1		The Router shall support automatic switching and Forced switching as analogous to SDH systems	Functional Verification
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.	Declaration
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	Functional Verification
3.19.4		**Linear protection mechanisms**	Declaration
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	Functional Verification
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	Declaration
3.19.5		**OAM Requirements**	Declaration
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	Declaration
3.20		**Scalability Requirements**	Declaration
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.	Declaration
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	Declaration
3.20.2 .2		The Router shall accept untagged, priority tagged and C-tagged frames through a IEEE 802.1Q port	check functionality as per Lab Test- Refer Test No. 16 of Compendium
3.20.3		**Q-in-Q or IEEE 802.1ad mode Requirements**	Declaration
3.20.3 .1		The Routers shall perform classification and service delineation based on outer Q tag and outer IEEEE 802.1p bits. (i.e. ignore inner tag).	Declaration
	a.	It shall support VLAN stacking as per IEEE 802.1ad	Functional Verification
	b.	It shall have minimum of 4094 S-VIDs. VIDs “0” and “FFFF” is reserved	Declaration
	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	Declaration
	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	Declaration
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	check functionality as per Lab Test- Refer Test No. 16 of Compendium
	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**	Declaration
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	Functional Verification
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	Declaration
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	Declaration
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	Functional Verification

3.21.2.2		The Router shall support MPLS-TP OAM requirements e as per RFC 5860 or ITU G.8113.1 / G.8113.2	Functional Verification
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	Declaration
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	Functional Verification
3.21.3		**Configuration**	Information
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)	Functional Verification
3.21.4		**Performance monitoring**	Declaration
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	Functional Verification
3.21.4.2		The router shall support measurement of delay, Jitter, Ethernet alarm signal and Ethernet test signal function	Declaration
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	Declaration
3.21.5		**Fault Management**	
3.21.5.1		The Router shall support MPLS-TP Fault management OAM shall be as per RFC 6427 or ITU G.8113.1 / G.8113.2	Check functionality as per Lab Test-Refer Test No. 16 of Compendium for RFC 6427 and Functional verification for ITU rec.
3.21.5.2		The Router shall support Ethernet OAM, Connectivity Fault Management (CFM) shall be as per IEEE 802.3ah and IEEE 802.1ag	Functional Verification
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	Declaration
3.21.5.4		The Router shall support Connection verification for MPLS Transport Profile LSP shall be as per RFC 6428	Declaration
3.21.5.5		The Router shall support Alarms in the eMS. If any performance bounds (Frame Delay, Frame Delay Variation, and Frame Loss) are exceeded, the alarm shall be raised	Functional Verification
3.21.5.6		The Router shall support MPLS fault management shall as per RFC4377 and RFC4378	Declaration
3.21.5.7		The Router shall support MPLS Connectivity verification and route tracing as per RFC 6426	Declaration
3.21.5.8		The Router shall support MPLS BFD for LSP as per RFC5884	Declaration
		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	Functional Verification
3.21.6 .2		The Router shall support service Ping, IP Ping, IP Trace Route	Functional Verification
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	Functional Verification
3.21.8		**SNMP Manageability**	
3.21.8 .1		The Router shall support SNMP v2 & SNMP v3	Functional Verification
3.21.8 .2		The Router shall support RMON (Remote Monitoring) MIB I, II	Declaration
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	Functional Verification
Part III		**eMS/NMS Requirement**	
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	Functional Verification
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	Functional Verification
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	Functional Verification
3.22.4		The eMS shall have suitable system level backup mechanism for taking backup of eMS data of at least one month	Declaration
3.22.5		The eMS shall provide the visual presentation of the Network Element's status and the alarms	Functional Verification
3.22.6		The eMS shall support to take any Network Element out-of-service & in-service through the eMS. It shall be possible to restart the Network Element from eMS	Functional Verification
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	Declaration
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	Functional Verification

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	Declaration
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	Functional Verification
3.22.11		The response time for query/command on any operator terminal, local or remote shall be 10 seconds or less	Functional Verification
3.22.12		The eMS shall manage upto 5000 nodes	Declaration
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	Declaration
3.23.1.2		The eMS shall provide Service Level view that shows VPN Topologies and end customer to customer paths and traces	Functional Verification
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	Functional Verification
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	Functional Verification
3.23.1.5		The eMS shall provide total alarm visibility of all NEs under its management	Functional Verification
	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 customize according to user requirement	Functional Verification
3.23.1 7		The eMS shall support to send critical alarm alerts through SMS or e-mail and the same shall be configurable	Functional Verification
3.23.1.8		The eMS shall support alarm reduction through correlation & suppression based on object modeling	Declaration
3.23.1.9		The eMS shall support turn on or off the correlation rule	Declaration
3.23.1.10		The eMS shall support pre-defined correlation rule support	Declaration
3.23.1.11		The eMS shall support accessibility of affected alarm details from a single point	Declaration

3.23.1.12		The eMS shall provide Information about all suppressed alarms	Declaration
3.23.1.13		The eMS shall provide Information about all affected objects	Declaration
3.23.1.14		The eMS shall provide following topology views	Functional Verification
	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	Functional Verification
3.23.1.16		The fault management system shall support the following functions	Functional Verification
	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	Functional Verification
	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	Functional Verification
3.23.2.2		The eMS system shall support multiple types of discovery including following	Functional Verification
	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.	Functional Verification
3.23.2.4		The eMS system shall support for SNMP v3 based discovery and management of supported devices to provide added security	Declaration
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	Declaration

3.23.2.6.		Discovery shall identify and model router redundancy so that alarms generated from these virtual addresses are automatically excluded	Declaration
3.23.2.7		The eMS system shall support map grouped by network topology, geographical locations of the equipments and user group/departments	Declaration
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	Declaration
3.23.2.9		The eMS system shall support user-configurable discovery control to manage the frequency and scope network discovery	Declaration
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	Declaration
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	Functional Verification
3.24.2		The eMS shall do configuration changes for network devices from a central location	Functional Verification
3.24.3		The eMS shall capture and keep record of any configuration change happening on a network device	Declaration
3.24.4		The eMS shall keep a record of who does what change for auditing purpose	Declaration
3.24.5		The eMS shall support bare metal configuration of network devices	Functional Verification
3.24.6		The eMS shall show the difference between 2 configuration in color coded text format so that changes are visually identified	Declaration
3.24.7		The eMS shall provide configuration roll back option, so that a device can be brought to a good state configuration	Functional Verification
3.24.8		The eMS shall provide capability to follow an approval workflow before some or all changes can be implemented	Declaration
3.24.9		The eMS shall perform ACL updates on selected or all network devices	Declaration
3.24.10		The eMS shall generate compliance reports for management	Declaration
3.24.11		The eMS shall provide easy custom report generation capability	Declaration
3.24.12		The eMS shall detect and report vulnerabilities which exist on the network devices in the environment	Declaration
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	Functional Verification
	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	Functional Verification
3.25.1.2		The eMS shall be able to discover and keep the device Information	Functional Verification
3.25.1.3		The eMS shall be able to keep track on any change in the network inventory reporter chronologically	Functional Verification
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	Functional Verification
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	Declaration
	a.	Discovery of infrastructure	Declaration
	b.	Maintaining an accurate inventory of the Routers	Declaration
	c.	Configuring and patching the NE's	Declaration
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	Functional Verification
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	Declaration
3.25.1.9		The eMS shall provide patch management to keep computers up-to-date and complaint with our security requirements	Declaration
3.25.1.10		The eMS shall be capable to verify installation status of patches	Declaration
3.25.1.11		The software distribution function shall provide flexible and scalable delivery, installation, and configuration of software	Declaration
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.	Declaration
3.25.1.13		The eMS shall schedule reports to run at a later time including repeating intervals	Declaration
3.25.1.14		The eMS shall support PDF & CSV as report formats	Declaration
3.25.1.15		The eMS shall provide facility to administrators to easily customize reports or create new reports	Declaration
3.25.2		**Software Management**	
3.25.2.1		The eMS shall support to carry out the following tasks under the software management function.	Declaration
	a.	Loading of new system software	Functional Verification
	b.	Manage different versions of software	Functional Verification

	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	Functional Verification
	d.	Installation of software patches	Functional Verification
	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	Declaration
	f.	The eMS shall support FTP/TFTP for downloading of Software, configuration, patches etc., to the Network Element	Functional Verification
	g.	The operator terminals (local & remote) shall not allow loading of any software without the terminal administrator's authorization	Declaration
	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	Declaration
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	Functional Verification
3.25.3		**Helpdesk Management**	
3.25.3 .1		The eMS shall provide flexibility of logging, viewing, updating and closing incidents manually	Functional Verification
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	Declaration
3.25.2 .3		The eMS shall provide flexibility of incident assignment based on the workload, category or location	Functional Verification
3.25.3 .4		The eMS shall support each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming	Functional Verification
3.25.3 .5		The eMS shall support the escalation policy shall allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact	Declaration
3.25.3 .6		The eMS shall support web-base knowledge database to store useful history incident resolution	Functional Verification
3.25.3 .7		The eMS shall have access on different knowledge articles for different users	Declaration
3.25.3 .8		The eMS shall be able to log and escalate user interactions and requests	Declaration
3.25.3 .9		The eMS shall provide status of registered calls to end-users over email and through web	Declaration
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	Declaration
3.25.3 .11		The eMS shall have the capability to track work history of calls to facilitate troubleshooting	Declaration
3.25.3 .12		The eMS shall support tracking of SLAs for call requests within the help desk through service types	Functional Verification
3.25.3 .13		The eMS shall support request management, problem management, configuration management and change management	Declaration

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	Declaration
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	Declaration
3.25.3 .16		The eMS shall have executive dashboard for viewing the service desk KPIs in graph & chart format	Declaration
3.25.3 .17		The eMS shall provide seamless integration to log incident automatically via system and network management	Declaration
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.	Functional Verification
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	Functional Verification
3.26.3		The eMS shall support provision of performance measurements (e.g. QoS/CoS) for the following	Functional Verification
	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	Functional Verification
	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	Functional Verification
	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.	Functional Verification
3.26.7		The eMS shall also provide automated calculation of service achievement, management and operational report for SLA and Non-SLA services	Functional Verification
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	Documentation
3.26.9		The eMS shall support the following reports	Functional Verification
	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	Declaration
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 behaviours	Functional Verification
3.26.12		The eMS shall provide network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization, etc.) for network infrastructure	Functional Verification
3.26.13		The eMS shall identify over-and under-utilized links and assist in maximizing the utilization of current resources	Declaration
3.26.14		The eMS shall give performance of Network devices like CPU, memory & buffers, etc, LAN and WAN interfaces and network segments	Declaration
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	Declaration
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	Declaration
3.26.17		The eMS shall the following performance reports	Declaration
	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	Declaration
	b.	Capacity planning report which provides a view of under-and-over utilized elements	Declaration
	c.	Service Level report that shows the elements with the worst availability and worst response time – the two leading metrics used to monitor SLAs	Declaration
3.26.18		The eMS shall have a built-in report authoring tool to customize performance reports	Declaration
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	Declaration
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	Declaration
3.26.21		The eMS shall provide Latency (both one way and round trip times) report for critical devices and links	Functional Verification
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	Declaration

	a.	Ingress and egress bandwidth profile per User to Network Interface (UNI).	Functional Verification
	b.	Ethernet services supported on each port	Functional Verification
	c.	Layer 2 protocol transport for Ethernet and PPP	Declaration
	d.	Hardware assisted Layer 2 forwarding	Declaration
	e.	MAC address for each port	Functional Verification
	f.	L2 Learning parameters: Sources learning per Port/VLAN/Source address	Declaration
	g.	Dynamic MAC learning limit on each port	Declaration
	h.	The no. of source MAC addresses learnt from bridge port	Declaration
	i.	Automatic/manual disabling of MAC addresses learning for the VLAN	Declaration
	j.	MAC address limit	Declaration
	k.	Aging time (Aging Time or No Aging) for MAC addresses	Declaration
	l.	L2 Aging on every port	Declaration
	m	Disable MAC address learning.	Declaration
	n.	Policy to discard all Ethernet frames based on MAC destination address	Declaration
	o.	Allowable MAC destination address	Functional Verification
	p.	Spanning Tree Protocol as per IEEE 802.1d	Functional Verification
	q.	Queues to prioritize BPDUs	Declaration
	r.	Each port to drop BPDU if those BPDUs have a root bridge identifier which is lower (better) than the current Spanning Tree root	Declaration
	s.	Each port to drop BPDU regardless of the BPDU content	Declaration
	t.	RSTP as per IEEE 802.1w	Functional Verification
	u.	MSTP as per IEEE 802.1s	Declaration
	v.	Link-layer discovery protocol as per IEEE 802.1ab	Functional Verification
	w.	Logical Link Control (LLC) as per IEEE 802.2	Functional Verification
	X,	Flow Control as per IEEE 802.3x	Declaration
	y.	Link aggregation as per IEEE 802.3ad	Functional Verification
	z.	Static/LACP Link Aggregation Groups (LAG) on client ports	Declaration
	aa.	IGMPv2 and v3 as per RFC 2236 and 4604 respectively. (applicable for type Ito XII Routers)	Declaration
	bb.	PAT	Functional Verification
	cc.	NAT as per RFC 3022	Functional Verification
3.27.1 .2		The eMS shall support configuration of the following VLAN Parameters	Declaration
	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	Functional Verification
	b.	Configuration of VLAN bridging as per IEEE 802.1ad	Functional Verification
	c.	Configuration of user isolation per outer VLAN tag on a per port basis	Declaration
	d.	Enable/Disable VLAN ingress filtering, VLAN tag overlapping	Declaration
	e.	Insertion and removal of second tag	Declaration

	f.	Encapsulation translation and rewrites Push, Pop and translate for IEEE 802.1Q or Q-in-Q/IEEE 802.1ad tags.	Declaration
	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	Declaration
	h.	VLAN stacking	Declaration
	i.	S-VLAN tags and priority	Functional Verification
	j.	Q-in-Q as per IEEE 802.1Q	Functional Verification
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.	Functional Verification
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	Declaration
	b.	OSPF routes, adjacencies and areas	Functional Verification
	c.	Filtering route based on administrative costs	Declaration
	d.	Setting of Administrative costs, virtual links, area route aggregation, inter area route aggregation, route leaking	Declaration
	e.	BGP-OSPF interaction	Declaration
	f.	OSPF Not So Stubby Area (NSSA) as per RFC 3101	Declaration
	g.	OSPF Opaque LSA option as per RFC 5250	Declaration
	h.	OSPF for IPv6 as per RFC 5340	Functional Verification
	i	OSPF Stub Area	Declaration
	j.	OSPF graceful restart as per RFC 3630	Declaration
	k.	OSPF Sham Links	Declaration
3.27.2.3		The eMS shall support configuration of the following FRR & BFD features	Declaration
	a.	Fast Reroute Extensions to RSVP-TE for LSP Tunnels as per RFC 4090	Declaration
	b.	Bidirectional Forwarding Detection (BFD) as per RFC5880, 5881, 5883	Functional Verification
3.27.2.4		The eMS shall support configuration of the following BGP features	Declaration
	a.	BGPv4 as per RFC 4271, RFC 2283	Declaration
	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	Declaration
	c.	Transparent LAN using BGP	Declaration
	d.	Encryption of BGP peering session	Declaration
	e.	Default route to individual BGP peers	Declaration
	f.	Soft reset the BGP session on any or all peers	Declaration
	g.	Policy Routing to enable flexibility in making changes to the normal routing process based on the characteristics of the traffic	Declaration
	h.	Multiple BGP sessions	Declaration
	i.	Ingress and egress route filtering	Declaration
	j.	Weight metric, Local Pref metric and Multi Exit Discriminator (MED) metric	Declaration

	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	Functional Verification
	l.	Interior BGP (iBGP) peering with other border routers	Functional Verification
	m.	Exterior BGP multi-path support-to-support load balancing	Functional Verification
	n.	Multi Protocol BGP (MP BGP) as per RFC4760	Functional Verification
	o.	Next Generation Multicast VPN features (MVPN using MP-BGP)	Declaration
	p	BGP for Load balancing	Declaration
	q.	BGP Route Reflection (RR) as per RFC 4456	Functional Verification
3.27.2 .5		The eMS shall support configuration of the following Multicast features	Declaration
	a.	Prioritization of multicast traffic	Functional Verification
	b.	Multicast table	Declaration
	c.	Multicast ACL	Declaration
	d.	Multicast Load Balancing traffic across multiple interfaces	Functional Verification
	e.	Administratively Scoped IP Multicast	Declaration
	f.	IPv4 Multicast address space as per RFC 2365	Declaration
	g.	Internet Group Management Protocol, Version 3 as per RFC 3376	Declaration
	h.	Source based and shared distribution trees	Declaration
	i.	Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) as per RFC 3446	Declaration
	j.	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) as per RFC 5059	Declaration
	k.	Protocol Independent Multicast - Sparse Mode (PIM-SM): as per RFC 4601	Functional Verification
	l.	Rendezvous Point (RP) on both leaf and non-leaf nodes	Declaration
	m.	Multicast Source Discovery Protocol (MSDP) as per RFC 3618	Declaration
	n.	Bootstrap Router Mechanism for PIM Sparse Mode	Declaration
	o.	PIM Source Specific Multicast (PIM-SSM) as per RFC 3569	Declaration
	p.	Source-Specific Multicast for IP as per RFC 4607	Declaration
	q.	Operation of Anycast Services	Declaration
	r.	Dynamic broadcast Source Failover using Anycast routing	Declaration
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	Declaration
	a.	Various MPLS Configurations as per RFC3813, RFC 3031, 3032, 3443	Declaration
	b.	Static & dynamic MPLS LSP Configurations & LSP Path optimizations	Functional Verification
	c.	Generalized TTL Security Mechanism (GTSM) as per RFC5082	Declaration
	d.	Configuration / mappings of MPLS class of service	Functional Verification
	e.	Limiting the number of routes per VRF	Declaration
	f.	Set Thresholds to provide traps and alarms when a certain number of routes are exceeded	Declaration
	g.	LDP attributes as per RFC5036, 3037, 3478	Functional Verification
	h.	Generic Virtual Private Networks Configurations as per RFC 4364	Declaration

	i.	L2VPN Configurations as per RFC 4664, 4665, 4906	Functional Verification
	j.	VPLS, H-VPLS, VPWS, EoMPLS, multi-segment PWS and Pseudo wire redundancy	Functional Verification
	k.	Disable learning, FIB size limit on a per VPLS service basis	Declaration
	l.	Creation, selection, and registration of an Autonomous System (AS) (Private and	Declaration
		overlapping Autonomous System Numbers) as per RFC1930	
	m.	Inter AS/Inter VPN configurations as per RFC4364	Declaration
	n.	Enable cRTP as per RFC2508	Declaration
	o.	MPLS Auto-bandwidth	Declaration
	p	LSP Mode Scalability Options through VPLS using LDP as per RFC4762	Declaration
	q.	MPLS-TP configurations as per G.8110, G.8112, RFC6371, 5860, 5950, 5951	Functional Verification
	r.	MPLS-TP survivability framework configurations as per RFC 6372 or ITU-T G.8131/G.8132	Declaration
	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	Declaration
3.27.3.2		**The eMS shall support Fault Management features of MPLS**	
	a.	MPLS based Recovery as per RFC 3469	Declaration
	b.	MPLS-TP fault management parameters as per RFC 5884 and 4379 or G.8121	Functional Verification
	c.	MPLS-TP fault management parameters as per RFC 5860 or ITU Y.SUP4	Functional Verification
	d.	MPLS-TP fault management parameters RFC 5586 or ITU G.8113.1	Functional Verification
	e.	MPLS-TP Fault OAM as per RFC 6427 or ITU G.8113.1 / G.8113.2	Declaration
	f.	Ethernet OAM, Connectivity Fault Management (CFM) as per IEEE 802.3ah, IEEE 802.1ag	Declaration
	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	Declaration
	h.	Connection verification for MPLS Transport Profile LSP as per RFC 6428	Functional Verification
	i.	If any performance bounds (Frame Delay, Frame Delay Variation, and Frame Loss) are exceeded, the alarm shall be raised in the eMS	Declaration
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	Functional Verification
	b.	MPLS-TP OAM based on Y.1731	Functional Verification
	c.	Measurement of delay, Jitter, Ethernet alarm signal and Ethernet test signal function	Functional Verification
	d.	Set end-to-end performance bounds for Frame Delay, Frame Delay Variation, and Frame Loss for each flow	Declaration
	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	Functional Verification
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	Functional Verification
	ii.	Create traffic classes based on their property, such as, voice, video, data, priority	Functional Verification
	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)	Functional Verification
	iv.	Assign traffic classes to each customer (VLAN ID)	Functional Verification
	v.	Assign CIR, EIR, CBS, and EBS template to each customer (VLAN ID).	Functional Verification
	vi.	Define CIR, EIR, CBS and EBS for storm suppression (Broadcast/Multicast).	Functional Verification
	vii.	Assign storm suppression control on each port	Declaration
	viii.	CIR/EIR to be configured in steps of 1Mbps	Functional Verification
	ix.	User bandwidth is to be configured in steps of	Functional Verification
		• 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	Functional Verification
	xi.	Define trust boundary by trusting the interfaces in the network	Declaration
	xii.	Classify the incoming packet based on DSCP value	Functional Verification
	xiii.	Assign traffic class QoS profiles to the interfaces	Functional Verification
	xiv	Define Policy Control List. Configure rule and corresponding action for the following	
		• IEEE 802.1p values (0 to 7)	Functional Verification
		• VLAN ID	Functional Verification
		• Source MAC address	Functional Verification
		• Destination MAC address	Functional Verification
		• Ether Type or Protocol	Functional Verification
		• Incoming/Destination IP address and mask	Functional Verification
		• Source/Destination TCP/UDP Port	Functional Verification
		• Type of Service (ToS) Precedence bits.	Functional Verification
		• UDP/TCP socket	Functional Verification
		• Default queue for non-matching traffic	Functional Verification
	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]	Declaration
	xvi.	Modify QoS profile mapping (DSCP, COS/User Priority, EXP, Drop Precedence, Traffic Class)	Declaration

	xvii.	Configure marking/shaping scheme, such as, Single Rate Two Color or Two Rate Three Color marking scheme	Declaration
	xviii	Configure meter as Color blind or color aware	Declaration
	xix	Define congestion avoidance management – Configure dropping mechanism, such as, Tail Drop, WRTD (Weighted Random Tail Drop), WRED, Selective Packet Discard etc	Declaration
	xx.	WRTD-Configure No of masking bits	Declaration
	xxi.	WRED-Configure Thresholds for Dropping the traffic (Minimum threshold, Maximum threshold)	Functional Verification
	xxii.	Define queues on each port, queue buffer size and their priority group (Strict Priority, DRR, SDWRR).	Functional Verification
	xxiii	Configure queuing mechanism on each port, such as, SPQ – Strict Priority Queuing, WFQ – Weighted fair Queuing.	Functional Verification
	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.	Functional Verification
	xxv.	Configure weights for the WRR/SDWRR/MDRR/WFQ queues	Functional Verification
	xxvi.	Configure Shapping Rate on port wise or queue wise	Declaration
	xxvii	Define customer profile for Hierarchical QOS based on	Functional Verification
		• 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	Functional Verification
	xxix	Define bandwidth profile for different types of Category – Gold, Silver, Bronze	Functional Verification
3.27.4.2		**The eMS shall support the following Traffic Engineering configuration management features**	
	i.	End-to-End traffic tunnels with 2Mbps granularity	Functional Verification
	ii.	Multiple paths for a TE tunnel to provide protection	Functional Verification
	iii.	Modify/re-optimize TE tunnels	Declaration
	iv.	Options for automatic and manual selection of TE path	Declaration
	v.	LSP based Traffic Engineering as per RFC 5654	Functional Verification
	vi.	VLAN Tunnel based Traffic Engineering as per IEEE 802.1Qay	Functional Verification
	vii.	Bandwidth management feature both for Compression and Filtering	Declaration
	viii.	Traffic Engineering Over MPLS as per RFC 2702	Declaration
	ix.	Traffic parameter attributes (peak rates, average rates, permissible burst size, etc.)	Functional Verification
	x.	Generic path selection and management attributes	Declaration
		• 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	Declaration

	Xii.	Preemption attribute (preemptor enabled, non-preemptor, preemptable, and non-preemptable)	Declaration
	xiii.	Resilience Attribute	Declaration
	xiv.	Policing attribute	Declaration
	xv.	Resource Attributes	Declaration
	xvi.	Maximum Allocation Multiplier	Declaration
	xvii.	Resource Class Attribute	Declaration
	xviii.	Dynamic MPLS Traffic Engineering	Declaration
	xix.	Traffic Engineering Extensions to OSPF Version 2 as per RFC 3630	Declaration
	xx.	Router Address TLV	Declaration
	xxi.	Configure Link TLV	Declaration
		• 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	Declaration
	xxiii.	Extended IS Reachability TLV	Declaration
		• Administrative Group (color, resource class)	
		• IPv4 Interface Address	
		• IPv4 Neighbor Address	
		• Maximum Link Bandwidth	
		• Maximum Reservable Link Bandwidth	
		• Unreserved Bandwidth	
	xxiv.	Extended IP Reachability TLV	
	xxv.	OSPF inter area MPLS Traffic Engineering	Declaration
	xxvi.	IGP Traffic Engineering database for Constraint Based Shortest Path First (CSPF) calculations for tunneling	Declaration
	xxvii.	Priorities for TE tunnels	Functional Verification
	xxviii.	RSVP as per RFC 2205	Declaration
	xxix.	RSVP to provide the label distribution and capability to do CSPF signaling based on the IGP link state database	Declaration
	xxx.	IGP Area tunneling for RSVP	Declaration
	xxxi.	Traffic control and policy control parameters	Declaration
	xxxii.	Interfaces to support RSVP-TE signaling	Declaration
	xxxiii.	Aggregation of Martini circuits within an RSVP – TE tunneled LSP	Declaration
	xxxiv.	RSVP and RSVP-TE Extensions to RSVP for LSP Tunnels as per RFC 3209	Declaration
	xxxv.	Configure reservation styles	Declaration
		• Fixed Filter (FF) Style	Declaration
		• Wildcard Filter (WF) Style	Declaration
		• Shared Explicit (SE) Style	Declaration
	xxxvi.	Define administrative policy to Rerouting Traffic Engineered Tunnels	Declaration

	xxxvii.	MPLS Fast Reroute Extensions to RSVP-TE for LSP Tunnels, as per RFC 4090	Declaration
	xxxviii.	RSVP Refresh Reduction Extensions as per RFC 2961	Declaration
	xxxix.	Pseudo-Wire Emulation	Functional Verification
	xL	Pseudo-Wire Emulation Edge-to-Edge (PWE3) as per RFC 3916, 3985	Declaration
	xLi	PWE3 Control Word for Use over an MPLS PSN as per RFC 4385	Declaration
	xLii.	Encapsulation Methods for Transport of Ethernet over MPLS Networks as per RFC 4448	Declaration
	xLiii.	Pseudo wire Setup and Maintenance using LDP as per RFC 4447	Declaration
	xLiv.	Pseudowire (PW) Management Information Base (MIB) as per RFC 5601	Declaration
	xLv.	Point-to-Multipoint (P2MP) LSP	Declaration
	xLvi.	Point to Multipoint MPLS TE LSPs	Declaration
	xLvii.	Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs) as per RFC 5601	Declaration
	xLviii.	M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs) as per RFC 5120	Declaration
	xLix.	MPLS Support of Differentiated Services as per RFC 3270	Functional Verification
	L.	Support of Differentiated Services-aware MPLS Traffic Engineering as per RFC 3564	Declaration
	Li.	Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering as per RFC 4124	Declaration
	Lii.	Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering	Functional Verification
	Liii.	Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering as per RFC 4127	Functional Verification
	Liv.	Bandwidth profiles (CIR, EIR, CBS, and EBS) for each LSP	Declaration
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	Functional Verification
	b.	No of packets dropped for each class of service	Functional Verification
	c.	Bandwidth utilization of each link	Functional Verification
	d.	Bandwidth Management Report	Declaration
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)	Functional Verification
	ii.	Grooming of SDH under CESoPSN options from multiple interfaces including combining fractional E1	Declaration
	iii.	Change of Parameters of SAToP interface like VCID, Tunnel Label etc	Functional Verification
	iv.	Change of Parameters of CESoPSN interfaces	Functional Verification
	v.	View of the configuration of all the interfaces	Functional Verification
3.27.5.2		The eMS shall support the following Circuit Emulation fault management features	Declaration
	i.	Test Loop back at different granularities at different interfaces from different locations like near end, far end, intermediate locations	Functional Verification

	ii.	Detection of various types of defects in SAToP interfaces like Stray Packets, Malformed Packets, Excessive Packet Loss rate, Buffer Overrun, Remote Packet Loss	Functional Verification
	iii.	Detection of various types of defects in CESoPSN interfaces like misconnection, mistype, loss of packets, loss of synchronisation etc	Functional Verification
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	Functional Verification
3.27.6		**Synchronisation**	
3.27.6.1		The eMS shall support the following Synchronisation configuration management features	Declaration
	i	Selection of I, II, III, IVth frequency synchronisation reference	Declaration
	ii	(External, TDM Interface, IP Interface (SyncE), Holdover mode etc)	Declaration
	iii.	Manual change of Frequency synchronisation reference	Declaration
	iv.	PTP reference assignment (Primary, Secondary etc) for 1588v2 Phase sync	Functional Verification
	v.	NTP Server (Primary/Secondary) Assignment	Functional Verification
3.27.6.2		The eMS shall support the following Synchronisation fault management features	
	i.	Set limits for Frequency synchronisation accuracy	Declaration
	ii.	Frequency Synchronisation Alarm: When the synchronisation exceeds the limits, Signal fail etc	Declaration
	iii.	PTP Error Message	Declaration
	iv	NTP Error Message	Declaration
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]	Functional Verification
	ii.	G.8032 Ring protection configuration	Functional Verification
	iii.	MPLS-TP Linear Protection configuration requirements as per IETF standards OR Ethernet/MPLS SNC based protection as per ITU-T standards	Functional Verification
3.28		**VPN Management**	
3.28.1		The eMS shall support efficient provisioning of VPN services across the network with the following functions	Declaration
	a.	VPN Provisioning	Declaration
	b.	VPN Data Collection	Declaration
	c.	VPN Management Tool	Declaration
3.28.2		**VPN Provisioning**	Declaration
		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:	Declaration
3.28.2.1		The VPNMS (eMS) shall support Step-by-step Information-assisted population of templates	Functional Verification
3.28.2.2		The VPNMS (eMS) shall support Operators who shall add, delete, or modify customer VPNs. They shall set up extranet relationships	Functional Verification
3.28.2.3		The VPNMS (eMS) shall support templates shall be converted into appropriate commands and shall be downloaded to the network	Functional Verification

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	Functional Verification
	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	Declaration
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	Declaration
3.28.2 .7		The VPNMS (eMS) shall support smart collection whereby the VPNMS collects only changed configuration files from the Routers	Declaration
3.28.2 .8		The VPNMS (eMS) shall support display of VPN topology with following	Functional Verification
	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	Functional Verification
3.28.2 .10		The eMS shall support generation of SLA reports with annually, monthly, weekly, hourly time-scales. Following reports can be generated	Functional Verification
	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	Functional Verification
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	Declaration
3.28.2 .13		The VPNMS (eMS) shall support generation of following accounting reports:	Declaration
	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	Functional Verification
	b.	Application Type Summary Report – To provide total packets and total K bytes for each application type	Functional Verification
	c.	Customer Summary Report – To provide total packets and total KB for each customer plus additional reports for customer site and application type	Functional Verification
	d.	PE to PE Traffic Summary Report – Reports on all traffic between PE to PE, plus additional reports for the following	Functional Verification

	i.	PE to connected CE	Declaration
	ii.	PE to remote CE	Declaration
	iii.	PE traffic and	Declaration
	iv.	PE to CE	Declaration
	e.	CE to CE Traffic Summary Report-Reports on all traffic between CE to CE	Functional Verification
	f.	Type of Service Summary Report-Provides total packets and total KB for each type of service	Functional Verification
	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)	Functional Verification
	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)	Functional Verification
	i.	Traffic Volume (PE-CE) Report-Provides Information on all traffic between PE to (by type of service)	Functional Verification
3.28.2.14		The VPNMS (eMS) shall support third party tools for the following	Declaration
	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	Declaration
	a.	Data Collection shall be done at each Provider Edge location	Functional Verification
	b.	Import of traffic flow data from the PE Router which consist of following attributes	Functional Verification
	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	Functional Verification
	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	Declaration
	e.	Support for script files to be invoked for further processing	Declaration
	f.	Shall support unsolicited event notification to generate messages on encountering errors	Declaration
	g.	Export of data to the VPN Provisioning function	Declaration
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	Declaration

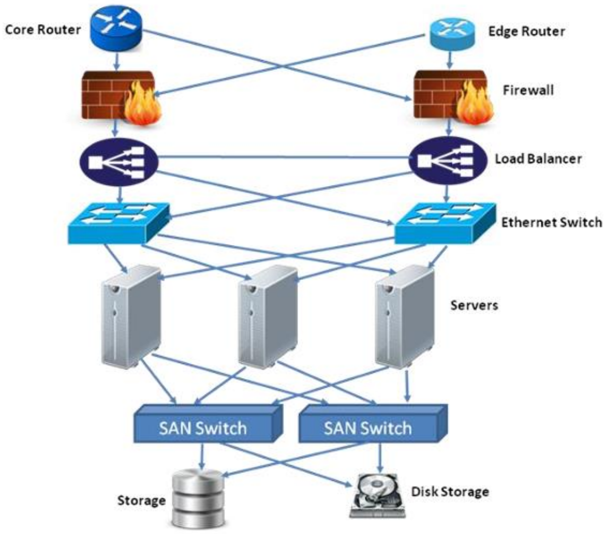
3.28.4 .1		Template based automatic configuration generation to enable configuration and provisioning of any managed network services like MPLS VPN	Functional Verification
3.28.4 .2		Multiple discrete customer networks that use the same unregistered IP address ranges	Functional Verification
3.28.4 .3		Telnet Gateway Server to allow download of configuration files to CE & PE Routers	Functional Verification
3.28.4 .4		The system administration function allows user-based authentication	Functional Verification
3.28.4 .5		GUI based operation to support following tools	Declaration
	a.	Element Manager - creates and manages domains and elements (including uploading of configurations generated in the template manager).	Functional Verification
	b.	Template Manager - Creates and manages templates and template data, and for generation of configurations	Functional Verification
	c.	Log Viewer - views records of system activity, allowing sorting on various criteria	Functional Verification
	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	Functional Verification
	e.	Permission Manager - creates and manages permission group (the means by which users are given access rights)	Functional Verification
	f.	User Manager – manages individual users	Functional Verification
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	Functional Verification
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 either of the following methods	Declaration
	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	Declaration
	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	Declaration
	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	Declaration
	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	Declaration
	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	Declaration
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	Functional Verification
	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	Functional Verification
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	Functional Verification
3.29.3		Features: The SLA Management system shall support the following features	Functional Verification
	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	Declaration
3.29.5		The SLA Management system shall be capable of extending support to additional services required in the future	Declaration
3.29.6		The SLA Management system shall provide service metrics to be defined using Key Quality Indicators (KQIs)	Functional Verification
3.29.7		The SLA Management system shall provide resource metrics to be defined using Key Performance Indicators (KPIs)	Functional Verification
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	Functional Verification
3.29.9		The SLA Management system shall have the capability to use various mathematical and logical operations for calculating KQI and KPI metrics	Functional Verification
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	Declaration
	b.	Fault data sources for relevant alarms	Declaration
	c.	Operational data sources like trouble tickets	Declaration
3.29.11		The SLA Management system shall allow defining thresholds to detect SLA violations	Functional Verification
3.29.12		The SLA Management system shall generate service quality alerts when anomalies are detected based on a comparison to historical KQI trends	Functional Verification
3.29.13		The SLA Management system shall allow different thresholds to be configured for different times of day	Functional Verification
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)	Declaration
3.29.15		The SLA Management system shall collect data via standards-based, open interfaces	Declaration

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	Functional Verification
3.29.17		The SLA Management system shall use trouble ticket data to compute key KQIs like the MTTR	Functional Verification
3.29.18		The SLA Management system shall compute availability KQIs using the fault data source	Functional Verification
3.29.19		The SLA Management system shall calculate availability KQIs to monitor for SLA violations	Functional Verification
3.29.20		The SLA Management system shallgenerate SLA violation Information in real time when a KQI/KPI threshold is violated so the Network Operation Center can be alerted to this condition	Functional Verification
3.29.21		The SLA Management system shall forward service quality alarms to other systems via SNMP	Declaration
3.29.22		The SLA Management system shall aggregate Service Quality Records over time on a per customer/service basis	Functional Verification
3.29.23		The SLA Management system shall create historical trends based on quality parameters	Functional Verification
3.29.24		In response to a threshold violation, it shall provide following automatic task	Declaration
	a.	Generate an alert	Declaration
	b.	Forward an email/SMS	Declaration
	c.	Execute a customized script	Declaration
3.29.25		The SLA Management system shall provide viewing and editing displays of Service Definitions	Functional Verification
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	Declaration
3.29.27		The SLA Management system's dashboard shall provide instant visibility to potential alerts in the services	Declaration
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	Declaration
3.29.29		The SLA Management system shall provide user-configurable reports indicating SLA compliance on a per-customer basis	Functional Verification
3.29.30		The SLA Management system shall provide option for the scheduling of reports	Functional Verification
3.29.31		The SLA Management system shall provide reports to users via a web-based interface	Functional Verification
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	Functional Verification
3.29.33		The SLA Management system shall deliver network management reports via a secure Web site	Functional Verification
3.29.34		The SLA Reports include latency, packet loss, jitter, error apart from the availability and the link utilization reports	Functional Verification
3.29.35		It shall generate detailed and summary reports for all the above parameters. The reports are customer friendly	Declaration
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	Functional Verification

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	Functional Verification
3.29.38		The SLA Management system shall store all collected service quality data with a timestamp including the date and time received	Functional Verification
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	Declaration
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	Declaration
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	Functional Verification
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	Declaration
3.29.43		The SLA Management system shall provide a real-time availability based service management view	Declaration
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	Functional Verification
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	Functional Verification
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	Functional Verification
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	Declaration
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	Declaration
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	Functional Verification
3.30.2		The provisioning management system shall support consistent and simplified service activation methodology across services	Functional Verification
3.30.3		The provisioning management system shall allow one touch network / service provisioning for all the services as mentioned in the earlier sections	Functional Verification
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	Functional Verification
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)	Functional Verification

