वर्गीय आवश्यकताएँ

सं:टीईसी/जीआर/आरएस/डब्लूएफएस-001/02/मार्च-17

(सं:जीआर/वाईफ़ाई-01/01.अप्रैल 2007 को अधिक्रमित करता है)

GENERIC REQUIREMENTS

No.: TEC/GR/RS/WFS-001/02/MAR-17

(Supersedes No. GR/WiFi-01/01.April.2007)

वाईफ़ाई हॉटस्पॉट

Wi-Fi Hotspot

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलालभवन, जनपथ, नई दिल्ली–110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release 2: March, 2017

Price: ₹ 800/-

FOREWORD

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India.

Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

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 GR pertains to the generic requirements of a Wi-Fi Hotspot. Wi-Fi Hotspot shall provide a high-speed wireless access at public places by creation of hotspots at various locations such as Airports, Hotels, Info-kiosks; multiple dwelling units etc. through installation of Wi-Fi Access Points based solution.

CONTENTS

HISTORY SHEET

Sl. No.	GR No.	Title	Remarks
1.	No. GR/WiFi-01/01.April 2007	Wi-Fi Hotspot	First Issue
2.	No.: TEC/GR/RS/WFS-001/02/MAR-17	Wi-Fi Hotspot	Second Issue

REFERENCES

a) TEC GRs/IRs	
TEC/SD/DD/EMC-221/05/OCT-16	Electromagnetic compatibility standard for Telecommunication Equipment Equipments
TEC/GR/R/WiFi-002/02.DEC-15	Wi-Fi Access Point (AP)
TEC/GR/IT/FWS-001/04/MAR-14	Firewall System
TEC/GR/IT/LSW-01/05/MAR 2014	LAN switch
TEC/GR/I/TCP-001/04 MAR-12	Routers
b) QA Documents	
QM-115	Reliability Methods and Predictions or any other International Standard Quality manual
QM-118	Quality and Reliability in Product Design
QM-205	Guidelines for standard of workmanship for printed boards
QM-206	Guidelines for standard of workmanship for printed board
QM-210	Acceptability of Printed Board Assemblies Containing Surface
QM-301	Transmission Equipment's General Documentation
QM-333	Specification for Environmental testing telecommunication equipment
c) ITU-T Recommendations	
ITU-T M 3010	Principles for a telecommunications management network
d) Other Standards	
IEEE802.1q	IEEE standards for local and metropolitan area networks–Virtual Bridge Local Area Networks
IEEE 802.1x	Standards for Local and metropolitan area networks—Port-Based Network Access Control

IEEE 802.11b	IEEE Standard for Information technology— Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer(PHY)specifications—Amendment
IEEE 802.11d	Information technology--Telecommunications and information Exchange between systems—Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications: Specification for Operation in Additional Regulatory Domains
IEEE 802.11g	IEEE standard for information technology– Telecommunications and information exchange between systems–Local and metropolitan area networks–specific requirements – Part 11: wireless LAN medium access control (MAC)and physical layer(PHY)specifications–Amendment 4: further higher – speed physical layer extension in the 2.4GHz band
IEEE 802.11i	IEEE Standard for Information technology-- Telecommunications and information exchange between system- -Local and metropolitan area networks: Specific requirements--Part11:WirelessLANMedium Access Control(MAC)and Physical Layer (PHY) specifications--Amendment6:Medium Access Control (MAC) Security Enhancements
IEEE 802.3	Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection(CSMA/CD) Access Method and Physical Layer Specifications.
IEEE 802.11a	Supplement to IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band

IEEE 802.11n	IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – Amendment 5: enhancements for higher throughput
IEEE 802.11ac	IEEE Standard for Information technology-- Telecommunications and information exchange between systems—Local and metropolitan area networks-- Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.
CISPR 22 (2008)	Limits and methods of measurement of radio disturbance characteristics of Information Technology equipment
IEC 61000-4-2 (2008)	Testing and measurement techniques of Electrostatic discharge immunity test
IEC 61000-4-3 (2010)	Radiated RF Electromagnetic Field Immunity test
IEC 61000-4-4 (2012)	Testing and measurement techniques of electrical fast transients/burst immunity test
IEC 61000-4-5(2014)	Test & Measurement techniques for Surge immunity tests
IEC 61000-4-6(2013)	Immunity to conducted disturbances, induced by radio frequency fields
IEC 61000-4-11(2004)	Voltage dips, shot interruptions and voltage variations immunity tests
RFC 2222	Simple Authentication and Security Layer (SASL)
RFC 2253	The LDAP Data Interchange Format(LDIF) - Technical Specification
RFC 2849	The LDAP Data Interchange Format(LDIF) - Technical Specification

