टेस्ट गाइड

टीईसी ४८०४१: २०२५

(सं: टीईसी/टीएसटीपी/जी आर/आई टी/आर ए एस- ००३/०३ मार्च २०१२ को अधिक्रमित करता है)

TEST GUIDE

TEC 48041:2025

(Supersedes No. : TEC/TSTP/GR/IT/RAS-003/03/MAR 2012)

for

ब्रॉड बैंड रिमोट एक्सेस सर्वर

Broadband Remote Access Servers

(जीआर सं: टीईसी ४८०४०: २०२५)

(Standard No.: TEC 48040:2025)

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 02: November, 2025

FOREWORD

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

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

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

ABSTRACT

This Test Guide of testing pertains to Test Schedule and Test procedures for **Broadband Remote Access Servers.**

CONTENTS

Section	*Item*	*Page No.*
A	History Sheet	5
B	Introduction	5
C	General information for Approval against GR/IR/Spec	6
D	Testing team	7
E	List of the test instruments	7
F	Equipment Configuration offered	7
G	Equipment/System Manuals	8
H	Clause- wise Test Type and Test No.	9
I	Test Setup & Procedures	55
J	Summary of test results	56

A. HISTORY SHEET

Sl. No.	Standard No.	Title	Remarks
1.	TEC/TSTP/GR/IT/RAS-003/03/MAR 2012	TSTP for Broadband Remote Access Server	Issue No. 1
2.	TEC 48041:2025	Test Guide for Broadband Remote Access Server	Conversion of TSTP to Test Guide

B. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance/functionality/ requirements/ performance of the **Broadband Remote Access Servers** as per TEC Standard No. 48040:2025 to be deployed-in or implemented through Indian Telecom Network.

C. General information:

Sl. No.	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 GR/IR/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			

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.: -

Cl. No	Sub Cl.	Clause	Type of Test	Compliance
			Physical Check / Declaration / Documentation/ Report from Accredited Test Lab / Functional Verification / Information / Lab Test (Test Reference)	**Complied / Not Complied / Submitted / Not Submitted / Not Applicable (Indicate Annexure No for Test Results)**
1.1		Scope	Information	
		This document lays down the generic requirement for Broadband Remote Access Server (BRAS) and related Policy Implementation System (PIS). The BRAS (described in chapter one of this document) will connect to DSLAM or any other access node through Ethernet based access/ aggregation network of Service provider (SP). PIS is described in chapter two of this document.	Information	
1.2		Introduction	Information	
		Broadband Remote Access Server (BRAS) acts as intelligent controller of layer 2 network below it. It shall provide the layer 3 network functions such as terminating PPPoE sessions, forwarding IP traffic, IP address assignment, billing, authentication, UDR generation, etc to the layer 2 network below it. It shall provide Broadband access services through the Ethernet based access/ aggregation network which includes DSL aggregation Ethernet to the Home (ETTH), Wi-Fi, Wi-max, etc. The BRAS shall be capable of rate limiting, traffic policing and traffic shaping the individual customer's traffic based on session or port. The BRAS shall be able to be configured for QoS to each customer/ session. However BRAS shall not	Information	

<table>
<tr><td></td><td></td><td>police traffic specified by SP e.g. DNS, RTSP (VoD), IPTV, etc.</td><td></td><td></td></tr>
<tr><td>1.3</td><td></td><td>Category: The Broadband RAS shall be categorised into the following:</td><td>Declaration</td><td></td></tr>
<tr><td></td><td></td><td><table>
<tr><th>Category</th><th>Full duplex backplane capacity</th><th>Packet forwarding rate for 64 byte packets</th><th>Concurrent mix of PPPoE and IPoE sessions</th><th>L2TP tunnels/ sessions</th></tr>
<tr><td>High end</td><td>100 Gbps</td><td>150 MPPS</td><td>96,000</td><td>5,000/ 25,000</td></tr>
<tr><td>Middle end</td><td>30 Gbps</td><td>45 MPPS</td><td>48,000</td><td>1,000/ 5,000</td></tr>
<tr><td>Low end</td><td>8 Gbps</td><td>12 MPPS</td><td>12,000</td><td>100/ 500</td></tr>
</table></td><td>Functional Verification</td><td></td></tr>
<tr><td></td><td></td><td>BBRAS shall support both inner and outer VLAN tag on all down stream interfaces to identify the individual user. Total number of VLANS supported per chassis shall be equal to the total number of subscribers supported on the chassis. Further no. of hardware queue supported by BBRAS shall be equal to PPPoE/ IPoE sessions. Actual backplane, packet forwarding, session and L2TP requirement shall be indicated by tendering authority. No. of PPPoE/ IPoE sessions required shall be multiple of no. of user to be served by BBRAS and no. of services per user. The BBRAS may be offered for one or more of the category for type approval.</td><td>Functional Verification</td><td></td></tr>
<tr><td>1.4</td><td></td><td>Architecture: The Broadband RAS shall have following architectural features:</td><td>Functional Verification</td><td></td></tr>
<tr><td></td><td>i.</td><td>The equipment shall be Carrier class with a modular chassis design. The BBRAS shall have an availability of atleast 99.999%.</td><td>Physical Verification</td><td></td></tr>
<tr><td></td><td>ii.</td><td>BBRAS shall combine full BBRAS, Routing and Circuit Aggregation functionality as defined in the GR in single chassis.</td><td>Physical Verification (Refer GR BRAS)</td><td></td></tr>
<tr><td></td><td>iii.</td><td>The BBRAS shall have architecture so as to provide no single point of failure</td><td>Physical Verification</td><td></td></tr>
<tr><td></td><td>iv.</td><td>The wire-speed forwarding shall be supported on all the interface ports with all QoS features and other features enabled.</td><td>Functional Verification</td><td></td></tr>
</table>

	v.	The BBRAS shall be capable of working with -48 V DC (Negative 48 V DC) with a voltage variation – 40 V to – 57 V D.C.	Functional Verification	
	vi.	The equipment shall be mountable in 19" rack.	Physical Verification	
	vii.	The performance of device shall not be degraded upon enabling of one or more features.	Functional Verification	
	viii.	All type of interfaces shall be supplied on at least two cards mounted in different physical slots of chassis.	Physical Verification	
	ix.	Wherever the redundant interface(s) have been asked, the same shall be provided using interface(s) on different cards mounted in different physical slots of chassis.	Physical Verification	
	x.	The removal or addition of any cards shall not disrupt traffic on other cards.	Physical Verification	
	xi.	A single point failure on the equipment shall not result in network or network management system downtime.	Physical Verification	
	xii.	All the interfaces on the devices shall be supported as integrated interfaces and shall not require any external converters/ adapters.	Physical Verification	
	xiii.	No interfaces shall be provided in the Control Card/ module in all the devices expect.	Physical Verification	
	xiv.	The line interface slots in the devices shall be universal.	Physical Verification	
	xv.	Wherever additional time has been indicated for supporting / implementing a feature, the same feature shall be provided at no extra cost to SP.	Declaration	
	xvi.	The BRAS shall support NTP as per RFC 1305 or SNTP v4 as per RFC 2030.	Lab Test - Refer Test 12	
1.5		**Services:** BRAS shall provide following services:	Information	
	i.	Dial VPN services	Functional Verification	