3.30.6		The provisioning management system shall maintain a real-time database of the existing customer / services / resources	Functional Verification
3.30.7		The provisioning management system shall support remote software and configuration upgrades/ downgrades for large number of Nes	Functional Verification
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	Functional Verification
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	Functional Verification
3.30.1 0		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	Functional Verification
3.30.1 1		The provisioning management system shall provide GUI-based features for all applications such as system configuration, service provisioning etc	Functional Verification
3.30.1 2		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	Functional Verification
3.30.1 3		The provisioning management system shall configure the physical and logical connections of the core, aggregation and access	Functional Verification
3.30.1 4		The provisioning management system shall perform auto discovery features as following	Declaration
	a.	Underlying Transmission Technology	Declaration
	b.	IP Device Type (Layer 2 and Layer 3)	Declaration
	c.	Routing / Signaling /MPLS Protocols	Declaration
	d.	Device Information e.g. Cards, Ports, Interfaces, IP addresses, MAC addresses, etc	Declaration
	e.	Device Physical and Logical Connectivity	Declaration
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.	Functional Verification
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	Lab Test - Refer Test No. 19 of Compendium
	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:	Declaration
	a.	Protocol details at all layers of TCP/IP stack	Declaration
	b.	PHY I/F at each layer	Declaration
	c.	Database structures	Declaration
	d.	Number formats	Declaration
	e.	Node addressing system	Declaration
	f.	Complete application software details etc	Declaration
	g.	eMS software check-sum	Declaration

3.33		**eMS Hardware Requirements**	
3.33.1		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	Declaration
		 Core Router Edge Router Firewall Load Balancer Ethernet Switch Servers SAN Switch SAN Switch Storage Disk Storage **Figure 13: Typical Redundant eMS Network Architecture**	Declaration
3.33.1 .1		The Core/Edge router shown in figure is the existing or the being deployed MPLS Network of the Service Provider	Information
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	Information
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	Information
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	Information
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	Information
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	Information
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	Information
3.33.1 .8		The Type of server required shall be specified by the purchaser	Information
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	Information
3.33.1 .10		The eMS solution runs in high availability mode with redundancy i.e. N+1 (Active or Passive) configuration	Declaration
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	Declaration

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	Declaration
4		**INTERCONNECTIVITY & INTER-OPERABILITY REQUIREMENTS**	
		This chapter describes the interface, interconnectivity and inter-operability requirements for the Routers.	
		Interface Requirements	
4.1		The router shall be capable of supporting the following types of interfaces. However the actual number of interfaces shall be decided by the purchaser	Declaration
			Declaration
		,	
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	

xxiii.		2.5G BASE-T Electrical Interface		
xxiv.		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		Declaration
	b.	The Router shall be based on commercially available pluggable (CFP/QSFP28/QSFP+/QFP/SFP/XFP) optics for all optical interfaces		Declaration
	c.	The Router shall support full duplex capabilities on all Ethernet ports		Declaration
	d.	The Router shall support to monitor transmit and receive power on all optical interface ports on the Router		Declaration
	e.	The interface cards shall be hot pluggable on chassis based Routers		Declaration
4.2.2		**100G Optical Interface**		
4.2.2. 1		**Specifications**		
		Window of operation	Around 1300 nm	Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Data Rate in each lane	25.78125Gbps	
		Mean launch power, each Lane	-4.5 to +4.5 dBm	Output power Test-Refer Lab. Test No. 11 of Compendium
		Distance coverage	10/40 Km	Receiver Senstivity-Refer Lab. Test No. 13 of Compendium
4.2.2. 2		The 100G interface shall be as per IEEE 802.3ba standard		Declaration
4.2.2. 3		The interface shall be based on QSFP28, CFP or CPAK		Declaration
4.2.3		**40G Optical Interface**		
4.2.3. 1		**Specifications**		
		Window of operation	Around 1300 nm	Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Data Rate in each lane	10 Gbps	
		Mean launch power, each Lane	-4.5 to +4.5 dBm	Output power Test-Refer Lab. Test No. 11 of Compendium
		Distance coverage	10 Km	Receiver Senstivity-Refer Lab. Test No. 13 of Compendium
4.2.3. 2		The 40G interface shall be as per IEEE 802.3ba standard		Declaration
4.2.3. 3		The interface shall be based on QSFP+/QFP or CFP		Declaration
4.2.4		**10G Optical Interface**		

4.2.4. 1		**Specifications**				
		Wavelengths		850nm, 1310 nm and 1550 nm windows		Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Wavelength		Wideband / Narrow Band (Coloured λ interface to DWDM) (Purchaser shall specify the wavelength required)		
		Distance Coverage		300m/10Km/40Km/80Km		Optical Output Power and Receiver Sensitivity-Refer Lab. Test No. 11 and 13 of Compendium
		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		Declaration
		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		Declaration
		Fiber		G.652 single mode		Declaration
		10G Interface Type	**Distance**	**Wavelength**	**Avg. Launch Power (dBm)**	
		10GBASE-SR/SW	300m	850 nm	-7.3 to -1.0	Receiver sensitivity-Refer Lab. Test No. 13 of Compendium
						Optical spectrum-Refer Lab. Test No. 12 of Compendium
						Output power Test-Refer Lab. Test No. 11 of Compendium
		10GBASE-LR/LW	10 km	1310 nm	-8.2 to 0.5	Receiver sensitivity-Refer Lab. Test No. 13 of Compendium
						Optical spectrum-Refer Lab. Test No. 12 of Compendium

						Output power Test-Refer Lab.
						Test No. 11 of Compendium
		10GBASE-ER/EW	40 km	1550 nm	-4.7 to 4.0	Receiver sensitivity-Refer Lab. Test No. 13 of Compendium Optical spectrum-Refer Lab. Test No. 12 of Compendium Output power Test-Refer Lab. Test No. 11 of Compendium
		10GBASE-ZR	80 km	1550 nm	0 to 4	Receiver sensitivity-Refer Lab. Test No. 13 of Compendium Optical spectrum-Refer Lab. Test No. 12 of Compendium Output power Test-Refer Lab. Test No. 11 of Compendium
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				Declaration
	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				Declaration
	c.	The Router shall support Optional direct coupling to MUX input of third party DWDM system through colored λ interface				Declaration
	d.	The interface shall be based on SFP+ or XFP				Declaration
4.2.5		**1G Optical Interface**				
4.2.5.1		**Specifications**				
		Wavelength		850nm multimode, 1310 nm/1550 nm single mode		Optical spectrum-Refer Lab. Test No. 12 of Compendium
		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.		Declaration

		Distance Coverage(Multimode)			500 m		Optical Output Power and Receiver Senstivity-Refer Lab. Test No. 11 and 13 of Compendium
		Distance Coverage(Single Mode)			10/40/70 km. SFP+		Optical Output Power and Receiver Senstivity-Refer Lab. Test No. 11 and 13 of Compendium
	4.2.5.1	**1G Interface Type**	Fiber	**Dist.**	**wavelength**	**Avg. Launch Power (dBm)**	
		1GBASE-SX	MM	200-500M	850 nm	-9 to -3	Receiver Senstivity-Refer Lab. Test No. 13 of Compendium
							Optical spectrum-Refer Lab. Test No. 12 of Compendium
							Output power Test-Refer Lab. Test No. 11 of Compendium
		1GBASE-LX	SM	10 KM	1310 nm	-9 to -3	Receiver Senstivity-Refer Lab. Test No. 13 of Compendium
							Optical spectrum-Refer Lab. Test No. 12 of Compendium
							Output power Test-Refer Lab. Test No. 11 of Compendium
		1GBASE-EX	SM	40 KM	1310 nm	-5 to 0	Receiver Senstivity-Refer Lab. Test No. 13 of Compendium
							Optical spectrum-Refer Lab. Test No. 12 of Compendium
							Output power Test-Refer Lab. Test No. 11 of Compendium
		1GBASE-LX	SM	70 KM	1550 nm	-2.0 to + 3.0	Receiver Senstivity-Refer

				Lab. Test No. 13 of Compendium Optical spectrum-Refer Lab. Test No. 12 of Compendium Output power Test-Refer Lab. Test No. 11 of Compendium
4.2.5.2		**Features**		
	a.	The Router shall support 1000BaseSX, 1000BaseLX, 1000BaseZX as per IEEE 802.3		Declaration
	b.	The Router shall support 1000BaseT as per IEEE 802.3ab, 1000Base SX/LX as per IEEE 802.3z		Declaration
	c.	The interface shall be based on SFP		Physical varification
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		Lab Test Refer Test No. 1 of Compendium Ethernet test, Refer Lab. Test No. 10 of Compendium
4.2.6.2		The interface shall be based on SFP		Physical varification
4.2.7		**STM-16 POS Optical Interface**		
4.2.7.1		**Specifications**		
		Wavelength	1310nm and 1550 nm windows	Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Distance Coverage	10 /40 km depending on type of SFP+	Optical Output Power and Receiver Senstivity-Refer Lab. Test No. 11 and 13 of Compendium
		Fiber	G.652 single mode	Declaration
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**		
		Wavelength	1310nm and 1550 nm windows	Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Distance Coverage	10 to 40 km depending on type of SFP+	Optical Output Power and Receiver Senstivity-Refer Lab. Test No. 11 and 13 of Compendium
		Fiber	G.652 single mode	Declaration
4.2.8. 2		**Features**		
	a.	The STM-1 POS interface shall support PPP, RFC 1661		Declaration
	b.	The STM-1 POS interface shall support ML-PPP		Declaration
4.2.9		**Channelised STM-1 Optical Interface**		
4.2.9. 1		**Specifications**		
		Wavelength	1310nm and 1550 nm windows	Optical spectrum-Refer Lab. Test No. 12 of Compendium
		Distance Coverage	10 /40 km depending on type of SFP+	Optical Output Power and Receiver Sensitivity-Refer Lab. Test No. 11 and 13 of Compendium

		Fiber	G.652 single mode	Declaration
4.2.9.2		**Features**		
	a.	Each Channelised STM-1 port shall support upto 63 E1 circuits		Lab Test - Refer Lab. Test No. 14 of Compendium
	b.	The E1 circuits may carry TDM traffic to be transported over Circuit Emulation or IP traffic		Declaration
	c.	Within the channelised STM-1 port, each logical E1 channel is configurable as unframed E1 and channelised E1		Functional Verification
	d.	The channelised STM-1 port shall support the IP protocol and the ppp encapsulation protocol		Declaration
	e.	The channelised STM-1 port along with all channelised E1 virtual ports shall support Multilink PPP (MLPPP) as per RFC 1990		Declaration
	f.	Channelized for PPP and MLPPP also		Declaration
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.		Lab test - refer test 5,6,7,8 of compendium
	b.	The E1 IP interface shall support Framed and Unframed.		Declaration
	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.		Declaration
	d.	The channelised E-1 port shall support the IP protocol and ppp encapsulation protocol		Declaration
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.		Lab test - refer test 5,6,7,8 of compendium
	b.	The E1 CE interface shall support Framed and Unframed.		Declaration
	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.		Declaration
	d.	Each channel shall carry TDM traffic to be carried using Circuit Emulation Protocols.		Declaration
4.2.12.		**10/100 Base-T Electrical Interface**		Lab Test – as per relevant test in compendium
4.2.12.1		The Router shall support 10/100 Base-T, 100mt, Full duplex, autosensing		Lab Test – as per relevant test in compendium
4.2.12.2		The interface shall be based on SFP		Declaration
4.2.13		***25 G Optical Interface** The specifications/limits/values of the interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures		Lab Test – as per relevant test in compendium
4.2.14		***50 G Optical Interface** The specifications/limits/values of the interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures		Lab Test – as per relevant test in compendium

4.2.15		***200 G Optical Interface** The specifications/limits/values of the Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures	Lab Test – as per relevant test in compendium
4.2.16		***400 G Optical Interface** The specifications/limits/values of the Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures	Lab Test – as per relevant test in compendium
4.2.17		***Fast Ethernet Optical Interface** The specifications/limits/values of the Ethernet interface are as per Annexure-H in Annexure to ERs document available in https://www.mtcte.tec.gov.in/annexures	Lab Test – as per relevant test in compendium
4.2.18		**45 Mbps Interface**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
4.2.20.1		The NX64 interface shall be as per ITU-T G.823, Annex-I	
4.2.21		**CDMA Interface**	Lab Test – as per relevant test in compendium
4.2.21.1		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**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
4.2.23.1		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**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium

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**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
4.2.28.1		The ADSLx interface shall be as per ETSI EN 300 001. Annex-J1	
4.2.29		**SHDSL Interface**	Lab Test – as per relevant test in compendium
4.2.29.1		The SHDSL interface shall be as per G.991.2. Annex-J1	
4.2.30		**VDSLx Interface**	Lab Test – as per relevant test in compendium
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**	Lab Test – as per relevant test in compendium
4.2.31.1		The ISDN BRI interface shall be as per Q.931, Annex-D1	
4.2.32		**ISDN PRI Interface**	Lab Test – as per relevant test in compendium
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	Declaration
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	Declaration
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	Functional Verification
	b.	MSPW	Functional Verification
	c.	VLAN hand over	Functional Verification
	d.	MPLS-TP and IP/MPLS interworking	Functional Verification
4.3.4		**Inter ISP:**	

4.3.4.1		Inter ISP Operations shall be as per RFC4364	Declaration
5.0		**Quality Requirement**	
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.	Declaration
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.	Declaration
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.	Declaration
6.0		**EMI/EMC REQUIREMENTS**	Report from Accredited Lab
		GENERAL ELECTROMAGNETIC COMPATIBILITY (EMC) REQUIREMENTS:	Information
		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.	Declaration
	a)	**Conducted and radiated emission (applicable to telecom equipment):**	Declaration
		Name of EMC Standard: "CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".	Declaration
		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	Declaration
	b)	**Immunity to Electrostatic discharge:**	Declaration
		Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".	Declaration
		Limits:- i) Contact discharge level 2 {± 4 kV} or higher voltage;	Declaration
		ii) Air discharge level 3 {± 8 kV} or higher voltage;	Declaration
	c)	**Immunity to radiated RF:**	Declaration
		Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".	Declaration
		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.	Declaration

	d)	**Immunity to fast transients (burst):**	Declaration
		Name of EMC Standard: IEC 61000-4-4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".	Declaration
		Limits:- Test Level 2 i.e. a) 1 kV for AC/DC power lines;	Declaration
		b) 0. 5 kV for signal / control / data / telecom lines;	Declaration
	e)	**Immunity to surges:**	Declaration
		Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test”.	Declaration
		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	Declaration
		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.	Declaration
	f)	**Immunity to conducted disturbance induced by Radio frequency fields:**	Declaration
		Name of EMC Standard: IEC 61000-4-6 (2013) with amendments) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio-frequency fields”.	Declaration
		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.	Declaration
	g)	**Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):**	Declaration
		Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”.	Declaration
		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)	Declaration
		ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and	Declaration
		iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.	Declaration
		iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10s.	Declaration
	h)	**Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):**	Declaration
		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.	Declaration
		Limits:- i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.	Declaration

		ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.	Declaration
		iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.	Declaration
		iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C.	Declaration
		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.	Declaration
		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:	Declaration
		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	Declaration
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..	Declaration
8		**SECURITY REQUIREMENTS**	
8.1		**Security Requirements for the Routers**	
8.1.1		**Port Address Translation (PAT)**	
8.1.1.1		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	Functional Verification
8.1.2		**Network Address Translation (NAT)**	Declaration
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	Functional Verification
8.1.3		**DHCP:**	
8.1.3.1		The Router shall support DHCP	Functional Verification
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	Declaration
8.1.3.3		The Router shall support Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Functional Verification

8.1.3.4		The Router shall support DHCPv6 prefix delegation	Declaration
8.1.3.5		The Router shall support DHCP for IPv6 relay agent	Declaration
8.1.3.6		The Router shall support DHCPv6 prefix delegation via AAA	Declaration
8.1.3.7		The Router shall support DHCPv6 Server Stateless Auto Configuration	Declaration
8.1.3.8		The Router shall support DHCPv6 relay - reload persistent interface ID option	Declaration
8.1.3.9		The Router shall support DHCP - DHCPv6 Individual Address Assignment	Declaration
8.1.3.10		The Router shall support DHCP IPv6 Prefix Delegation RFC 8415	Declaration
8.1.3.11		The Router shall support DNS Extensions to Support IP Version 6 as per RFC 3596	Declaration
8.1.3.12		The Router shall support DNS Configuration options for DHCPv6 as per RFC 3646	Declaration
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	Functional Verification
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	Declaration
8.1.4.3		The Router shall support Unknown Unicast Flood Blocking (UUFB)	Declaration
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	Functional Verification
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	Functional Verification
8.1.6.2		The Router shall support Dynamic ARP Inspection (IPv4 only)	Declaration
8.1.6.3		The Router shall support Neighbour Spoofing in IPv6	Declaration
8.1.6.4		The Router shall support IP/MAC address anti spoofing	Declaration
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	Functional Verification
8.1.8		**DOS Attacks:** The Router shall support Blocking IP DoS attacks from:	
	a.	Unknown Protocol	Declaration
	b.	UDP Short header/Flood	Declaration
	c.	TCP Packets without flag	Declaration
	d.	Oversized TCP packets	Declaration
	e.	SYN attack	Declaration
	f.	IP Spoofing	Declaration
	g.	IP Stream Option	Declaration
	h.	IP short header	Declaration

	i.	Internet Control Message Protocol (ICMP) Source quench /Mask request/ Mask reply/Large	Declaration
	j.	packet/Info Request and Reply/ Flood	Declaration
	k.	Too many fragments	Declaration
	l.	Call gapping	Declaration
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	Functional Verification
8.1.10		**Port Security:**	
8.1.10.1		The Router shall support Port Mirroring	Functional Verification
8.1.10.2		The Router shall support Port level security mechanism to prevent unauthorized nodes from accessing the switch	Declaration
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	Declaration
8.1.11		**Port Binding:**	
8.1.11.1		The Router shall support Dynamic binding of MAC address with port	Functional Verification
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.	Functional Verification
		It shall be possible to deny traffic based on the following:	
	a.	Source Interface type	Functional Verification
	b.	Source/ destination MAC	Functional Verification
	c.	VLAN ID	Functional Verification
	d.	Protocol Type (TCP/UDP/IP etc.)	Functional Verification
8.1.12.2		The Router shall support Access Control Lists for controlled SNMP Access only to the SNMP manager or the NMS workstation	Declaration
8.1.12.3		The Router shall support ACLs at layer 2-4 in hardware	Declaration
8.1.12		The Router shall support ACLs can limit telnet and SNMP access to the router	Declaration
.4			
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	Declaration
8.1.12.6		The Router shall support classification capabilities at line rate	Declaration
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	Declaration
8.1.12.8		The Router shall support Time based access list to control the usage of application and resource based on time parameters	Declaration
8.1.12.9		The Router shall support Standard access control lists for IPv6	Declaration
8.1.12.10		The Router shall support Extended access control lists for IPv6	Declaration

8.1.12 .11		The Router shall support IPv6 ACL extensions for IPSec authentication header (applicable for type I to XII Routers)	Declaration
8.1.12 .12		The Router shall support Secure Shell (SSH) support over IPv6	Declaration
8.1.13		**IPSec & Encryption**	
8.1.13 .1		The Router shall support IP Security (IPSec) for Management plane	Declaration
8.1.13 .2		The Router shall support site-to-site and remote access IPSec VPN & SSL VPN	Functional Verification
8.1.13 .3		The Router shall support security Architecture for the Internet Protocol as per RFC 4301	Declaration
8.1.13 .4		The Router shall support IP Authentication Header as per RFC 4302	Declaration
8.1.13 .5		The Router shall support IP Encapsulation Security Payload as per RFC 4303	Declaration
8.1.13 .6		The Router shall support IKEv2 as per RFC 5996	Functional Verification
8.1.13 .7		The Router shall support Local Key Distribution Function (LKDF) for delivering Authentication Keys	Declaration
8.1.13 .8		The Router shall support 3DES and other strong ESP cipher algorithms as per RFC 2451 and RFC 3602	Declaration
8.1.13 .9		The Router shall support Transport Layer Security (TLS) Protocol Version 1.2 as per RFC 5246	Declaration
8.1.13 .10		The Router shall support UDP Encapsulation of IPsec ESP Packets as per RFC 3948	Declaration
8.1.13 .11		IPv6 IPSec VPN	Functional Verification
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	Functional Verification
	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.	Declaration
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	Declaration
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	Functional Verification
	b.	Configure to control/limit multicast, broadcast, DLF traffic on per tunnel basis.	Declaration
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	Functional Verification
8.2.3		**Unicast Reverse Path forwarding (URPF):**	
	a.	Configuration of selected interfaces and users	Functional Verification
8.2.4		**DOS Attacks**	

	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	Functional Verification
8.2.5		**ICMP Rate limiting**	
	a.	Configurations to control the rate at which a user is able to ping any of its interface, logical or physical	Functional Verification
8.2.6		**Port Security**	
	a.	Port level security mechanism control configurations	Functional Verification
	b.	Configure to control port to port traffic	Functional Verification
8.2.7		**Port Binding**	
	a.	Port binding parameters configurations	Functional Verification
8.2.8		**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	Functional Verification
	b.	Configure Access Control Lists for controlled SNMP Access only to the SNMP manager or the NMS workstation.	Declaration
	c.	Configure ACLs to limit telnet and SNMP access to the router	Declaration
	d.	Configure Time based access list to control the usage of application and resource based on time parameters	Declaration
8.2.9		**IPSec & Encryption**	
	a.	IP Security (IPSec), IPSec VPN & SSL VPN configurations as per RFC4301, 4302, 4303, 3715, 3948	Declaration
	b.	Internet Security Association and Key Management Protocol (ISAKMP), Local Key Distribution Function (LKDF)configurations as per RFC5996	Declaration
	c.	IKE Keep alive configurations	Functional Verification
	d.	TLS Protocol configurations as per RFC5246	Declaration
8.2.10		**Lawful Interception / Port Mirroring**	
	a.	Configure local and remote Port mirroring over L2/L3 network with Option to filter incoming / outgoing traffic	Functional Verification
	b.	Configuration to mirror a particular service from a particular port or on per SVLAN/PW basis to a probe port	Declaration
	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].	Declaration
8.2.11		**Fault Management**	
	a.	Protocol anomaly detection alarms	Functional Verification
	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	Declaration
8.2.12		**Performance Management**	
	a.	Report any unauthorized activity	Declaration
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	Declaration
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	Functional Verification
	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	Functional Verification
	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	Declaration
8.3.1.5		The eMS system shall be protected against intentional or accidental abuse, unauthorized access and loss of communication	Declaration
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	Functional Verification
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	Declaration
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	Declaration
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	Declaration
8.3.2		**LOG Capturing/Analysis**	
8.3.2.1		The eMS shall support Collection of logs via either of the following methods	Functional Verification
	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	Declaration
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	Declaration
8.3.2.4		The eMS shall support support log compression capability for storage optimization (compression level at least 50%).	Declaration
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	Declaration
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	Declaration
8.3.2.7		Parting of logs or filtering of logs shall not be done at any stage of log collection or log storage	Declaration
8.3.2.8		The eMS shall support Single Global View of all the data across sites/geographies	Declaration
8.3.2.9		The eMS shall be scalable to support from 5000 devices up to 20000 devices	Declaration
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	Declaration
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	Declaration
8.3.2.12		The eMS shall support compliance to Regulations shall be supported with data archival	Declaration
8.3.2.13		Log parsing shall use only XML and shall not use any other proprietary parsing mechanisms	Declaration
8.3.2.14		The eMS shall support two factor authentications to login to the system	Declaration
8.3.2.15		The eMS shall support watch list feature to monitor desired data like specific IP addresses, usernames and other data	Declaration
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	Functional Verification
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	Declaration
8.3.3.3		The eMS shall categorize all event collected by device into event taxonomies for easier classification and management	Declaration
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	Declaration
8.3.3.5		The eMS shall support Alert suppression for specific events	Declaration
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	Declaration
8.3.3.7		The eMS shall support Email of scheduled reports to recipients	Declaration

8.3.3.8		Email notifications shall contain the content of the report capable of being saved as HTML and/or PDF	Declaration
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	Declaration
8.3.3.10		The eMS shall support facility to view Summary of all Dashboard views for the entire enterprise	Declaration
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	Declaration
8.3.3.12		The eMS shall support event display Window for all alerts	Declaration
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	Declaration
8.3.4		**Reporting**	
8.3.4.1		Reports shall be available for compliance and supported devices	Declaration
8.3.4.2		The system shall allow modification of existing reports and creation of new reports (through wizard).	Declaration
8.3.4.3		Reports shall be available in the following exported formats	Functional Verification
	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	Declaration
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	Declaration
8.3.4.6		The process shall allow applying filters and sorting to query results	Functional Verification
8.3.5		**Security Features**	
8.3.5.1		Log transaction between Client/Agent & Engine shall support SSL/encryption.	Functional Verification
8.3.5.2		The eMS shall have the 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	Declaration
8.3.5.3		Archival Information and summary Information shall be provided separately	Declaration
8.3.5.4		The eMS shall maintains audit trail for the management activities of individual users accessing and using the application	Declaration
8.3.5.5		The eMS shall support capability to create and assign role-based views	Functional Verification
8.3.5.6		The eMS shall support mechanism for protection of unauthorized access on the Log Database	Declaration
8.3.5.7		Incident status and escalation shall be supported and a record of action taken shall be maintained	Declaration
8.3.5.8		The eMS shall support Robust & scalable architecture to handle high volume of data with high Events per second	Declaration
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	Functional Verification

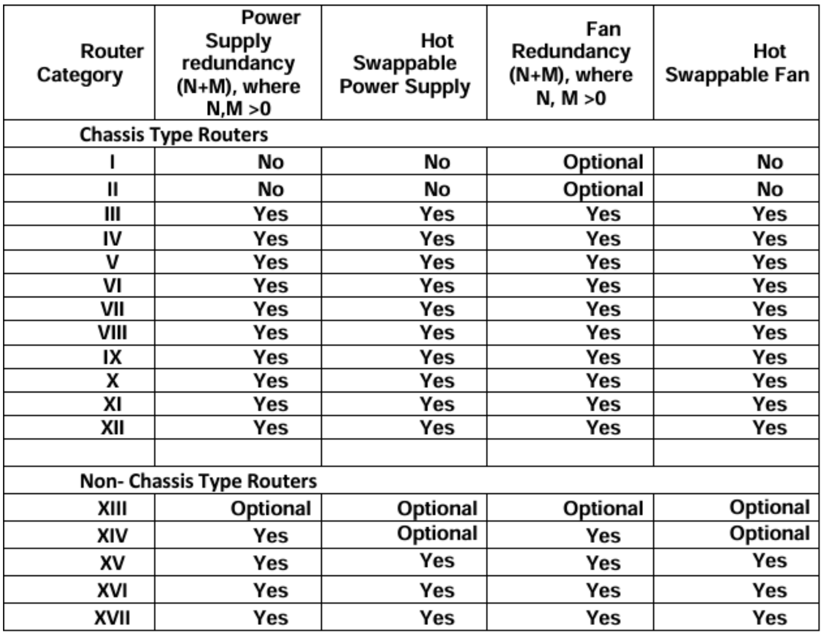
8.3.6.2		The eMS shall support following types of correlation	
	a.	Rule-Based correlation	Declaration
	b	Vulnerability Based Correlation	Declaration
	c.	Statistical Based	Declaration
	d.	Historical Based	Declaration
8.3.6.3		The eMS shall display summarization of events	Declaration
8.3.6.4		The eMS shall support rules for popular IDS, firewalls, antivirus, etc. The exact requirement to be specified by the purchasing authority vide clause10.4.1	Declaration
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	Declaration
8.3.6.6		The eMS shall support capability to correlate all the fields in a log without normalizing the logs at collection points	Declaration
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	Declaration
8.3.6.8		The eMS shall support 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	Declaration
8.3.7		**Forensic Capabilities**	Declaration
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	Functional Verification
8.3.7.2		The eMS shall support quick and easy access to real-time as well as historical operational data	Declaration
8.3.7.3		The eMS shall provide tool for comprehensive trend and historical analysis of logs and their reporting	Declaration
8.3.7.4		Following categories of predefined graphs and queries shall be supported	Declaration
	a.	Firewall, including Top Firewall Interface, File Access through Firewall, and Login Failure Summary	Declaration
	b	Database, such as Login Activity, Authorization Level and Authorization Level by User	Declaration
	c.	Intrusion detection, including Top Attack Signatures, Attack Type by Severity Level, and IDS Signature Summary	Declaration
	d.	Operations, such as Device Activity Analysis, Activity by Event Category, and	Declaration
		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	Declaration
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 manage 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	Declaration
8.3.8.2		The eMS shall support integration of DAS/NAS and SAN	Declaration

8.3.8.3		The eMS shall support entire Life Cycle management solution for log retention and purging after log retention period is over	Declaration
8.3.8.4		The eMS shall support Online and offline storage of logs which is needed for log retention	Declaration
8.3.8.5		The eMS shall enable offline storage of logs with automated tools for log purging and retrieval from offline storage	Declaration
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	Declaration
9		**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	Declaration
9.1.2		All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations	Declaration
9.1.3		All cables shall be of Gigabit Ethernet ready standards	Declaration
9.1.4		The equipment shall have adequate cooling arrangements	Declaration
9.1.5		The actual dimensions and weight of the equipment shall be furnished by the manufacturers	Declaration
9.2		**OPERATIONAL REQUIREMENTS** The system shall meet the following maintenance & operational requirements	
9.2.1		The equipment shall be designed for continuous operation	Declaration
9.2.2		The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level	Declaration
9.2.3		Suitable visual indications shall be provided, to indicate the healthy and unhealthy conditions	Declaration
9.2.4		The design of the equipment shall not allow plugging of a module in the wrong slot or upside down	Declaration
9.2.5		The removal or addition of any cards shall not disrupt traffic on other cards (applicable for type Chassis based Routers)	Declaration
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	Declaration
9.2.7		A power down condition shall not cause loss of connection configuration data storage	Declaration
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	Declaration
9.2.9		The system shall support built in power diagnostics system to detect hardware failures	Declaration
9.2.10		The router shall be 19"/ 23" Euro Rack Mountable	Physical
			varification
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	Declaration
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%	Declaration
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.	Declaration

9.3.3		The equipment power supply shall meet the following requirements	Declaration
	i.	The equipment shall be able to function over the range specified in the respective sections, without any degradation in performance.	Declaration
	ii.	The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity	Declaration
	iii.	The derived DC voltages shall have protection against short circuit and overload	Declaration
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.	Declaration
9.4		**INSTALLATION REQUIREMENTS**	
9.4.1		The equipment shall have	
	i.	Proper earthing arrangement	Declaration
	ii.	Protection against short circuit / open circuit	Declaration
	iii.	Protection against accidental operations for all switches / controls provided in the front panel	Declaration
	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.	Declaration
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	Information
9.6		**MINIMUM EQUIPMENTS FOR 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.	Information
	a.	One Router of the offered category	Information
	b.	Minimum two interfaces of each type as per the category of the Router	Information
	c.	eMS server with eMS software including optional items (In case required for the offered category)	Information
10		**DESIRABLE REQUIREMENTS**	
		This chapter 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.	Information
10.1		**DOCUMENTATION**	
10.1.1		All technical documents shall be in English language both in CD- ROM and in hard copy	Documentation
10.1.2		The documents shall comprise of	Information
	i.	System description documents	Information
	ii.	Installation, Operation and Maintenance documents	Information
	iii.	Training documents	Information
	iv.	Repair manual	Information

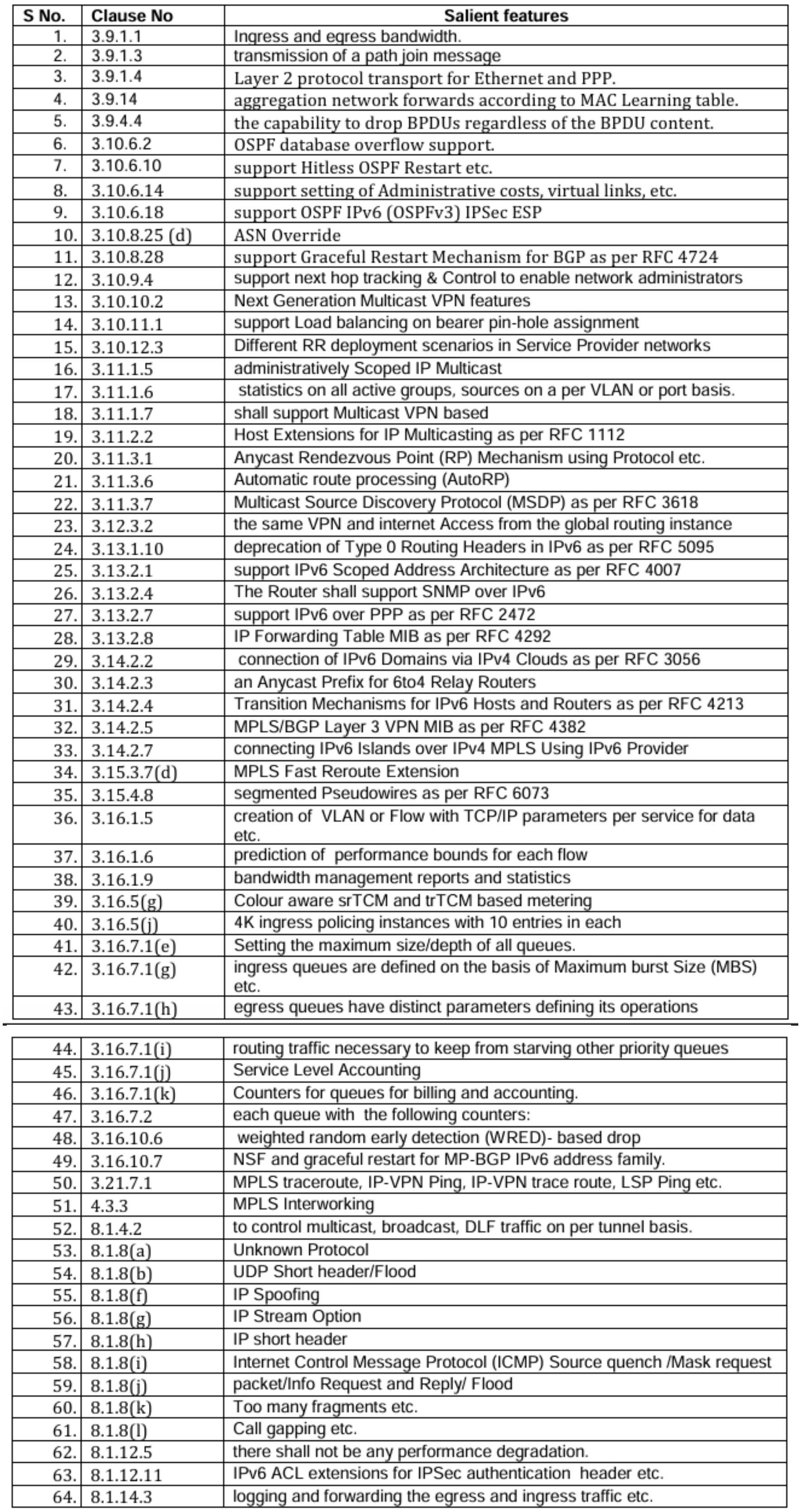
10.1.2 .1		**System description documents:** The following system description documents shall be supplied along with the system	
	i.	Over-all system specification and description of hardware and software	Documentation
	ii.	Equipment layout drawings	Documentation
	iii.	Cabling and wiring diagrams	Documentation
	iv.	Schematic drawings of all circuits in the system with timing diagrams wherever necessary	Documentation
	v.	Detailed specification and description of all Input / Output devices	Documentation
	vi.	Adjustment procedures, if there are any field adjustable units	Documentation
	vii.	Spare parts catalogue - including Information on individual component values, tolerances, etc. enabling procurement from alternative sources	Documentation
	viii.	Detailed description of software describing the principles, functions and interactions with hardware, structure of the program and data	Documentation
	ix.	Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data	Documentation
	x.	Program and data listings	Documentation
	xi.	Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification	Documentation
10.1.2 .2		**System operation documents:** The following system operation documents shall be available	
	i.	Installation manuals and testing procedures	Documentation
	ii.	Precautions for installation, operations and maintenance	Documentation
	iii.	Operating and Maintenance manual of the system	Documentation
	iv.	Safety measures to be observed in handling the equipment	Documentation
	v.	Man-machine language manual	Documentation
	vi.	Fault location and troubleshooting instructions including fault dictionary	Documentation
	vii.	Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement	Documentation
	viii.	Emergency action procedures and alarm dictionary	Documentation
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	Documentation
	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	Documentation
	iii.	The structure and scope of each document shall be clearly described	Documentation
	iv.	The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary Information	Documentation
	v.	All diagrams, illustrations and tables shall be consistent with the relevant text	Documentation
10.1.2 .4		**Repair Manual**	
	i.	List of replaceable parts used	Documentation
	ii.	Detailed ordering Information for all the replaceable parts	Documentation
	iii.	Procedure for trouble shooting and sub-assembly replacement	Documentation
	iv.	Test fixtures and accessories for repair	Documentation
	v.	Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions	Documentation

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.	Declaration
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.	Declaration
10.2.3		All installation materials, consumables and spare parts to be supplied.	Declaration
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.	Declaration
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.	Declaration
10.2.6		Special tools required for wiring shall be provided along with the equipment.	Declaration
10.3		**MAINTENANCE REQUIREMENTS:**	Information
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.	Declaration
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.	Declaration
10.4		**GUIDELINES FOR TENDERING AUTHORITY**	Information
10.4.1		**The tendering authority shall specify the following parameters:**	Declaration
	1.	Category of Router	Declaration
	2.	Type & Quantity of each Type of Interface i.e. 100G, 40G, 10G, 1G etc (refer to clause 4.1)	Declaration
	3.	Wavelength, Distance criteria etc of each type of optical interface	Declaration
	4.	Wide band / Narrow band (Cλ interface for working with DWDM) optical interface for 10GE	Declaration
	5.	Buffer type for 1GE/10GE interfaces for the Core Routers	Declaration
	6.	Type of Circuit Emulation Standard required to be supported in their network	Declaration
	7.	Requirement of advanced Ipv6 features	Declaration
	8.	Requirement of optional Security features	Declaration
	9.	Requirement of eMS	Declaration
	10.	Requirement of eMS network as per clause 3.33.1	Declaration
	11.	Requirement of eMS network redundancy and network elements	Declaration
	12.	Type of Firewall Required for the eMS	Declaration
	13.	Type of Load Balancer Required for the eMS	Declaration
	14.	Type of Ethernet Switch Required for the eMS	Declaration
	15.	Category and Type of Server Required for the eMS	Declaration
	16.	Type of Storage Required for the eMS	Declaration
	17.	Requirement of Optional eMS features	Declaration
	18.	Scalability requirements for the SLA Management system like no.of business customers, maximum leads per customer etc may be provided	Declaration
	19.	North Bound interface required towards NMS	Declaration
	20.	Requirement of Optional Features	Declaration
	21.	Interfaces required to support SyncE features	Declaration
	22.	Requirement of control or switch card or both redundancy in case of categroy III and V Routers	Declaration

	23.	Ipv4 / Ipv6 Routes to be supported shall be specified for the aggregation and Core Routers among the options given	Declaration
	24.	Support of P and PE functionality on Core Routers	Declaration
	25.	Documentation requirements as per clause 10.1	Declaration
	26.	Additional Installation Requirements as per clause 10.2	Declaration
	27.	Maintenance Requirements as per clause 10.3	Declaration
	28.	The list of protocol support not required may be specified by the purchaser (refer to clause 3.10)	Declaration
	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.	Declaration
	30.	The requirement of SNMP/ Netconf to be specified by the purchasing authority as per clause 3.8.1.6	Declaration
	31.	The requirement of SNMP / gRPC/gNMI/Netconf to be specified by the purchasing authority as per clause 3.23.1.4	Declaration
	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	Declaration
	33.	Minimum value of MTBF required may be indicated (refer to clause 5.1)	Declaration
	34.	Applicable environmental category to be specified (refer to clause 5.3)	Declaration
	35.	The SFP Type requirement for 10G Optical interface as per clause 4.2.4.1	Declaration
	36.	Port Address Translation ferature as per clause 8.1.1.1	Declaration
	37.	Network Address Translation as per RFC 3022, as per clause 8.1.2.1	Declaration
	38.	The eMS Security requirements /features as per clause 8.3.6.4, 8.3.6.8, 8.3.7.4 e	Declaration
		Note#1 Suggestive Power Supply & Fan Unit Redundancy & Hot Swappable features requirement	Declaration
			Declaration

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.	Declaration
10.4.2		The following clauses are optional for Tendering Authority in respect of Non- Chassis Router:	Declaration

			Declaration
10.5		Feature mapping for various Category of Routers	Information (Refer GR TEC 48050:2025)

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.