CHAPTER-1

1.0 Introduction

1.1 This document contains the Generic Requirements for Wi-Fi Hotspot.

1.2 Wi-Fi equipment shall be complaint to IEEE 802.11a/b/g/n/ac.

2.0 Description

2.1 Typical architecture of a Wi-Fi Hotspot is as below:

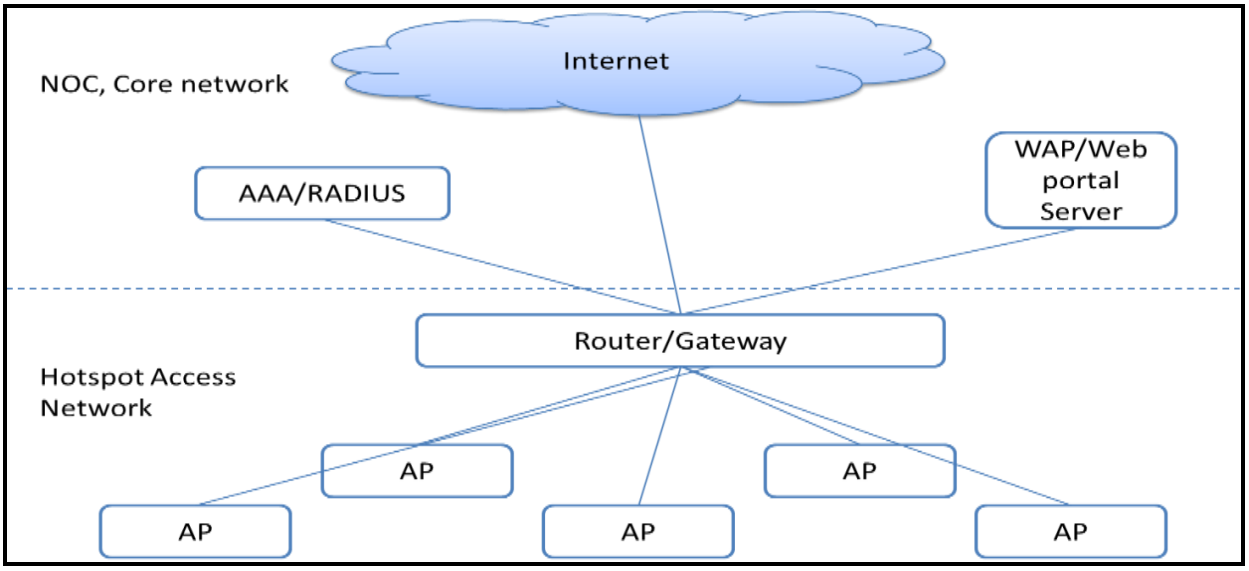

Figure 1 : Typical Architecture of Wi-Fi Hotspot

2.2 Wi-Fi Hotspot deployment shall provide

2.2.1 a high-speed wireless access at public places by creation of hotspots at various locations such as Airports, Hotels, Info-kiosks, multiple dwelling units etc. through installation of Wi-Fi Access Points based solution.

2.2.2 comprehensive and flexible billing capabilities and multiple authentication techniques for its customers through a Central Network Operations Centre (NOC) with back end systems for Authentication, Authorization, Accounting, Security Management, Network Management, Billing and Customer Provisioning & Management.

2.2.3 WLAN infrastructure that can scale transparently to support deployments of any size, from small cafes to large airports, convention centers, hotels, enterprise

offices, educational institution etc. The highlights of the solution shall be:

a) In addition to manual configuration, the Access Points should optionally support auto-configuration in the field via DHCP protocols.
b) Location specific branding and content at the individual Wi-Fi Hotspots.
c) Multiple Authentication methods for end users.
d) Multiple and Flexible Billing solutions.
e) Remote Monitoring of Wi-Fi Hotspots, Wi-Fi clients.
f) QoS based services to Wi-Fi end users which allows wireless bandwidth to be segmented and metered out on a per-user basis.