	ii.	The Differentiated Services model shall be implemented in compliance with RFC 2474, RFC 2597, RFC 3140 and RCF 3246 RFC 3260.	Functional Verification	
	iii.	Differentiated bandwidth access service as following:	Functional Verification	
		a. Separate bandwidth per customer	Functional Verification	
		b. Dedicated bandwidth per customer via committed access rates (CAR), which are definable. Following shall be supported: Committed Information Rate (CIR), Peak Information Rate (PIR), Committed Burst Size (CBS), and Maximum Burst Size (MBS).	Functional Verification	
		c. Range of configurable rates from kbps to Mbps (depending on the access mechanism allowances)	Functional Verification	
	iv.	High Speed Internet access. – Internet access services shall be available through the Ethernet based access/ aggregation network. The Internet access bandwidth shall be controlled as per the access contract subscribed by the customer. The various upstream/downstream access speeds shall vary from 64 Kbps, to 1Gbps in steps of 64 Kbps. The customer shall be able to change his bandwidth (self service provisioning) on as and when need basis through the WEB portal service selection system.	Functional Verification	
	v.	Interactive gaming: interactive gaming services shall be supported.	Functional Verification	
	vi.	VLAN and Gigabit Ethernet services. – it shall be possible to identify individual customers based upon Port, Virtual LAN (VLAN), port + VLAN and port + VLAN range for applying SLA.	Functional Verification	
	vii.	Voice and video telephony over IP	Functional Verification	
	viii.	Differentiated priority access with Quality of Service mechanisms shall be supported. Low latency and low jitter (for voice/Video conferencing applications), Low latency (for streaming applications), Low loss (for mission-critical	Functional Verification	

		applications as well as signalling or VPNs) and Best effort for data traffic shall be available. Differentiated priority access service as following shall be available:		
		a. Separate priority per customer.	Functional Verification	
		b. Range of queue depths configurable for differentiated priority.	Functional Verification	
		c. Application Recognition and priority for separate applications for one customer also configurable.	Functional Verification	
	ix.	Wholesale Services – It shall be possible to sell the access network to the other ISPs as last mile connection for their customers. Separate Virtual router/ VRF shall be configured for the ISP for this application.	Functional Verification	
	x.	Content Delivery Services - These Services shall be provided with content servers connected to the BRAS. This service shall allow SP to have a control over the access by the customers to the contents. Following content delivery applications shall be supported: • Video Broadcast (multicast): • Video on Demand – VoD (unicast) • Point to point/ multipoint Video Conferencing	Functional Verification	
1.6		**Functional requirement :**BRAS shall support following :	Information	
	i.	Point-to-Point Protocol for PAP & CHAP authentication over the PPP link.	Functional Verification	
	ii.	BBRAS shall support IPV6. following shall be supported	Information	
		a. IPv6 over PPPoE	Functional Verification	
		b. Dual stack subscriber support over PPP	Functional Verification	
		c. Prefix delegation via DHCP	Functional Verification	

		d. Independent IPCPv4 and IPCPv6 operation shall be supported.	Functional Verification	
		e. IPv6 over L2TP over IPv4	Functional Verification	
		f. L2TP LNS support for IPv6	Functional Verification	
		g. Radius extensions to support for v6 Radius attributes	Functional Verification	
		h. IPv6 packets over Ethernet (RFC 2464)	Functional Verification	
		i. Neighbour Discovery for IPv6 (RFC 2461	Lab Test	
		j. QoS for IPv6 interfaces	Functional Verification	
		k. IPv6 packet flows for a given user can be classified by the Traffic Class and assigned to different queues. Additionally, IPv6 packets can be TOS (traffic class)	Functional Verification	
		l. Packet Classification for IPv6 traffic	Functional Verification	
		m. DNS client for v6	Functional Verification	
		n. Router advertisements (stateless and stateful auto configuration)	Functional Verification	
		o. Static v6 host names	Functional Verification	
		p. Full IPv6 Multicast feature implementation including MLDv1, MLDv2 and PIM, PIM-SSM	Functional Verification	
		q. capability to block all MC traffic originated by user and sent into the network	Functional Verification	
		r. OSPFv3	Functional Verification	
	iii.	PPPoE as per RFC 2516.	Functional Verification	

	iv.	It shall push the customer sessions initially to Subscriber Service Selection System (SSSS)/Subscriber Service Selection Centre (SSSC) in case of DHCP based access.	Functional Verification	
	v.	The BRAS shall provide the ability to collect statistical information on IP flows, packet and byte counts on all interfaces and users/flows simultaneously, without reducing traffic flow, and without adversely affecting device performance.	Functional Verification	
	vi.	The BRAS shall have capability of forwarding the egress and ingress traffic on a per-logical channel basis to a central location in the network for Lawful Interception and Monitoring.	Functional Verification	
	vii.	The BRAS shall support the ability to monitor established sessions with usernames. The BRAS shall support Command Line Interface Management from local Console Management Port and shall support remote out of band management through an auxiliary port.	Functional Verification	
	viii.	The BRAS shall support hitless switchover of PPPoE and DHCP Sessions in case of the failure of the primary modules.	Functional Verification	
	ix.	IP Services / Policy Management: The BRAS shall support following bandwidth control features:	Functional Verification	
		a. Rate Limit Profile (RLP)	Functional Verification	
		b. Single-rate and two-rate RLPs where maximum allowable traffic flow shall be supported per logical interface, per line module and per system.	Functional Verification	
		c. IP Traffic shaping	Functional Verification	
		d. The BRAS shall support IP over Bridged Ethernet (RFC 2684)	Functional Verification	
	x.	The BRAS shall support :	Functional Verification	
		a. Support for PAP and CHAP protocols for validation of users.	Functional Verification	

		b. PPP session limiting per-port	Functional Verification	
		c. IP session limiting per port	Functional Verification	
		d. IGMP and RTSP request limiting per session/port	Functional Verification	
1.7		**Radius Client:** This allows the BRAS to validate a user on a centralized Radius server. Accounting packets on connect and disconnect are also to be sent to this Radius server. In case of no response from the primary Radius server, the Radius client shall support one or more backup servers. Radius Client shall allow the BRAS to validate a user on a centralized Radius server. Accounting packets on connect and disconnect are also to be sent to this Radius server. In case of no response from the primary Radius server, the Radius client shall support one or more backup servers. BRAS shall support the following:	Functional Verification	
	i.	RFCs:	Functional Verification	
		a. RFC 2716: PPP EAP TLS Authentication Protocol	Functional Verification	
		b. RFC 2865: Radius	Functional Verification	
		c. RFC 2866: Radius Accounting	Functional Verification	
		d. RFC 2867: Radius Accounting Modifications for Tunnel Protocol Support	Functional Verification	
		e. RFC 2868: Radius attributes for tunnel support	Functional Verification	
		f. RFC 2869: Radius extension	Functional Verification	
		g. RFC 3162: Radius and IPv6	Functional Verification	

		h. RFC 3576: Dynamic authorization extension to Radius	Functional Verification	
	ii.	Duplication of Radius accounting packets, so that accounting information is sent to the Radius server specified by the domain name and to a pre-configured Radius accounting server simultaneously.	Functional Verification	
	iii.	Periodic or Interim Accounting records generation shall be supported, configurable time intervals (minimum of five minutes) shall be supported.	Functional Verification	
	iv.	"round-robin" selection of radius servers per domain. This allows the load of a Radius server to be shared amongst a Radius server pool. The BRAS device will distribute Radius requests equally between the pooled Radius servers.	Functional Verification	
	v.	Radius server backup, per domain. In the event that the default Radius server fails, it shall use second and third Radius server backup purposes	Functional Verification	
	vi.	Domain- name stripping: the ability to strip the domain-name portion of the username attribute, before sending the Access-Request packet to the RADIUS server	Functional Verification	
	vii.	RADIUS VSAs (Vendor Specific Attributes) for at least the following features:	Functional Verification	
		a. Specification of primary and secondary DNS server IP addresses to be returned to the subscriber.	Functional Verification	
		b. Selection of service profile or template to be used for a particular subscriber.	Functional Verification	
		c. Selection of local IP address pools.	Functional Verification	
		d. . Dynamic interface creation parameters	Functional Verification	
		e. Enabling/disabling of IGMP/ IGMP groups.	Functional Verification	
		f. Source Address Validation to protect against Denial of Service attacks.	Functional Verification	