I. TEST SETUP & PROCEDURES:

1. Test No.	
2. Test Details	Name and Other relevant details
3. Test Instruments Required	1. <Name> 2.
4. Test Setup	
5. Test Procedure	Testing Steps may be written here.... 1) .... 2) .... 3) ....
6. Test Limits	(if any)
7. Expected Results	1. ....<values>........... 2.............<values>........... 3. Other tests (test name)

Further Test Setup & Procedures may be added as per requirement

J. SUMMARY OF TEST RESULTS

TEC Standard No.____________________________________

TEC Test Guide No. __________

Equipment name & Model No. _____________

Clause No.	*Compliance* *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	*Remarks /* *Test Report Annexure No.*

[Add as per requirement]

Date:

Place:

Signature & Name of TEC testing Officer /

** Signature of Applicant / Authorized Signatory*

** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.*

(Compendium of Test Guides of IT)

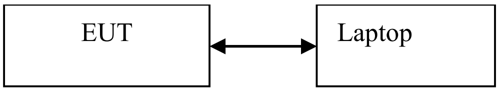
COMPENDIUM OF
TEST SETUP AND TEST PROCEDURES
FOR PRODUCTS WHOSE
SPECIFICATIONS ARE RELEASED FROM 'IT' DIVISION

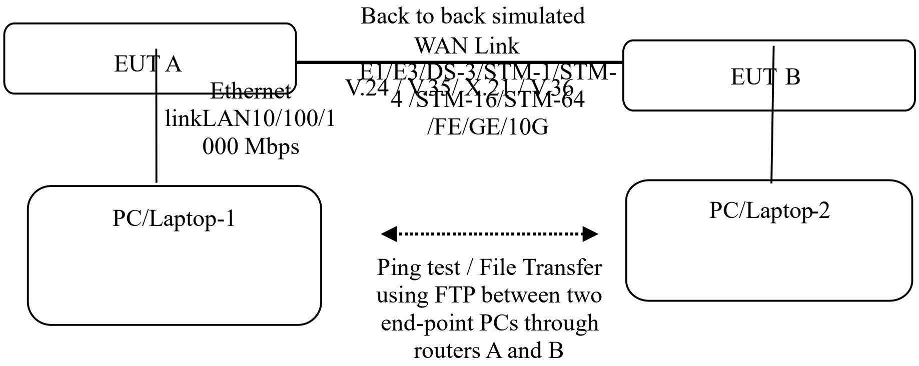
Telecommunication Engineering Centre
Department of Telecommunications
Khurshid Lal Bhavan, Janpath
New Delhi-110 001
India

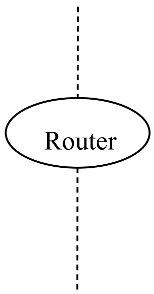
History Sheet

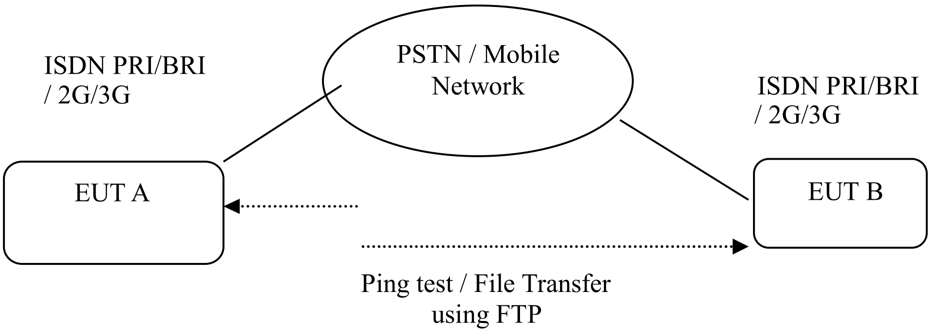
S.No.	Name & Number	Remarks
1	Compendium of Tests	1st issue March 2014
2.	Compendium of Tests	2nd issue September 2014
3.	Compendium of Tests	3rd issue November 2014
4.	Compendium of Tests	4th issue December 2014
5.	Compendium of Tests	5th issue April 2015
6.	Compendium of Tests	6th issue April 2016 after incorporation of detailed protocol tests as per RFC's
7.	Compendium of Tests TEC 48169:2024	7th issue July 2024 after incorporating additional interfaces

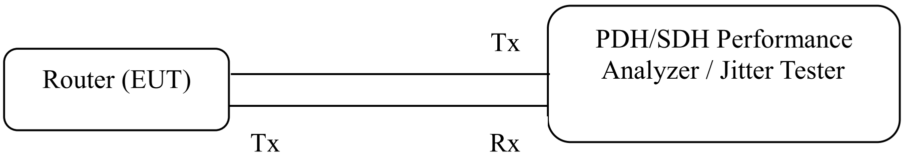
Table of Contents

Test No.	1
Test Details	Test for 10/100/1000 Auto-negotiation Ethernet Interface
Test Instruments Required	1. Laptop
Test Setup	
Test Procedure	1. Set the Laptop Ethernet interface speed to 10Mbps and see whether the EUT is syncing with the Laptop. I.e. the Ethernet interface lamp of the Laptop shall glow. 2. Repeat the above for 100Mbps 3. Repeat the same for 1000Mbps [In case required]
Expected Results	Enclose the Screen Capture Results

Test No.	2
Test Details	Test for the Availability of Service
Test Instruments Required	1. PC / Laptop – 2 Nos
	 Back to back simulated WAN Link EUT A EUT B V.24 / V.35/ X.21 / V.36 E1/E3/DS-3/STM-1/STM-4 /STM-16/STM-64 /FE/GE/10G Ethernet linkLAN10/100/1000 Mbps PC/Laptop-1 PC/Laptop-2 Ping test / File Transfer using FTP between two end-point PCs through routers A and B
Test Procedure	1. Connect the V.24 / V.35 /V.36/X.21/ E1 / E3 / DS-3 / STM-1 / STM-4/STM16/STM-64/FE/GE/10G interface as the case may be as shown in the setup. 2. Connect the PC/Laptop to the 10/100/1000Mbps LAN link as shown 3. Configure the Interface IP of the EUT as well as the PC/Laptop 4. Carry out the Ping test from PC/Laptop-1 to PC/Laptop-2 and see whether it is reachable as well as there are no packet drop 5. Carry out file transfer from PC/Laptop-1 to PC/Laptop-2 6. In case of Nx64, repeat the test at different speeds
Expected Results	Enclose the Ping Results

Test No.	3
Test Details	Test for the Availability of Service (Devices without Ethernet Interface)
Test Instruments Required	1. PC / Laptop – 2 Nos 2. Router or Interface converter in case the EUT do not have the 10/100/1000 Ethernet interface
Test Setup	
Test Procedure	1. Connect the EUT as shown in the setup. 2. Connect the PC/Laptop to the 10/100/1000 Mbps LAN link as shown 3. In case of V.24/V.36/V.37/ V.11/X.21 Interface, same may be connected to the PC/Laptop through a Router acting as interface converter. 4. Configure the Interface IP of the HSL Driver if required, Routers as well as the PC/Laptop 5. Carry out the Ping test from PC/Laptop-1 to PC/Laptop-2 and see whether it is reachable as well as there are no packet drop 6. Carry out file transfer from PC/Laptop-1 to PC/Laptop-2 7. In case of Nx64, repeat the test at different speeds. 8. Carry out Telnet check also.
Expected Results	Enclose the Results/screenshots

Test No.	4
Test Details	PRI/BRI / 2G/3G wave functional test
Test Instruments Required	1. PSTN / 2G/3G conne :tivity
Test Setup	 PSTN / Mobile Network ISDN PRI/BRI / 2G/3G ISDN PRI/BRI / 2G/3G EUT A EUT B Ping test / File Transfer using FTP
Test Procedure	1. Connect EUT A and EUT B through PSTN in case of PRI/BRI. 2. Connect EUT A and EUT B through Mobile Network in case of 2G/3G. In such case EUT shall be equipped with 2G/3G interface cards along with SIM 3. Test for Ping and File Transfer from EUT A to EUT B
Expected Results	Enclose the Ping Results

Test No.	5	
Test Details	Test for Output Jitter	
Test Instruments Required	1. PDH/SDH Performance Analyser or Jitter Tester	
Test Setup	PDH/SDH Interface in loopback mode Rx  Tx PDH/SDH Performance Analyzer / Jitter Tester Router (EUT) Tx Rx	
Test Limits	Limits for Output Jitter [Maximum Permissible Jitter at Output Interfaces] for PDH interfaces (64Kbps, 2, 34, 45, 140Mbps)	Refer Table 1/G.823
	Limits for Output Jitter [Maximum Permissible Jitter at Output Interfaces] for SDH interfaces (STM-1, STM-4, STM-16, STM-64)	Refer Table 1/G.825

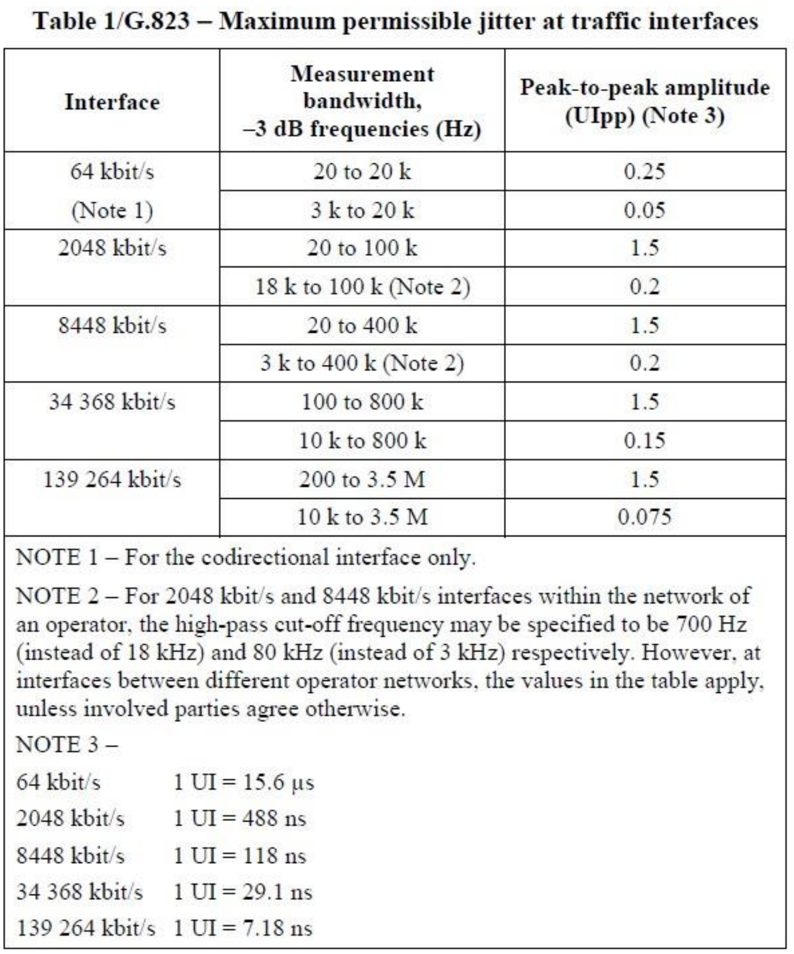
Standards Reference	**Table 1/G.823**
	

Table 1/G.823 – Maximum permissible jitter at traffic interfaces

Interface	Measurement bandwidth, –3 dB frequencies (Hz)	Peak-to-peak amplitude (UIpp) (Note 3)
64 kbit/s	20 to 20 k	0.25
(Note 1)	3 k to 20 k	0.05
2048 kbit/s	20 to 100 k	1.5
	18 k to 100 k (Note 2)	0.2
8448 kbit/s	20 to 400 k	1.5
	3 k to 400 k (Note 2)	0.2
34 368 kbit/s	100 to 800 k	1.5
	10 k to 800 k	0.15
139 264 kbit/s	200 to 3.5 M	1.5
	10 k to 3.5 M	0.075

NOTE 1 – For the codirectional interface only.

NOTE 2 – For 2048 kbit/s and 8448 kbit/s interfaces within the network of an operator, the high-pass cut-off frequency may be specified to be 700 Hz (instead of 18 kHz) and 80 kHz (instead of 3 kHz) respectively. However, at interfaces between different operator networks, the values in the table apply, unless involved parties agree otherwise.

NOTE 3 –

64 kbit/s	1 UI = 15.6 μs
2048 kbit/s	1 UI = 488 ns
8448 kbit/s	1 UI = 118 ns
34 368 kbit/s	1 UI = 29.1 ns
139 264 kbit/s	1 UI = 7.18 ns

Table 1/G.825

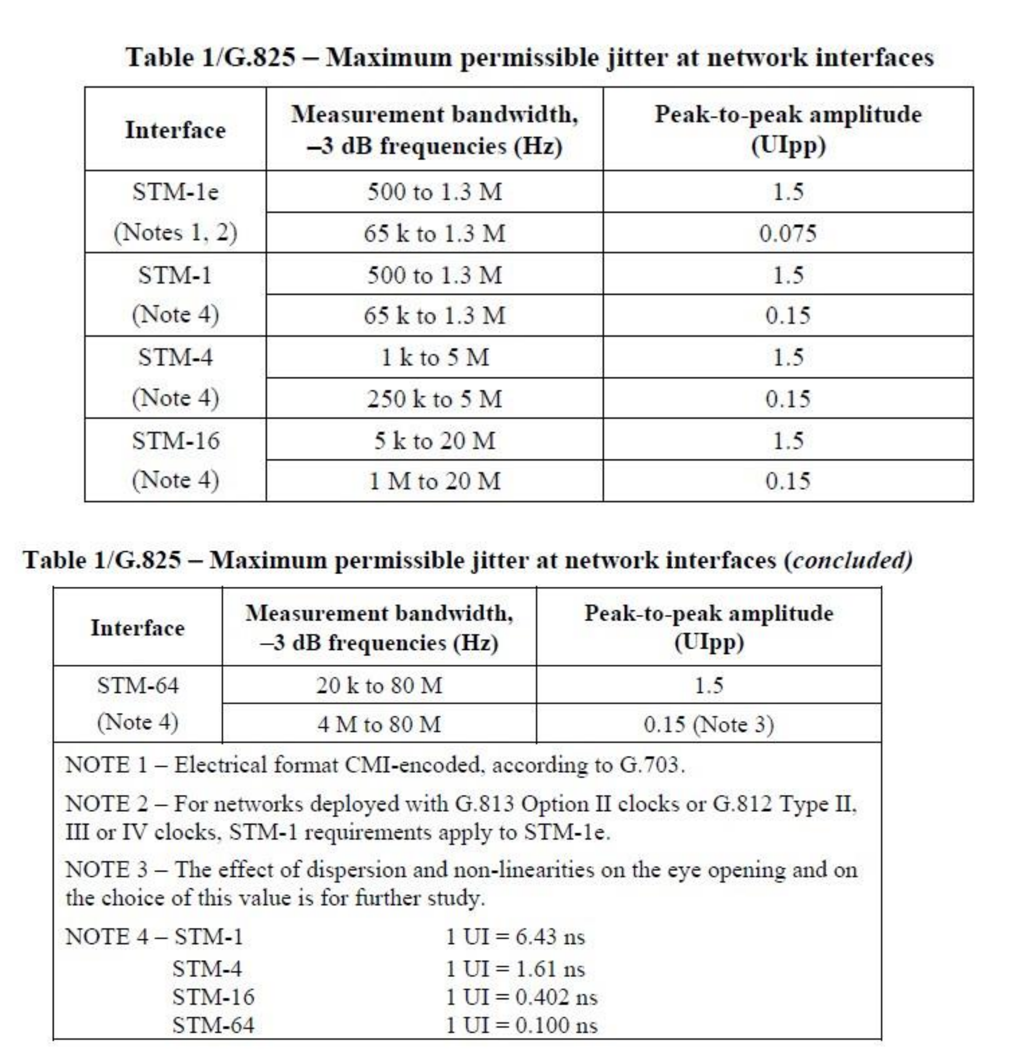


Table 1/G.825 – Maximum permissible jitter at network interfaces

Interface	Measurement bandwidth, –3 dB frequencies (Hz)	Peak-to-peak amplitude (UIpp)
STM-1e (Notes 1, 2)	500 to 1.3 M	1.5
	65 k to 1.3 M	0.075
STM-1 (Note 4)	500 to 1.3 M	1.5
	65 k to 1.3 M	0.15
STM-4 (Note 4)	1 k to 5 M	1.5
	250 k to 5 M	0.15
STM-16 (Note 4)	5 k to 20 M	1.5
	1 M to 20 M	0.15

Table 1/G.825 – Maximum permissible jitter at network interfaces (*concluded*)

Interface	Measurement bandwidth, –3 dB frequencies (Hz)	Peak-to-peak amplitude (UIpp)
STM-64 (Note 4)	20 k to 80 M	1.5
	4 M to 80 M	0.15 (Note 3)

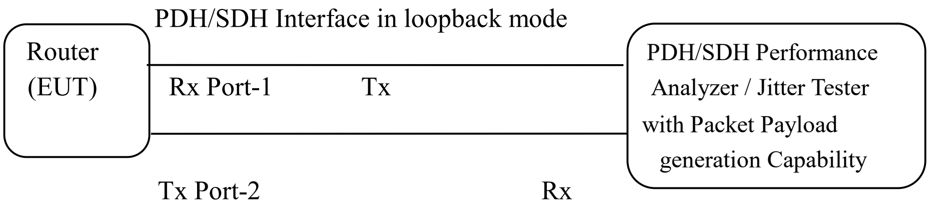
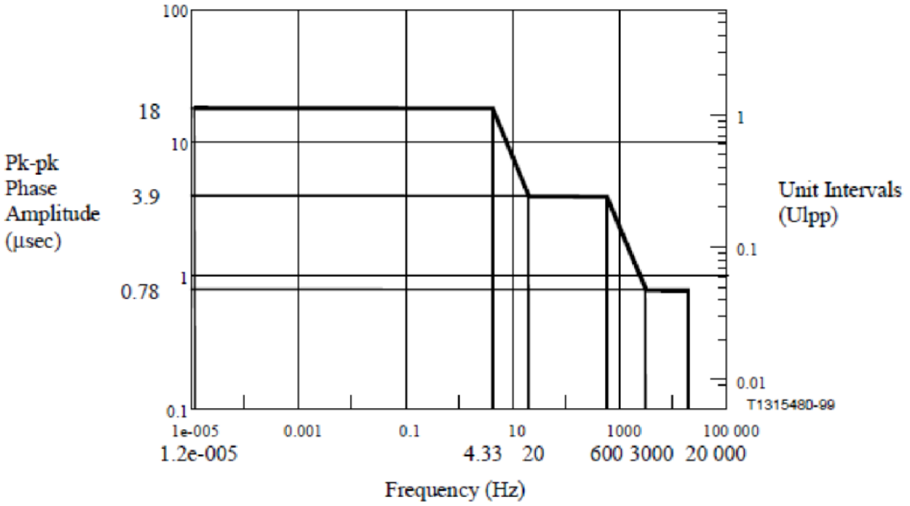
NOTE 1 – Electrical format CMI-encoded, according to G.703.

NOTE 2 – For networks deployed with G.813 Option II clocks or G.812 Type II, III or IV clocks, STM-1 requirements apply to STM-1e.

NOTE 3 – The effect of dispersion and non-linearities on the eye opening and on the choice of this value is for further study.

NOTE 4 –		
	STM-1	1 UI = 6.43 ns
	STM-4	1 UI = 1.61 ns
	STM-16	1 UI = 0.402 ns
	STM-64	1 UI = 0.100 ns

Test Procedure	1. Connect the setup as shown in the figure. 2. Measure the output jitter on the connected PDH/SDH interface 3. Verify whether the output jitter is within the tolerance limits as specified in the relevant ITU specifications as indicated above. 4. Enclose the test results
Expected Results	Enclose the Test Results

Test No.	6	
Test Details	Test for Input Jitter Tolerance	
Test Instruments Required	1. PDH/SDH Performance analyser with POS capability for SDH and Packet Payload Capability for PDH	
Test Setup	 PDH/SDH Interface in loopback mode Router (EUT) Rx Port-1 Tx Tx Port-2 Rx PDH/SDH Performance Analyzer / Jitter Tester with Packet Payload generation Capability	
Test Limits		
	64 Kbps co-directional interface input jitter and wander tolerance limit	Refer Figure 12/G.823
	2048 Kbps input jitter and wander tolerance limit	Refer Figure 13/G.823
	34.368 Mbps input jitter and wander tolerance limit	Refer Figure 15/G.823
	44.736 Mbps input jitter and wander tolerance limit	Refer Figure 9/G.824
	STM-1e Jitter Tolerance Requirement for 2048Kbps Networks	Refer Figure 2/G.825
	STM-4 Jitter Tolerance Requirement	Refer Figure 3/G.825
	STM-16 Jitter Tolerance Requirement	Refer Figure 4/G.825
	STM-64 Jitter Tolerance Requirement	Refer Figure 5/G.825
Standards reference	**Figure 12/G.823**	
	 **Figure 12/G.823 – 64 kbit/s input jitter and wander tolerance limit**	
	Figure 13/G.823	

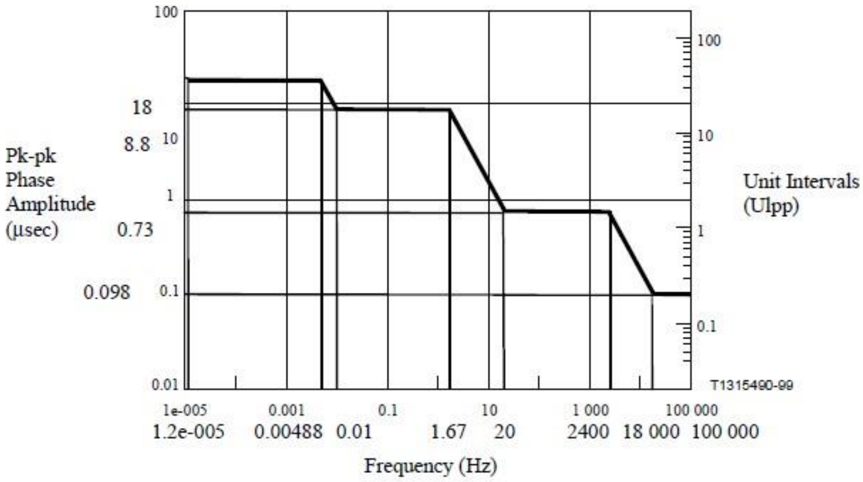


Figure 13/G.823 – 2048 kbit/s input jitter and wander tolerance limit

Figure 15/G.823

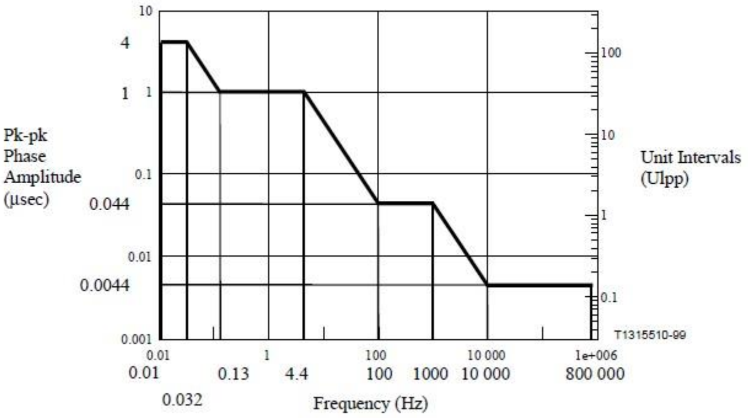


Figure 15/G.823 – 34 368 kbit/s input jitter and wander tolerance limit

Figure 9/G.824

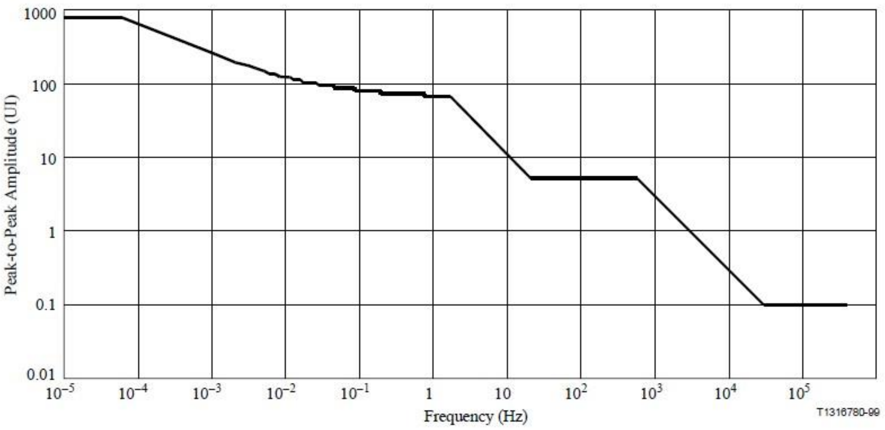


Figure 9/G.824 – Jitter and wander tolerance of 44 736 kbit/s input ports

Figure 2/G.825

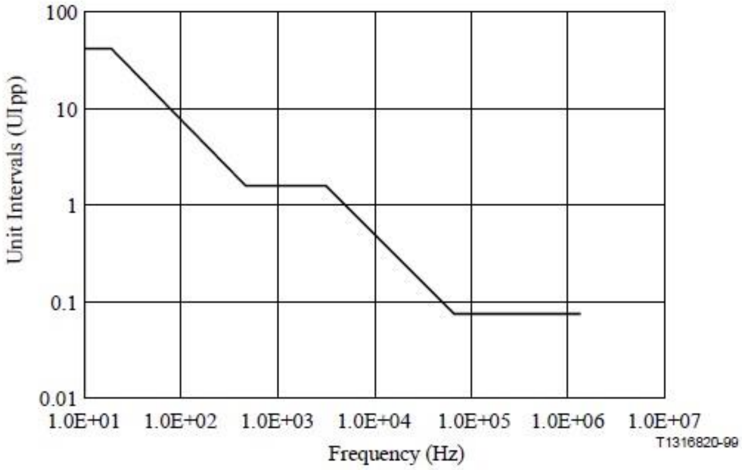
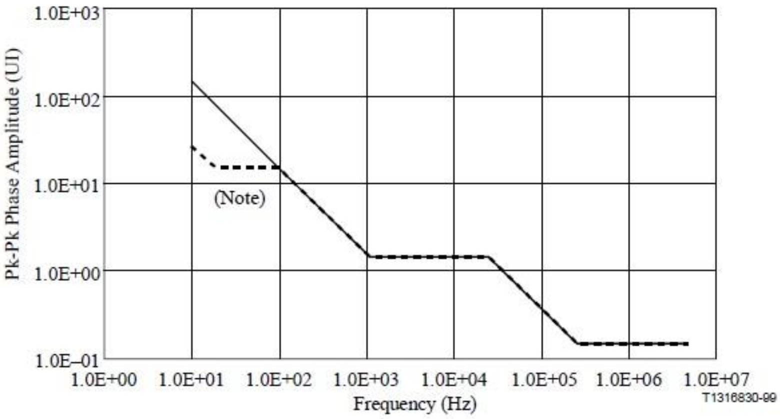


Figure 2/G.825 – STM-1e jitter tolerance requirement (applies to 2048 kbit/s networks only)

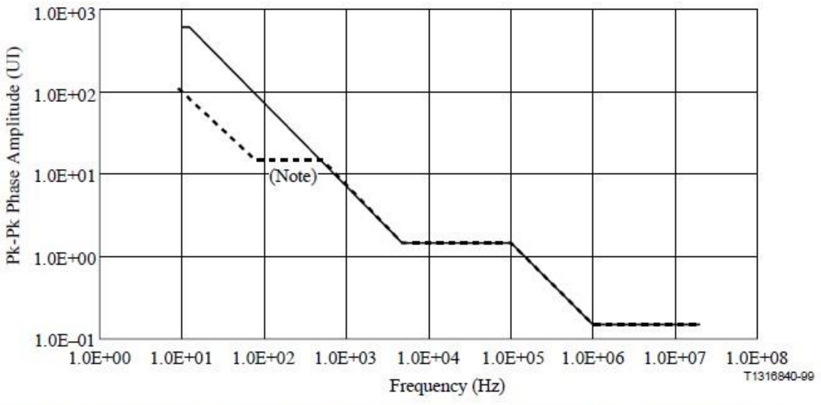
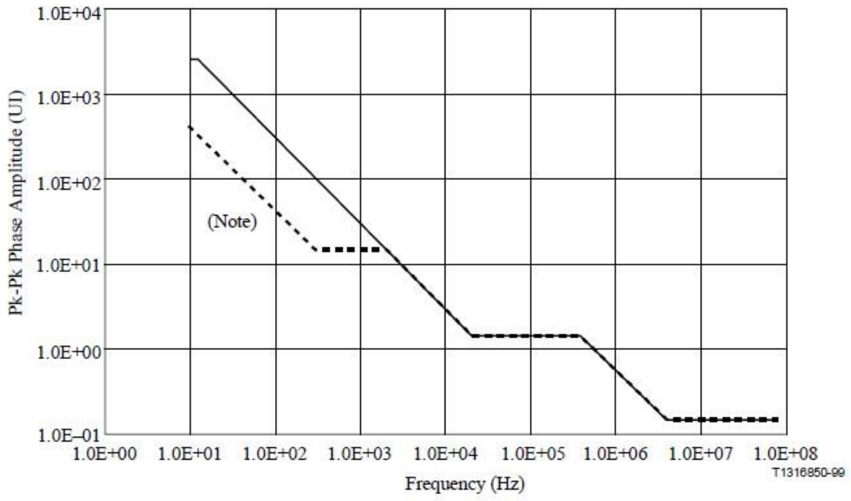
Figure 3/G.825

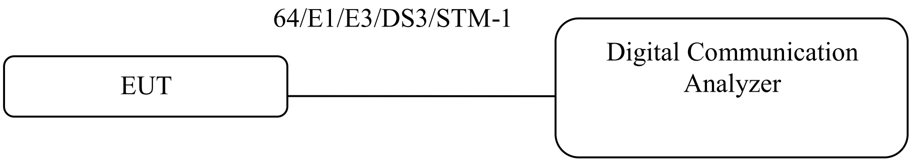
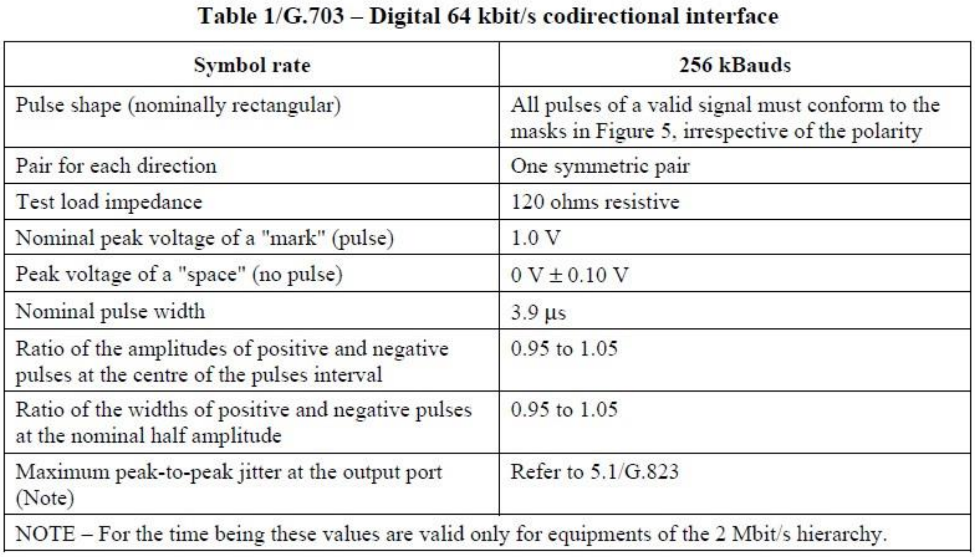


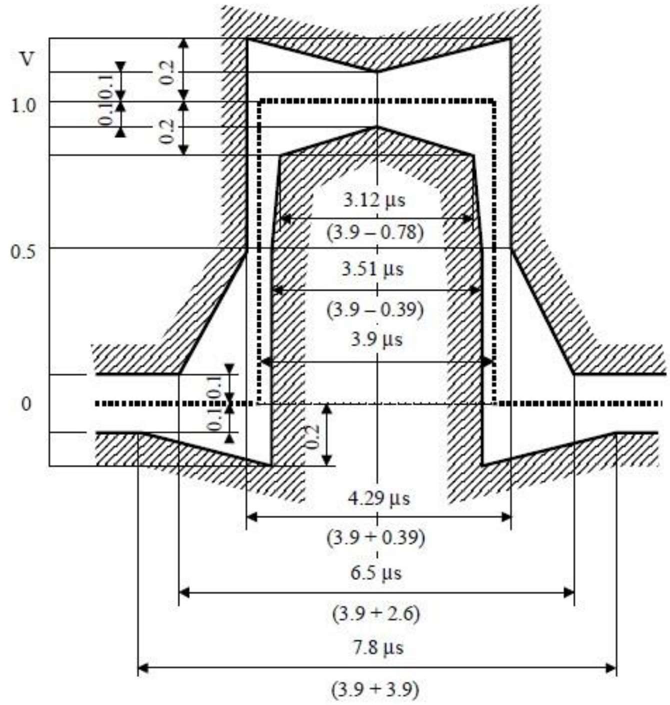
NOTE – The dashed curve is the requirement for 1544 kbit/s networks for frequencies less than 100 Hz.