1.8		**IP address assignment:** The BRAS shall be able to assign IP addresses using the following mechanisms:	Functional Verification	
	i.	Dynamic assignment through a pool of IP addresses stored within the BRAS.	Functional Verification	
	ii.	Assignment of an IP address from a Radius server (IP address per user)	Functional Verification	
	iii.	Support for DHCP server assignment, where one or more DHCP servers can be configured per domain. It shall support DHCP Proxy for configuration of PPP-based subscribers and DHCP Relay for configuration of non-PPP subscribers. The BRAS shall support following RFCs for the DHCP Server functionality.	Functional Verification	
		a. RFC 2131 Dynamic Host Configuration Protocol.	Functional Verification	
		b. RFC 3046 DHCP Relay Agent Information Option.	Functional Verification	
		c. RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.	Functional Verification	
		d. RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	Functional Verification	
		e. RFC951: bootstrap protocol 13 TEC Standard No. 48040:2025	Functional Verification	
		f. Option 82 as per RFC 3046.	Functional Verification	
		g. It shall be possible to provide IP address based upon port ID , VLAN , etc.	Functional Verification	
	iv.	Assignment from a downstream ISP Node	Functional Verification	
	v.	Support for multiple IP address pools (both public and private), allocated at connect time, based on the domain name entered by the user. It shall be possible to configure at least 500 domains. It shall be possible to assign unique address pool to each domain.	Functional Verification	

	vi.	SNMP traps shall be sent when a configurable IP pool utilization threshold has been reached. This threshold shall be user-configurable	Functional Verification	
	vii.	Support for the Radius attributes “framed-IP-address” to allow IP address and subnet assignment directly from the Radius server	Functional Verification	
	viii.	Duplicate address assignment check- BRAS shall have a configurable feature where in the event of duplicate IP address assignment; the user access attempt is rejected.	Functional Verification	
1.9		**Routing features**	Functional Verification	
	i.	BRAS shall support following OSPF protocol features:	Functional Verification	
		a. The BRAS shall support OSPF V2 as per RFC 2328.	Functional Verification	
		b. The BRAS shall support OSPF Not So Stubby Area (NSSA) RFC 3101.	Functional Verification	
		c. The BRAS shall support RFC1850, OSPFv2 MIB.	Functional Verification	
		d. The BRAS shall support RFC2370, Opaque LSA option.	Functional Verification	
		e. RFC 2740, OSPF for IPv6.	Functional Verification	
		f. The BRAS shall support OSPF Stub Area.	Functional Verification	
		g. The BRAS shall support “Hitless OSPF Restart” RFC 3623. (link state redundancy) or OSPF graceful restart.	Functional Verification	
		h. The BRAS shall support Traffic Engineering (TE) extensions to OSPF v2 (OSPF-TE) as per RFC 3630.	Functional Verification	
		i. OSPF Sham Links.	Functional Verification	
		j. Latest version of OSPF with support of variable length sub-netting shall be supported.	Functional Verification	

		k. Bidirectional Forwarding Detection shall be supported.	Functional Verification	
	ii.	BGP – BRAS shall support following features:	Functional Verification	
		a. RFC 4271 & 1772, BGPv4	Functional Verification	
		b. RFC1997, BGP Communities Attribute	Functional Verification	
		c. RFC 2270: Using a Dedicated AS for Sites Homed to a Single Provider. 14 TEC Standard No. 48040:2025	Functional Verification	
		d. RFC 2385: Protection of BGP Session via the TCP MD5 Signature Option.	Functional Verification	
		e. RFC 2439, BGP Route Flap Damping	Functional Verification	
		f. RFC 2918, Route Refresh Capability for BGP-4	Functional Verification	
		g. RFC 3065, Autonomous System Confederations for BGP	Functional Verification	
		h. RFC 3107, Carrying Label Information in BGP-4	Functional Verification	
		i. BGP Extended Communities Attribute	Functional Verification	
		j. BGP4 Multi path support to enable load balancing between multiple exterior BGP peers from the same downstream router.	Functional Verification	
		k. Exterior BGP multi-hop support-to-support load balancing between two EBGP peers connected by two or more links.	Functional Verification	
		l. Prefix List tracking & Control to enable network administrators to control peering requirements with exterior BGP peers.	Functional Verification	

		m. Policy Routing to enable flexibility in making changes to the normal routing process based on the characteristics of the traffic.	Functional Verification	
	iii.	BRAS latency shall be less than 100 µs for traffic flowing from one interface to other interface on a different line card through the switching fabric, with all the ACL and filtering on at full load.	Functional Verification	
	iv.	**Multicast feature- The BRAS shall support following:**	Functional Verification	
		a. It shall support IGMP snooping v2 and field upgradeable to v3 as and when desired by SP as described in RFC 1112, RFC 2236, and RFC 3376 with IGMP Routing Policies to filter IGMP requests.	Functional Verification	
		b. The BRAS shall support PIM- SM (Protocol Independent Multicast Sparse Mode, RFC 2362)	Functional Verification	
		c. RFC 3446, Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP). If feature is not supported at day one, same shall be made available free of cost within 6 months of deployment.	Functional Verification	
		d. RFC 3569, An Overview of Source-Specific Multicast (SSM) to ensure that no user initiates a source within the multicast domain and limit users only to the range of multicast address in SSM. If feature is not supported at day one, same shall be made available free of cost within 6 months of deployment	Functional Verification	
		e. Multicast ACL to ensure security	Functional Verification	
		f. Multicast Load Balancing traffic across multiple interfaces per flow based	Functional Verification	
		g. Dynamic broadcast Source Failover using Anycast routing.	Functional Verification	
		h. RFC 2365, Administratively Scoped IP Multicast.	Functional Verification	

		i. RFC 3618, Multicast Source Discovery Protocol (MSDP). If feature is not supported at day one, same shall be made available free of cost within 6 months of deployment.	Functional Verification	
		j. The BRAS shall support atleast 200 multicasting groups for all categories of BRAS. The BRAS shall support Wire-rate multicast performance with atleast 5000 multicast streams per multicasting group for High End BRAS, 2000 for Middle End and 1000 for Low End BRAS The multicast protocols to be supported shall be IGMP version 2 upgradeable to version 3, PIM-S and Multicast BGP. Number of simultaneous and concurrent PPP sessions shall be as per clause 1.0.2.	Functional Verification	
	v.	MPLS features: BRAS shall optionally support MPLS PE Router functionality as defined in .latest TEC standard on BGP/MPLS Virtual Private Network available on TEC website (https://tec.gov.in/standardsspecifications).	Functional Verification (Refer to TEC Website)	
1.10		**Virtual routing:** The Broadband BRAS shall support Multiple Virtual Routers capability that allows the platform to partitioned into multiple logical entities, which allow wholesaling of broadband access services by subdividing the DSL Access network among multiple resellers. The BRAS shall support the following functionality of working as Virtual Routers. Virtual routing functionality can be provided by MPLS based VPN (in such case the VRF configured shall be equivalent to VR in terms of output and input to BRAS; configuration of such VPN shall be possible through EMS, running of MP-BGP shall not be required) .	Functional Verification	
	i.	The BRAS shall support at least 200 Virtual Routers for High End, 100 Virtual Routers for Medium End and 20 Virtual Router for Low end per chassis.	Functional Verification	
	ii.	Each virtual router shall maintain independent routing table and shall support minimum of 1000 routing table entries. Each Virtual Router shall be capable of functioning as independent routing entity with independent routing tables	Functional Verification	

	iii.	Each Virtual router shall be configurable independently for RIP, OSPF and BGP routing protocols.	Functional Verification	
	iv.	BRAS shall support minimum of 2 SNMP servers with version 2 per Virtual router. It shall be possible to extend the SNMP Management for Virtual routers to the desired customers.	Functional Verification	
	v.	The virtual routers shall be assigned to various service providers or corporate customers for wholesale application. The console access to individual Virtual router shall be supported.	Functional Verification	
	vi.	Authentication and authorization for Virtual Routers shall be supported for telnet (login) access to BRAS.	Functional Verification	
	vii.	The ADSL subscribers shall be able to map to different Virtual router based on domain name or as assigned by Radius server during login (Authorization). The non-authenticated customer shall be able to be 16 TEC Standard No. 48040:2025 configured statically to a pre defined Virtual router.	Functional Verification	
	viii.	Individual virtual router shall support configuration of addresses for AAA, server, DNS server, IP address pool, per subscriber based QoS policy, etc. The BRAS shall also support sending duplicate accounting records to distinct locations.	Functional Verification	
1.11		**Tunnelling:** It shall be possible for the Broadband RAS clients to be tunnelled back using L2TP protocol.	Functional Verification	
	i.	It shall be possible to support Layer 2 Access concentrator functionality (LAC)	Functional Verification	
	ii.	It shall be possible to support Layer 2 Network Services functionality (LNS)	Functional Verification	
	iii.	The BRAS shall be able to aggregate PPP sessions into L2TP tunnels (LAC function).	Functional Verification	
	iv.	It shall be possible to tunnel customer traffic through Generic Routing Encapsulation(GRE) Tunnel	Functional Verification	
	v.	The tunnelling parameters can either be defined locally on the BRAS or controlled via tunnelling attributes sent via RADIUS.	Functional Verification	

1.12		**Quality of Service:** The following features shall be supported in the BRAS to ensure traffic prioritization and QoS:	Functional Verification	
	i.	The BRAS shall be capable of rate limiting, traffic policing and traffic shaping the individual customer's traffic. The BRAS shall be able to be configured for QoS to each customer. The BRAS shall apply the configured QoS Policy for individual customer.	Functional Verification	
	ii.	The BRAS shall be capable of rate limiting, traffic policing and traffic shaping the individual customer's traffic. The BRAS shall be able to be configured for QoS to each customer. The BRAS shall apply the configured QoS Policy for individual customer. Class-based scheduling/queuing with at least 8 Classes that provides configurable minimum bandwidth allocation to each class. Committed Access Rate, Traffic Policing, sub rate service offering At least three level dropping precedence levels in each queue.	Functional Verification	
	iii.	The BRAS shall support a Diffserv-aware hierarchical scheduler that allows it to manage the network so that any potential congestion in the Access Network between the BRAS and the CPEs can be avoided. The hierarchical scheduler in the BRAS must be able to model the congestion points in the broadband network planned. The BRAS must make sure that no more traffic is inserted in the layer 2 network than is allowed according to its knowledge of the logical topology and customer policy constraints.	Functional Verification	
	iv.	The hierarchical scheduler in the device shall be able to model the congestion points in at least two subsequent Ethernet hops.	Functional Verification	
	v.	The BRAS shall support at least 4 layers of hierarchy (i.e. physical port, outer VLAN, inner LAN/port id and session scheduler).	Functional Verification	
	vi.	Hierarchical scheduling shall be resource efficient in the sense that any traffic shall be capable of using the unused bandwidth that has been allocated to other traffic classes.	Functional Verification	

	vii.	The hierarchical scheduler shall support allocating downstream bandwidth based on policy configuration across PPP, Ethernet, and IP technologies.	Functional Verification	
	viii.	Per subscriber class-based queuing, which allows a set of different traffic classes per IP interface and subscriber	Functional Verification	
	ix.	Per subscriber and per IP interface queuing as follows:	Functional Verification	
		a. HRR – Hierarchical Round Robin.	Functional Verification	
		b. SPQ – Strict Priority Queuing.	Functional Verification	
		c. HRR and SPQ queue profiles can be attached to a physical port, sub-port level (for example VLAN) and IP interface (subscriber).	Functional Verification	
		d. Wire speed forwarding on all interfaces and all packet sizes even with classification and QoS activated on all interfaces.	Functional Verification	
		e. Functionality such as IP QOS, tunnel termination / initiation, BGP peering, etc. shall not reduce the effective throughput of the BRAS device.	Functional Verification	
		f. The BRAS shall be able to police both upstream and downstream traffic for traffic aggregates and for sub-classes of the aggregate using the same topology information that exists for the hierarchical scheduler.	Functional Verification	
		g. The BRAS shall support RED and WRED policing of upstream traffic using the same topology information that exists for the hierarchical scheduler for upstream traffic aggregates and subaggregates based on class.	Functional Verification	
		h. BRAS shall support hierarchical shaping, scheduling and policing for the control of traffic through the access node and any other IP device that do not have IP awareness	Functional Verification	
		i. The BRAS shall be able to police the use of DSCPs received from customer traffic and remark traffic if it does	Functional Verification	

		not match with the customer profile data – including potentially dropping unauthorized traffic.		
		j. The BRAS shall support Diffserv queuing for the Assured forwarding (AF) and Expedited forwarding.	Functional Verification	
		k. The BRAS shall support multiple queues per user with the appropriate scheduling mechanism to effectively implement Diffserv queuing behaviour (strict priority, Weighted Fair Queuing). Thus BRAS shall have n+ 1 queue per concurrent session to deliver QoS on per customer for n services.	Functional Verification	
		l. The BRAS shall support mapping of DSCP to VLAN or other traffic engineering capabilities in the Regional Network.	Functional Verification	
	x.	The BRAS shall support the capability to fragment Assured Forwarding (AF) and Best Effort (BE) traffic in order to constrain the perturbing impact of AF and BE packets on EF traffic delay, for e.g. using a mechanism such as MLPPPLFI (RFC 1990).	Functional Verification	
1.13		**High Availability Features:** The Broadband RAS shall have the following features to ensure high availability and redundancy. Redundancy features shall be with active and standby arrangement so that the network is not affected due to equipment failures. Redundancy does not imply “spare unit”.	Functional Verification	
	i.	The control modules shall support 1:1 redundancy and switching module shall support N+1 redundancy.	Functional Verification	
	ii.	The power supply components shall be load sharing, hot swappable and redundant even under maximum load operation.	Functional Verification	
	iii.	All interface modules shall support non-disruptive hot swap capabilities (Online Insertion and Removal).	Functional Verification	
	iv.	The BRAS shall have natural cooling arrangement which shall not involve any forced cooling such as by using fans etc in the BRAS. However if the forced cooling is unavoidable and fans etc are to be used in the BRAS, these shall be DC operated and shall not impact MTBF of BRAS. The DC operated fans	Functional Verification	

		shall be available in redundant configuration and shall be hot swappable.		
	v.	The BRAS shall support online software reconfiguration to ensure that changes made to its configuration take place with immediate effect.	Functional Verification	
	vi.	The BRAS shall support non-disruptive expansion of memory to ensure that software upgrades do not disrupt the normal BRAS operation or else the BBRAS shall be equipped with full memory since beginning.	Functional Verification	
	vii.	The BRAS shall support dynamic online reconfiguration both locally and from remote location and ensure that changes made shall take place with immediate effect.	Functional Verification	
	viii.	The BRAS shall support comprehensive hardware and software fault isolation and recovery tools.	Functional Verification	
	ix.	The BRAS shall support non-blocking and high availability architecture. The router shall have no single point of failure.	Functional Verification	
	x.	The BRAS shall have mechanism to prevent Head of Line (HOL) blocking on all interfaces.	Functional Verification	
	xi.	The BRAS shall support N+1 redundancy of Switch Cards. Failure of one Switch Card shall not lead to: -	Functional Verification	
		a. Degradation in the performance of router.	Functional Verification	
		b. Degradation in any service levels.	Functional Verification	
		c. Reduction in switching capacity.	Functional Verification	
	xii.	BRAS shall support Non Stop forwarding (NSF) supported by graceful restart extensions (e.g. helper mode) or Non Stop Routing (NSR) supported to facilitate non stop services such as L3VPN and L2VPN for the following as per IETF standard as and when finalised:	Functional Verification	
		a. BGP	Functional Verification	