Figure 3/G.825 – STM-4 jitter tolerance

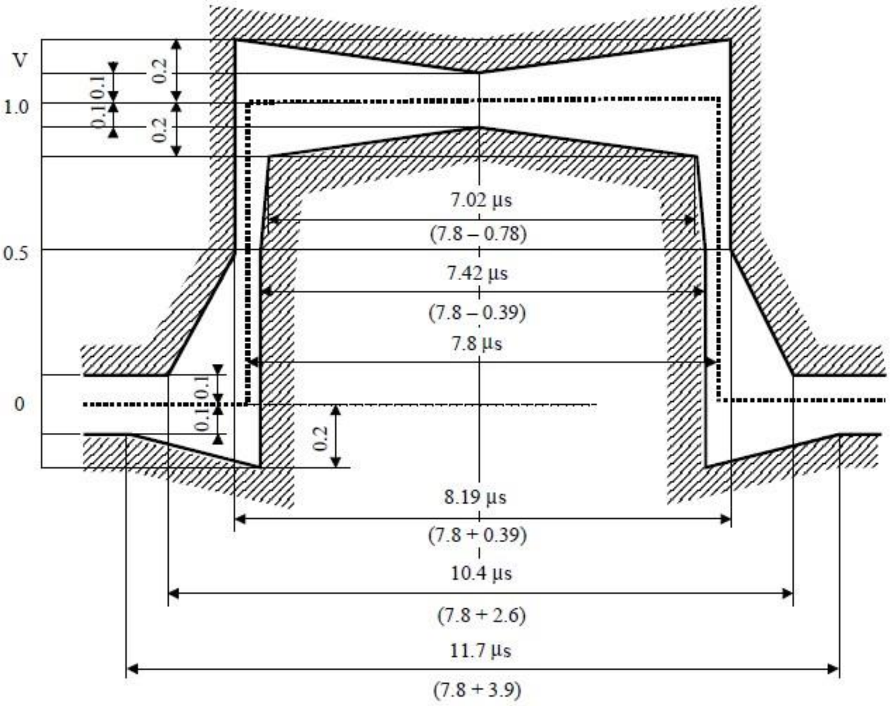
Figure 4/G.825

	 NOTE – The dashed curve is the requirement for 1544 kbit/s networks for frequencies less than 500 Hz. **Figure 4/G.825 – STM-16 jitter tolerance**
	Figure 5/G.825
	 NOTE – The dashed curve is the requirement for 1544 kbit/s networks for frequencies less than 2 kHz. **Figure 5/G.825 – STM-64 jitter tolerance**
Test Procedure	1. Connect the setup as shown in the figure. 2. Configure the Router with Port-1 as IP-1 and Port-2 as IP-2 3. Configure the POS in the SDH analyser with Source Address as IP-1 and destination address as IP-2 4. Configure Router-A for Static routing the packets 5. SDH Analyser shall introduce Jitter over the generated packets with PRBS pattern as per G.825 6. Measure the Jitter tolerance as per the Mask and Range of frequencies 7. Take a plot of the Jitter tolerance along with the Mask
Expected Results	Enclose the Test Results

<table>
<tr><td>Test No.</td><td>7</td></tr>
<tr><td>Test Details</td><td>Test for Output Pulse Mask for PDH/SDH interfaces</td></tr>
<tr><td>Test Instruments Required</td><td>1. Digital Communication Analyser OR Digital Storage Oscilloscope</td></tr>
<tr><td>Test Setup</td><td>
</td></tr>
<tr><td>Test Limits</td><td><table>
<tr><td>Limits for Pulse shape & characteristics for 64Kbps co-directional interface</td><td>Refer Table-1 and Figure-5 G.703</td></tr>
<tr><td>Limits for Pulse shape & characteristics for 2048kbps (E1) interface</td><td>Refer Table-7 and Figure-15 G.703</td></tr>
<tr><td>Limits for Pulse shape & characteristics for 34Mbps interface</td><td>Refer Table-9 and Figure-17 G.703</td></tr>
<tr><td>Limits for Pulse shape & characteristics for 44.736Mbps (DS3) Interface</td><td>Refer Table-6 and Figure-14 G.703</td></tr>
<tr><td>STM-1</td><td>Refer Table-12 and Figure-22,23 G.703</td></tr>
</table></td></tr>
<tr><td>Standards reference</td><td><b>Table-1 and Figure-5 G.703</b>

<b>Table 1/G.703 – Digital 64 kbit/s codirectional interface</b>
<table>
<tr><th>Symbol rate</th><th>256 kBauds</th></tr>
<tr><td>Pulse shape (nominally rectangular)</td><td>All pulses of a valid signal must conform to the masks in Figure 5, irrespective of the polarity</td></tr>
<tr><td>Pair for each direction</td><td>One symmetric pair</td></tr>
<tr><td>Test load impedance</td><td>120 ohms resistive</td></tr>
<tr><td>Nominal peak voltage of a "mark" (pulse)</td><td>1.0 V</td></tr>
<tr><td>Peak voltage of a "space" (no pulse)</td><td>0 V ± 0.10 V</td></tr>
<tr><td>Nominal pulse width</td><td>3.9 μs</td></tr>
<tr><td>Ratio of the amplitudes of positive and negative pulses at the centre of the pulses interval</td><td>0.95 to 1.05</td></tr>
<tr><td>Ratio of the widths of positive and negative pulses at the nominal half amplitude</td><td>0.95 to 1.05</td></tr>
<tr><td>Maximum peak-to-peak jitter at the output port (Note)</td><td>Refer to 5.1/G.823</td></tr>
<tr><td colspan="2">NOTE – For the time being these values are valid only for equipments of the 2 Mbit/s hierarchy.</td></tr>
</table></td></tr>
</table>



a) Mask for single pulse

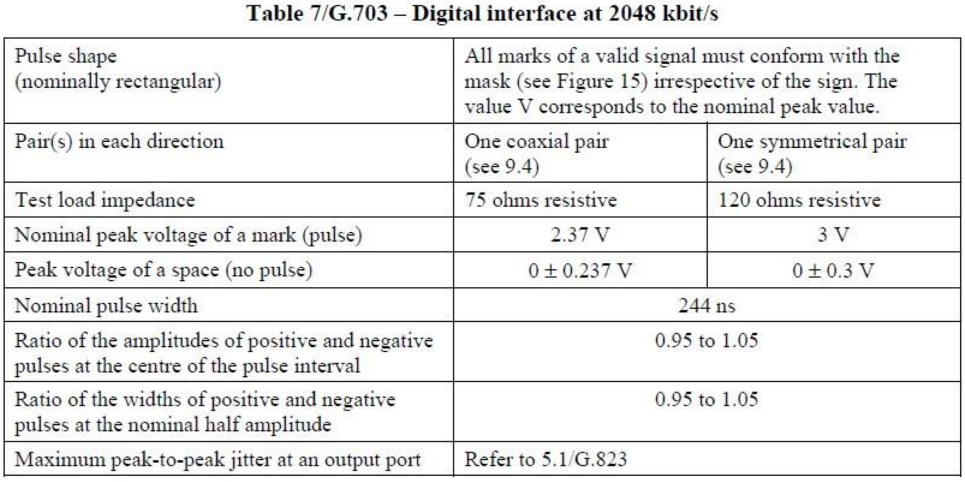


b) Mask for double pulse

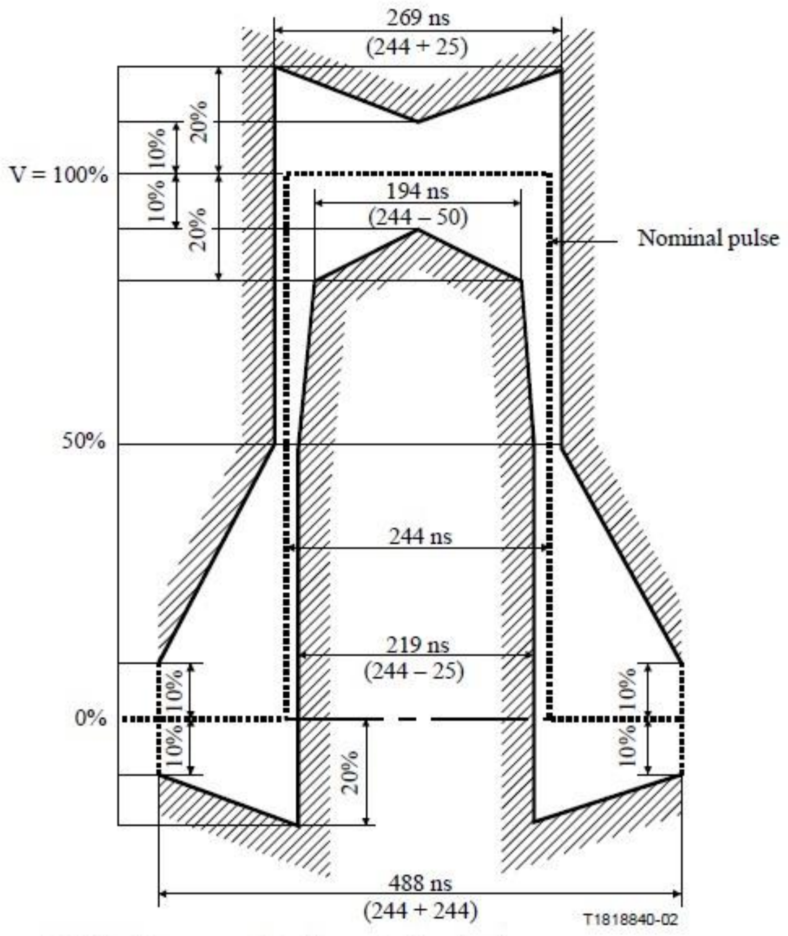
NOTE – The limits apply to pulses of either polarity.

Table-7 and Figure-15 G.703

Table 7/G.703 – Digital interface at 2048 kbit/s



Pulse shape (nominally rectangular)	All marks of a valid signal must conform with the mask (see Figure 15) irrespective of the sign. The value V corresponds to the nominal peak value.	
Pair(s) in each direction	One coaxial pair (see 9.4)	One symmetrical pair (see 9.4)
Test load impedance	75 ohms resistive	120 ohms resistive
Nominal peak voltage of a mark (pulse)	2.37 V	3 V
Peak voltage of a space (no pulse)	0 ± 0.237 V	0 ± 0.3 V
Nominal pulse width	244 ns	
Ratio of the amplitudes of positive and negative pulses at the centre of the pulse interval	0.95 to 1.05	
Ratio of the widths of positive and negative pulses at the nominal half amplitude	0.95 to 1.05	
Maximum peak-to-peak jitter at an output port	Refer to 5.1/G.823	



NOTE – V corresponds to the nominal peak value.

Figure 15/G.703 – Mask of the pulse at the 2048 kbit/s interface

Table-9 and Figure-17 G.703

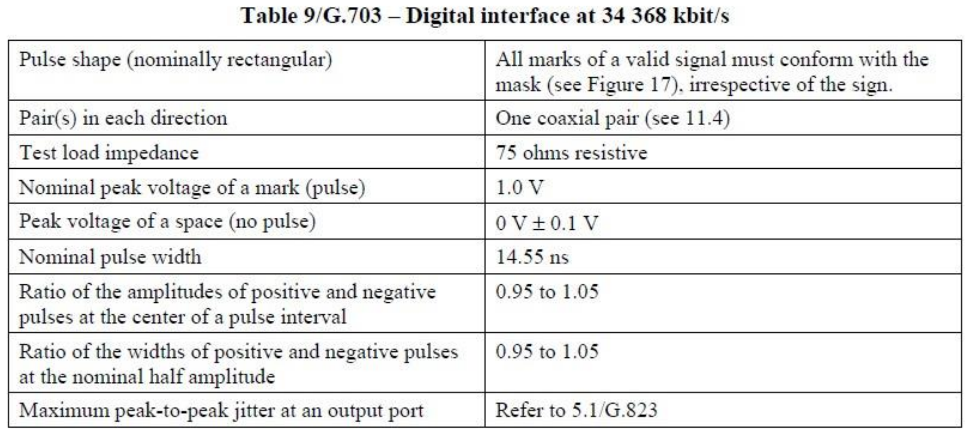


Table 9/G.703 – Digital interface at 34 368 kbit/s

Pulse shape (nominally rectangular)	All marks of a valid signal must conform with the mask (see Figure 17), irrespective of the sign.
Pair(s) in each direction	One coaxial pair (see 11.4)
Test load impedance	75 ohms resistive
Nominal peak voltage of a mark (pulse)	1.0 V
Peak voltage of a space (no pulse)	0 V ± 0.1 V
Nominal pulse width	14.55 ns
Ratio of the amplitudes of positive and negative pulses at the center of a pulse interval	0.95 to 1.05
Ratio of the widths of positive and negative pulses at the nominal half amplitude	0.95 to 1.05
Maximum peak-to-peak jitter at an output port	Refer to 5.1/G.823

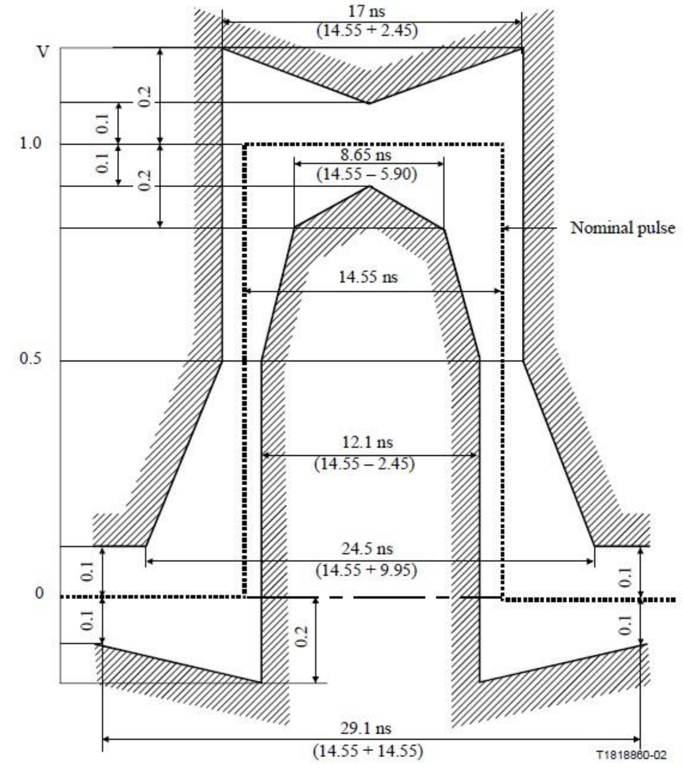


Figure 17/G.703 – Pulse mask at the 34 368 kbit/s interface

S

Table-6 and Figure-14 G.703

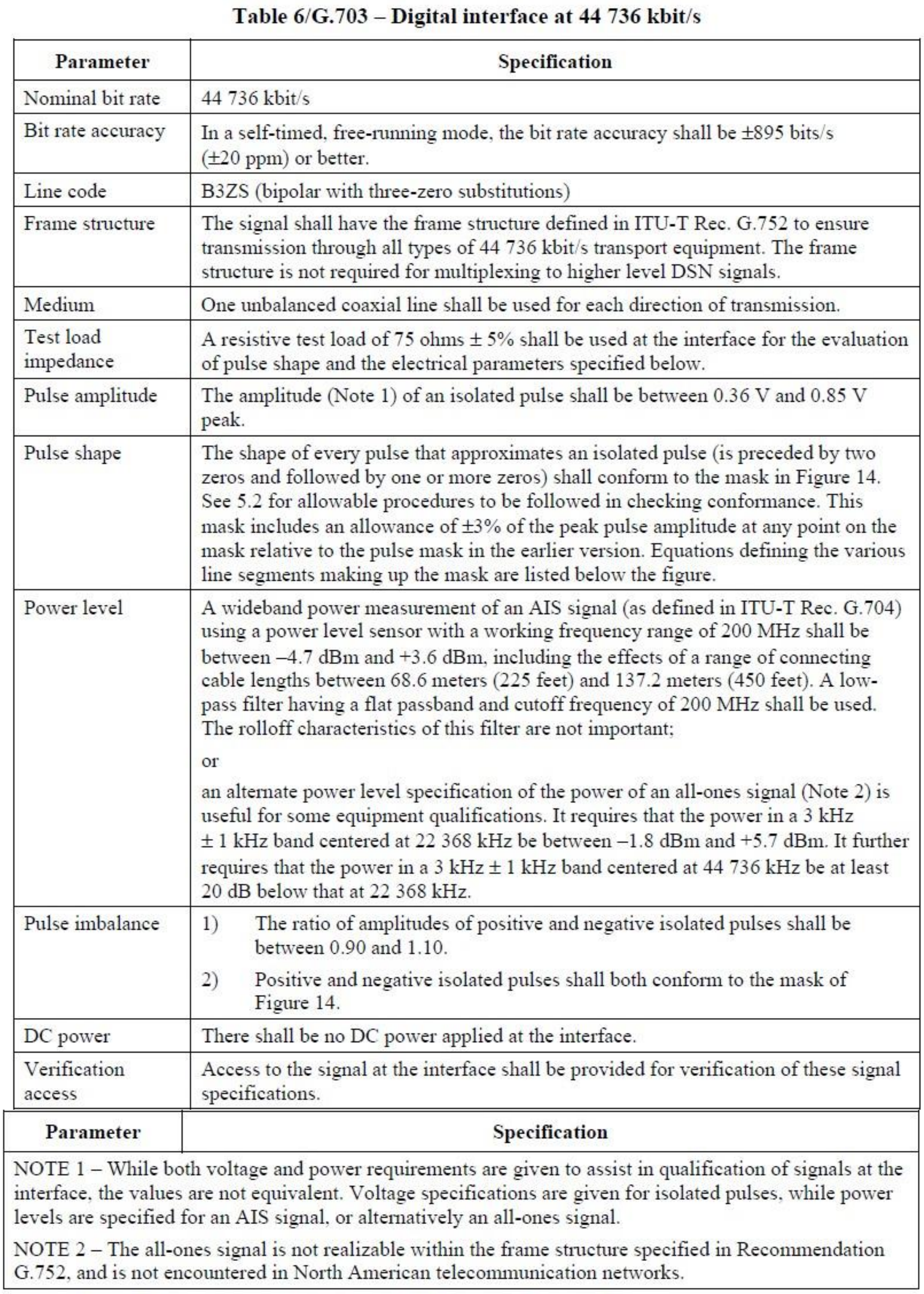


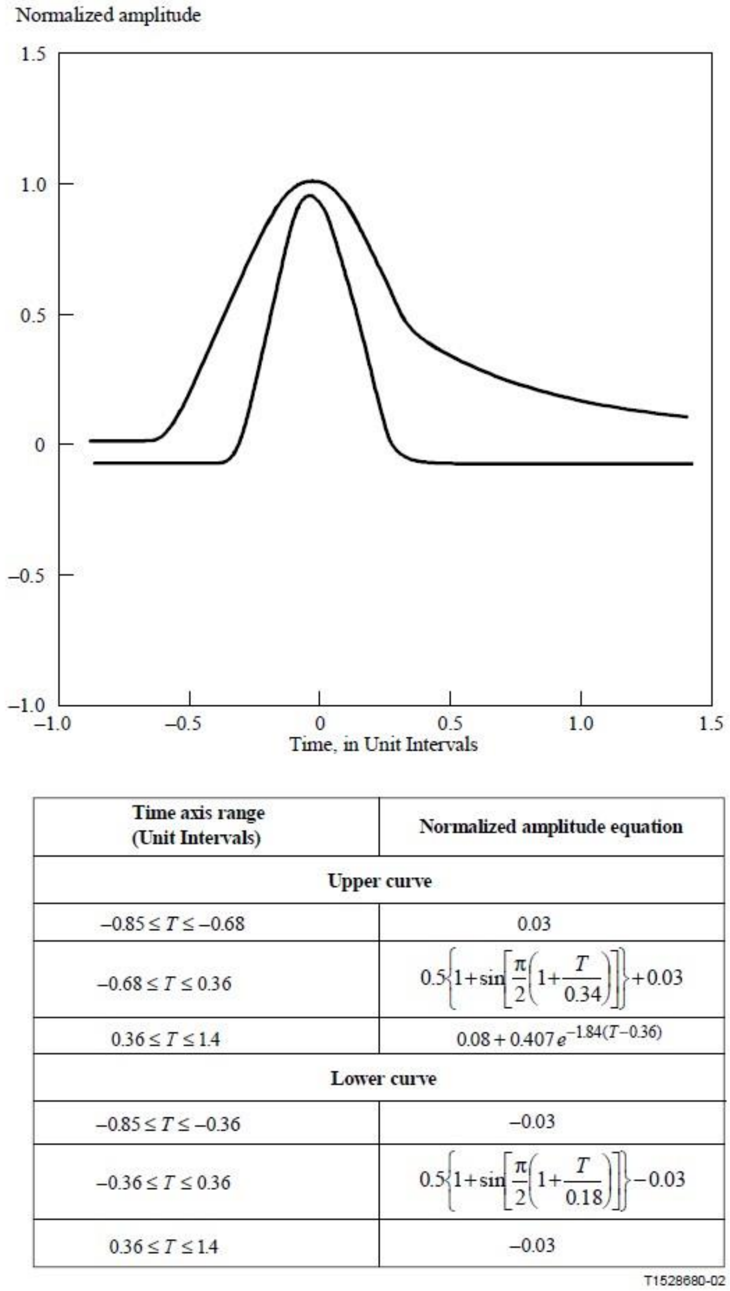
Table 6/G.703 – Digital interface at 44 736 kbit/s

Parameter	Specification
Nominal bit rate	44 736 kbit/s
Bit rate accuracy	In a self-timed, free-running mode, the bit rate accuracy shall be ±895 bits/s (±20 ppm) or better.
Line code	B3ZS (bipolar with three-zero substitutions)
Frame structure	The signal shall have the frame structure defined in ITU-T Rec. G.752 to ensure transmission through all types of 44 736 kbit/s transport equipment. The frame structure is not required for multiplexing to higher level DSN signals.
Medium	One unbalanced coaxial line shall be used for each direction of transmission.
Test load impedance	A resistive test load of 75 ohms ± 5% shall be used at the interface for the evaluation of pulse shape and the electrical parameters specified below.
Pulse amplitude	The amplitude (Note 1) of an isolated pulse shall be between 0.36 V and 0.85 V peak.
Pulse shape	The shape of every pulse that approximates an isolated pulse (is preceded by two zeros and followed by one or more zeros) shall conform to the mask in Figure 14. See 5.2 for allowable procedures to be followed in checking conformance. This mask includes an allowance of ±3% of the peak pulse amplitude at any point on the mask relative to the pulse mask in the earlier version. Equations defining the various line segments making up the mask are listed below the figure.
Power level	A wideband power measurement of an AIS signal (as defined in ITU-T Rec. G.704) using a power level sensor with a working frequency range of 200 MHz shall be between –4.7 dBm and +3.6 dBm, including the effects of a range of connecting cable lengths between 68.6 meters (225 feet) and 137.2 meters (450 feet). A low-pass filter having a flat passband and cutoff frequency of 200 MHz shall be used. The rolloff characteristics of this filter are not important; or an alternate power level specification of the power of an all-ones signal (Note 2) is useful for some equipment qualifications. It requires that the power in a 3 kHz ± 1 kHz band centered at 22 368 kHz be between –1.8 dBm and +5.7 dBm. It further requires that the power in a 3 kHz ± 1 kHz band centered at 44 736 kHz be at least 20 dB below that at 22 368 kHz.
Pulse imbalance	1) The ratio of amplitudes of positive and negative isolated pulses shall be between 0.90 and 1.10. 2) Positive and negative isolated pulses shall both conform to the mask of Figure 14.
DC power	There shall be no DC power applied at the interface.
Verification access	Access to the signal at the interface shall be provided for verification of these signal specifications.

Parameter	Specification

NOTE 1 – While both voltage and power requirements are given to assist in qualification of signals at the interface, the values are not equivalent. Voltage specifications are given for isolated pulses, while power levels are specified for an AIS signal, or alternatively an all-ones signal.

NOTE 2 – The all-ones signal is not realizable within the frame structure specified in Recommendation G.752, and is not encountered in North American telecommunication networks.



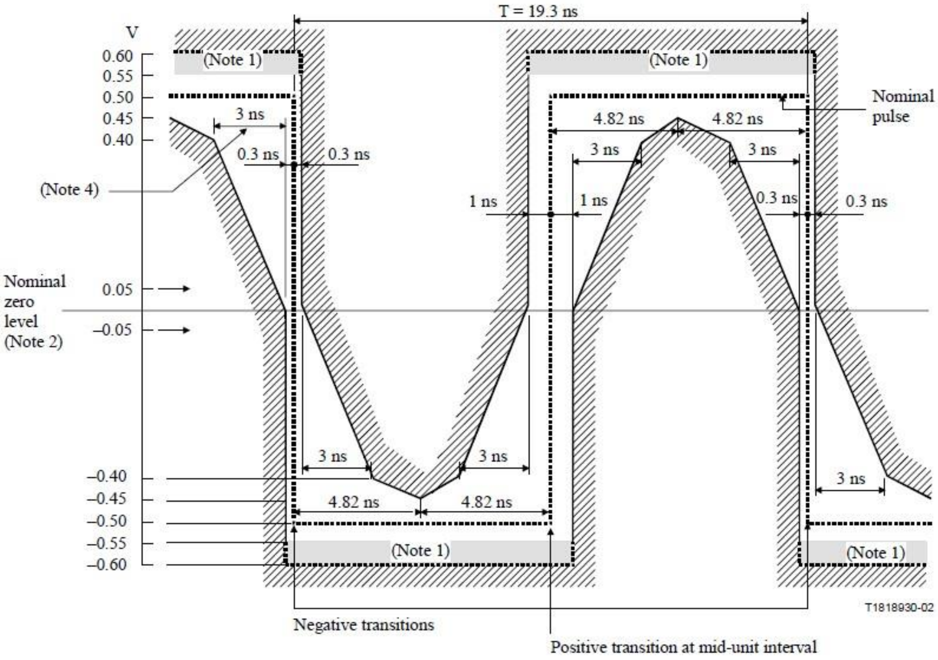
Time axis range (Unit Intervals)	Normalized amplitude equation
Upper curve	
$-0.85 \le T \le -0.68$	0.03
$-0.68 \le T \le 0.36$	$0.5\left\{1+\sin\left[\frac{\pi}{2}\left(1+\frac{T}{0.34}\right)\right]\right\}+0.03$
$0.36 \le T \le 1.4$	$0.08+0.407e^{-1.84(T-0.36)}$
Lower curve	
$-0.85 \le T \le -0.36$	-0.03
$-0.36 \le T \le 0.36$	$0.5\left\{1+\sin\left[\frac{\pi}{2}\left(1+\frac{T}{0.18}\right)\right]\right\}-0.03$
$0.36 \le T \le 1.4$	-0.03

Figure 14/G.703 – 44 736 kbit/s interface isolated pulse mask and equations

Table-12 and Figure-22,23 G.703

Table 12/G.703 – Digital interface at 155 520 kbit/s

Pulse shape	Nominally rectangular and conforming to the masks shown in Figures 22 and 23
Pair(s) in each direction	One coaxial pair
Test load impedance	75 ohms resistive
Peak-to-peak voltage	1 ± 0.1 V
Rise time between 10% and 90% amplitudes of the measured steady state amplitude	≤2 ns
Transition timing tolerance referred to the mean value of the 50% amplitude points of negative transitions	Negative transitions: ±0.1 ns Positive transitions at unit interval boundaries: ±0.5 ns Positive transitions at mid-unit intervals: ±0.35 ns
Return loss	≥15 dB over frequency range 8 MHz to 240 MHz
Maximum peak-to-peak jitter at an output port	Refer to 5.1/G.825



NOTE 1 – The maximum "steady state" amplitude should not exceed the 0.55 Vlimit. Overshoots and other transients are permitted to fall into the dotted area, bounded by the amplitude levels 0.55 V and 0.6 V, provided that they do not exceed the steady state level by more than 0.05 V. The possibility of relaxing the amount by which the overshoot may exceed the steady state level is under study.

NOTE 2 – For all measurements using these masks, the signal should be AC coupled, using a capacitor of not less than 0.01 μF, to the input of the oscilloscope used for measurements.

The nominal zero level for both masks should be aligned with the oscilloscope trace with no input signal. With the signal then applied, the vertical position of the trace can be adjusted with the objective of meeting the limits of the masks. Any such adjustment should be the same for both masks and should not exceed ±0.05 V. This may be checked by removing the input signal again and verifying that the trace lies within ±0.05 V of the nominal zero level of the masks.

NOTE 3 – Each pulse in a coded pulse sequence should meet the limits of the relevant mask, irrespective of the state of the preceding or succeeding pulses, with both pulse masks fixed in the same relation to a common timing reference, i.e. with their nominal start and finish edges coincident.

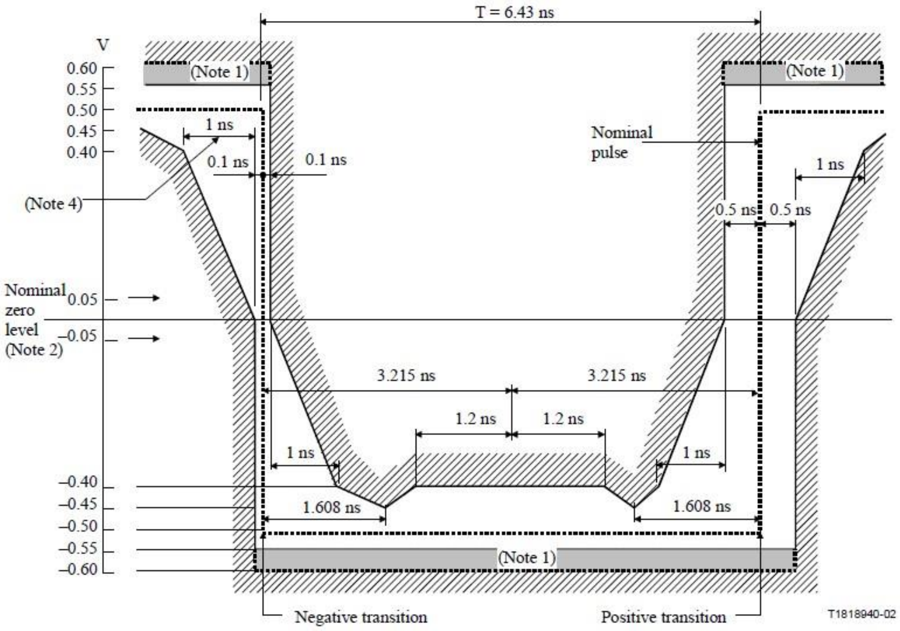
The masks allow for HF jitter caused by intersymbol interference in the output stage, but not for jitter present in the timing signal associated with the source of the interface signal.

When using an oscilloscope technique to determine pulse compliance with the mask, it is important that successive traces of the pulses overlay in order to suppress the effects of low frequency jitter. This can be accomplished by several techniques [e.g. a) triggering the oscilloscope on the measured waveform or b) providing both the oscilloscope and the pulse output circuits with the same clock signal].

These techniques require further study.

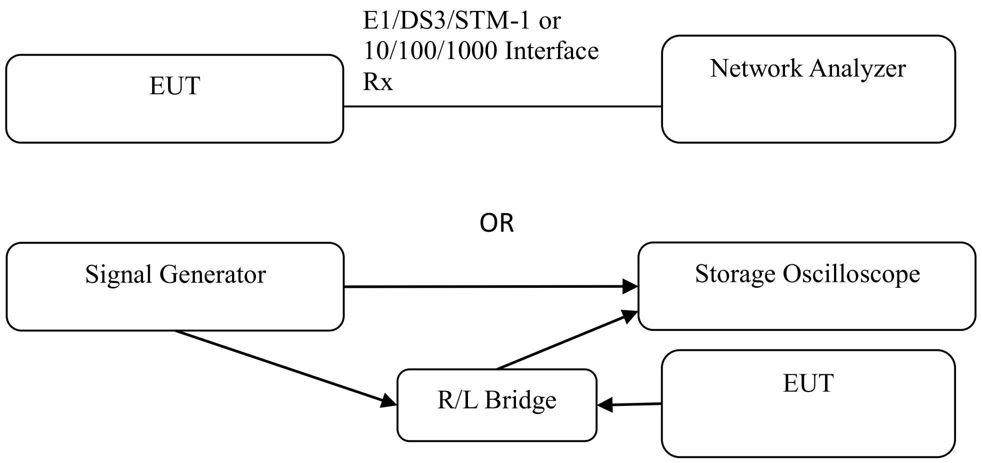
NOTE 4 – For the purpose of these masks, the rise time and decay time should be measured between –0.4 V and 0.4 V, and should not exceed 2 ns.

Figure 22/G.703 – Mask of a pulse corresponding to a binary 0 (at the 155 520 kbit/s interface)

	 T = 6.43 ns V 0.60 0.55 0.50 0.45 0.40 (Note 1) (Note 1) 1 ns 0.1 ns 0.1 ns Nominal pulse 1 ns (Note 4) 0.5 ns 0.5 ns Nominal zero level (Note 2) 0.05 –0.05 3.215 ns 3.215 ns 1.2 ns 1.2 ns 1 ns 1 ns –0.40 –0.45 –0.50 –0.55 –0.60 1.608 ns 1.608 ns (Note 1) Negative transition Positive transition T1818940-02 NOTE 1 – The maximum "steady state" amplitude should not exceed the 0.55 V limit. Overshoots and other transients are permitted to fall into the dotted area, bounded by the amplitude levels 0.55 V and 0.6 V, provided that they do not exceed the steady state level by more than 0.05 V. The possibility of relaxing the amount by which the overshoot may exceed the steady state level is under study. NOTE 2 – For all measurements using these masks, the signal should be AC coupled, using a capacitor of not less than 0.01 µF, to the input of the oscilloscope used for measurements. The nominal zero level for both masks should be aligned with the oscilloscope trace with no input signal. With the signal then applied, the vertical position of the trace can be adjusted with the objective of meeting the limits of the masks. Any such adjustment should be the same for both masks and should not exceed ±0.05 V. This may be checked by removing the input signal again and verifying that the trace lies within ±0.05 V of the nominal zero level of the masks. NOTE 3 – Each pulse in a coded sequence should meet the limits of the relevant mask, irrespective of the state of the preceding or succeeding pulses, with both pulse masks fixed in the same relation to a common timing reference, i.e. with their nominal start and finish edges coincident. The masks allow for HF jitter caused by intersymbol interference in the output stage, but not for jitter present in the timing signal associated with the source of the interface signal. When using an oscilloscope technique to determine pulse compliance with the mask, it is important that successive traces of thepulses overlay in order to suppress the effects of low frequency jitter. This can be accomplished by several techniques [e.g. a) triggering the oscilloscope on the measured waveform or b) providing both the oscilloscope and the pulse output circuits with the same clock signal]. These techniques require further study. NOTE 4 – For the purpose of these masks, the rise time and decay time should be measured between –0.4 V and 0.4 V, and should not exceed 2 ns. NOTE 5 – The inverse pulse will have the same characteristics, noting that the timing tolerance at the level of the negative and positive transitions are ±0.1 ns and ±0.5 ns respectively. **Figure 23/G.703 – Mask of a pulse corresponding to a binary 1 (at the 155 520 kbit/s interface)**
Test Procedure	1. Connect the EUT as shown in the figure. 2. Enable the Port if required. 3. See whether the output pulse is within the mask/limits as indicated above.
Expected Results	Enclose the Test Results with the Pulse shape & the Pulse Mask

Test No.	8
Test Details	Test for Return Loss (This test is applicable to 64Kbps / 2048Kbps / 34Mbps/45Mbps/STM-1 interfaces)
Test Instruments Required	1. Network Analyser for PDH/SDH Interfaces 2. Vector Network Analyser with Balun to convert to differential voltage OR Signal Generator, Storage Oscilloscope & Return Loss Bridge

Test Setup

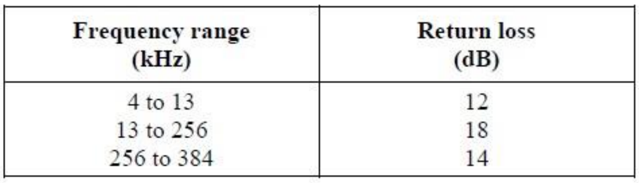


Test Limits

Minimum Return loss limits at input port for 64Kbps co-directional interface	Refer clause 4.2.1.3 of G.703
Minimum Return loss limits at output port for 64Kbps co-directional interface	Refer clause 4.2.1.2 of G.703
Minimum Return loss limits at input port for 2048 kbps (E1) interface	Refer clause 9.3 of G.703
Minimum Return loss limits at output port for 2048 kbps (E1) interface	Refer clause 9.2 of G.703
Minimum Return loss limits at input port for 34Mbps interface	Refer clause 11.3 of G.703
Minimum Return loss limits at output port for 34Mbps interface	Refer clause 11.2 of G.703
Minimum Return loss limits at input port for STM-1 interface	≥15 dB over frequency range 8 MHz to 240 MHz
Minimum Return loss limits at output port for STM-1 interface	≥15 dB over frequency range 8 MHz to 240 MHz

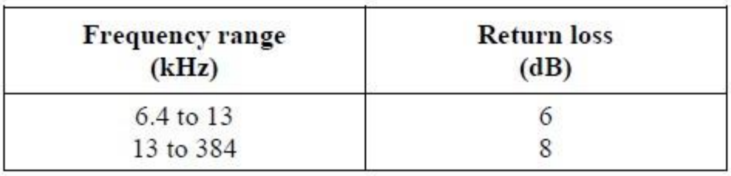
Standards Reference

clause 4.2.1.3 of G.703



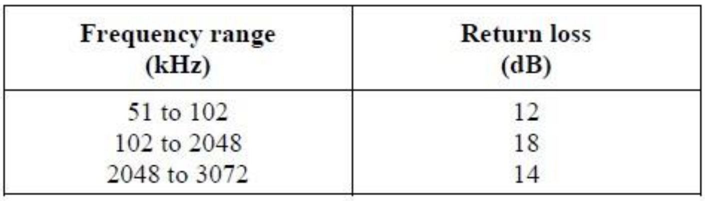
Frequency range (kHz)	Return loss (dB)
4 to 13	12
13 to 256	18
256 to 384	14

clause 4.2.1.2 of G.703



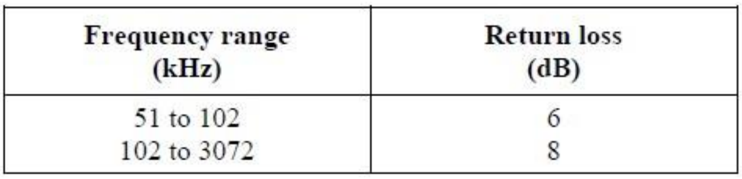
Frequency range (kHz)	Return loss (dB)
6.4 to 13	6
13 to 384	8

clause 9.3 of G.703



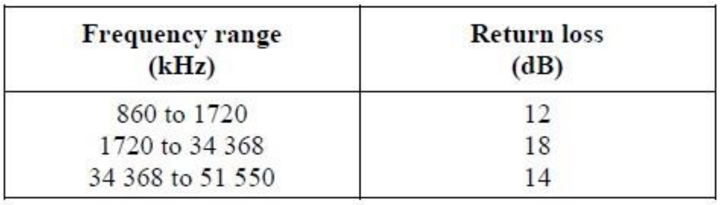
Frequency range (kHz)	Return loss (dB)
51 to 102	12
102 to 2048	18
2048 to 3072	14

clause 9.2 of G.703



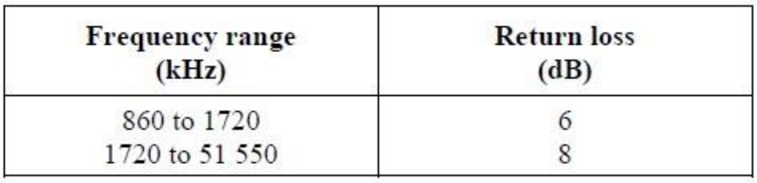
Frequency range (kHz)	Return loss (dB)
51 to 102	6
102 to 3072	8

clause 11.3 of G.703



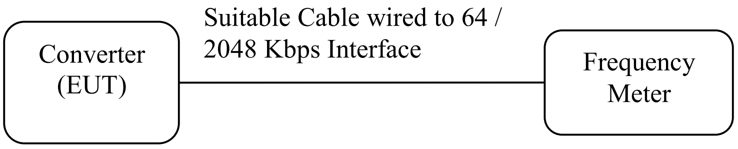
Frequency range (kHz)	Return loss (dB)
860 to 1720	12
1720 to 34 368	18
34 368 to 51 550	14

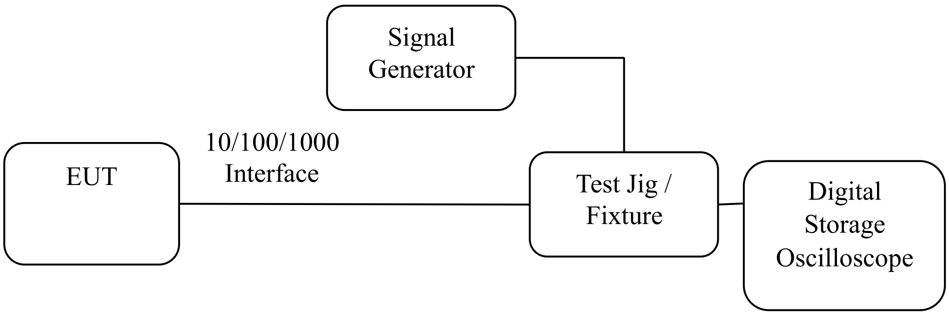
clause 11.2 of G.703



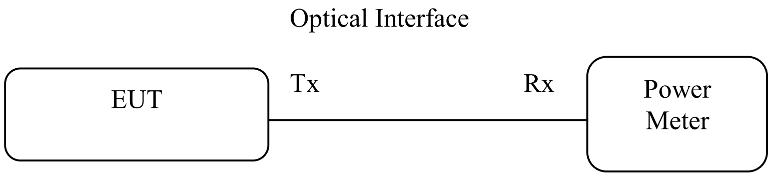
Frequency range (kHz)	Return loss (dB)
860 to 1720	6
1720 to 51 550	8

Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the input port return loss using the Network Analyser 3. Check whether the Return Loss is within the specified limits
Expected Results	Enclose the Test Results

<table>
<tr><td>Test No.</td><td>9</td></tr>
<tr><td>Test Details</td><td>Test for Output Frequency</td></tr>
<tr><td>Test Instruments Required</td><td>1. Frequency Meter</td></tr>
<tr><td>Test Setup</td><td>
</td></tr>
<tr><td>Test Limits</td><td><table><tr><td>64Kbps</td><td>±100 ppm</td></tr><tr><td>2048Kbps</td><td>±50 ppm</td></tr></table></td></tr>
<tr><td>Test Procedure</td><td>1. Connect the test setup as shown in figure using a suitable cable wired to the 64/2048Kbps interface
2. Measure the Output Frequency using the Frequency Meter</td></tr>
<tr><td>Expected Results</td><td>Enclose the Test Results</td></tr>
</table>

<table>
<tr><td>Test No.</td><td>10</td></tr>
<tr><td>Test Details</td><td>Test for Ethernet Interface
1. Differential output voltage
2. AC Differential input impedance
3. Output Jitter</td></tr>
<tr><td>Test Instruments Required</td><td>1. 2. Digital Storage Oscilloscope
3. Ethernet parameters measurement test Jig/Fixture
Signal generator</td></tr>
<tr><td>Test Setup</td><td>
</td></tr>
<tr><td>Test Limits</td><td>
<table>
<tr><td>Differential output voltage, loaded 10Base-T</td><td>Refer 14.3.1.2.1of IEEE802.3 Section1 Differential output voltage</td></tr>
<tr><td>Differential output voltage, 100Base-T</td><td>Refer 23.5.1.2.1 of IEEE802.3 Section2 Peak differential output voltage</td></tr>
<tr><td>Differential output voltage, loaded 1000Base-T</td><td>Refer 40.6.1.2.1 of IEEE802.3 Section3 Peak differential output voltage</td></tr>
<tr><td>Differential input impedance - 10BaseT</td><td>Refer 14.3.1.3.4 of IEEE802.3 Section-1AC differential input impedance</td></tr>
<tr><td>Receiver differential input impedance - 100Base-T</td><td>Refer 23.5.1.3.3 of IEEE802.3 Section-2 Receiver differential input impedance</td></tr>
<tr><td>10Base-T Output timing Jitter</td><td>Refer 14.3.1.2.3of IEEE802.3 Section 3 Output timing jitter</td></tr>
<tr><td>100base-T Output timing Jitter</td><td>Refer 23.5.1.2.5 of IEEE802.3 Section 3 Output timing jitter</td></tr>
<tr><td>1000Base-T Transmitter output Jitter</td><td>Refer 40.6.1.2.6 of IEEE802.3 Section 3 Transmitter Timing Jitter</td></tr>
</table>
</td></tr>
<tr><td>Test Procedure</td><td>1. Connect the test setup as shown in figure to the 10/100/1000Base-T interface
2. The test Jig / Fixture is an electronics hardware attached to the oscilloscope / Network analyser for the measurement of Ethernet parameters
3. Measure the Ethernet parameters</td></tr>
<tr><td>Expected Results</td><td>Enclose the Test Results</td></tr>
</table>

Note:	1. Tests can be conducted under one of the following options a. Test facility in TEC if available. b. Any Test Location in India including the premises of the trader/manufacturer of the product approved by RTEC where the Test facility is available for testing by RTEC.
	2. In case it is not possible to carry out the tests as above, the test results from any one of the following options can be accepted. RTEC shall verify whether the test results are within the prescribed limits. a. Results from any Indian/Foreign lab accredited as per ISO 17025 and having Ethernet Physical interface testing included in the scope of accreditation b. In house test results of the Equipment Under Test (EUT) in case of Foreign OEM c. In house test results of the Ethernet chipsets used in the EUT, from the OEM of the Ethernet chipset. The physical availability of the Ethernet Chipset in the EUT shall be verified by the RTEC. The following remark shall be indicated in the TAC. "The chipset number/code of the Ethernet chipset used in the equipment offered for testing: ……………….."