		b. Graceful restart for OSPF – as per RFC 3623	Functional Verification	
		c. Graceful restart for LDP – as per RFC 3478.	Functional Verification	
	xiii.	**Non-Stop Forwarding:** BRAS shall support NSF as follows:	Functional Verification	
		a. Any disruption in the Control Plane (for Routing & Connection Mgt), which shall cause a switchover to a standby Control Card, shall not affect forwarding of data in the line cards.	Functional Verification	
		b. During the switchover of Switch Card or Control Card, all active LSPs and the underlying Martini circuits shall be protected, remain operative and shall not be lost.	Functional Verification	
		c. Forwarding entries on the line cards, such as IP prefixes and outgoing encapsulations shall not be affected by the loss of the active switch card.	Functional Verification	
	xiv.	**Non Service Affecting Upgrades**	Functional Verification	
		a. Protection of memory address space for all running processes.	Functional Verification	
		b. Dynamic Bandwidth upgrade for LSP and Circuits without restart.	Functional Verification	
		c. The BRAS shall support LSP shared explicit mode for make before break operations.	Functional Verification	
1.14		**Management and Security:** The Broadband RAS shall be able to connect to Centralized Element Management System (EMS) and Subscriber Service Selection Centre (SSSC) as described in chapter 2 of this document. The BRAS shall support the following management and security features.	Functional Verification (Refer GR BRAS)	
	i.	SNMP: The BRAS shall support SNMP V2 upgradeable to V3. With support for standard MIBs such as MIB support for BGP4, OSPF, MIB I, MIB II. The Public and Private MIBs shall be provided to SP.	Functional Verification	

	ii.	The BRAS shall be configurable for the parameters such as real time and historical statistics, ability to view connect rates, retransmissions and other key statistics for troubleshooting, accounting and system utilization. The BRAS shall be able to give service level agreements to the customers. The system shall be able to connect to IP network and generate billing statistics for each of them depending upon connectivity, speed of operations, volume of data transacted and the service level agreements used for the connections.	Functional Verification	
	iii.	Telnet, FTP / TFTP support: The BRAS shall support Telnet client and server functionality. It shall support FTP /TFTP for software upgrades over the network.	Functional Verification	
	iv.	The BRAS shall support the ability to monitor established calls with usernames. The EMS shall be able to maintain call history, track calls 20 TEC Standard No. 48040:2025 states and various stages of call set up, reasons for disconnect, retrains, connect speeds, receive speeds transmit speeds etc	Functional Verification	
	v.	The BRAS shall support Command Line Interface Management from local Console Management Port and shall support remote out of band management through an auxiliary port.	Functional Verification	
	vi.	The BRAS shall generate system alarms and trigger traps and events messages to the EMS. The BRAS shall support filtering of alarm and event messages to the EMS.	Functional Verification	
	vii.	The BRAS shall support the pre-planned timed reboot to upgrade to a new hardware/software version.	Functional Verification	
	viii.	The BRAS shall be able to provide the information to centralised EMS on the number of calls in progress, calls in set up phases and percentage of successful calls / unsuccessful calls etc.	Functional Verification	
	ix.	Access Security: The BRAS shall have at least one level of password protection features. Multiple levels of management access privileges for privileged (configuration), and non-privileged (read-only) tasks shall be supported.	Functional Verification	

		a. Implement Access Lists on the BBRAS to ensure SNMP access only to the SNMP manager or the NMS or the SSSC or BPS.	Functional Verification	
		b. Multiple Privilege Levels shall be supported to provide different level of access.	Functional Verification	
		c. Remote Authentication Dial-In User Service (RADIUS).	Functional Verification	
		d. Reverse Path Forwarding (IP source address Validation) which helps in controlling denial of service and Smurf attacks.	Functional Verification	
1.15		**Interface Requirements:** The Broadband RAS shall be capable of supporting one or more type of the following LAN & WAN interfaces as indicated below for connecting to the IP/MPLS network. The BRAS shall support atleast 4096 VLAN per GE / Fast Ethernet interface. The number of interface port and types shall be specified by the tendering authority at the time of procurement:	Functional Verification	
	i.	10/ 100/ Base Tx. auto sensing; IEEE 802.3u compliant, full duplex	Functional Verification	
	ii.	Gigabit Ethernet; IEEE 802.3z compliant, full duplex, Optical(Sx and Lx) and electrical Interfaces to be supported	Functional Verification	
	iii.	10 Gigabit Ethernet as per IEEE 802.3z full duplex (for High End BRAS only) Optical (Sx and Lx) shall be supported.	Functional Verification	
	iv.	STM-1 (Single mode and Multi mode) as per the latest TEC standard on STM-1 available on TEC website (https://tec.gov.in/standardsspecifications).	Functional Verification	
	v.	STM-4 (Single Mode and Multi mode) as per the latest TEC standard on STM-4 available on TEC website.	Functional Verification	
	vi.	STM-16 (Single Mode and Multi mode) as per the latest TEC standard on STM-16 available on TEC website	Functional Verification	
	vii.	All WAN interfaces shall support 100 ms buffering.	Functional Verification	

	viii.	BRAS shall support Packet over SDH as per RFC 2615 for STM interfaces.	Functional Verification	
1.16		**Element Management System (EMS):** BRAS shall be manageable from central EMS for all FCAPS (fault, configuration, accounting, performance and security) functions as per TEC standard on eMS available on TEC website (https://tec.gov.in/standards-specifications). EMS shall provide FCAPS information to NMS over standard interfaces as described in TEC standard on eMS available on TEC website .	Functional Verification (Refer GR eMS)	
	Functional and Technical Requirements of Policy Implementation System (PIS) for IP Network			
2.1		**Introduction**		
		This documents describes generic requirements of various components of Policy Implementation System which shall be used in service provider's (SP) IP Network to implement the policies, e.g. user access right, bandwidth, etc. All applications shall support IPv4 and IPv6 simultaneously. The Figure.2 shows block diagram of Policy Implementation System (PIS) for IP network. It shall include following components;	Information (Refer GR BRAS)	
	i.	**Directory server:** It shall store user profile. It shall be as per TEC GR: GR/ISA-01/01.	Declaration (Refer GR ISP Application)	
	ii.	**AAA:** It shall be used for authentication, authorization and accounting of user sessions. It shall get the profile of user and fetch the same at the start of session to BRAS/ SSSC. It shall be as per TEC GR: GR/ISA-01/01.	Declaration (Refer GR ISP Application)	
	iii.	**Billing:** Billing application of SP shall be used	Declaration	
	iv.	**Subscriber Service Selection System (SSSS):** It shall be Web portal with Radius client. The web portal shall be as per TEC GR: GR/ISA01/01. It shall be user interfaced to the network policy implementation architecture. SSSS shall act as a "Portal" into the network, where advertisements, automatic provisioning and service registration shall take place. The portal shall offer personalization for each end-user in its presentation of services	Functional Verification (Refer GR ISP Application)	

		based on the information stored in the directory. It shall authenticate the user by AAA server through Radius client. It shall allow the users to modify certain fields in directory server database e.g. password. SSSS shall be integrated SSSC to change the current user session parameters e.g. speed. SSSS shall be deployed in the network in such a way that in case of unavailability of one SSSS, the load of the same shall be shared by other SSSSs deployed in the SP's IP network		
	v.	**Subscriber Service Selection Centre (SSSC):** It shall be the intelligence of PIS. It shall integrate with BRAS by COPS/ RADIUS to enforce the policies. It shall download the profile of users at the start of session through AAA server. It shall integrate with SSSS to change the current user session parameters e.g. speed. It shall also integrate with billing system to check the account balance of users. It shall optionally keep the usage history of users and present the same with account balance to users through SSSS in case the same is not available through billing system. It is optional that AAA server and SSSC can be implemented on the same hardware. Detail description is provided in clause 1.2 of this document.	Functional Verification (Refer GR BRAS Clause 1.2)	
	vi.	**BRAS:** It shall be the policy implementation point in the IP network. It is assumed that all network related policy shall be enforced through 23 TEC Standard No. 48040:2025 BRAS only. BRAS shall be as per chapter 1 of this document. It shall be integrated with SSSC for policy implementation	Functional Verification (Refer GR BRAS Chapter-1)	
	vii.	**Provisioning system:** It shall be used to provision users in directory server and service templates in the SSSC. It shall also inform the billing system of every provisioning. Detail requirement is provide in clause 2.3. It is envisaged that network element shall be provisioned through their respective element management system (EMS) through NMS (network management system).	Functional Verification (Refer Clause 2.3 below)	
		Tendering authority shall provide current and future user base, concurrency figure, CDR generation per day per user and average session per user for the dimensioning of PIS.	Declaration	