<table>
<tr><td>Test No.</td><td>11</td></tr>
<tr><td>Test Details</td><td>Test for output Power [Mean Launch Power]</td></tr>
<tr><td>Test Instruments Required</td><td>1. Optical Power Meter</td></tr>
<tr><td>Test Setup</td><td>
</td></tr>
<tr><td>Test Limits</td><td>
<table>
<tr><td>STM-1 Short Haul / Long Haul</td><td>Refer Table-2/G.957</td></tr>
<tr><td>STM-4 Short Haul / Long Haul</td><td>Refer Table-3/G.957</td></tr>
<tr><td>STM-16 Short Haul / Long Haul</td><td>Refer Table-4/G.957</td></tr>
<tr><td>FE Short Haul/Long Haul (100BASE-FX/SX/LX)</td><td>Refer IEEE 802.3u</td></tr>
<tr><td>GE Short Haul (1000BASE-SX)</td><td>Refer clause 38.3.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3</td></tr>
<tr><td>GE Long Haul (1000BASE-LX)</td><td>Refer clause 38.4.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3</td></tr>
<tr><td>10 GE Short Haul/Long Haul (10G-SR/LR/ER)</td><td>Refer table 52-7 for SR, 52-12 for LR and 52-16 for ER of IEEE 802.3ae specifications</td></tr>
<tr><td>40 GE (SR4/LR4)</td><td>Refer Table 86-6 for SR4 and 87-7 for LR4 of IEEE 802.3ba specifications</td></tr>
<tr><td>100 GE (SR10/LR4/ER4)</td><td>Refer Table 86-6 for SR10, 88-7 for LR4/ER4 of IEEE 802.3ba specifications</td></tr>
<tr><td>25 GE (SR/LR/ER)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>50 GE (SR/LR/ER/FR)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>200 GE (SR4/LR4/DR4/FR4)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>400 GE (SR8/LR8/DR4/FR8)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
</table>
</td></tr>
</table>

Standards Reference

Table-2/G.957

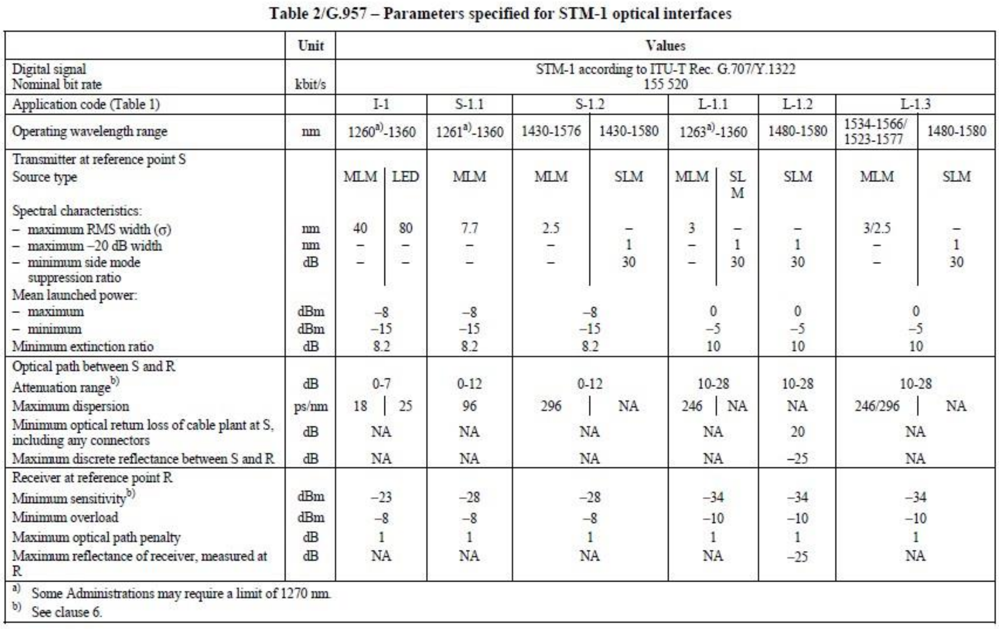


Table 2/G.957 – Parameters specified for STM-1 optical interfaces

	Unit	Values									
Digital signal Nominal bit rate	kbit/s	STM-1 according to ITU-T Rec. G.707/Y.1322 155 520									
Application code (Table 1)		I-1		S-1.1	S-1.2		L-1.1		L-1.2	L-1.3	
Operating wavelength range	nm	1260[a)]-1360		1261[a)]-1360	1430-1576	1430-1580	1263[a)]-1360		1480-1580	1534-1566/ 1523-1577	1480-1580
Transmitter at reference point S											
Source type		MLM	LED	MLM	MLM	SLM	MLM	SL M	SLM	MLM	SLM
Spectral characteristics:											
– maximum RMS width (σ)	nm	40	80	7.7	2.5	–	3	–	–	3/2.5	–
– maximum –20 dB width	nm	–	–	–	–	1	–	1	1	–	1
– minimum side mode suppression ratio	dB	–	–	–	–	30	–	30	30	–	30
Mean launched power:											
– maximum	dBm	–8		–8	–8		0		0	0	
– minimum	dBm	–15		–15	–15		–5		–5	–5	
Minimum extinction ratio	dB	8.2		8.2	8.2		10		10	10	
Optical path between S and R											
Attenuation range[b)]	dB	0-7		0-12	0-12		10-28		10-28	10-28	
Maximum dispersion	ps/nm	18	25	96	296	NA	246	NA	NA	246/296	NA
Minimum optical return loss of cable plant at S, including any connectors	dB	NA		NA	NA		NA		20	NA	
Maximum discrete reflectance between S and R	dB	NA		NA	NA		NA		–25	NA	
Receiver at reference point R											
Minimum sensitivity[b)]	dBm	–23		–28	–28		–34		–34	–34	
Minimum overload	dBm	–8		–8	–8		–10		–10	–10	
Maximum optical path penalty	dB	1		1	1		1		1	1	
Maximum reflectance of receiver, measured at R	dB	NA		NA	NA		NA		–25	NA	

[a)] Some Administrations may require a limit of 1270 nm.

[b)] See clause 6.

Table-3/G.957

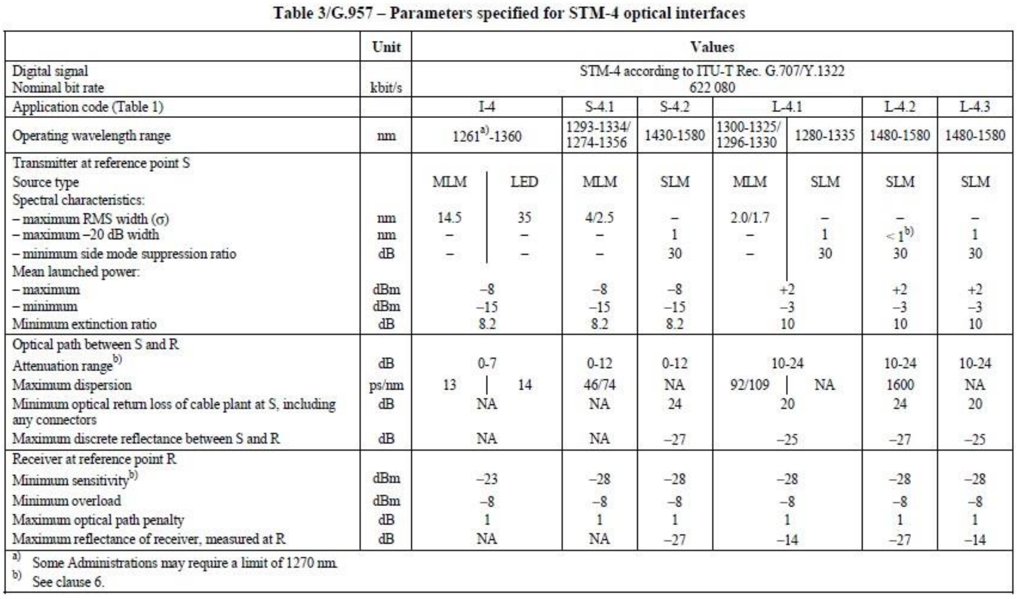


Table 3/G.957 – Parameters specified for STM-4 optical interfaces

	Unit	Values							
Digital signal Nominal bit rate	kbit/s	STM-4 according to ITU-T Rec. G.707/Y.1322 622 080							
Application code (Table 1)		I-4		S-4.1	S-4.2	L-4.1		L-4.2	L-4.3
Operating wavelength range	nm	1261[a)]-1360		1293-1334/ 1274-1356	1430-1580	1300-1325/ 1296-1330	1280-1335	1480-1580	1480-1580
Transmitter at reference point S									
Source type		MLM	LED	MLM	SLM	MLM	SLM	SLM	SLM
Spectral characteristics:									
– maximum RMS width (σ)	nm	14.5	35	4/2.5	–	2.0/1.7	–	–	–
– maximum –20 dB width	nm	–	–	–	1	–	1	< 1[b)]	1
– minimum side mode suppression ratio	dB	–	–	–	30	–	30	30	30
Mean launched power:									
– maximum	dBm	–8		–8	–8	+2		+2	+2
– minimum	dBm	–15		–15	–15	–3		–3	–3
Minimum extinction ratio	dB	8.2		8.2	8.2	10		10	10
Optical path between S and R									
Attenuation range[b)]	dB	0-7		0-12	0-12	10-24		10-24	10-24
Maximum dispersion	ps/nm	13	14	46/74	NA	92/109	NA	1600	NA
Minimum optical return loss of cable plant at S, including any connectors	dB	NA		NA	24	20		24	20
Maximum discrete reflectance between S and R	dB	NA		NA	–27	–25		–27	–25
Receiver at reference point R									
Minimum sensitivity[b)]	dBm	–23		–28	–28	–28		–28	–28
Minimum overload	dBm	–8		–8	–8	–8		–8	–8
Maximum optical path penalty	dB	1		1	1	1		1	1
Maximum reflectance of receiver, measured at R	dB	NA		NA	–27	–14		–27	–14

[a)] Some Administrations may require a limit of 1270 nm.

[b)] See clause 6.

Table-4/G.957

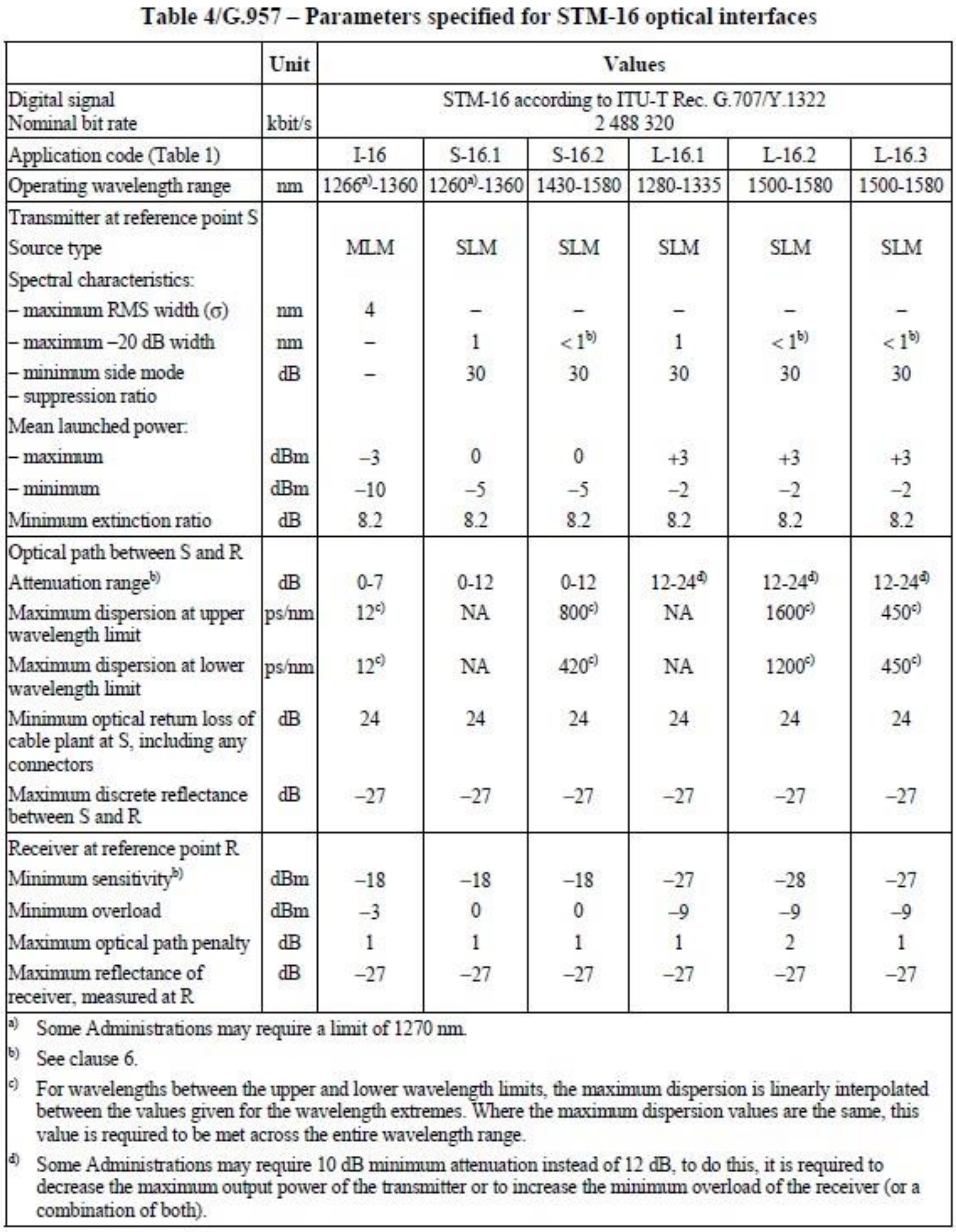


Table 4/G.957 – Parameters specified for STM-16 optical interfaces

	Unit	Values					
Digital signal Nominal bit rate	kbit/s	STM-16 according to ITU-T Rec. G.707/Y.1322 2 488 320					
Application code (Table 1)		I-16	S-16.1	S-16.2	L-16.1	L-16.2	L-16.3
Operating wavelength range	nm	1266[a]-1360	1260[a]-1360	1430-1580	1280-1335	1500-1580	1500-1580
Transmitter at reference point S							
Source type		MLM	SLM	SLM	SLM	SLM	SLM
Spectral characteristics:							
– maximum RMS width (σ)	nm	4	–	–	–	–	–
– maximum –20 dB width	nm	–	1	< 1[b]	1	< 1[b]	< 1[b]
– minimum side mode – suppression ratio	dB	–	30	30	30	30	30
Mean launched power:							
– maximum	dBm	–3	0	0	+3	+3	+3
– minimum	dBm	–10	–5	–5	–2	–2	–2
Minimum extinction ratio	dB	8.2	8.2	8.2	8.2	8.2	8.2
Optical path between S and R							
Attenuation range[b]	dB	0-7	0-12	0-12	12-24[d]	12-24[d]	12-24[d]
Maximum dispersion at upper wavelength limit	ps/nm	12[c]	NA	800[c]	NA	1600[c]	450[c]
Maximum dispersion at lower wavelength limit	ps/nm	12[c]	NA	420[c]	NA	1200[c]	450[c]
Minimum optical return loss of cable plant at S, including any connectors	dB	24	24	24	24	24	24
Maximum discrete reflectance between S and R	dB	–27	–27	–27	–27	–27	–27
Receiver at reference point R							
Minimum sensitivity[b]	dBm	–18	–18	–18	–27	–28	–27
Minimum overload	dBm	–3	0	0	–9	–9	–9
Maximum optical path penalty	dB	1	1	1	1	2	1
Maximum reflectance of receiver, measured at R	dB	–27	–27	–27	–27	–27	–27

[a] Some Administrations may require a limit of 1270 nm.

[b] See clause 6.

[c] For wavelengths between the upper and lower wavelength limits, the maximum dispersion is linearly interpolated between the values given for the wavelength extremes. Where the maximum dispersion values are the same, this value is required to be met across the entire wavelength range.

[d] Some Administrations may require 10 dB minimum attenuation instead of 12 dB, to do this, it is required to decrease the maximum output power of the transmitter or to increase the minimum overload of the receiver (or a combination of both).

Clause 38.3.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3

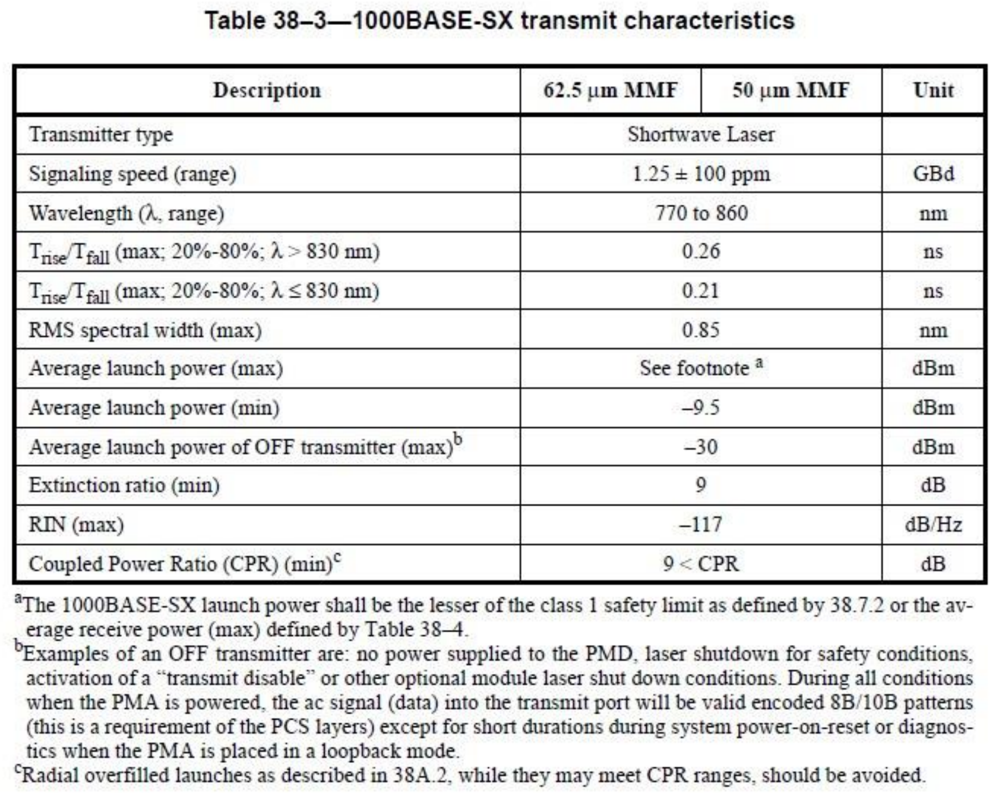


Table 38–3—1000BASE-SX transmit characteristics

Description	62.5 µm MMF	50 µm MMF	Unit
Transmitter type	Shortwave Laser		
Signaling speed (range)	1.25 ± 100 ppm		GBd
Wavelength (λ, range)	770 to 860		nm
T_{rise}/T_{fall} (max; 20%-80%; λ > 830 nm)	0.26		ns
T_{rise}/T_{fall} (max; 20%-80%; λ ≤ 830 nm)	0.21		ns
RMS spectral width (max)	0.85		nm
Average launch power (max)	See footnote [a]		dBm
Average launch power (min)	–9.5		dBm
Average launch power of OFF transmitter (max)[b]	–30		dBm
Extinction ratio (min)	9		dB
RIN (max)	–117		dB/Hz
Coupled Power Ratio (CPR) (min)[c]	9 < CPR		dB

[a] The 1000BASE-SX launch power shall be the lesser of the class 1 safety limit as defined by 38.7.2 or the average receive power (max) defined by Table 38–4.

[b] Examples of an OFF transmitter are: no power supplied to the PMD, laser shutdown for safety conditions, activation of a "transmit disable" or other optional module laser shut down conditions. During all conditions when the PMA is powered, the ac signal (data) into the transmit port will be valid encoded 8B/10B patterns (this is a requirement of the PCS layers) except for short durations during system power-on-reset or diagnostics when the PMA is placed in a loopback mode.

[c] Radial overfilled launches as described in 38A.2, while they may meet CPR ranges, should be avoided.

Clause 38.4.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3

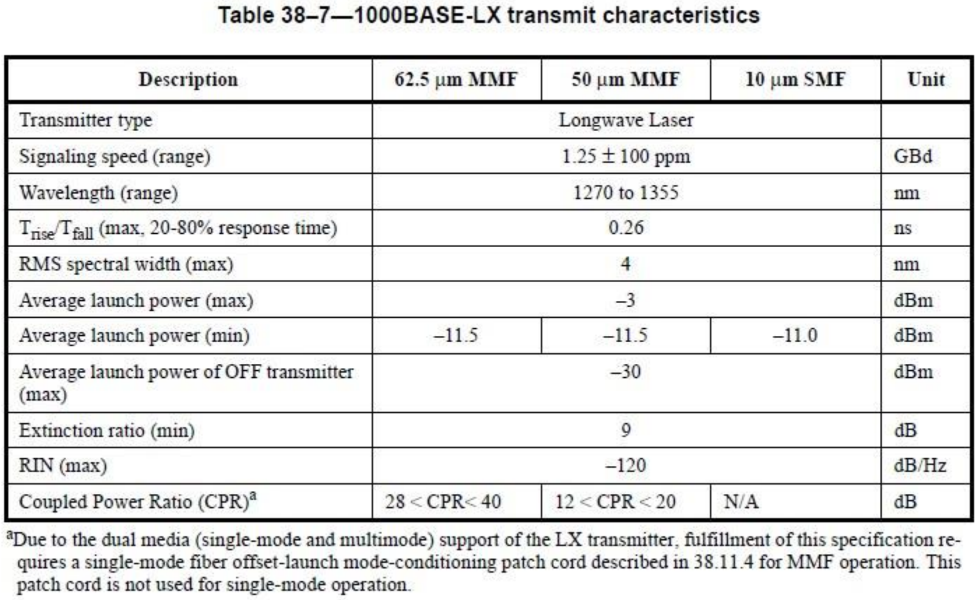


Table 38–7—1000BASE-LX transmit characteristics

Description	62.5 µm MMF	50 µm MMF	10 µm SMF	Unit
Transmitter type	Longwave Laser			
Signaling speed (range)	1.25 ± 100 ppm			GBd
Wavelength (range)	1270 to 1355			nm
T_{rise}/T_{fall} (max, 20-80% response time)	0.26			ns
RMS spectral width (max)	4			nm
Average launch power (max)	–3			dBm
Average launch power (min)	–11.5	–11.5	–11.0	dBm
Average launch power of OFF transmitter (max)	–30			dBm
Extinction ratio (min)	9			dB
RIN (max)	–120			dB/Hz
Coupled Power Ratio (CPR)[a]	28 < CPR< 40	12 < CPR < 20	N/A	dB

[a] Due to the dual media (single-mode and multimode) support of the LX transmitter, fulfillment of this specification requires a single-mode fiber offset-launch mode-conditioning patch cord described in 38.11.4 for MMF operation. This patch cord is not used for single-mode operation.

Table 52-7 for SRof IEEE 802.3ae specifications

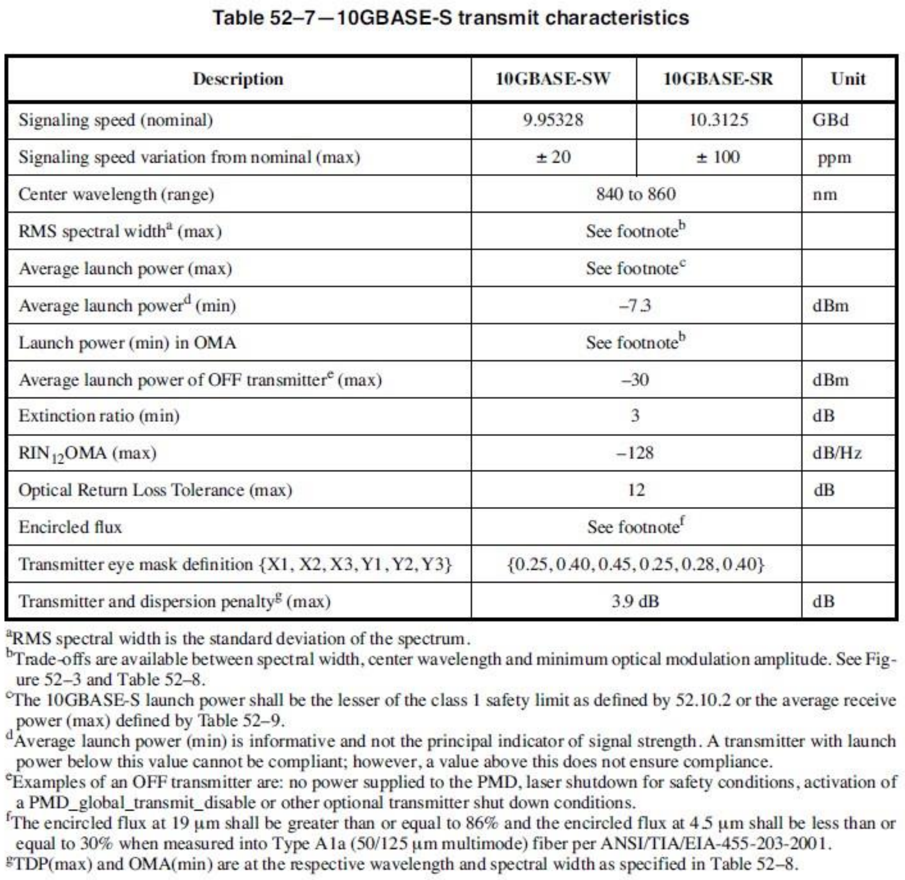


Table 52–7—10GBASE-S transmit characteristics

Description	10GBASE-SW	10GBASE-SR	Unit
Signaling speed (nominal)	9.95328	10.3125	GBd
Signaling speed variation from nominal (max)	± 20	± 100	ppm
Center wavelength (range)	840 to 860		nm
RMS spectral width[a] (max)	See footnote[b]		
Average launch power (max)	See footnote[c]		
Average launch power[d] (min)	−7.3		dBm
Launch power (min) in OMA	See footnote[b]		
Average launch power of OFF transmitter[e] (max)	−30		dBm
Extinction ratio (min)	3		dB
$RIN_{12}OMA$ (max)	−128		dB/Hz
Optical Return Loss Tolerance (max)	12		dB
Encircled flux	See footnote[f]		
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3}	{0.25, 0.40, 0.45, 0.25, 0.28, 0.40}		
Transmitter and dispersion penalty[g] (max)	3.9 dB		dB

[a] RMS spectral width is the standard deviation of the spectrum.

[b] Trade-offs are available between spectral width, center wavelength and minimum optical modulation amplitude. See Figure 52–3 and Table 52–8.

[c] The 10GBASE-S launch power shall be the lesser of the class 1 safety limit as defined by 52.10.2 or the average receive power (max) defined by Table 52–9.

[d] Average launch power (min) is informative and not the principal indicator of signal strength. A transmitter with launch power below this value cannot be compliant; however, a value above this does not ensure compliance.

[e] Examples of an OFF transmitter are: no power supplied to the PMD, laser shutdown for safety conditions, activation of a PMD_global_transmit_disable or other optional transmitter shut down conditions.

[f] The encircled flux at 19 µm shall be greater than or equal to 86% and the encircled flux at 4.5 µm shall be less than or equal to 30% when measured into Type A1a (50/125 µm multimode) fiber per ANSI/TIA/EIA-455-203-2001.

[g] TDP(max) and OMA(min) are at the respective wavelength and spectral width as specified in Table 52–8.

Table 52-12 for LR of IEEE 802.3ae specifications

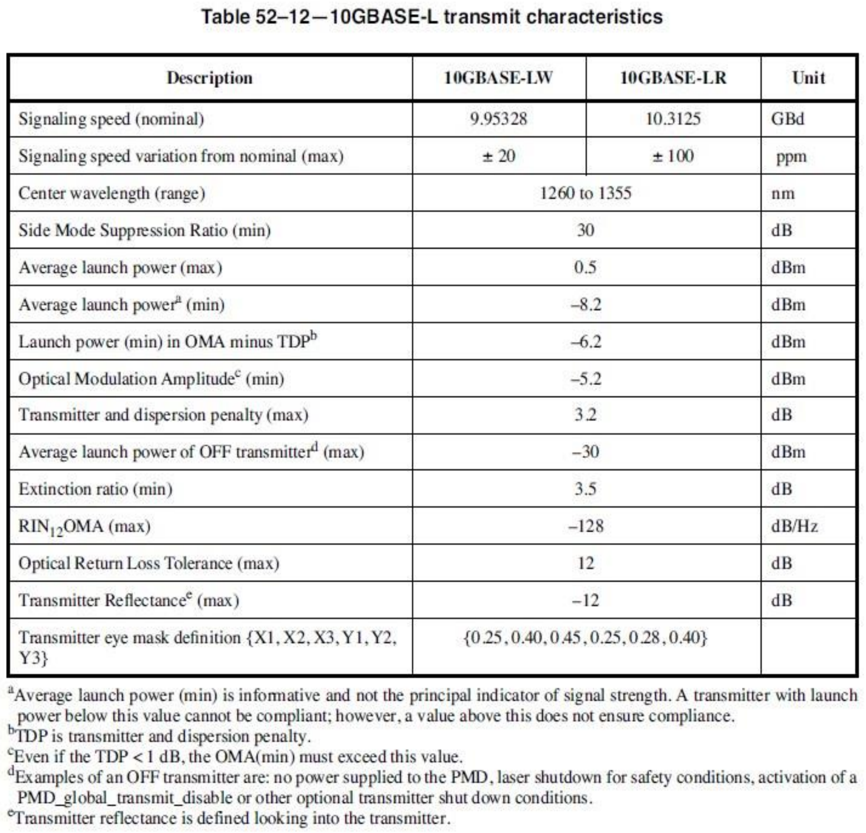


Table 52–12—10GBASE-L transmit characteristics

Description	10GBASE-LW	10GBASE-LR	Unit
Signaling speed (nominal)	9.95328	10.3125	GBd
Signaling speed variation from nominal (max)	± 20	± 100	ppm
Center wavelength (range)	1260 to 1355		nm
Side Mode Suppression Ratio (min)	30		dB
Average launch power (max)	0.5		dBm
Average launch power[a] (min)	−8.2		dBm
Launch power (min) in OMA minus TDP[b]	−6.2		dBm
Optical Modulation Amplitude[c] (min)	−5.2		dBm
Transmitter and dispersion penalty (max)	3.2		dB
Average launch power of OFF transmitter[d] (max)	−30		dBm
Extinction ratio (min)	3.5		dB
$RIN_{12}OMA$ (max)	−128		dB/Hz
Optical Return Loss Tolerance (max)	12		dB
Transmitter Reflectance[e] (max)	−12		dB
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3}	{0.25, 0.40, 0.45, 0.25, 0.28, 0.40}		

[a] Average launch power (min) is informative and not the principal indicator of signal strength. A transmitter with launch power below this value cannot be compliant; however, a value above this does not ensure compliance.

[b] TDP is transmitter and dispersion penalty.

[c] Even if the TDP < 1 dB, the OMA(min) must exceed this value.

[d] Examples of an OFF transmitter are: no power supplied to the PMD, laser shutdown for safety conditions, activation of a PMD_global_transmit_disable or other optional transmitter shut down conditions.

[e] Transmitter reflectance is defined looking into the transmitter.

Table 52-16 for ER of IEEE 802.3ae specifications

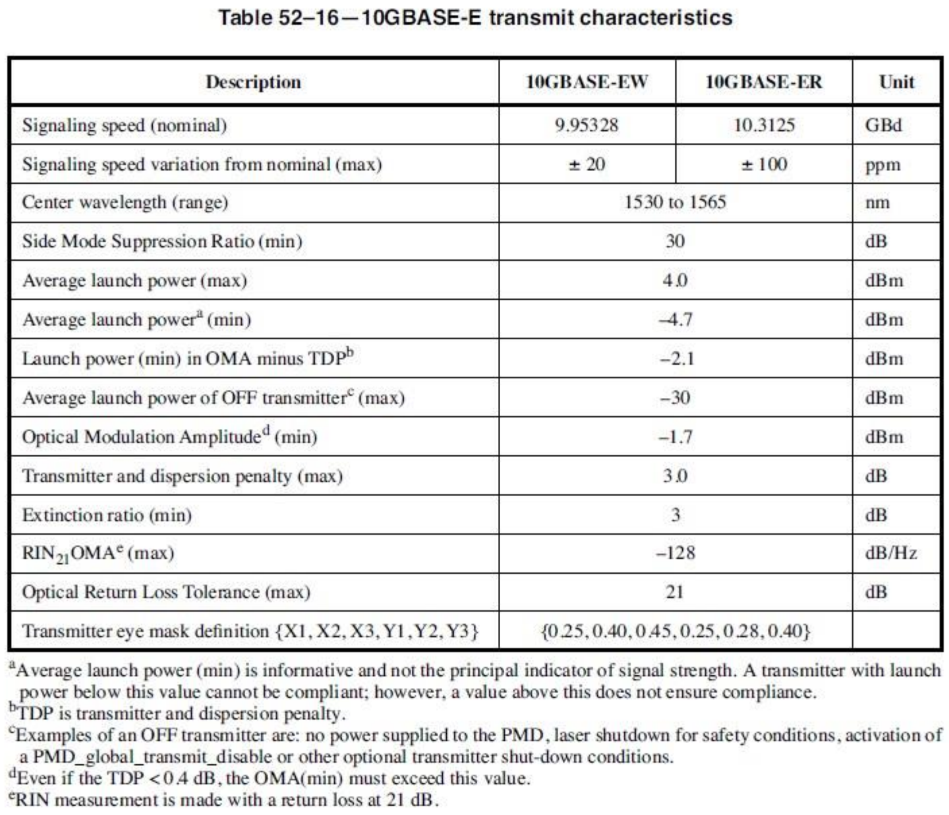


Table 52–16—10GBASE-E transmit characteristics

Description	10GBASE-EW	10GBASE-ER	Unit
Signaling speed (nominal)	9.95328	10.3125	GBd
Signaling speed variation from nominal (max)	± 20	± 100	ppm
Center wavelength (range)	1530 to 1565		nm
Side Mode Suppression Ratio (min)	30		dB
Average launch power (max)	4.0		dBm
Average launch power[a] (min)	–4.7		dBm
Launch power (min) in OMA minus TDP[b]	–2.1		dBm
Average launch power of OFF transmitter[c] (max)	–30		dBm
Optical Modulation Amplitude[d] (min)	–1.7		dBm
Transmitter and dispersion penalty (max)	3.0		dB
Extinction ratio (min)	3		dB
$RIN_{21}OMA$[e] (max)	–128		dB/Hz
Optical Return Loss Tolerance (max)	21		dB
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3}	{0.25, 0.40, 0.45, 0.25, 0.28, 0.40}		

[a] Average launch power (min) is informative and not the principal indicator of signal strength. A transmitter with launch power below this value cannot be compliant; however, a value above this does not ensure compliance.
[b] TDP is transmitter and dispersion penalty.
[c] Examples of an OFF transmitter are: no power supplied to the PMD, laser shutdown for safety conditions, activation of a PMD_global_transmit_disable or other optional transmitter shut-down conditions.
[d] Even if the TDP < 0.4 dB, the OMA(min) must exceed this value.
[e] RIN measurement is made with a return loss at 21 dB.