2.2		**Detail requirement of SSSC:** The SSSC shall support the functionalities given below:	Functional Verification	
	2.2.1	SSSC shall provide templates for creation of services. Templates shall include information regarding charging, etc.	Functional Verification	
	2.2.2	The SSSC Provisioning interface shall include XML/SOAP/HTTP/LDAP. These shall interface with provisioning system, CRM and other systems of SP as required.	Functional Verification	
	2.2.3	The SSSC shall support bulk provisioning through text written macro.	Functional Verification	
	2.2.4	The SSSC shall provide Resource Admission Control for the network. It shall prevent contention in the network bandwidth by RTP traffic in order to preserve performance.	Functional Verification	
	2.2.5	The SSSC shall be able to deny service authentication / resource reservations in response to network contention.	Functional Verification	
	2.2.6	The SSSC shall allow SP to activate service offerings on real time basis and automatically provision the BRAS, as and when the same is requested by the customer.	Functional Verification	
	2.2.7	The SSSC shall track service usage, activates multiple service sessions simultaneously for a given user with a capability to track each session separately. It shall be possible to track all sessions of user to take session admission control decision.	Functional Verification	
	2.2.8	The SSSC shall allow flexible accounting rules for user session based on the policy defined. It can be flat based, time based, etc.	Functional Verification	
	2.2.9	The BRAS and SSSC shall support both clientless and client (PPPoE) based login services.	Functional Verification	
	2.2.10	The SSSC shall support both Post paid and pre paid customer access. It shall be capable of supporting all users as pre-paid.	Functional Verification	
	2.2.11	The SSSC shall support location specific content to the subscribers based on parameters like BRAS hostname, interface name etc.	Functional Verification	

	2.2.12	The SSSS or SSSC shall not be in the path of data flow.	Functional Verification	
	2.2.13	The SSSC shall support protocols like SOAP/XML/CORBA for Admission Control to be implemented along with the Content Servers / Middleware. Admission control mechanism shall ensure enough resources available for 24 TEC Standard No. 48040:2025 serving the request and allow service to be accessed after it reserves resources. If resources are not available, the service shall be denied to the user with the feedback to user.	Functional Verification	
	2.2.14	The SSSC shall be able to control / modify policies / profile in BRAS for automatic provisioning and management.	Functional Verification	
	2.2.15	The SSSC shall support web based GUI for service definition and subscriber management, policies and store them in a central location.	Functional Verification	
	2.2.16	The SSSC shall be able to decide dynamically while activating the services on the basis of the RADIUS information and directory server profile data.	Functional Verification	
	2.2.17	Dynamic Service Selection via web, with policy assignment based on standard protocols like COPS (RFC 2748) and RADIUS (as per RFC 2865 & 2866) shall be supported.	Functional Verification	
	2.2.18	The SSSC shall support protocols like XML/SOAP for Admission Control to be implemented along with the content servers.	Functional Verification	
	2.2.19	The SSSS shall not constitute a single point of failure. SSSC fail over shall be seamless and shall not affect any subscriber active at that moment. SSSC shall be deployed in cluster configuration and with Disaster Recovery planning with identical equipment hardware and software.	Functional Verification	
	2.2.20	The SSSC shall facilitate collection of usage-based statistics per subscriber.	Functional Verification	
	2.2.21	The SSSC shall display the transaction details made by the customer like total number of bytes downloaded in a given period with other details like date, time etc with summary at the	Functional Verification	

		bottom for Internet Service & similar format for other services and correlate the same with the plan subscribed by the user so as to ensure that the same is within the permitted usage limit.		
	2.2.22	The SSSC shall also pop up the messages to the customer as and when the user is in the verge of exceeding the usage limit. This limit shall be configurable like 60%, 70% etc	Functional Verification	
	2.2.23	The SSSC shall give customized screen for the user to change his password and view his other personal information like usage details etc.	Functional Verification	
	2.2.24	The SSSC shall support the virtual partitioning of domain specific resources (interfaces to access subscriber profiles, authentication and accounting) to best support a wholesale model.	Functional Verification	
	2.2.25	The SSSC shall allow SP to define new services, modify the existing one and even delete the offered services under authorized username and password.	Functional Verification	
	2.2.26	The SSSC shall also allow the SP to define the minimum set of services that will be available by default to all customers. Subsequent modification in the profile can be done by the subscriber himself through self-selection.	Functional Verification	
	2.2.27	The SSSS in conjunction with SSSC shall be able to dynamically update the changes based on the changes made in the profile like defining new service, modifying existing service and subscriber real time status like expiry of the balanced hour in case of pre-paid service. 25 TEC Standard No. 48040:2025	Functional Verification	
	2.2.28	SSSC shall provide session history, track sessions states and various stages of session set up, reasons for disconnect, retrains, connect speeds, receive speeds transmit speeds etc. tendering authority shall provide storage requirement of session history data.- optional in case the same is provided by billing system.	Functional Verification	
	2.2.29	The SSSS/SSSC provides a service catalogue capability that allows the service provider to define services using a set of	Functional Verification	

		graphical tools. The service catalogue contains a comprehensive list of the services available for subscription, as well as services that the organization plans to provide in the future. The system allows these services to be grouped by category, such as Access Service or Content Service, and further divide them into subgroups such as DSL Access or Cable Access etc. Each catalogue of service can have a number of different price plans depending upon the Service Quality to be delivered associated with it.		
	2.2.30	The SSSC shall work in conjunction with the BRAS to activate new services for subscribers automatically, without any manual provisioning done by SP.	Functional Verification	
	2.2.31	Using SSSC through SSSS the end users shall be able to choose from a variety of content, services and providers on their customized Service Selection Portal. This action shall activate a set of policies that interact with the BRAS to customize the connection between the user and the appropriate provider and/or desired content. Using the SSSS/SSSC , SP shall be able to offer a single service or multiple services, each with its own set of policies (e.g. QoS, bandwidth, security) and its own accounting mechanism (flat rate, pay-per-volume, pay-per-time, etc). Usage-based rating and accounting information shall be collected by the billing application. Tendering authority shall provide the format and method of this CDR transfer.	Functional Verification	
	2.2.32	The SSSS/SSSC shall allow end-users to access a variety of ISPs, Content Providers, who can be selected on a static or dynamic basis.	Functional Verification	
	2.2.33	The SSSS/SSSC shall provide the corporate customers the ability to manage their access configuration and network usage such as bandwidth.	Functional Verification	
	2.2.34	It shall not use NAT/NAPT in the data path to any of the services.	Functional Verification	