Table 86-6 for SR4/SR10 of IEEE 802.3ba specifications

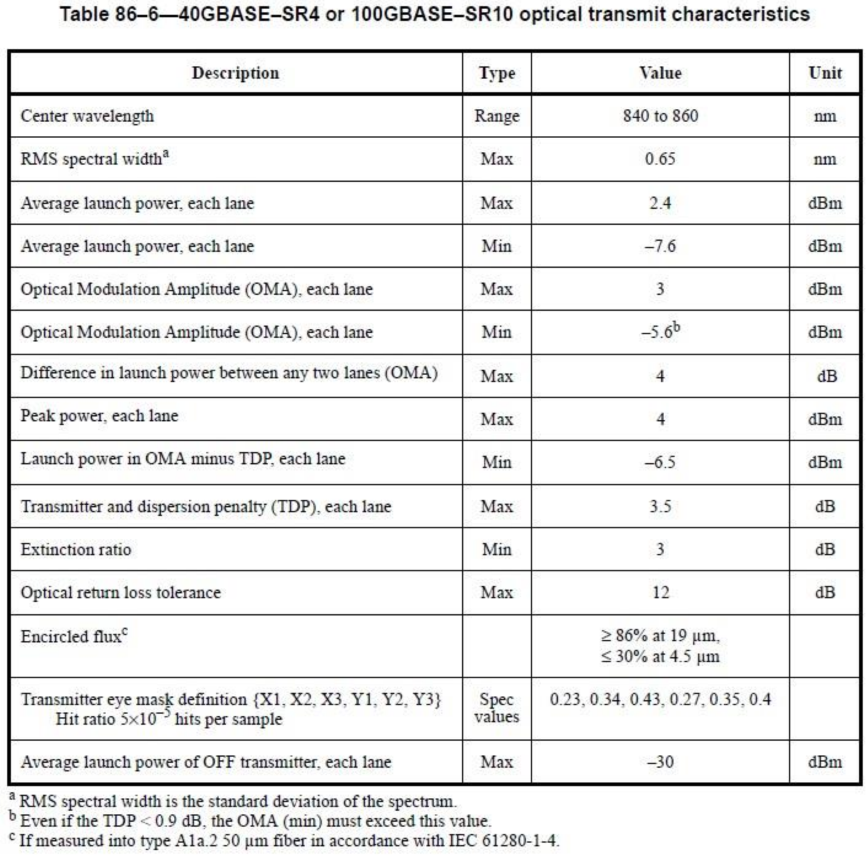


Table 86–6—40GBASE–SR4 or 100GBASE–SR10 optical transmit characteristics

Description	Type	Value	Unit
Center wavelength	Range	840 to 860	nm
RMS spectral width[a]	Max	0.65	nm
Average launch power, each lane	Max	2.4	dBm
Average launch power, each lane	Min	–7.6	dBm
Optical Modulation Amplitude (OMA), each lane	Max	3	dBm
Optical Modulation Amplitude (OMA), each lane	Min	–5.6[b]	dBm
Difference in launch power between any two lanes (OMA)	Max	4	dB
Peak power, each lane	Max	4	dBm
Launch power in OMA minus TDP, each lane	Min	–6.5	dBm
Transmitter and dispersion penalty (TDP), each lane	Max	3.5	dB
Extinction ratio	Min	3	dB
Optical return loss tolerance	Max	12	dB
Encircled flux[c]		≥ 86% at 19 µm, ≤ 30% at 4.5 µm	
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3} Hit ratio 5×10^{-5} hits per sample	Spec values	0.23, 0.34, 0.43, 0.27, 0.35, 0.4	
Average launch power of OFF transmitter, each lane	Max	–30	dBm

[a] RMS spectral width is the standard deviation of the spectrum.
[b] Even if the TDP < 0.9 dB, the OMA (min) must exceed this value.
[c] If measured into type A1a.2 50 µm fiber in accordance with IEC 61280-1-4.

Table 87-7 for LR4 of IEEE 802.3ba specifications

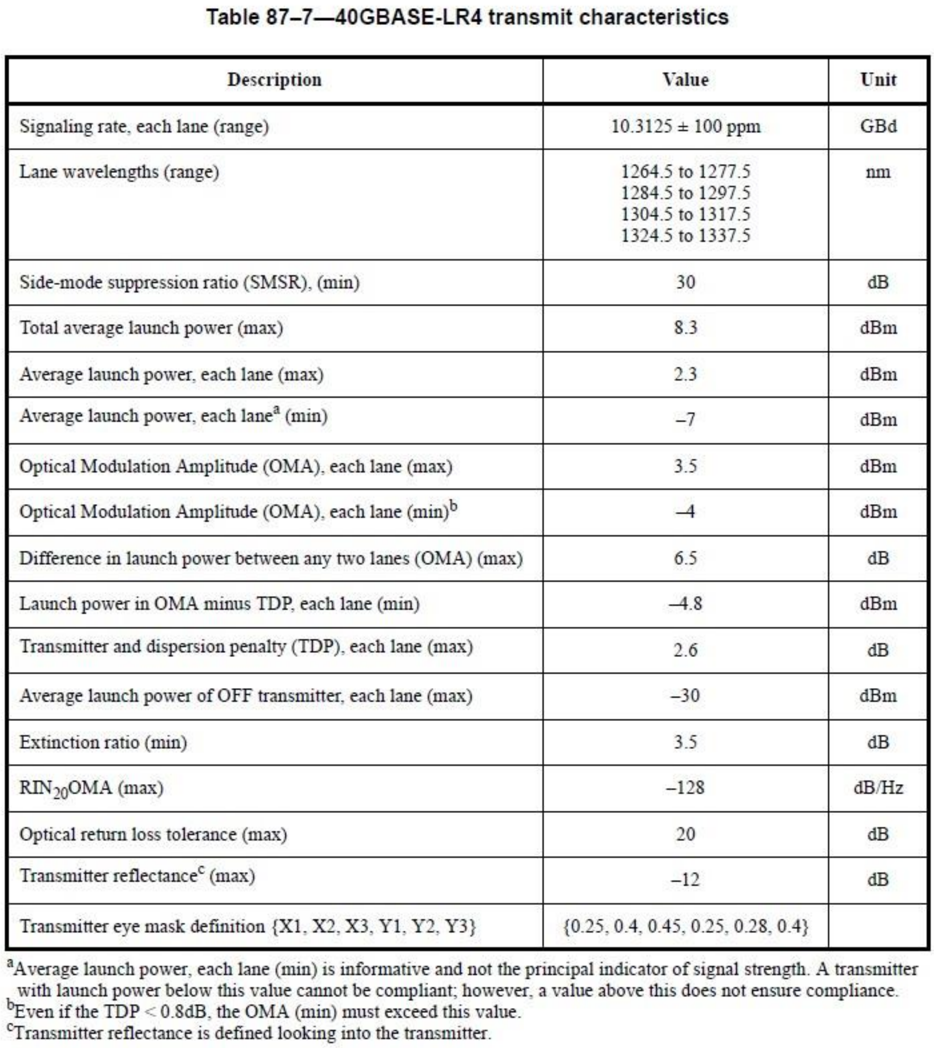


Table 87–7—40GBASE-LR4 transmit characteristics

Description	Value	Unit
Signaling rate, each lane (range)	10.3125 ± 100 ppm	GBd
Lane wavelengths (range)	1264.5 to 1277.5 1284.5 to 1297.5 1304.5 to 1317.5 1324.5 to 1337.5	nm
Side-mode suppression ratio (SMSR), (min)	30	dB
Total average launch power (max)	8.3	dBm
Average launch power, each lane (max)	2.3	dBm
Average launch power, each lane[a] (min)	–7	dBm
Optical Modulation Amplitude (OMA), each lane (max)	3.5	dBm
Optical Modulation Amplitude (OMA), each lane (min)[b]	–4	dBm
Difference in launch power between any two lanes (OMA) (max)	6.5	dB
Launch power in OMA minus TDP, each lane (min)	–4.8	dBm
Transmitter and dispersion penalty (TDP), each lane (max)	2.6	dB
Average launch power of OFF transmitter, each lane (max)	–30	dBm
Extinction ratio (min)	3.5	dB
$\text{RIN}_{20}\text{OMA}$ (max)	–128	dB/Hz
Optical return loss tolerance (max)	20	dB
Transmitter reflectance[c] (max)	–12	dB
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3}	{0.25, 0.4, 0.45, 0.25, 0.28, 0.4}	

[a] Average launch power, each lane (min) is informative and not the principal indicator of signal strength. A transmitter with launch power below this value cannot be compliant; however, a value above this does not ensure compliance.

[b] Even if the TDP < 0.8dB, the OMA (min) must exceed this value.

[c] Transmitter reflectance is defined looking into the transmitter.

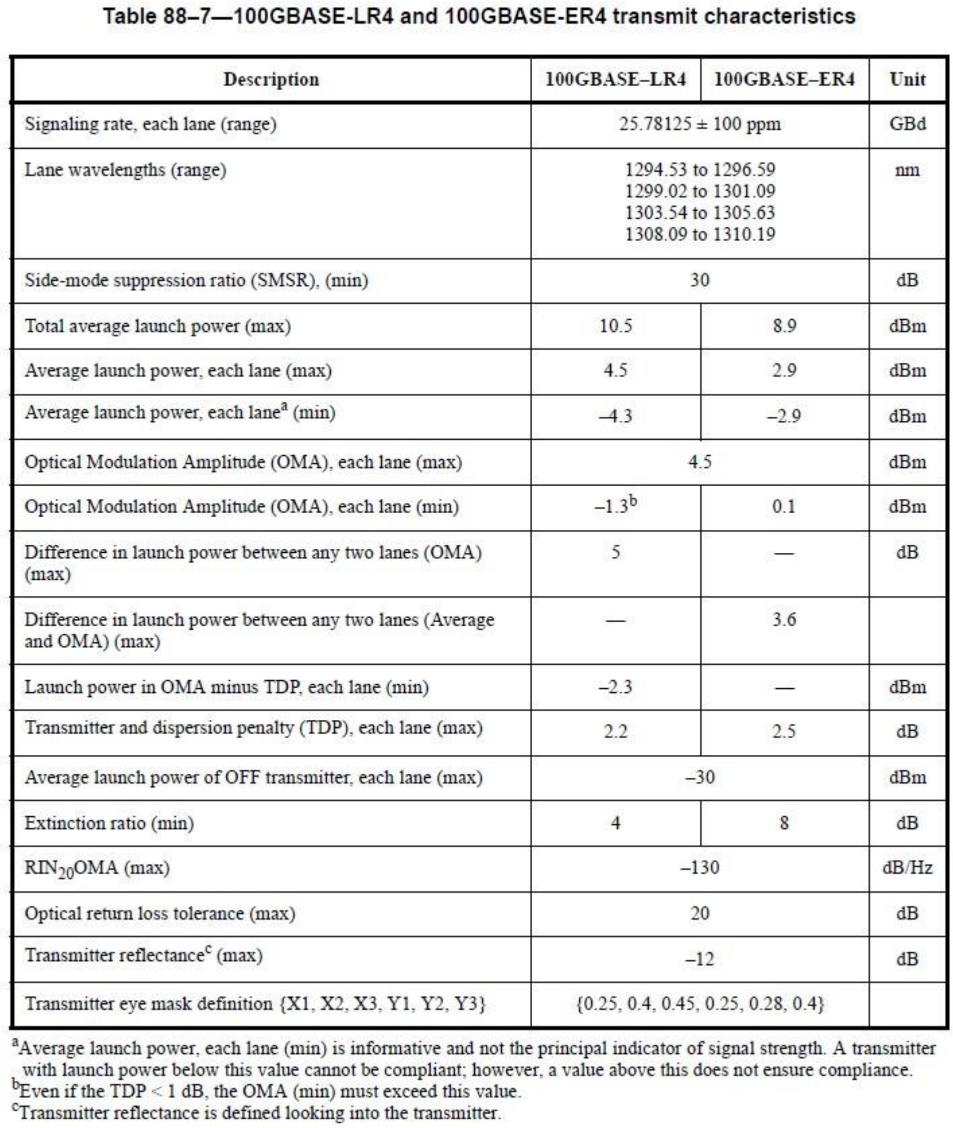
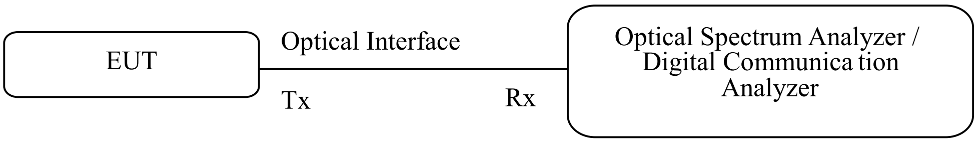
	Table 88-7 for LR4/ER4 of IEEE 802.3ba specifications
	

Table 88–7—100GBASE-LR4 and 100GBASE-ER4 transmit characteristics

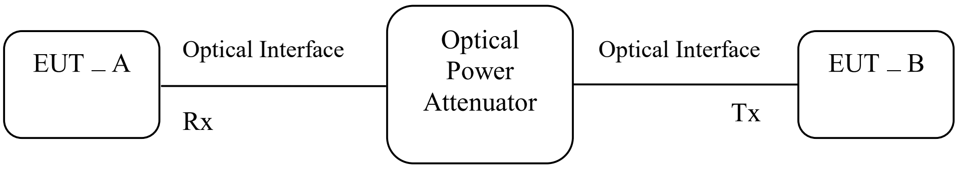
Description	100GBASE–LR4	100GBASE–ER4	Unit
Signaling rate, each lane (range)	25.78125 ± 100 ppm		GBd
Lane wavelengths (range)	1294.53 to 1296.59 1299.02 to 1301.09 1303.54 to 1305.63 1308.09 to 1310.19		nm
Side-mode suppression ratio (SMSR), (min)	30		dB
Total average launch power (max)	10.5	8.9	dBm
Average launch power, each lane (max)	4.5	2.9	dBm
Average launch power, each lane[a] (min)	–4.3	–2.9	dBm
Optical Modulation Amplitude (OMA), each lane (max)	4.5		dBm
Optical Modulation Amplitude (OMA), each lane (min)	–1.3[b]	0.1	dBm
Difference in launch power between any two lanes (OMA) (max)	5	—	dB
Difference in launch power between any two lanes (Average and OMA) (max)	—	3.6	
Launch power in OMA minus TDP, each lane (min)	–2.3	—	dBm
Transmitter and dispersion penalty (TDP), each lane (max)	2.2	2.5	dB
Average launch power of OFF transmitter, each lane (max)	–30		dBm
Extinction ratio (min)	4	8	dB
$RIN_{20}OMA$ (max)	–130		dB/Hz
Optical return loss tolerance (max)	20		dB
Transmitter reflectance[c] (max)	–12		dB
Transmitter eye mask definition {X1, X2, X3, Y1, Y2, Y3}	{0.25, 0.4, 0.45, 0.25, 0.28, 0.4}		

[a] Average launch power, each lane (min) is informative and not the principal indicator of signal strength. A transmitter with launch power below this value cannot be compliant; however, a value above this does not ensure compliance.
[b] Even if the TDP < 1 dB, the OMA (min) must exceed this value.
[c] Transmitter reflectance is defined looking into the transmitter.

Test Procedure	1. Connect the Setup as shown in the figure. 2. Enable the output Optical Port 3. Measure the optical output power 4. Check whether the output power is within the specification limits
Expected Results	Enclose the Test Results

<table>
<tr><td>Test No.</td><td colspan="2">12</td></tr>
<tr><td>Test Details</td><td colspan="2">Wavelength/Spectrum / Extinction Ratio</td></tr>
<tr><td>Test Instruments Required</td><td colspan="2">1. Optical Spectrum Analyser or Digital Communication Analyser</td></tr>
<tr><td>Test Setup</td><td colspan="2">
</td></tr>
<tr><td rowspan="13">Test Limits</td><td>STM-1 Short Haul / Long Haul</td><td>Refer Table-2/G.957</td></tr>
<tr><td>STM-4 Short Haul / Long Haul</td><td>Refer Table-3/G.957</td></tr>
<tr><td>STM-16 Short Haul / Long Haul</td><td>Refer Table-4/G.957</td></tr>
<tr><td>FE Short Haul/Long Haul (100BASE-FX/SX/LX)</td><td>Refer IEEE 802.3u</td></tr>
<tr><td>GE Short Haul (1000BASE-SX)</td><td>Refer clause 38.3.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3</td></tr>
<tr><td>GE Long Haul (1000BASE-LX)</td><td>Refer clause 38.4.1 Transmitter optical specifications of IEEE 802.3 2008 Section-3</td></tr>
<tr><td>10 GE Short Haul/Long Haul (10G-SR/LR/ER)</td><td>Refer table 52-7 for SR, 52-12 for LR and 52-16 for ER of IEEE 802.3ae specifications</td></tr>
<tr><td>40 GE (SR4/LR4)</td><td>Refer Table 86-6 for SR4 and 87-7 for LR of IEEE 802.3ba specifications</td></tr>
<tr><td>100 GE (SR10/LR4/ER4)</td><td>Refer Table 86-6 for SR10, 88-7 for LR4/ER4 of IEEE 802.3ba specifications</td></tr>
<tr><td>25 GE (SR/LR/ER)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>50 GE (SR/LR/ER/FR)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>200 GE (SR4/LR4/DR4/FR4)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>400 GE (SR8/LR8/DR4/FR8)</td><td>Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures</td></tr>
<tr><td>Standards Reference</td><td colspan="2">Refer the Standards Reference in Test 11</td></tr>
<tr><td>Test Procedure</td><td colspan="2">1. Connect the Setup as shown in the figure.
2. Enable the output Optical Port
3. Measure the Wavelength/Spectrum / Extinction Ratio
4. Check whether the Wavelength/Spectrum / Extinction Ratio is within the specification limits</td></tr>
</table>

Expected Results	Enclose the Test Results

Test No.	13	
Test Details	Test for Receiver Sensitivity	
Test Instruments Required	1. Optical Attenuator	
Test Setup	 EUT _ A Optical Interface Rx Optical Power Attenuator Optical Interface Tx EUT _ B	
Test Limits	STM-1 Short Haul / Long Haul	Refer Table-2/G.957 (Given under Test-11)
	STM-4 Short Haul / Long Haul	Refer Table-3/G.957 (Given under Test-11)
	STM-16 Short Haul / Long Haul	Refer Table-4/G.957 (Given under Test-11)
	FE Short Haul/Long Haul (100BASE-FX/SX/LX)	Refer IEEE 802.3u
	GE Short Haul (1000BASE-SX)	Refer clause 38.3.2 Receiver optical specifications of IEEE 802.3 2008 Section-3
	GE Long Haul (1000BASE-LX)	Refer clause 38.4.2 Receiver optical specifications of IEEE 802.3 2008 Section-3
	10 GE Short Haul/Long Haul (10G-SR/LR/ER)	Refer table 52-9 for SR, 52-13 for LR and 52-17 for ER of IEEE 802.3ae specifications
	40 GE (SR4/LR4)	Refer Table 86-8 for SR4 and 87-8 for LR4 of IEEE 802.3ba specifications
	100 GE (SR100/LR4/ER4)	Refer Table 86-8 for SR100, 88-8 for LR4/ER4 of IEEE 802.3ba specifications
	25 GE (SR/LR/ER)	Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures
	50 GE (SR/LR/ER/FR)	Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures
	200 GE (SR4/LR4/DR4/FR4)	Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures
	400 GE (SR8/LR8/DR4/FR8)	Refer Annexure H in Annexure to ER document available in https://www.mtcte.tec.gov.in/annexures

Standards Reference

Clause 38.3.2 Receiver optical specifications of IEEE 802.3 2008 Section-3

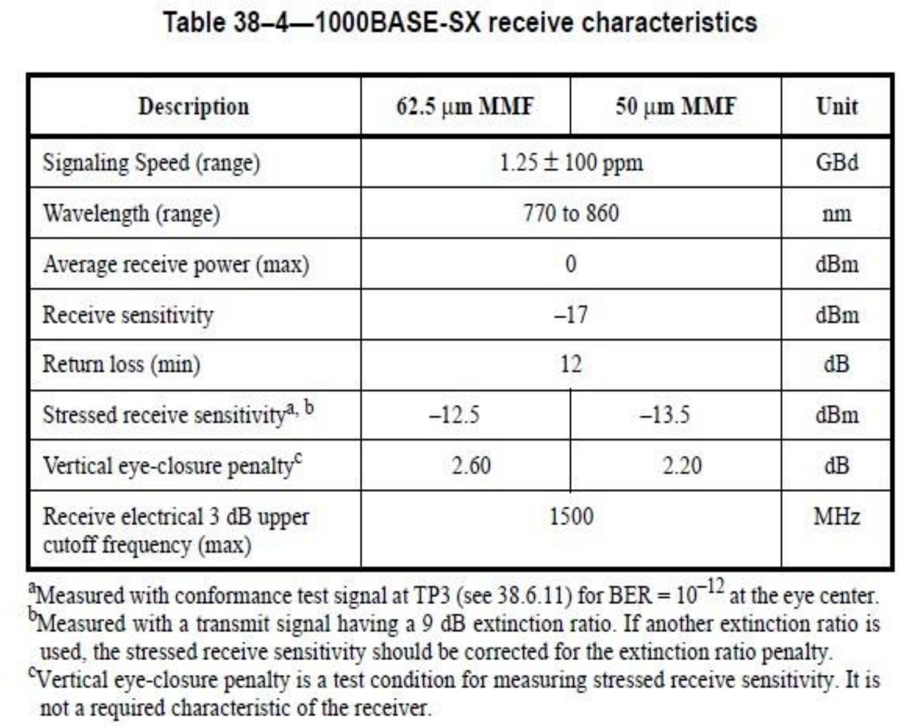


Table 38–4—1000BASE-SX receive characteristics

Description	62.5 µm MMF	50 µm MMF	Unit
Signaling Speed (range)	1.25 ± 100 ppm		GBd
Wavelength (range)	770 to 860		nm
Average receive power (max)	0		dBm
Receive sensitivity	–17		dBm
Return loss (min)	12		dB
Stressed receive sensitivity[a, b]	–12.5	–13.5	dBm
Vertical eye-closure penalty[c]	2.60	2.20	dB
Receive electrical 3 dB upper cutoff frequency (max)	1500		MHz

[a] Measured with conformance test signal at TP3 (see 38.6.11) for BER = 10^{-12} at the eye center.

[b] Measured with a transmit signal having a 9 dB extinction ratio. If another extinction ratio is used, the stressed receive sensitivity should be corrected for the extinction ratio penalty.

[c] Vertical eye-closure penalty is a test condition for measuring stressed receive sensitivity. It is not a required characteristic of the receiver.

Clause 38.4.2 Receiver optical specifications of IEEE 802.3 2008 Section-3

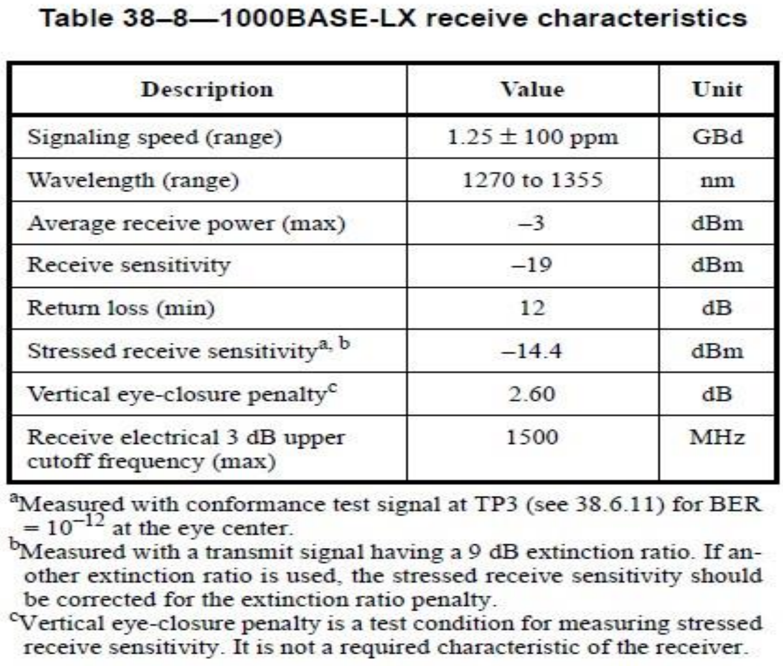


Table 38–8—1000BASE-LX receive characteristics

Description	Value	Unit
Signaling speed (range)	1.25 ± 100 ppm	GBd
Wavelength (range)	1270 to 1355	nm
Average receive power (max)	–3	dBm
Receive sensitivity	–19	dBm
Return loss (min)	12	dB
Stressed receive sensitivity[a, b]	–14.4	dBm
Vertical eye-closure penalty[c]	2.60	dB
Receive electrical 3 dB upper cutoff frequency (max)	1500	MHz

[a] Measured with conformance test signal at TP3 (see 38.6.11) for BER = 10^{-12} at the eye center.

[b] Measured with a transmit signal having a 9 dB extinction ratio. If another extinction ratio is used, the stressed receive sensitivity should be corrected for the extinction ratio penalty.

[c] Vertical eye-closure penalty is a test condition for measuring stressed receive sensitivity. It is not a required characteristic of the receiver.

Table 52-9 for SR of IEEE 802.3ae specifications

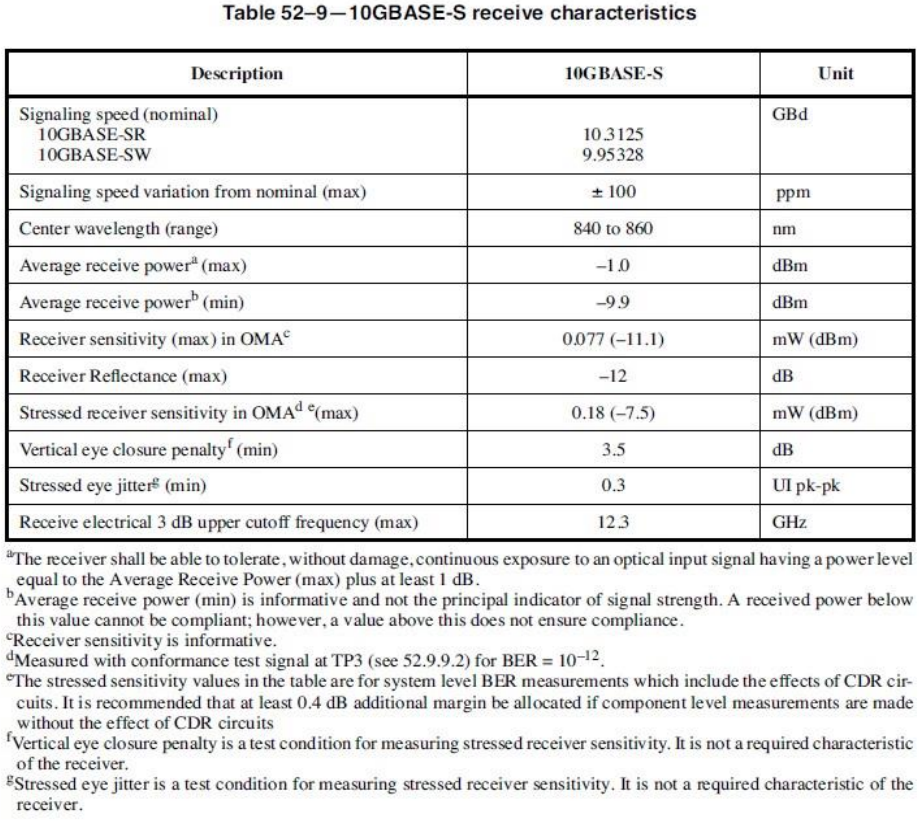


Table 52–9—10GBASE-S receive characteristics

Description	10GBASE-S	Unit
Signaling speed (nominal) 10GBASE-SR 10GBASE-SW	 10.3125 9.95328	GBd
Signaling speed variation from nominal (max)	± 100	ppm
Center wavelength (range)	840 to 860	nm
Average receive power[a] (max)	–1.0	dBm
Average receive power[b] (min)	–9.9	dBm
Receiver sensitivity (max) in OMA[c]	0.077 (–11.1)	mW (dBm)
Receiver Reflectance (max)	–12	dB
Stressed receiver sensitivity in OMA[d] [e](max)	0.18 (–7.5)	mW (dBm)
Vertical eye closure penalty[f] (min)	3.5	dB
Stressed eye jitter[g] (min)	0.3	UI pk-pk
Receive electrical 3 dB upper cutoff frequency (max)	12.3	GHz

[a] The receiver shall be able to tolerate, without damage, continuous exposure to an optical input signal having a power level equal to the Average Receive Power (max) plus at least 1 dB.

[b] Average receive power (min) is informative and not the principal indicator of signal strength. A received power below this value cannot be compliant; however, a value above this does not ensure compliance.

[c] Receiver sensitivity is informative.

[d] Measured with conformance test signal at TP3 (see 52.9.9.2) for BER = 10^{-12}.

[e] The stressed sensitivity values in the table are for system level BER measurements which include the effects of CDR circuits. It is recommended that at least 0.4 dB additional margin be allocated if component level measurements are made without the effect of CDR circuits

[f] Vertical eye closure penalty is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

[g] Stressed eye jitter is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

Table 52-13 for LR of IEEE 802.3ae specifications

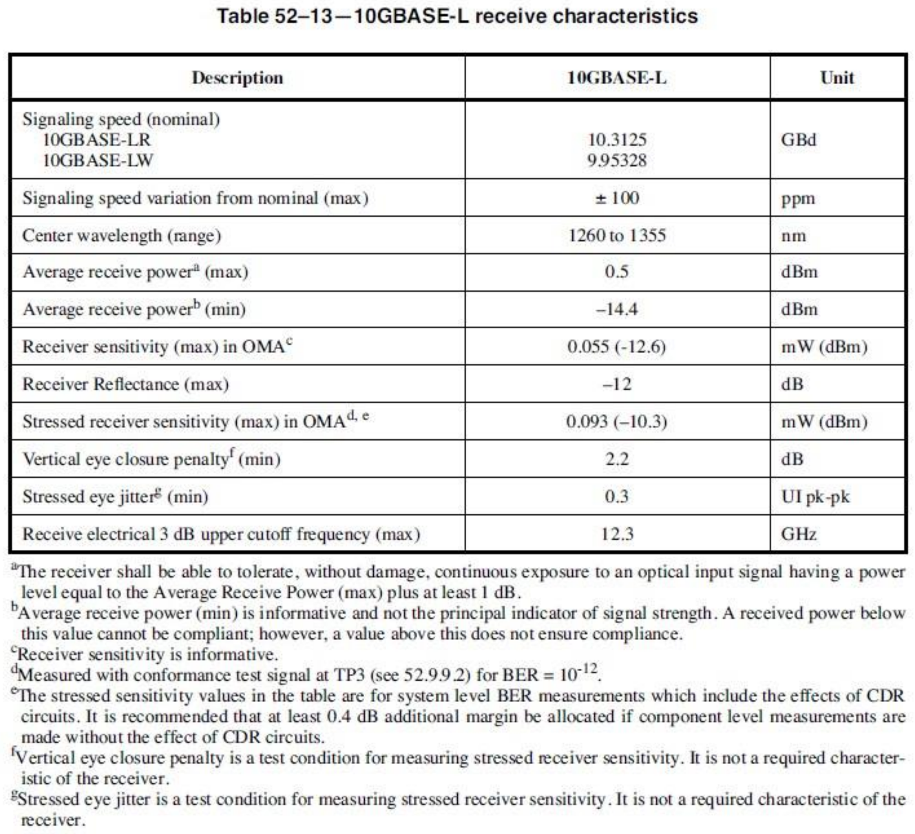


Table 52–13—10GBASE-L receive characteristics

Description	10GBASE-L	Unit
Signaling speed (nominal) 10GBASE-LR 10GBASE-LW	 10.3125 9.95328	GBd
Signaling speed variation from nominal (max)	± 100	ppm
Center wavelength (range)	1260 to 1355	nm
Average receive power[a] (max)	0.5	dBm
Average receive power[b] (min)	–14.4	dBm
Receiver sensitivity (max) in OMA[c]	0.055 (-12.6)	mW (dBm)
Receiver Reflectance (max)	–12	dB
Stressed receiver sensitivity (max) in OMA[d, e]	0.093 (–10.3)	mW (dBm)
Vertical eye closure penalty[f] (min)	2.2	dB
Stressed eye jitter[g] (min)	0.3	UI pk-pk
Receive electrical 3 dB upper cutoff frequency (max)	12.3	GHz

[a] The receiver shall be able to tolerate, without damage, continuous exposure to an optical input signal having a power level equal to the Average Receive Power (max) plus at least 1 dB.

[b] Average receive power (min) is informative and not the principal indicator of signal strength. A received power below this value cannot be compliant; however, a value above this does not ensure compliance.

[c] Receiver sensitivity is informative.

[d] Measured with conformance test signal at TP3 (see 52.9.9.2) for BER = 10^{-12}.

[e] The stressed sensitivity values in the table are for system level BER measurements which include the effects of CDR circuits. It is recommended that at least 0.4 dB additional margin be allocated if component level measurements are made without the effect of CDR circuits.

[f] Vertical eye closure penalty is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

[g] Stressed eye jitter is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

Table 52-17 for ER of IEEE 802.3ae specifications

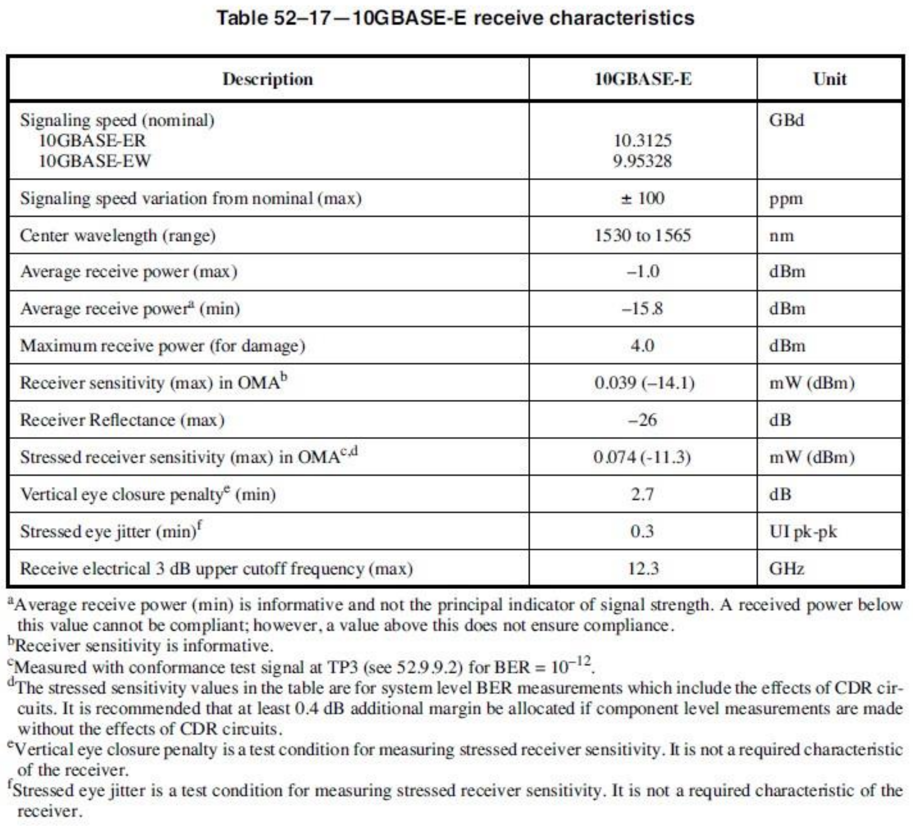


Table 52–17—10GBASE-E receive characteristics

Description	10GBASE-E	Unit
Signaling speed (nominal) 10GBASE-ER 10GBASE-EW	 10.3125 9.95328	GBd
Signaling speed variation from nominal (max)	± 100	ppm
Center wavelength (range)	1530 to 1565	nm
Average receive power (max)	–1.0	dBm
Average receive power[a] (min)	–15.8	dBm
Maximum receive power (for damage)	4.0	dBm
Receiver sensitivity (max) in OMA[b]	0.039 (–14.1)	mW (dBm)
Receiver Reflectance (max)	–26	dB
Stressed receiver sensitivity (max) in OMA[c,d]	0.074 (-11.3)	mW (dBm)
Vertical eye closure penalty[e] (min)	2.7	dB
Stressed eye jitter (min)[f]	0.3	UI pk-pk
Receive electrical 3 dB upper cutoff frequency (max)	12.3	GHz

[a] Average receive power (min) is informative and not the principal indicator of signal strength. A received power below this value cannot be compliant; however, a value above this does not ensure compliance.

[b] Receiver sensitivity is informative.

[c] Measured with conformance test signal at TP3 (see 52.9.9.2) for BER = 10^{-12}.

[d] The stressed sensitivity values in the table are for system level BER measurements which include the effects of CDR circuits. It is recommended that at least 0.4 dB additional margin be allocated if component level measurements are made without the effects of CDR circuits.

[e] Vertical eye closure penalty is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

[f] Stressed eye jitter is a test condition for measuring stressed receiver sensitivity. It is not a required characteristic of the receiver.

Table 86-8 for SR4/SR100 of IEEE 802.3ba specifications

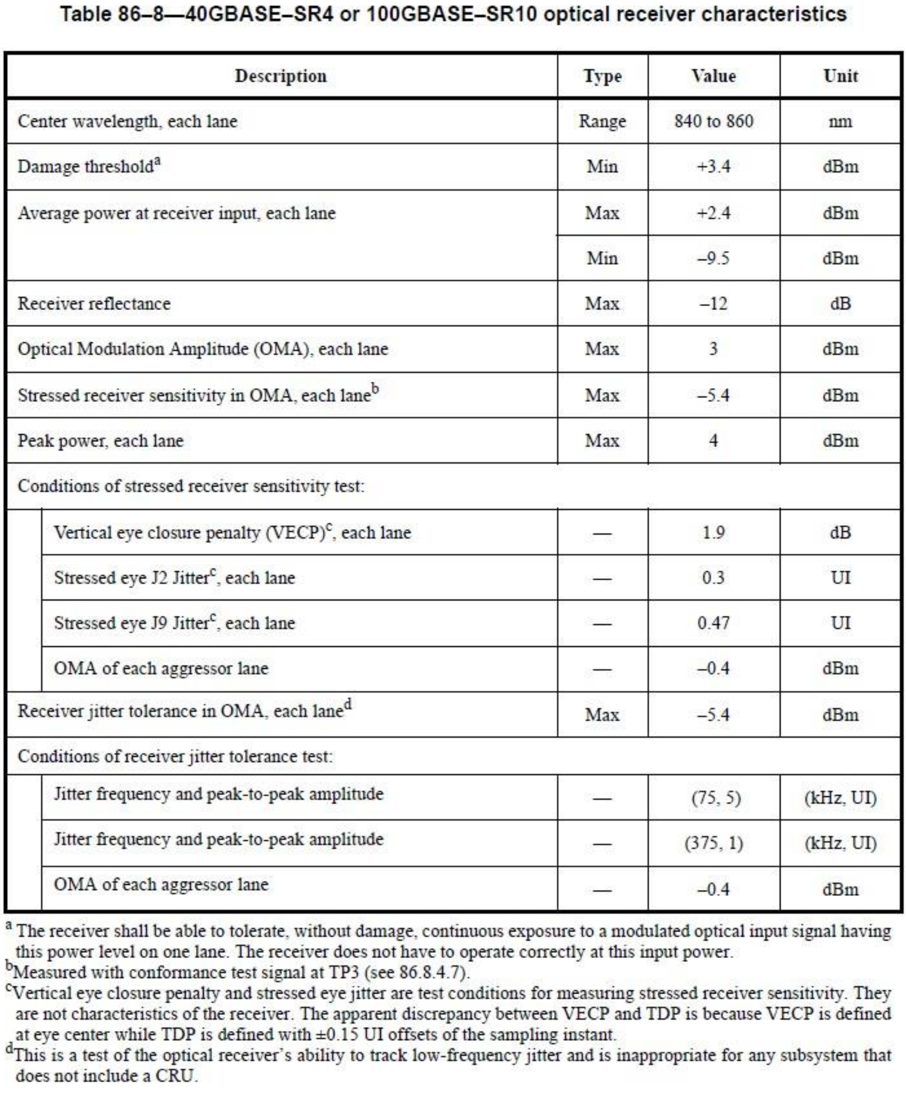


Table 86–8—40GBASE–SR4 or 100GBASE–SR10 optical receiver characteristics

Description	Type	Value	Unit
Center wavelength, each lane	Range	840 to 860	nm
Damage threshold[a]	Min	+3.4	dBm
Average power at receiver input, each lane	Max	+2.4	dBm
	Min	–9.5	dBm
Receiver reflectance	Max	–12	dB
Optical Modulation Amplitude (OMA), each lane	Max	3	dBm
Stressed receiver sensitivity in OMA, each lane[b]	Max	–5.4	dBm
Peak power, each lane	Max	4	dBm
Conditions of stressed receiver sensitivity test:			
Vertical eye closure penalty (VECP)[c], each lane	—	1.9	dB
Stressed eye J2 Jitter[c], each lane	—	0.3	UI
Stressed eye J9 Jitter[c], each lane	—	0.47	UI
OMA of each aggressor lane	—	–0.4	dBm
Receiver jitter tolerance in OMA, each lane[d]	Max	–5.4	dBm
Conditions of receiver jitter tolerance test:			
Jitter frequency and peak-to-peak amplitude	—	(75, 5)	(kHz, UI)
Jitter frequency and peak-to-peak amplitude	—	(375, 1)	(kHz, UI)
OMA of each aggressor lane	—	–0.4	dBm

[a] The receiver shall be able to tolerate, without damage, continuous exposure to a modulated optical input signal having this power level on one lane. The receiver does not have to operate correctly at this input power.

[b] Measured with conformance test signal at TP3 (see 86.8.4.7).

[c] Vertical eye closure penalty and stressed eye jitter are test conditions for measuring stressed receiver sensitivity. They are not characteristics of the receiver. The apparent discrepancy between VECP and TDP is because VECP is defined at eye center while TDP is defined with ±0.15 UI offsets of the sampling instant.

[d] This is a test of the optical receiver's ability to track low-frequency jitter and is inappropriate for any subsystem that does not include a CRU.

Table 87-8 for LR4 of IEEE 802.3ba specifications

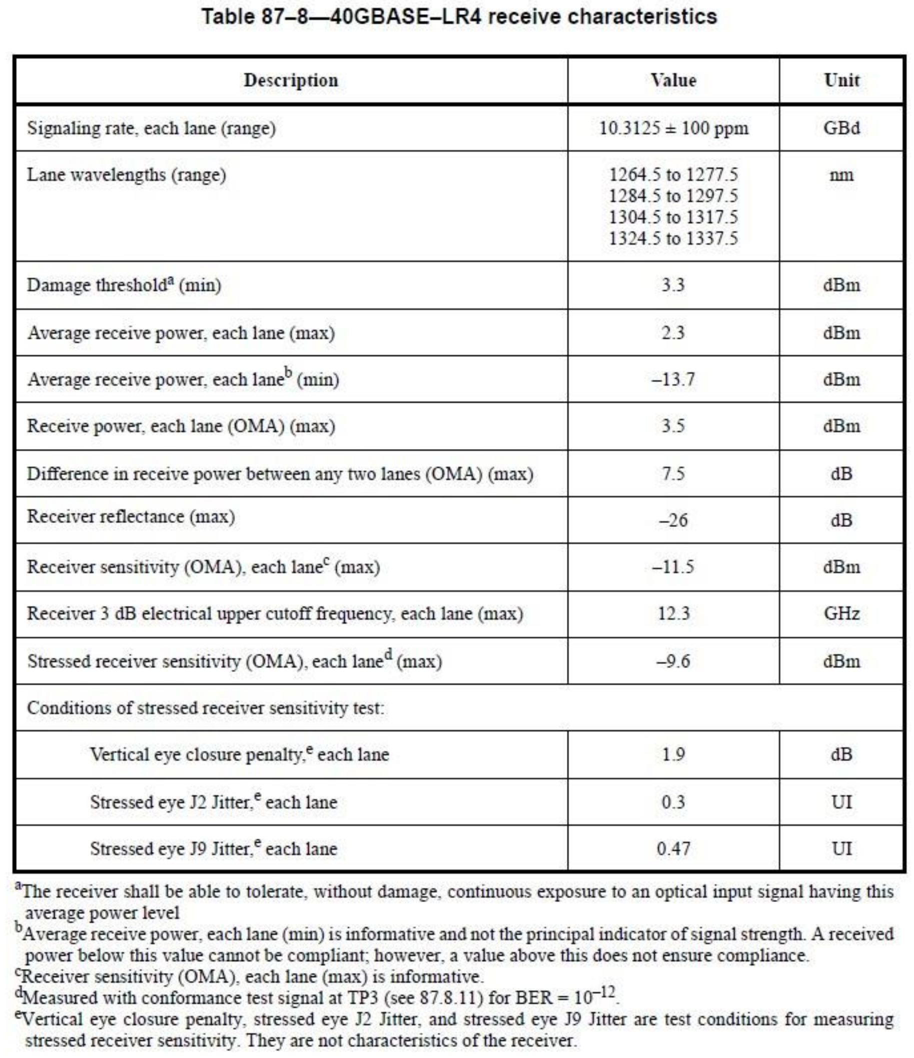


Table 87–8—40GBASE–LR4 receive characteristics

Description	Value	Unit
Signaling rate, each lane (range)	10.3125 ± 100 ppm	GBd
Lane wavelengths (range)	1264.5 to 1277.5 1284.5 to 1297.5 1304.5 to 1317.5 1324.5 to 1337.5	nm
Damage threshold[a] (min)	3.3	dBm
Average receive power, each lane (max)	2.3	dBm
Average receive power, each lane[b] (min)	–13.7	dBm
Receive power, each lane (OMA) (max)	3.5	dBm
Difference in receive power between any two lanes (OMA) (max)	7.5	dB
Receiver reflectance (max)	–26	dB
Receiver sensitivity (OMA), each lane[c] (max)	–11.5	dBm
Receiver 3 dB electrical upper cutoff frequency, each lane (max)	12.3	GHz
Stressed receiver sensitivity (OMA), each lane[d] (max)	–9.6	dBm
Conditions of stressed receiver sensitivity test:		
Vertical eye closure penalty,[e] each lane	1.9	dB
Stressed eye J2 Jitter,[e] each lane	0.3	UI
Stressed eye J9 Jitter,[e] each lane	0.47	UI

[a] The receiver shall be able to tolerate, without damage, continuous exposure to an optical input signal having this average power level

[b] Average receive power, each lane (min) is informative and not the principal indicator of signal strength. A received power below this value cannot be compliant; however, a value above this does not ensure compliance.

[c] Receiver sensitivity (OMA), each lane (max) is informative.

[d] Measured with conformance test signal at TP3 (see 87.8.11) for BER = 10^{-12}.

[e] Vertical eye closure penalty, stressed eye J2 Jitter, and stressed eye J9 Jitter are test conditions for measuring stressed receiver sensitivity. They are not characteristics of the receiver.

Table 88-8 for LR4/ER4 of IEEE 802.3ba specifications

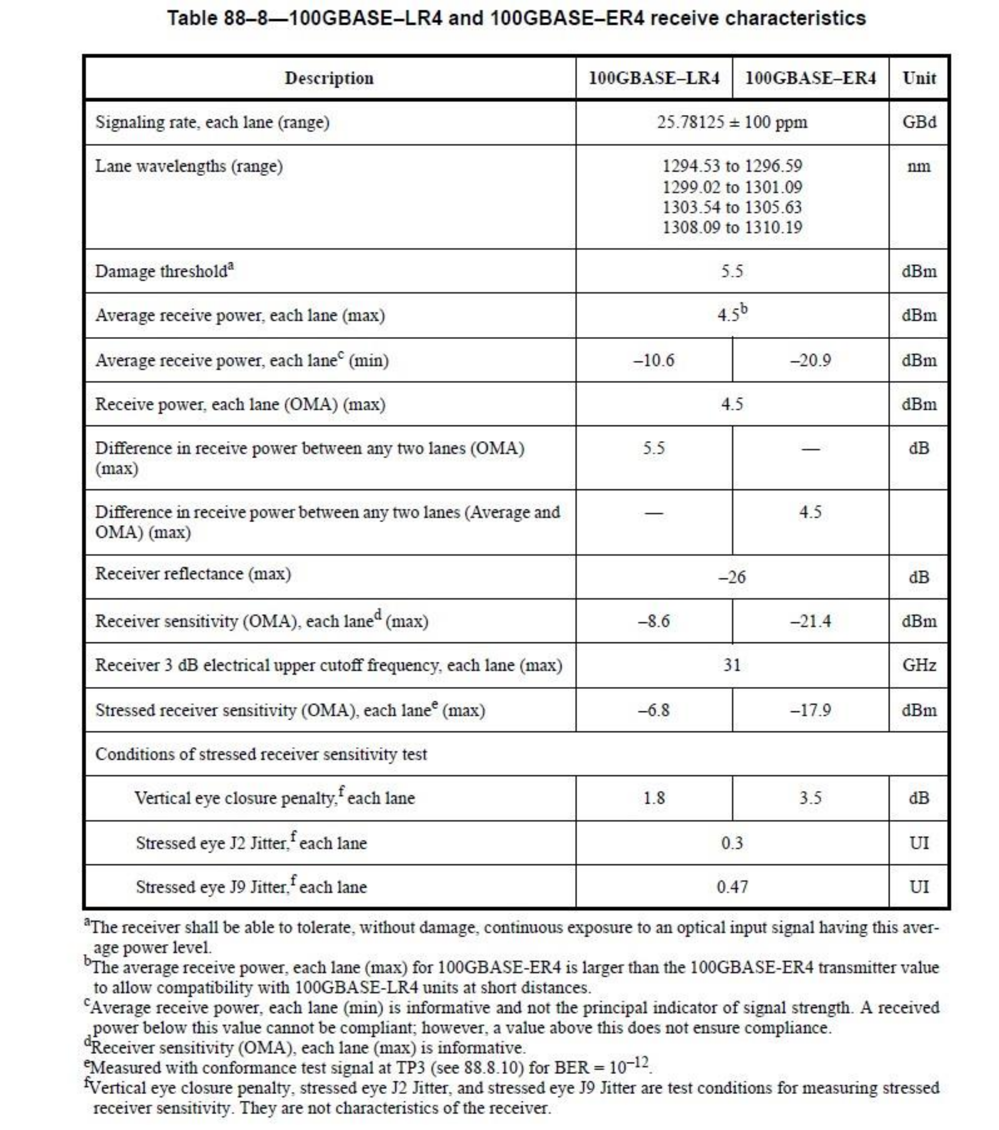


Table 88–8—100GBASE–LR4 and 100GBASE–ER4 receive characteristics

Description	100GBASE–LR4	100GBASE–ER4	Unit
Signaling rate, each lane (range)	25.78125 ± 100 ppm		GBd
Lane wavelengths (range)	1294.53 to 1296.59 1299.02 to 1301.09 1303.54 to 1305.63 1308.09 to 1310.19		nm
Damage threshold[a]	5.5		dBm
Average receive power, each lane (max)	4.5[b]		dBm
Average receive power, each lane[c] (min)	–10.6	–20.9	dBm
Receive power, each lane (OMA) (max)	4.5		dBm
Difference in receive power between any two lanes (OMA) (max)	5.5	—	dB
Difference in receive power between any two lanes (Average and OMA) (max)	—	4.5	
Receiver reflectance (max)	–26		dB
Receiver sensitivity (OMA), each lane[d] (max)	–8.6	–21.4	dBm
Receiver 3 dB electrical upper cutoff frequency, each lane (max)	31		GHz
Stressed receiver sensitivity (OMA), each lane[e] (max)	–6.8	–17.9	dBm
Conditions of stressed receiver sensitivity test			
Vertical eye closure penalty,[f] each lane	1.8	3.5	dB
Stressed eye J2 Jitter,[f] each lane	0.3		UI
Stressed eye J9 Jitter,[f] each lane	0.47		UI

[a] The receiver shall be able to tolerate, without damage, continuous exposure to an optical input signal having this average power level.

[b] The average receive power, each lane (max) for 100GBASE-ER4 is larger than the 100GBASE-ER4 transmitter value to allow compatibility with 100GBASE-LR4 units at short distances.

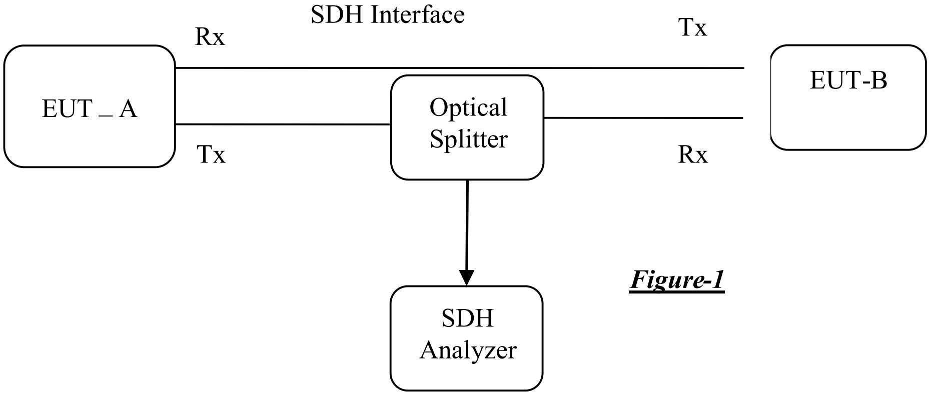
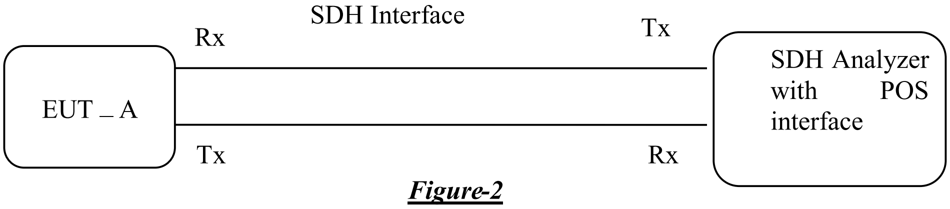
[c] Average receive power, each lane (min) is informative and not the principal indicator of signal strength. A received power below this value cannot be compliant; however, a value above this does not ensure compliance.

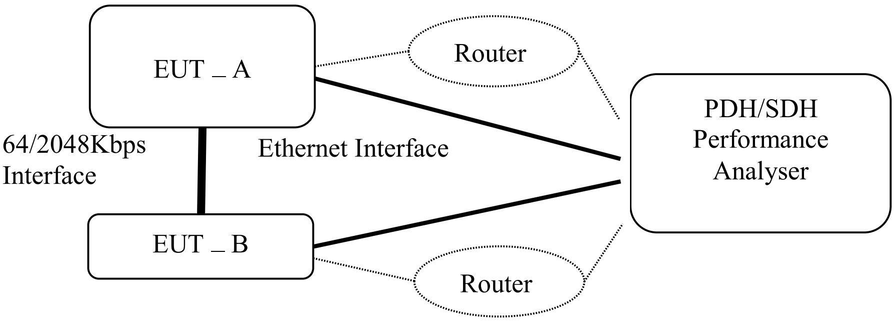
[d] Receiver sensitivity (OMA), each lane (max) is informative.

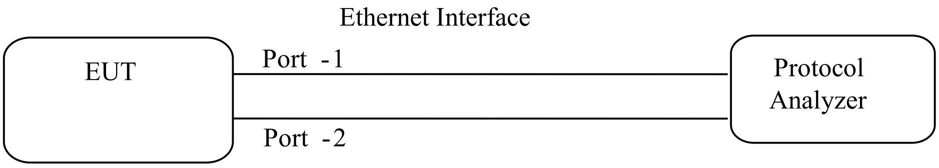
[e] Measured with conformance test signal at TP3 (see 88.8.10) for BER = 10^{-12}.

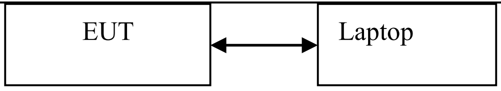
[f] Vertical eye closure penalty, stressed eye J2 Jitter, and stressed eye J9 Jitter are test conditions for measuring stressed receiver sensitivity. They are not characteristics of the receiver.

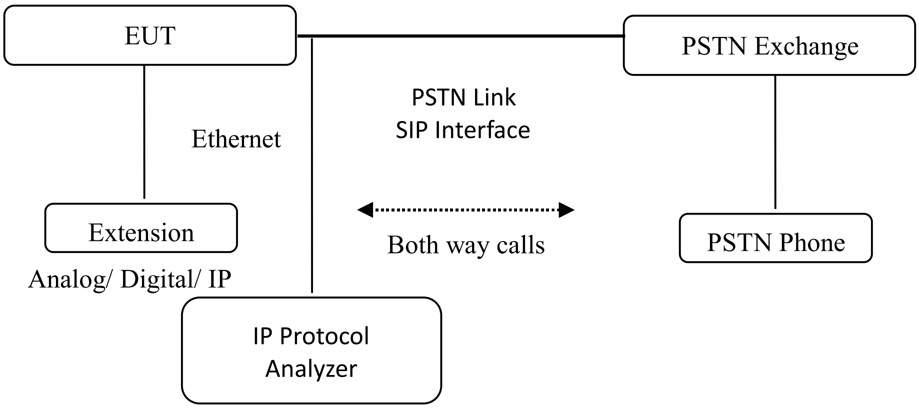
Test Procedure	1. Connect the setup as shown in the figure above. 2. Configure EUT B for sending packets to EUT A 3. Enable the output Optical Port of EUT B 4. Adjust the Optical Power Attenuator 5. Measure the Receiver Sensitivity 6. Verify whether the Receiver Sensitivity is within limits. 7. In case of Ethernet Optical Ports verify whether the Output Power / Receiver Sensitivity combination is able to meet the distance criteria requirements
Expected Results	Enclose the Test Results

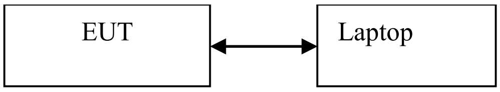
Test No.	14
Test Details	Test for SDH Payload Measurements
Test Instruments Required	1. SDH Network Analyser, Optical Splitter OR 2. SDH Analyser with POS capability
Test Setup	 SDH Interface Rx Tx EUT _ A Optical Splitter EUT-B Tx Rx SDH Analyzer ***Figure-1*** **OR**  SDH Interface Rx Tx EUT _ A SDH Analyzer with POS interface Tx Rx ***Figure-2***
Test Procedure	1. Connect the test setup as shown in figure. 2. The test setup in Figure-2 shall be used in case the SDH analyser has the POS interface. [Packet Over SDH] 3. The EUT-A shall be configured in the loopback mode such that the Packets sent from EUT-B / SDH Analyser is sent back. 4. Verify whether the SDH frame structure sent by the EUT is as per G.707 standards.
Expected Results	Enclose the Test Results

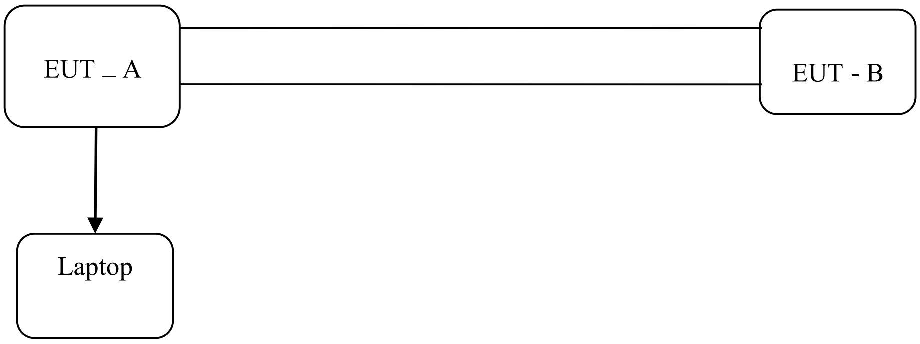
Test No.	15
Test Details	Test for Bit Error Rate [BER]
Test Instruments Required	1. PDH/SDH Performance Analyser
Test Setup	 EUT _ A Router PDH/SDH Performance Analyser 64/2048Kbps Interface Ethernet Interface EUT _ B Router
Test Limits	The EUT shall be able to work with a BER better than 1x10^{-10} measured in any 15 minutes interval for all the speed/s of digital interface.
Test Procedure	1. Connect the test setup as shown in figure using a suitable cable wired to the Ethernet interface 2. A Router may be used for interface conversion in case the PDH/SDH Analyser does not have the compatible interface. 3. Perform the BER performance for 15 minutes interval
Expected Results	Enclose the Test Results

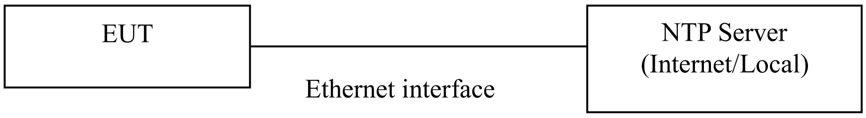
Test No.	16
Test Details	Test for Various Protocols
Test Instruments Required	1. IP Protocol Analyser
Test Parameters	As per various protocols being referred in the respective clause of the Test Schedule (TSTP)
Test Setup	 Ethernet Interface EUT Port -1 Port -2 Protocol Analyzer
Test Procedure	1. Connect the test setup as shown in figure 2. The EUT shall be configured through the CLI [Command Line Interface] or SNMP interface for the various tests like IPv4, IPv6, TCP, Static Routing, Dynamic Routing, BGP, PPP etc 3. Various test parameters shall be measured using this setup 4. The test results may be recorded.
Expected Results	Enclose the Test Results
	Note: 1. The test procedure for those RFC's which are forming part of the "compendium of test setup and test procedures for testing of RFC's of IETF" shall be performed as per the same. This test setup (at test no 16) is generic in nature and shall apply in case of RFC's which are not covered in the above referred compendium. 2. TEC New Delhi NGN Lab has this test facility 3. Where ever conformance tests are not available, functional tests shall be carried out. Moreover, wherever the specification requirement is to meet a specific functionality of the RFC, the clause of the RFC refereeing to the function shall be tested as per the functional test procedure. The functional test model available in the "compendium of test setup and test procedures for testing of RFC's of IETF" can be followed for those RFC's which are not covered in the compendium and where functional tests are carried out. 4. The protocol analyser shall be able to send various test packets to the EUT, check the response packet and check the conformance/functionality. Software tools like wireshark has got only the capability to analyse the received packets and do not have the capability to send test packets and measure the response. Hence the tools like wireshark cannot be used for this test. 5. In case the product is offered (with the same product version) is 'IPv6 Readylogo Certified', then the tests against RFC 4862, RFC 4443, RFC 4291, RFC 2460, RFC 4861, RFC 1981 and RFC 5095 (where ever referred in the Test Schedule) which are covered as part of the 'IPv6 Readylogo certification' shall not be carried out. I.e. in this case, the product version of the 'IPv6 Readylogo certificate' and the offered product shall be the same. Later versions than the certified versions will not come under the purview of this condition.

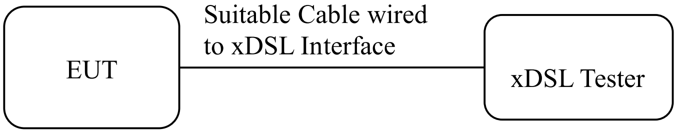
Test No.	17
Test Details	Test for Various Protocols using Wireshark
Test Instruments Required	1. Laptop/PC
Test Parameters	1. TCP as per RFC 793 2. UDP as per RFC 768
Test Setup	
Test Procedure	1. Connect the test setup as shown in figure 2. Load a suitable protocol analysis software such as Wireshark in the Laptop 3. The EUT shall be configured through the CLI [Command Line Interface] or SNMP interface for the TCP & UDP test. 4. The IP Packets may be observed in the Wireshark for TCP/UDP Compliance 5. The test results may be recorded.
Expected Results	Enclose the Test Results

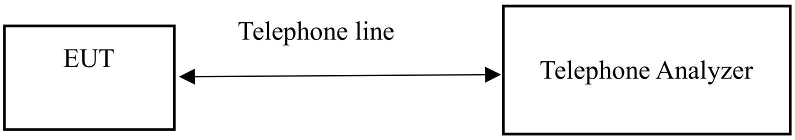
Test No.	18
Test Details	Test for the IP Protocol support for PSTN interface over IP - 1. SIP Protocol 2. IP version 4 3. Audio codecs 4. TCP protocol 5. RTP protocol 6. RTCP protocol
Test Instruments Required	1. IP Protocol Analyzer
Test Setup	 EUT PSTN Exchange PSTN Link SIP Interface Ethernet Extension Analog/ Digital/ IP Both way calls PSTN Phone IP Protocol Analyzer
Test Procedure	1. Connect the system, as shown in the above setup and configure the EUT to enable it to send and receive calls to/from PSTN using SIP interface with different audio codecs. 2. Make outgoing and incoming calls from SIP extension to PSTN phone and vice versa. 3. Take message traces from IP Protocol Analyzer for verifying support for a. SIP Protocol b. IP version 4 c. All the Audio codecs (G.711, G.723, G.726, G.729, G.729A, G.729B, G.728AB, G.725A, AMR and T.38) d. TCP protocol e. RTP protocol f. RTCP protocol
Expected Results	Enclose the message traces from IP Protocol Analyzer

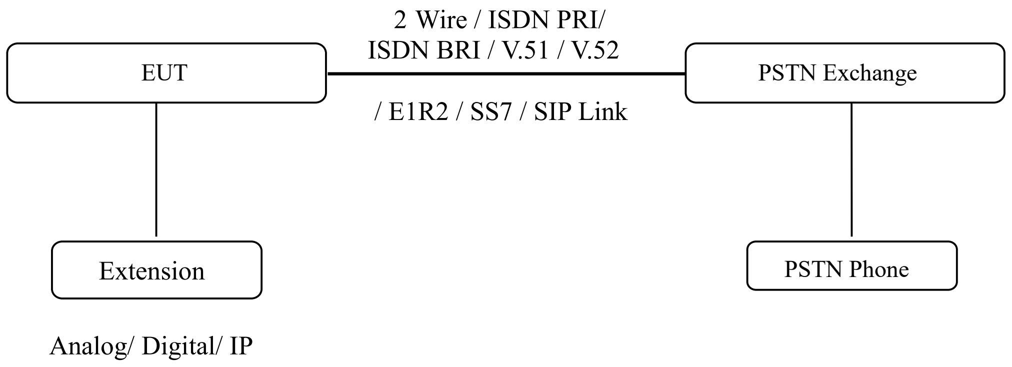
Test No.	19
Test Details	Test for Management Interface
Test Instruments Required	1. Laptop
Test Setup	
Test Procedure	1. Connect the EUT to the Laptop over Ethernet Interface as shown in the setup. 2. Load SNMP management software supplied by the Equipment Manufacturer or any other software [Freely downloadable from the Internet] 3. Configure EUT from the Laptop to act as the SNMP master. 4. Configure the SNMP software for SNMPv2 5. Check for the alarms [Traps] coming from the EUT to the Laptop. 6. Configure some parameters of the EUT from the Laptop through get and set commands.
Expected Results	Enclose the Test Results / Screen Shots

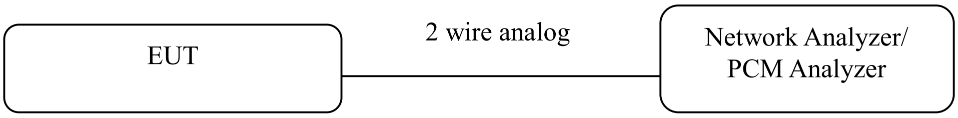
Test No.	20
Test Details	Test for Clock Extraction
Test Instruments Required	1. Laptop
Test Setup	
Test Procedure	1. Connect the test setup as shown in figure 2. Configure EUT-A for using the clock extracted from the interface connected to EUT-B [Slave Mode] 3. Verify the configuration about the usage of the clock 4. Verify whether the EUT-A is able to configure in Master Mode
Expected Results	Enclose the Command Line Interface [CLI] Results / Screenshots

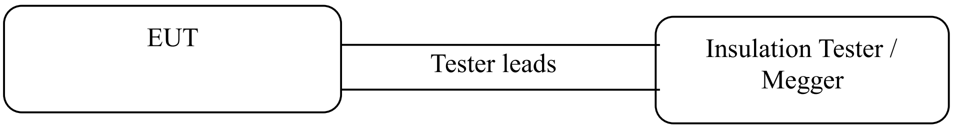
Test No.	21
Test Details	Test for NTP Server Synchronization support
Test Instruments Required	Nil
Test Setup	
Test Procedure	1. Setup the system as shown in the diagram above. 2. Configure the system to synchronize with NTP server, either located locally or on the internet. 3. The system should be able to synchronize with NTP server.
Expected Results	Enclose the Screen Capture Results

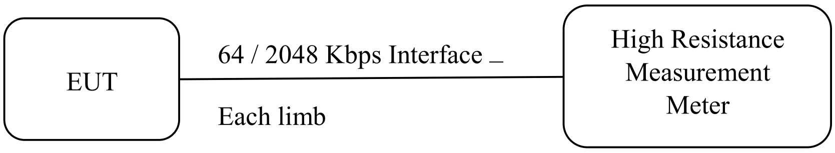
<table>
<tr><td>Test No.</td><td>22</td></tr>
<tr><td>Test Details</td><td>xDSL Line Tests
[The tests shall be limited to the tests specified under the Test Limits below]
<table>
<tr><td>ADSL Tests</td><td>Conformity Tests as per G.992.1, G.992.3, G.992.5</td></tr>
<tr><td>VDSL Tests</td><td>Conformity Tests as per G.993.1, G.993.2</td></tr>
<tr><td>SHDSL Tests</td><td>Conformity Tests as per G.991.2 Annex G</td></tr>
<tr><td>Other Tests for all xDSL interfaces</td><td>Support of Protocols - PPPoE as per RFC2516, PVC, VPI/VCI support FTP Speed Test
Metallic Loop Tests (Loop Resistance, Insulation Resistance, Capacitance)
Impulse Noise Protection</td></tr>
</table></td></tr>
<tr><td>Test Instruments Required</td><td>1. xDSL Tester [Capable of testing xDSL CPE’s].
2. In case the tester do not have the capability to measure some of the above tests, separate tester can be used
3. For Impulse Noise Tests test results from the OEM can be obtained.</td></tr>
<tr><td>Test Setup</td><td>
</td></tr>
<tr><td>Test Limits</td><td>
<table>
<tr><td>G.992.1</td><td>PSD [Power Spectral Density] as per Annexure-A</td></tr>
<tr><td>G.992.3</td><td>PSD</td></tr>
<tr><td>G.992.5</td><td>PSD</td></tr>
<tr><td>G.993.1</td><td>PSD and Return Loss as per clause 6.2 and 6.5</td></tr>
<tr><td>G.993.2</td><td>Profiles as per Clause 6.3, PSD as per clause 7.2</td></tr>
<tr><td>G.991.2</td><td>Return Loss as per Clause 11.3 and PSD as per Clause 11.5</td></tr>
<tr><td>PPPoE</td><td>Shall support PPPoE configuration as per RFC2516</td></tr>
<tr><td>PVC</td><td>Shall support PVC configuration</td></tr>
<tr><td>VPI/VCI</td><td>Shall support VPI/VCI configuration</td></tr>
<tr><td>FTP Speed Tests</td><td>1. ADSL2+ interface supporting 16Mbps speeds using 0.5mm copper loop distance of 2Km
2. VDSL2 interface supporting 30Mbps speeds using 0.5mm copper loop distance of 500m
3. SHDSL interface supporting 1.5Mbps speeds using 0.5mm copper loop distance of 2Km</td></tr>
<tr><td>Loop Resistance</td><td>As per Telephone line requirements</td></tr>
<tr><td>Insulation Resistance</td><td>As per Telephone line requirements</td></tr>
<tr><td>Capacitance</td><td>As per Telephone line requirements</td></tr>
<tr><td>Impulse Noise Protection[INP]</td><td>INP shall be better than 2</td></tr>
</table></td></tr>
<tr><td>Test Procedure</td><td>1. Connect the test setup as shown in figure
2. Measure the various parameters as per the test details and verify whether they are within the Test Limits.</td></tr>
<tr><td>Expected Results</td><td>Enclose the Test Results / Screen Shots</td></tr>
</table>

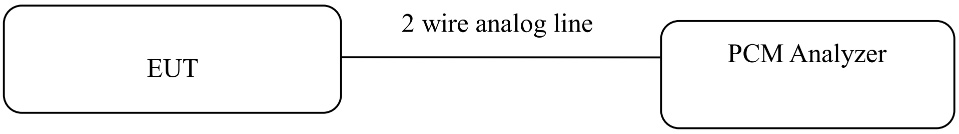
Test No.	23
Test Details	Test for Loop Current (for 2 wire analog interface only
Test Instruments	1. Telephone Analyzer Required
Test Setup	
Test Procedure	1. Setup the CTI equipment and Telephone analyser as shown in the test setup above while enabling the 2 wire analog interface on the EUT. 2. Measure the loop current on the telephone analyser .
Expected Results	1. The loop current in idle condition (on-hook) should not be more than 0.5 mA. 2. The loop current in the off-hook condition should not be more than 60 mA. 3. When CTI is connected to PSTN line (i.e. when customer calls IVRS facility) the current drawn from the line shall be less than 40 micro Amps. Enclose the test results

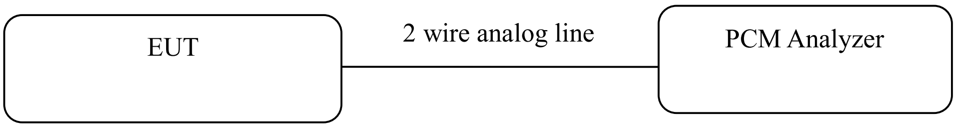
Test No.	24
Test Details	Test for the DTMF support
Test Instruments Required	Nil
Test Setup	 2 Wire / ISDN PRI/ ISDN BRI / V.51 / V.52 / E1R2 / SS7 / SIP Link EUT PSTN Exchange Extension PSTN Phone Analog/ Digital/ IP
Test Procedure	1. Setup the system as per above diagram and configure the EUT to enable it to send and receive calls to/from PSTN 2. Make an incoming call from PSTN phone to EUT and the Interactive Voice Response System should get activated and should prompt the user to dial a digit soon. 3. Program the IVRS to detect all DTMF tones and respond accordingly. 4. Check that the IVRS system responds properly to all dialled digits. 5. Make an outgoing call from EUT system to PSTN phone and activate the IVRS facility. Prompt the user to dial different digits. The EUTshall respond according to the dialled digits. 6. Make an incoming call from a mobile phone to EUT and check that the call matures.
Expected Results	Enclose the logs from EUT.