	2.2.35	The SSSS/SSSC shall have the capability of providing multiple simultaneous services (at least 5) at the same time.	Functional Verification	
	2.2.36	It shall be possible to provide the CDR to one or more billing servers which shall be selected depending on service.	Functional Verification	
	2.2.37	It shall terminate all service and generate the appropriate accounting records when the subscriber is disconnected abnormally	Functional Verification	
	2.2.38	There shall be a standard based protocol (such as Common Open Policy Service (COPS)) or RADIUS running between the SSSC and the BRAS for applying the QoS parameters selected by the subscriber. Some of the type of QoS parameters are Policy Routing, Traffic shaping, QoS Processing, Rate Limiting or Marking. Using this Policy module, the customer shall choose the services such as quality of service (QoS), VPN selection, and selection of ISPs. 26 TEC Standard No. 48040:2025	Functional Verification (Refer GR BRAS)	
	2.2.39	The SSSC shall store the profile in the directory server and read it through the AAA Server	Functional Verification	
	2.2.40	The SSSC shall support the accounting reports in the following formats –	Functional Verification	
		i) **Traffic Summary Report** - Displays total packets and total KB for traffic that can be mapped to the (Traffic) and otherwise to Unmappable Traffic.	Functional Verification	
		ii) **Application Type Summary Report** - Provides total packets and total K bytes for each application type.	Functional Verification	
		iii) **Customer Summary Report** - Provides total packets and total KB for each customer plus additional reports for customer site and application type.	Functional Verification	
		iv) **Type of Service Summary Report** - Provides total packets and total KB for each type of service.	Functional Verification	
		v) **Customer Traffic Volume Report** - Provides information on all traffic volume for a specific customer in packets or KB (by type of service).	Functional Verification	

		vi) **Network Traffic Volume Report** - Provides information on all traffic volume for the network in packets or KB (by type of service).	Functional Verification	
2.3		**Provisioning System**: The provisioning system shall also integrate with NMS/OSS for user/ service provisioning. It shall have all the permissions to write on every field of directory server database. It shall offer following features:	Functional Verification	
	2.3.1	The Provisioning System shall offer step-by-step information-assisted population of templates.	Functional Verification	
	2.3.2	SP shall be able to add, delete, or modify customers. In addition, they shall be able to easily set up extranet relationships.	Functional Verification	
	2.3.3	It shall support scheduling like when a new service or service change is entered, users have the ability to schedule the service activation time, enabling the service provider to make arrangements for hardware delivery or for other steps required prior to activation of the service. The following requirements shall be met:	Functional Verification	
		i. Scheduling of tasks at creation time.	Functional Verification	
		ii. Scheduling of tasks after creation time.	Functional Verification	
		iii. Scheduling of tasks once, hourly, daily weekly, monthly, yearly.	Functional Verification	
	2.3.4	It shall support configuration of the Service Level Agreement (SLA) monitoring parameters in the SSSC.	Functional Verification	
	2.3.5	The Provisioning System shall support the Application Programming Interfaces (APIs) to interface to third party tools (like NMS). Programmers can use these APIs to incorporate Provisioning System features in source code of third-party network-management software. This adds network management support for the services.	Functional Verification	

	2.3.6	The provisioning system should be capable of automating the personalized presentation of services for an end-user in the SSSC.	Functional Verification	
	2.3.7	It shall be accessed by SP's staff locally and remotely. It shall provide web based GUI for provisioning.	Functional Verification	
	2.3.8	It shall have multiple levels (at least 5) of access authorization through user name and password for administration, maintenance, provisioning, etc.	Functional Verification	
	2.3.9	The Provisioning system shall be a multi-user system. Tendering authority shall provide the no. of concurrent operators.	Functional Verification	
	2.3.10	It shall interface with the NMS so that the provisioning becomes automatic i.e. as soon as a subscriber is created/ modified/ deleted, the information shall go to the NMS where it will be displayed as non-attached subscriber. Once the port assignment has been done, the information shall be provided to the provisioning system and this time shall be recorded as commissioned time under designated / privileged operator command. Such privilege shall be assignable to each of the remote operator terminals.	Functional Verification	
	2.3.11	The Provisioning system shall be located at the two locations with one of them acting as Primary & the other as Backup acting as a disaster recovery site. When the Primary PMS fails, the Backup PMS shall take over the functions of the Primary PMS without loss of data or functionality. It shall be possible to update the secondary PMS by the Primary PMS on line.	Functional Verification	
	2.3.12	The provisioning system shall support step-by-step information-assisted population of templates.	Functional Verification	
	2.3.13	Operators shall be able to add, delete, or modify customer profile.	Functional Verification	
	2.3.14	Operators shall also be able to define and modify policies through GUI and store these profiles in the directory server	Functional Verification	

	2.3.15	Operators shall be able to define new services, modify the existing one and even delete the offered services under authorized username and password.	Functional Verification	
	2.3.16	Operators shall be able to define the minimum set of services that will be available by default to all customers. Subsequent modification in the profile can be done by the subscriber himself through self-selection.	Functional Verification	
	2.3.17	The provisioning system shall support Creation and management of permission groups for defining access rights for users in a group.	Functional Verification	
	2.3.18	The provisioning system shall support Management of individual users.	Functional Verification	
2.4		**Hardware and software Requirements of Policy Implementation System components**	Information	
	2.4.1	**Hardware requirements:**	Information	
		i. The Policy Implementation System servers shall have 64 bit processor with at least 1 GHz clock speed and at least 2 GB of ECC RAM per CPU. The server and processor shall be supported for hardware, perating system and application for at least 7 years. The Hardware shall include the FC-AL or SCSI Ultra-3 internal hard disk of 72 GB or more in RAID-1 or RAID-5 configuration. The servers and shared Disk 28 TEC Standard No. 48040:2025 (if applicable) shall have dual power supplies in redundant configuration. The HDD capacity and RAM shall be sufficient to meet the requirements of Policy Implementation System as described in this document. The hardware requirements are indicative only and actual requirement shall be as per the network/ networks requirement and shall be given by tendering authority.	Functional Verification	
		ii. The Policy Implementation System Server shall be connected to the LAN on FE (100 base T), GE (1000 Base T) and to SAN storage on Fibre channel interfaces.	Functional Verification	

		iii. All interfaces shall be distributed on more than one card in different slots for all servers.	Functional Verification	
	2.4.2	**Reliability, Availability, Performance and Scalability** Policy Implementation System Servers shall provide the Reliability, Availability, Performance and Scalability requirements as per TEC standard on NMS: available on TEC website (https://tec.gov.in/standards-specifications), as applicable to servers, with over 99.9% availability:	Functional Verification	
	2.4.3	**Power Supply**: All the Policy Implementation System Servers shall have Load Sharing, Hot Swappable and Redundant Power Supply. The Policy Implementation System Server power supply requirements are as follows:	Functional Verification	
		i. The Policy Implementation System shall be able to operate from an Exchange battery at a nominal –48 V DC (Negative 48 V DC) over the range –40 V DC to –57 V DC or with AC power supply 170-250V, 50 ± 2 Hz.	Functional Verification	
		ii. The power feeding arrangements to the Power supply units shall also be provided in redundant configuration.	Functional Verification	
	2.4.4	**Software Requirement:** The solution architecture shall be flexible to meet design requirements and shall be delivered in several hardware arrangements, or be customised to fit specific requirements. It shall provide the software requirements as per TEC standard on NMS: available on TEC website (https://tec.gov.in/standards-specifications)as applicable to Policy Implementation System components.	Functional Verification	
	2.4.5	**Security Administration and Management:** The Policy Implementation System Servers shall have Security Administration and management function for administering security policy and managing security related information. It shall as per TEC standard on NMS:. Available on TEC website (https://tec.gov.in/standards-specifications).	Functional Verification	
	2.4.6	**Compatibility**	Functional Verification	

		The application described in the document shall be ported on the operating system supplied with the server. Certification regarding the same shall be provided by Original Equipment Manufacturer.		

	Chapter 3 Engineering, Operational, Qualitative and Other Requirements			
3.1		**Engineering Requirements:** The system shall meet the following engineering requirements:	Declaration	
	a)	The equipment shall be fully solid state and adopt state of the art technology.	Declaration	
	b)	The equipment shall be compact, composite construction and lightweight. The actual dimensions and weight of the equipment shall be furnished by the manufacturers.	Declaration	
	c)	All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.	Declaration	
	d)	All LAN cables shall be of Gigabit Ethernet ready standards.	Declaration	
	e)	The equipment shall have adequate cooling arrangements to meet environmental conditions as specified in BSNL QA Document QM 333.	Declaration	
	f)	Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.	Declaration	
	g)	Each terminal block and individual tags shall be numbered suitably with clear identification code and shall correspond to the associated wiring drawings.	Declaration	
	h)	All controls, switches, indicators etc. shall be clearly marked to show their circuit diagrams and functions.	Declaration	
3.2		**Operational Requirement (OR):** The system shall meet the following maintenance & operational requirements:	Declaration	
	a)	The equipment shall be designed for continuous operation.	Declaration	
	b)	The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sealevel.	Declaration	
	c)	Suitable visual indications shall be provided to indicate the healthy and unhealthy conditions.	Declaration	
	d)	The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.	Declaration	

	e)	The removal or addition of any cards shall not disrupt traffic on other cards.	Declaration	
	f)	All mission critical modules shall be identified and provided in full redundant configuration for high reliability	Declaration	
	g)	A single point failure on the equipment shall not result in failure of whole equipment or Network Failure or network management system.	Declaration	
	h)	Special tools required for wiring shall be provided along with the equipment.	Declaration	
	i)	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	
	j)	In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.	Declaration	
	k)	Necessary alarms (indicators) for indication of faults at various levels of hardware shall be provided on the individual modules.	Declaration	
	l)	A power down condition shall not cause loss of connection configuration data storage.	Declaration	
	m)	Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.	Declaration	
	n)	The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with service provider network for voice, data and transmission systems, as the case may be.	Declaration	
3.3		**QUALITATIVE REQUIREMENTS (QR):** The system shall meet the following qualitative requirements:	Information	
	3.3.1	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	Declaration	

		document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.		
	3.3.2	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	
	3.3.3	The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue-March, 2010} (TEC14016:2010) "Standard for Environmental testing of Telecommunication Equipment" 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	
3.4		**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 and1.4 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. i) 1 kV for AC/DC power lines;	Declaration	
		ii) 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 :	Declaration	
		a) 2 kV peak open circuit voltage for line to ground coupling.	Declaration	
		b) 1 kV peak open circuit voltage for line to line coupling.	Declaration	
		ii) For telecom ports :	Declaration	
		a) 2kV peak open circuit voltage for line to ground.	Declaration	

		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:-	Declaration	

		i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.		
		ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms.Applicable Performance Criteria shall be C.	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 (TEC 11016:2016). 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	
3.5		**Safety Requirements :**	Declaration	
		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	
3.6		**Other Requirements:**	Declaration	
	a)	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.	Functional Verification	
	b)	Wherever, the standardized documents like ITU-T, IETF, QA and TEC documents are referred, the latest issue and number with the amendments shall be applicable.	Functional Verification	
	c)	**Power Supply:** The equipment power supply requirements are given for each of the category. In addition, it shall meet the following requirements:	Declaration	
		i. The equipment shall be able to function over the range specified in the respective chapters, 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	
		CHAPTER 4 **DOCUMENTATION, INSTALLATION AND SOFTWARE MAINTENANCE**		
4.1		**DOCUMENTATION:**	Information	
		This chapter describes the general requirements for documentation to be provided. This shall be applicable to all categories and sub-categories of equipment. All technical documents shall be in English language both in CDROM and in hard copy. The documents shall comprise of:	Information	
		i. System description documents Installation,	Information	
		ii. Operation and Maintenance documents	Information	
		iii. Training documents Repair manual	Information	
	4.1.1	**System description documents:** The following system description documents shall be supplied along with the system.	Declaration	
	a)	Over-all system specification and description of hardware and software	Declaration	
	b)	Equipment layout drawings.	Declaration	
	c)	Cabling and wiring diagrams	Declaration	
	d)	Schematic drawings of all circuits in the system with timing diagrams wherever necessary.	Declaration	
	e)	Detailed specification and description of all Input / Output devices	Declaration	
	f)	Adjustment procedures, if there are any field adjustable units.	Declaration	
	g)	Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources.	Declaration	
	h)	Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.	Declaration	

	i)	Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.	Declaration	
	j)	Program and data listings.	Declaration	
	k)	Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.	Declaration	
	4.1.2	**System operation documents:** The following system operation documents shall be available.	Declaration	
	a)	Installation manuals and testing procedures	Declaration	
	b)	Precautions for installation, operations and maintenance	Declaration	
	c)	Operating and Maintenance manual of the system	Declaration	
	d)	Safety measures to be observed in handling the equipment	Declaration	
	e)	Man-machine language manual.	Declaration	
	f)	Fault location and trouble shooting instructions including fault dictionary.	Declaration	
	g)	Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.	Declaration	
	h)	Emergency action procedures and alarm dictionary	Declaration	
	4.1.3	**Training Documents :**	Information	
	a)	Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available	Information	
	b)	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.	Information	
	c)	The structure and scope of each document shall be clearly described.	Information	
	d)	The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.	Information	

	e)	All diagrams, illustrations and tables shall be consistent with the relevant text.	Information	
	4.14	**Repair Manual:**	Information	
	a)	List of replaceable parts used	Information	
	b)	Detailed ordering information for all the replaceable parts	Information	
	c)	Procedure for trouble shooting and sub-assembly replacement	Information	
	d)	Test fixtures and accessories for repair	Information	
	e)	Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions.	Information	
4.2		**INSTALLATION :**	Information	
	a)	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	
	b)	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	
	c)	All installation materials, consumables and spare parts to be supplied.	Declaration	
	d)	All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.	Declaration	
	e)	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	
	f)	The equipment shall have:	Declaration	
	f(i)	Proper earthing arrangement	Declaration	
	f(ii)	Protection against short circuit / open circuit	Declaration	

	f(iii)	Protection against accidental operations for all switches / controls provided in the front panel.	Declaration	
	f(iv)	Protection against entry of dust, insects and lizards	Declaration	
4.3		SOFTWARE MAINTENANCE:	Information	
	a)	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 service provider network. These updates shall include new features and services and other maintenance updates.	Declaration	
	b)	The software for the support of all protocols and interfaces mentioned in this GR shall be ensured in the devices.	Declaration	
ANNEXURE – I Guidelines for tendering authority:				
	1.3	Backplane, packet forwarding, session and L2TP requirement to be indicated based upon user and service requirement as described in the clause. L2TP sessions are required for dial VPN services; tunnels are for individual VPN and sessions are for users of that VPN.	Information	
	1.9 iv j	Number of Multicasting group and Multicasting streams other that specified may be indicated.	Information	
	1.15	The number of interface port and types shall be specified as per requirement.	Information	
	2.1	Current and future user base, concurrency figure, CDR generation per day per user and average session per user for the dimensioning of PIS shall have to be provided.	Information	
	2.2.28	Current and future user base, concurrency figure, CDR generation per day per user and average session per user for the dimensioning of PIS shall have to be provided.	Information	
	2.2.31	Format of CDR data transfer shall be provided.	Information	
	2.3.9	Concurrent operator for provisioning system shall be provided.	Information	
	2.4.1	Hardware requirement for PIS servers shall be specified.	Information	

ANNEXURE-II Items to be mentioned on Type Approval Certificate:				
	i)	Model Number with Hardware and Software version	Information	
	ii)	Category of BRAS	Information	
	iii)	Interfaces	Information	
	iv)	Availability of Virtual Router support	Information	
	v)	Multicasting Group and Group Members	Information	

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.

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 (Compiled /Not Compiled /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'.*