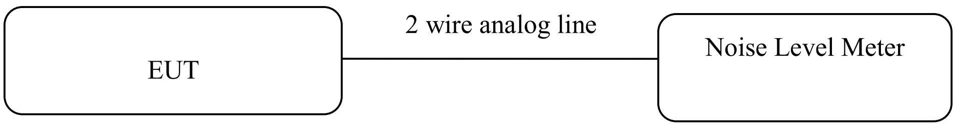
Test No.	25
Test Details	Test for Return Loss (2 wire interface only)
Test Instruments Required	1. Network Analyser or PCM Analyzer
Test Setup	
Test Limits	1. Balance Return Loss > 12 dB in the range 300Hz to 3400Hz 2. Echo Return Loss > 16 dB
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the Balance and Echo Return loss using the Test instrument. 3. Check whether the Return Loss is within the specified limits.
Expected Results	Enclose the Test Results

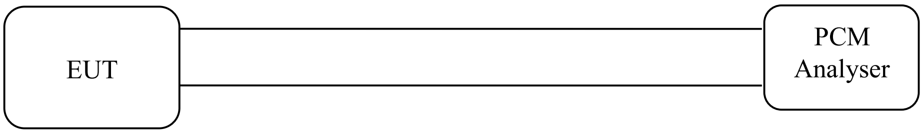
Test No.	26
Test Details	Test for Insulation Resistance (2 wire interface only)
Test Instruments Required	1. Insulation Tester / Megger
Test Setup	
Test Limits	1. Insulation resistance >= 5 Mega ohms
Test Procedure	2. Connect the Setup as shown in the figure. 3. Measure the Insulation resistance (between any two points not electrically connected) using the Test instrument leads. 4. Check whether the Insulation resistance is within the specified limits.
Expected Results	Enclose the Test Results

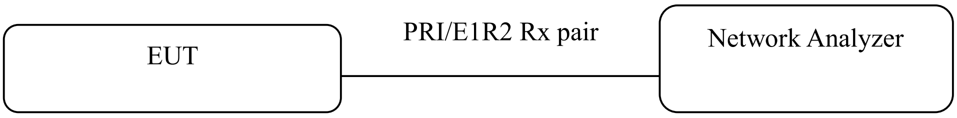
Test No.	27
Test Details	Test for Input Resistance
Test Instruments Required	1. High Resistance measurement Meter
Test Setup	 EUT 64 / 2048 Kbps Interface _ Each limb High Resistance Measurement Meter
Test Limits	> 5 Mohm
Test Procedure	1. Connect the test setup as shown in figure for Limb-A 2. Measure the Input resistance 3. Repeat the test for Limb-B
Expected Results	Enclose the Test Results

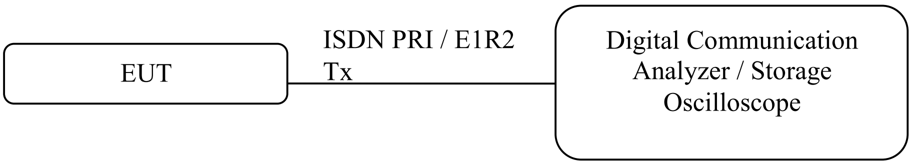
Test No.	28
Test Details	Test for Loudness Rating (SLR and RLR) (2 wire interface only)
Test Instruments Required	1. PCM Analyzer
Test Setup	
Test Limits	1. SLR at zero line +7dB 2. SLR at limiting line +12dB 3. RLR not louder than -6dB 4. RLR not quieter than -1dB
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the SLR and RLR values using test equipment. 3. Check whether the values are within the specified limits.
Expected Results	Enclose the Test Results

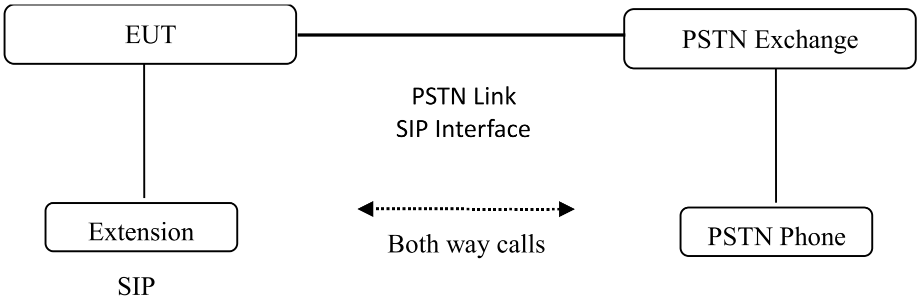
Test No.	29
Test Details	Test for Side Tone Masking Rate (STMR) (2 wire interface only)
Test Instruments Required	1. PCM Analyzer
Test Setup	
Test Limits	1. STMR > +8 dB
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the STMR value using test equipment for different line lengths. 3. Check whether the values are within the specified limits.
Expected Results	Enclose the Test Results

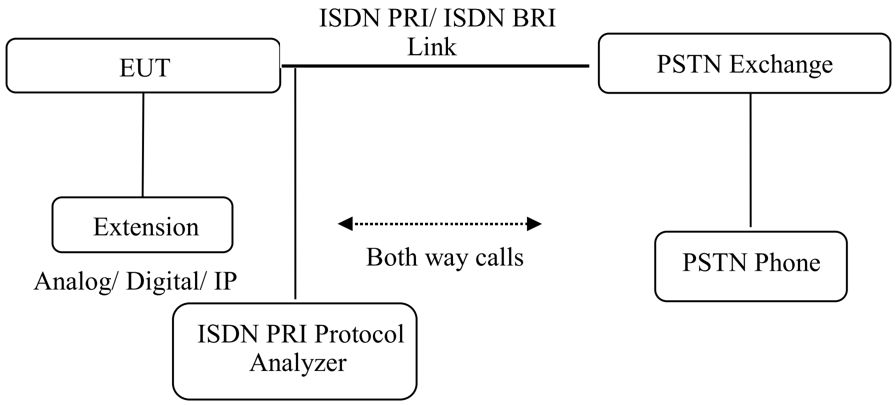
Test No.	30
Test Details	Test for Noise level (2 wire interface only)
Test Instruments Required	1. Noise Level Meter
Test Setup	
Test Limits	1. Noise level less than -65dBm
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the Noise level value across 600 ohms termination of EUT using test equipment. 3. Check whether the values are within the specified limits.
Expected Results	Enclose the Test Results

Test No.	31
Test Details	Test for Minimum Longitudinal Loss
Test Instruments Required	1. PCM Analyser
Test Setup	
Test Procedure	1. Connect the test setup as shown in figure 2. Measure the Minimum Longitudinal Loss using the PCM Analyser
Expected Results	Enclose the Results / Screenshots

Test No.	32
Test Details	Test for Return Loss (ISDN PRI/E1R2 interface)
Test Instruments Required	1. Network Analyser
Test Setup	
Test Limits	1. Refer clause 9.3 of ITU-T G.703 [Refer Test-8 for details]
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the input port return loss using the Network Analyser 3. Check whether the Return Loss is within the specified limits
Expected Results	Enclose the Test Results

Test No.	33
Test Details	Test for Output Pulse Mask (ISDN PRI/E1R2 interface)
Test Instruments Required	1. Digital Communication Analyser / Storage Oscilloscope
Test Setup	 EUT ISDN PRI / E1R2 Tx Digital Communication Analyzer / Storage Oscilloscope
Test Limits	Refer Figure-15 G.703 [Refer Test-7 for details]
Test Procedure	1. Connect the EUT as shown in the figure. 2. Enable the Port if required. 3. See whether the output pulse is within the mask/limits as indicated above.
Expected Results	Enclose the Test Results with the Pulse shape & the Pulse Mask

Test No.	34
Test Details	Test for support of Traffic report generation
Test Instruments Required	Nil
Test Setup	 EUT PSTN Exchange PSTN Link SIP Interface Extension Both way calls PSTN Phone SIP
Test Procedure	1. Connect the system, as shown in the above setup and configure the EUT to enable it to send and receive calls to/from PSTN using SIP interface. 2. Configure the system to generate traffic reports for IC and OG calls. 3. Make outgoing and incoming calls from SIP extension to PSTN phone and vice versa. 4. Check if the system is able to generate traffic report.
Expected Results	Enclose the traffic report.

Test No.	35
Test Details	Test for the ISDN PRI/BRI Protocols
Test Instruments Required	ISDN Protocol Analyzer
Test Setup	 ISDN PRI/ ISDN BRI Link EUT PSTN Exchange Extension Analog/ Digital/ IP Both way calls PSTN Phone ISDN PRI Protocol Analyzer
Test Procedure	1. Connect the system, as shown in the above setup and configure the EUT to enable it to send and receive calls to/from PSTN 2. Make outgoing and incoming calls from EUT extension to PSTN phone and vice versa. 3. Use ISDN PRI protocol Analyzer for verifying support of the following parameters in ISDN PRI / BRI messages - a. Call reference b. Bearer capability c. Called party number d. Calling party number e. Channel identification f. Numbering plan identification
Expected Results	Enclose the results from ISDN PRI / BRI Protocol Analyzer

Test No.	36
Test	Tests with connectivity over E1R2 Signaling
Tests involved	1. Line Signaling 2. Register Signaling 3. Fax Transmission
Test Setup	Typical connectivity of EUT with E1R2 Signaling Interface
	Note: E1R2 signaling to be tested between EUT and two Switches of different switching technologies.

Line Signaling and Register Signaling as per Chapter 2, Section B of GR G/LLT-01/04.DEC98 (Relevant clauses are given.)

2.5.2.1.1 Line signalling - Digital Type 1

Operating condition	Signaling				
	Forward			Backward	
	af	bf	cf	ab	bb
Idle	1	0	0	1	0
Seizure	0	0	0	1	0
Acknowledgement	0	0	0	1	1
Answer	0	0	0	0	1
Metering Pulse (180 - 270 ms)	0	0	0	1	1
Clear back	0	0	0	1	1
Clear forward	1	0	0	0 or 1	1
Release guard	1	0	0	1	0
Trunk Offering and Re-ringing					
a) TKO press key	0	0	1	1	1
b) False answer	0	0	1	0	1
c) Release key	0	0	0	0	1
d) "B" party on hook	0	0	0	1	1
e) Re-verify	0	0	1	1	1
Blocking	1	0	0	1	1

Notes:

1. For all supervisory signals bf = 0; a change to bf = 1 indicates a fault.
2. The trunk offering signal can be used as a control signal for echo suppresser in case of satellite application.
3 df, cb, db are spare bits, df =db = 1, and cb = 0, are assigned according to ITU-T Recommendation G732.

2.5.2.2.1 Line signalling - Digital Type 2

Operating condition	Signaling			
	Forward		Backward	
	af	bf	ab	bb
Idle	1	1	1	0
Seizure	0	1	1	0
Acknowledgement	0	1	1	1
Answer	0	1	0	1
Metering Pulse	0	1	1	1
Clear back	0	1	1	1
Clear forward	1	1	0 or 1	1
Release guard	1	1	1	0
Trunk Offering and Re-ringing				
a) TKO press key	0	0	1	1
b) False answer	0	0	0	1
c) Release key	0	1	0	1
d) "B" party on hook	0	1	1	1
e) Re-verify	0	0	1	1
Blocking	1	1	1	1

Forward	cf = 0
	df = 1
Backward	cb = 0
	db = 1

2.5.2.3.1 Line signalling - Digital Type 3

Operating condition	Signaling			
	Forward		Backward	
	af	bf	ab	bb
Idle	1	1	1	1
Seizure	0	1	1	1
Answer	0	1	0	1
Metering Pulse	0	1	1	1
Clear back	0	1	1	1
Clear forward	1	1	0 or 1	1
Release guard	1	1	1	0
Trunk Offering and Re-ringing				
a) TKO press key	0	0	1	1
b) False answer	0	0	0	1
c) Release key	0	1	0	1
d) "B" party on hook	0	1	1	1
e) Re-verify	0	0	1	1
Blocking	1	1	0	1

2.5.2.4.1 Line Signalling - Digital Type 4 (E&M signalling)

This signalling scheme is used over carrier circuits and is basically the same as that specified for ITU-T signalling system R2, analogue version as per recommendations Q.411, Q.412, Q.414, Q.415 and Q.416. It is of the out of band and low level continuous type (3825 Hz + 4 Hz) with tone-OFF in the answered condition (tone-ON-idle signalling). The system provides for link-by-link transmission of the line signals. The tone OFF condition in the forward (backward), direction is signalled by connecting earth to the send (receive) leg of the signalling channel. The signalling scheme available on the analogue media and corresponding sequence on TS16 of the 2048 kbit/s PCM stream is outlined in the table below :

Signal	Forward	Backward	af	bf	ab	bb
Idle	Tone ON	Tone ON	0	0	0	0
Seizure	Tone OFF	Tone ON	1	0	0	0
Answer	Tone OFF	Tone OFF	1	0	1	0
Metering Over channel	Tone OFF	Tone ON during the meter pulse followed by Tone OFF	1	0	1/0/1	0
Clear forward	Tone ON	Tone ON or OFF	0	0	0 or 1	0
Clear back	Tone OFF	Tone ON	1	0	0	0

Release guard	Tone ON	On recognition of clear forward Tone OFF followed by Tone ON	0	0	1/0	0
Blocking	Tone ON	Tone OFF	0	0	1	0
Echo canceller control						
(On O/G side)	Tone OFF	Tone ON	1	1	0	0
(On I/C side)	Tone OFF	Tone ON	1	0	0	1

Notes:

1. The period of backward tone off for release guard is 450 □ 90 ms, as per ITU-T R2 Recommendation Q.412. However, in existing electromechanical exchanges in the Indian network this may be of the order of 70-100 ms only. E-10B TAXs may provide the timing as per ITU-T R2 Recommendation Q.412.
2. The recognition time for a changed condition is 20 ms.
3. In transit exchanges, the answer signal is immediately repeated to the preceding exchange.
4. The metering signal has a duration of 180 to 270 ms.
5. A signal to switch “in” or “out” echo-suppresser is to be sent, while working over satellite circuits. The echo-suppresser is assumed to be provided along with the transmission equipment outside the exchange. The signal to switch echo-suppresser is carried out on M 2 wire.

2.0 : Register Signalling - Indian R2 Modified MFC Signalling

2.5.1.2.2.1 Indian R2 Modified MFC Signalling

2.5.1.2.2.1(a) The register signalling uses multi-frequency compelled sequence self-checking code. Generally end to end signalling is used except on national and international calls established through a TAX, in which case, the signalling is end-to-end between the originating exchange and the originating TAX and between originating TAX and the last exchange (TAX or local) using MFC.

2.5.1.2.2.1(b) In the existing TAXs, only 5 forward and 5 backward frequencies have been equipped (allowing 10 MF signals in each direction in 2/5 code), though provision exists for introduction of sixth frequency as per R2 scheme. In local MFC type exchanges, only 5 forward and 4 backward frequencies have been equipped.

2.5.1.2.2.1(c) The frequencies used in the backward direction are 660, 780, 900, 1020 and 1140 Hz. Those used in forward direction are 1380, 1500, 1620, 1740, and 1860 Hz. (Provision exists for addition of 1980 Hz in forward and 540 Hz in backward direction).

2.5.1.2.2.1(d) Forward signals

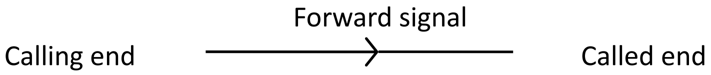
The forward frequencies can be used to send digits (when used as Group-I forward signals) or to send the category of calling subscriber (when used as group-II forward signals).

2.5.1.2.2.1(e) Backward signals

The backward frequencies can be used to make further demands (when used as Group-A backward signals), or to report back the called line condition to the calling side (when used as Group-B backward signals). In electronic exchanges all 5 backward frequencies shall be equipped.

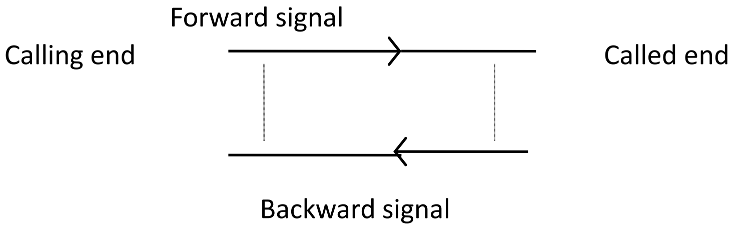
2.5.1.2.2.1(f) Signalling sequence

i)



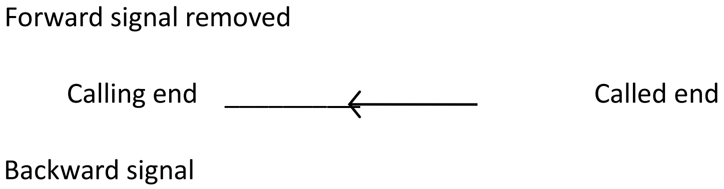
Calling end applies the forward signal as per the demand previously made by the called end (or the first digit start with). At the called end, this signal is examined for relevance and 2/5 validity.

ii)



Called end applies backward signal as per next requirement. The application of backward signal is recognised at calling end as the acknowledgement for reception of forward signal. The 2/5 validity is checked and the demand is decoded.

iii)



Forward signal is removed as an acknowledgement to the receipt of a backward signal.

iv) When the removal of a forward signal is recognised, the backward signal is also removed and this removal is recognised by the calling end, to end the sequence.

2.5.1.2.2.1(g) Significance of the Multi-frequency signals:

The significance of the forward signals and backward signals, as interpreted in the Indian network, are given in tables below :

Group I - Forward Signals

Signals	Indian National MFC scheme
I.1 I.2 I.3 I.4 I.5 I.6 I.7 I.8 I.9 I.10	Digit 1 Digit 2 Digit 3 Digit 4 Digit 5 Digit 6 Digit 7 Digit 8 Digit 9 Digit 0

Group II - Forward Signals

Signals	Indian National MFC scheme
II.1	Ordinary Subscriber
II.2	Priority Subscriber
II.3	Spare at present (proposed for use in future for 'maintenance equipment call')
II.4	Spare at present
II.5	Operator STD
II.6	coin box.
II.7	Spare
II.8	Spare
II.9	Spare
II.10	Spare

Group A - Backward Signals

Signals	Indian National MFC scheme
A.1	Send next digit (n+1)
A.2	Restart
A.3	Change over to reception of B-signals
A.4	Calling line identification-see note
A.5	Send category of the calling subscriber
A.6	Switch-through the speech path
A.7	Send last but two digit (n-2) } Not
A.8	Send last but three digit (n-3) } available in
A.9	Send last but one digit (n-1) } local exchange
A.10	Spare at present (may be used for } at present trunk congestion if network permits) }

Group B - Backward Signals

Signals	Indian National MFC scheme
B.1 B.2 B.3 B.4 B.5 B.6 B.7 B.8 B.9 B.10	Spare Changed number Called line busy Congestion Unallotted number Normal subscriber, free, with metering Spare Spare; not available in local exchange Spare; not available in local exchange Spare; not available in local exchange

Test No.	37
	SIGNALLING TEST FOR CONNECTIVITY BY CCS7
Test Setup	
Tests	1. Protocol Data Check 2. MTP Level 2 Tests 3. MTP Level 3 Tests 4. ISUP Tests 5. Interface Tests
Test arrangement:	At least 2 signaling link sets should be available to check various capabilities of CCS7 signaling. A suitable CCS7 protocol Simulator and Analyser is required to be connected to IP based Integrated Media Gateway for simulating and monitoring the messages. The testing shall be carried out as per the test description given in each Test sheet of the ITU-T document given in the following Test Schedule.

1. **Protocol Data check**: Check the document or obtain certificate from the vendor in support of the following sub paras:

1.1. Signalling network Management messages:

Check messages implemented in the system with Table 1 of ITU-T recommendation Q.704 (1988). Following signalling network management messages are optional for interface approval.

CNP, CNS, CSS, DLC, RSR, TFR and UPU.

1.2. ISUP messages: Check Heading Code implemented in the system with Table 3 of ITU-T recommendation Q.763 (1988). Following ISUP messages are optional for interface approval:

CMC, CMRJ, CMR, CQM, CQR, COT, DRS, FAA, FAR, FRJ, FOT, LPA, OLM, PAM, USR and UCIC.

1.3. Timer values: Check the values of Level 2 Timers, Level 3 Timers and Application call processing timers implemented in the system with the following documents:

Timer **Document Reference**

Level 2 Timers Page 3 MTP para 12.3 of National CCS7 specification for Local/Tandem exchanges No. G/CCS-01/01.JUN93.

Level 3 Timers Para 16.8 of ITU-T recommendation Q.704 (1988). Timers T11, T15, T16 are not applicable. Timers T7, T18, T19, T20, T21 & T24 are optional.

Application call Annex A to ITU-T recommendation Q.764 of call 1988. Timers T3 and T4 timers processing are not used. Timers T28, T31 and T32 are optional.

2. MTP Level 2 tests: The compatibility tests given in ITU-T Q.781 (1988) will be done on the CCS7 links of Integrated Media Gateway with a suitable CCS 7 protocol Simulator and Analyser. The protocol shall conform to the ITU-T test sheets mentioned below.

Tests for MTP2

Clause No.	Description		Test results
2.3 Clause from S/CCS 02/03	The functions and procedures relating to transfer of signaling messages over a data link shall be as per ITUT Rec. Q.703 (1993). This provides the layer 2 functions for the CCS7 protocol Stack.		ITU-T Rec. Q.781 validates the protocol specification in ITU-T Rec Q.703
	ITU-T Rec Q781 Test Cases		
SI No	Test case Description	Limits	Compliance Test Results
MTP2-1	Timer T2 - Q781:1.2	5-150sec	
MTP2-2	Timer T3- Q781:1.3	1-2sec	
MTP2-3	Timer T1 and T4 (Normal) – Q781:1.4	7.5-9.5sec	
MTP2-4	Normal Alignment - correct procedure (FISU) - Q781:1.5		
MTP2-5	Emergeny Alignment – Timer T4 - Q781:1.19	400-600msec	
MTP2-6	AERM: Error rate above normal threshold - Q781:7.3		
MTP2-7	Negative Acknowledgement - Q781:8.2		
MTP2-8	Retransmission Buffer Full - Q781:8.3		
MTP2-9	Excessive delay of acknowledgement - Q781:8.12		
MTP2-10	Restart of Timer T7 - DelayQ781:10.2		
MTP2-11	Timer T6 -Congestion Control Timer Q781:10.3	3-6sec	

3. MTP Level 3 tests: The compatibility tests given in ITU-T Q.782 (1988) will be done on the CCS7 links of Integrated Media Gateway with Suitable CCS7 Simulator and Analyser. The protocol shall conform to the ITU-T test sheets mentioned below.

Tests for MTP3

Clause No.	Description	Test Results
2.4 Clause from S/CCS-02/03	The functions and procedures relating to transfer of signaling messages between the signaling points shall be as per ITU-T Rec. Q.704 (1993). This provides the layer 3 functions for the CCS7 protocol stack	ITU-T Rec. Q.782 validates the protocol specification in ITUT Rec Q.704

	ITU-T Rec Q782 Test Cases	
Sl.No	**Test Cases Description**	
MTP3-1	Signalling linkset deactivation - Q782:1.2	
MTP3-2	Signalling linkset activation- Q782:1.3	
MTP3-3	Message with invalid DPC - Q782.2.2 – use a SLTM message.	
MTP3-4	Message with errorneous SI-Q782.2.3	
MTP3-5	Reception of an additional Changeover Order – Q782.3.6	
MTP3-6	Changeover to several links within a linkset - Q782:3.15	
MTP3-7	Additional CBD – Q782.4.3	
MTP3-8	No Acknowledgement to first CBD – Q782.4.4	
MTP3-9	Inhibition of an available link - Q782:7.1.1	
MTP3-10	Inhibition of an unavailable link – Q782:7.1.2	
MTP3-11	Local reject on available link – Q782:7.2.1	
MTP3-12	Forced unhibition of a link - sending LFU - Q782:7.10.1	
MTP3-13	Forced unhibition of a link - reception of LFU - Q782:7.10.2	
MTP3-14	Management Inhibiting Test: Periodic sending and receiving of LLI and LRI-Q 782: 7.17.1	
MTP3-15	Signalling link test: After activation of a Link-Q782:12.1	
	Miscellaneous MTP Test Cases	
MTPMisc-1	It shall be possible to assign the signaling data link to any timeslot of the PCM except timeslot 0.	

4. ISUP tests:

The compatibility tests given in ITU-T Q.784 (1991) will be done on the CCS7 links of Integrated Media Gateway with A Suitable CCS7 Simulator and Analyser. The protocol shall conform to the ITU-T test sheets mentioned below.

Test Cases for ISUP

Clause No.	Description	**Test Results**
	Clause from S/CCS-02/03	
5.1	ISUP shall be as per the functional description given in ITU-T Rec. Q.761 (09/97).	ITU-T Rec. Q.784 validates the protocol specification in ITU-T Rec Q.761Q.764
5.2	The messages, parameters and the parameter information used by ISUP shall be as per ITU-T Rec.Q.762(09/97)	
5.3	The formats and codes of ISUP messages and the parameters required to support basic bearer services and the supplementary services shall be as per ITU-T Rec. Q763(09/97)	

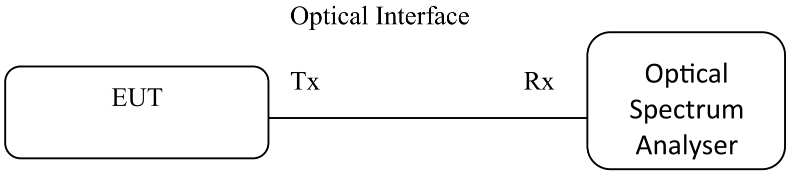
5.4	The ISUP signaling procedures for setting up and clearing down of national and international ISDN connections shall be as per ITU-T Rec. Q764(09/97)	
	ITU-T Rec.Q784 Test Cases	
SL.No.	Test Cases Description	
ISUP-1	Reset received on an idle circuit – Q784.1.2.1	
ISUP-2	Reset sent on an idle circuit – Q784.1.2.2	
ISUP-3	Circuit group reset received-Q784:1.2.5	
ISUP-4	Circuit group reset sent-Q784.1.2.6	
ISUP-5	CGB and CGU received - Q784:1.3.1.1	
ISUP-6	CGB and CGU sent - Q784:1.3.1.2	
ISUP-7	Circuit Blocking received– Q784.1.3.2.1	
ISUP-8	Circuit blocking sent – Q784.1.3.2.2	
ISUP-9	Continuity Check Test: CCR received: Q784:1.4.1	
ISUP-10	Continuity Check Test: CCR sent: Q784:1.4.2	
ISUP-11	Normal Call setup:Overlap operation(with SAM)-Q784:2.2.2	
ISUP-12	T7: Waiting for ACM - Q784:5.2.1	
ISUP-13	T9:Waiting for an answer message-Q784:5.2.2	
ISUP-14	T16 and T17: failure to receive a RLC – Q784.5.2.8	
ISUP-15	Reset of circuits during a call – outgoing circuit- Q784:5.3.1	
ISUP-16	Reset of circuits during a call – incoming circuit- Q784:5.3.2	
ISUP-17	Automatic repeat attempt - blocking of a circuit - Q784:6.2.2	
ISUP-18	Dual Seizure for controlling SP-Q784:6.3.1	

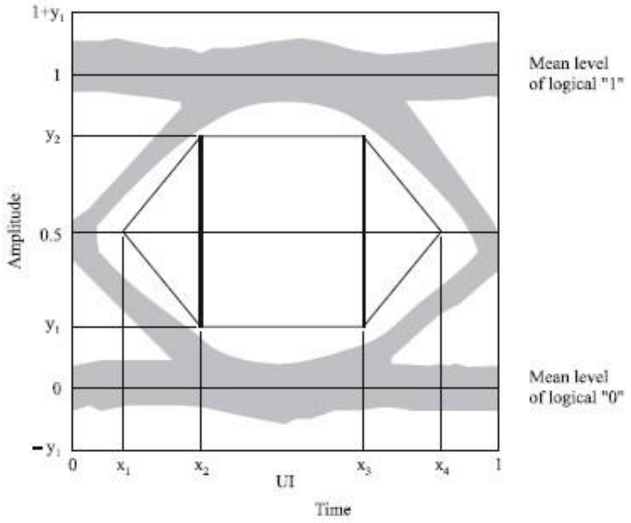
Test For ISUP Supplementary Services

Clause No.	Description	Test Results
	Clause No. S/CCS-02/03	
Chapter4	The general format for ISDN user part (ISUP) supplementary services shall be as per ITU-T Rec.Q.730(9/97)The implementation of the supplementary services shall be as per IT-T Rec. Q.731 to Q.737.	
Sl.No.	Test Case Description	
SUPP-1	Calling Line Identification Presentation (CLIP)-Q731.3(3/97)	
SUPP-2	Calling Line Identification Restriction(CLIR)-Q.731.4(3/97)	
SUPP-3	Connected Line Identification Presentation(COLP)-Q.731.5(3/97)	
SUPP-4	Connected Line Identification Restriction (COLR)-Q.731.6(3/97)	
SUPP-5	Malicious Call Identification (MCID)-Q.731.7(2/97)	
SUPP-6	Sub addressing (SUB)-Q.731.8(6/97)	

5 : Interface Tests for CCS7 Signaling

Clause No.	*Description*		Test Results
1	**Completed Call**	Check for ISUP Messages	
2	A-Party Release	Check for ISUP Messages	
3	B-Party Release	Check for ISUP Messages	
4	B-Party Engaged	Check for ISUP Messages	
5	Incomplete Dialling	-	
6	Call with 10 digit CLI	Check for ISUP Messages	
7	B Party No answer	Check for ISUP Messages	
8	Fax	Fax Transmission	
9	Modem connection	Set the codec to G711 & initiate call from Modem A to Modem B through VOIP network. The data transfer should be tested between the two modems.	
10	Modem Connection	Set the codec to G729 & initiate call from Modem A to modem B through VOIP network. The data transfer should be tested between the two modems.	

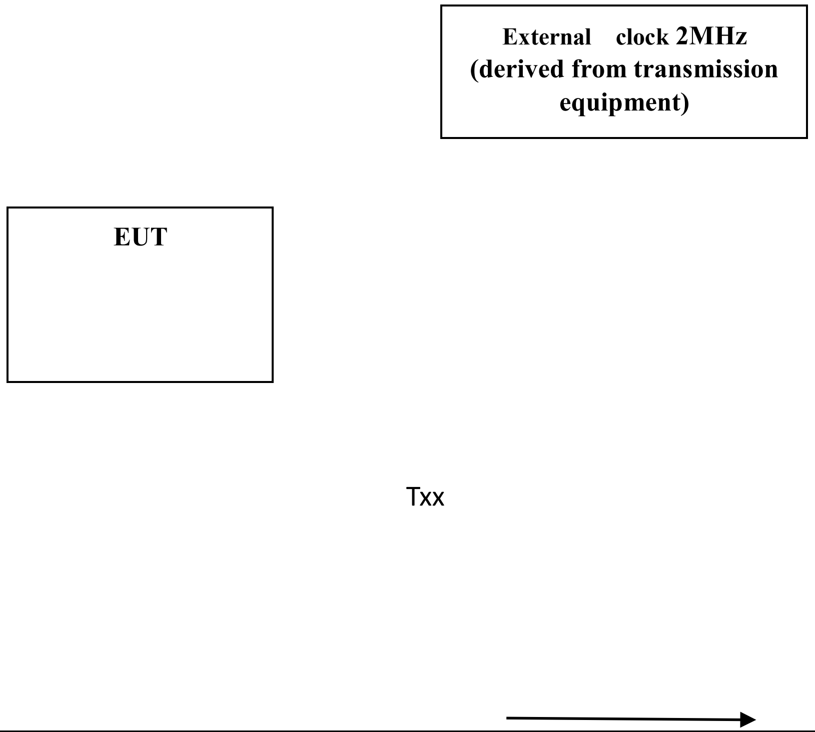
<table>
<tr><td>Test No.</td><td>38</td></tr>
<tr><td>Test Details</td><td>Eye Pattern for Optical Interfaces</td></tr>
<tr><td>Test Instruments Required</td><td>1. Optical Spectrum Analyser</td></tr>
<tr><td>Test Setup</td><td>


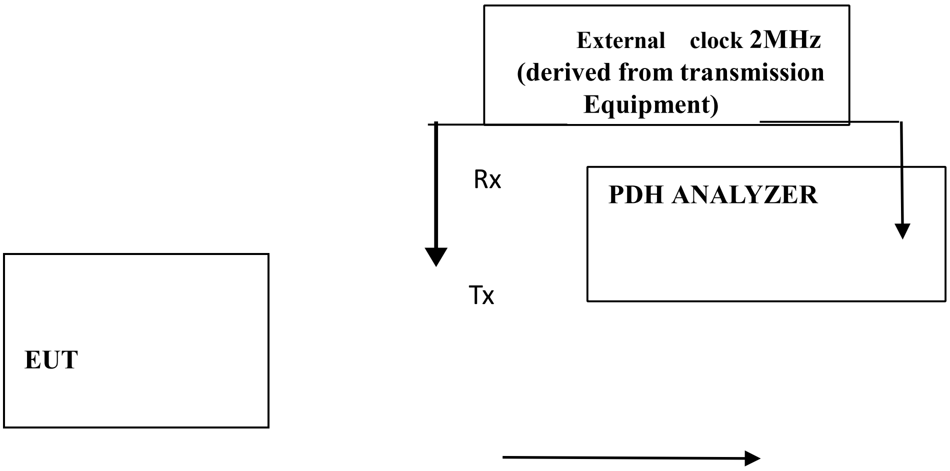
</td></tr>
<tr><td>Test Limits</td><td>
<table>
<tr><td>STM-1 Short Haul / Long Haul</td><td>Refer Figure-2/G.957</td></tr>
<tr><td>STM-4 Short Haul / Long Haul</td><td>Refer Figure-2/G.957</td></tr>
<tr><td>STM-16 Short Haul / Long Haul</td><td>Refer Figure-2/G.957</td></tr>
</table>
</td></tr>
<tr><td>Standards Reference</td><td>


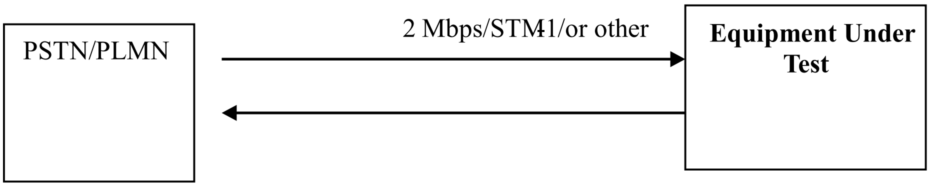
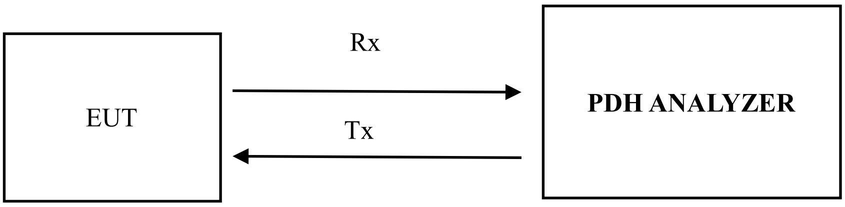
<table>
<tr><th></th><th>STM-1</th><th>STM-4</th></tr>
<tr><td>x_1/x_4</td><td>0.15/0.85</td><td>0.25/0.75</td></tr>
<tr><td>x_2/x_3</td><td>0.35/0.65</td><td>0.40/0.60</td></tr>
<tr><td>y_1/y_2</td><td>0.20/0.80</td><td>0.20/0.80</td></tr>
</table>
<table>
<tr><th></th><th>STM-16</th></tr>
<tr><td>$x_3–x_2$</td><td>0.2</td></tr>
<tr><td>y_1/y_2</td><td>0.25/0.75</td></tr>
</table>
G.957_F02

NOTE – In the case of STM-16, x_2 and x_3 of the rectangular eye mask need not be equidistant with respect to the vertical axes at 0 UI and 1 UI. The extent of this deviation is for further study. In view of the frequencies involved in STM-16 systems and the consequent difficulty of realizing this filter, the parameter values for STM-16 may need slight revision in light of experience.

Figure 2/G.957 – Mask of the eye diagram for the optical transmit signal
</td></tr>
<tr><td>Test Procedure</td><td>1. Connect the Setup as shown in the figure.
2. Enable the output Optical Port
3. Measure the optical spectrum / eye pattern
4. Check whether the spectrum / eye patternis within the specification limits</td></tr>
<tr><td>Expected Results</td><td>Enclose the Test Results</td></tr>
</table>

Test No.	39
Test Details	Test for Frequency Stability in Holdover Mode
Test Instruments Required	PDH Analyzer
Test Setup	 External clock 2MHz (derived from transmission equipment) EUT Txx
Test Procedure	1. Connect the Setup as shown in the figure. Synchronies both the EUT & PDH Analyser (Testing equipment) as per test setup from external timing reference which may be extracted from transmission equipment.) 2. After the EUT is synchronised and stabilised, remove the reference input. 3. It will go to holdover mode. 4. Now run the TIE measurement in holdover mode, which should be started at this point for 24 Hrs. 5. Measure Time Interval Error (TIE) on PDH analyzer 6. Clock stability should be calculated as follows: Clock stability= Time Interval Error (TIE)/Measurement Duration
Test Limits	Frequency Stability in Holdover Mode. Minimum stability of clock in holdover mode shall be 1*10-9 per day. The term 'minimum stability' implies that the stability should be equal to or better than the value specified.

Test No.	40
Test Details	Test for Bit Slip Measurement
Test Instruments Required	PDH Analyzer
Test Setup	 External clock 2MHz (derived from transmission Equipment) Rx PDH ANALYZER Tx EUT
Test Procedure	1. Connect the Setup as shown in the figure. Synchronize both the EUT & PDH Analyser (Testing equipment) as per test setup from external timing reference which may be extracted from transmission equipment.) 2. After the EUT is synchronised and stabilized, run the measurement (PRBS bit pattern) which should be started at this point for 96 Hrs. 3. Measure Slipon PDH analyzer for a period of atleast 96 hours of operation. In synchronised mode of operation, not more than 2 slips per day are permitted.
Test Limits	Under synchronized condition, slips observed at the 2048 Kbits interface of digital exchange/ EUT shall be less than or equal to 2 slips in 24 hours.

Test No.	*41*
Test Details	*Test for junction test*
Test Instruments Required	PDH Analyzer
Test Setup	(a)  PSTN/PLMN 2 Mbps/STM-1/or other **Equipment Under Test**  (b)
Test Procedure	1. *First connect the Setup as shown in the figure (a) as per interface applicable 2Mbps/STM-1/or other. Break the interface continuity either by soft command or physically removing the wire. Verify the status of link in break condition; alarm should appear, when reconnect the alarm should disappear.* 2. *Now connect the Setup as shown in the figure (b) as per interface applicable 2Mbps/STM-1/or other through PDH analyzer. Verify the status of link in healthy condition of interface from PDH analyzer. Now increase the BER gradually through PDH analyzer and observe the alarm condition. Note down the BER threshold level when alarm appear. This value of BER should be within accepting limits.*
Test Limits	Check all alarms and note down the values of thresholds regarding junction testing.