2.3 Wi-Fi equipment comprises mainly of

2.3.1 Access Points compliant to TEC/GR/R/WiFi-002/02.DEC-15

2.3.2 Client Adapters compliant to IEEE 802.11a/b/g/n/ac

2.3.3 Central Network Operations Centre (NOC) hardware and software for Wi-Fi. This shall comprise of the following functionality and components:

a. AAA, DHCP, DNS servers and software for secure authentication using IEEE802.1x/EAP & WPA and IEEE 802.I1i/WPA2 standards for Wi-Fi.
b. Billing software and hardware for billing Wi-Fi users.
c. Application servers and software for providing various applications such as SMS based authentication, location specific branding etc.

2.3.4 Enterprise Management, System management and monitoring of all components located at the NOC such as AAA, DHCP & DNS servers, Billing Application servers, LAN Switch, Firewall.

2.3.5 Router for connecting the NOC to the Internet as specified under Clause 3.5.10.

2.3.6 Central element Management System (eMS) having full FCAPS functionality for central management provisioning, accounting, monitoring of all Network elements in Wi-Fi network such as Access Points. This eMS shall be co-located at the Central NOC.

3.0 Functional/Operational Requirements

3.1 Network Architecture Requirement

3.1.1 Following equipment to be provided for each hotspot location:

a. Type A Access Point or Type B Access Point compliant to TEC/GR/R/WiFi-002/02.DEC-15 with built-in routing and bridging functionality with Ethernet LAN and WAN ports.

b. LAN Switch, as specified under Clause 3.5.9, for those hotspots having more than one Access Point. This functionality can be also integrated within Type-A or Type-B Access Point, in which case separate LAN switch is not required. LAN Switch used shall be sufficiently sized to address the maximum possible bandwidth possible on the hotspot network. The LAN ports shall be used for interconnecting the Access Points to increase the coverage area of the Wi-Fi Hotspot. The interconnection of Access Points shall be possible over the radio without the need of using the Ethernet LAN ports. Optionally, it shall be also possible to interconnect the Access Points in cascade using the Ethernet LAN on the Access Points.

c. Cabling materials such as CAT5/CAT5E/CAT-6 cable, antenna and associated accessories etc.

d. Power injector for Power over Ethernet at specified number of Access Points.

e. Appropriate Router as per clause 3.5.10 with Ethernet interfaces shall be used for connectivity

3.1.2 Central NOC:

a. A Central NOC for Management, Operation, Administration, Provisioning, Fault Management, Configuration, Authentication, Authorisation, Accounting & Billing of the complete Wi-Fi network including all Access Points, all network components and end users.

b. **Connectivity to the NOC:** The connectivity from all the Network elements (such as Access Points, Routers, LAN Switches etc.) to all the NOC components shall be through Internet/intranet. Appropriate Router, as

specified under Clause 3.5.10, shall be used for the purpose of NOC solutions.

3.2 Capacity Requirements

All the network components including the NOC (Billing, AAA, DNS,) database & eMS equipment shall be dimensioned & provided as per the following parameters:

3.2.1 Maximum number of Access Points per Hotspot.

3.2.2 Maximum number of concurrent user per Wi-Fi Access Point

3.2.3 Maximum number of CDRs per user per day

3.2.4 Total number of end customers

3.2.5 Average length of feeder CAT-5/CAT-5E/CAT-6 cable per Access Point

3.2.6 Minimum throughput per concurrent user

3.3 Services required to be provided

The Wi-Fi solution supplied shall allow end users after authentication to

3.3.1 Full access to the Internet for all public users including Web-based email, e-commerce sites & POP3 email services. Sharing of the Wi-Fi Access Point between public and private use with support for appropriate edge firewall capabilities where required.

3.3.2 Creation, Management and presentation of custom landing page based for each of Wi-Fi Hotspot with walled garden services being offered.

3.3.3 Authentication and allow service only to a definable set of Wi-Fi APs.

3.3.4 Roaming: The system must support in-roaming and out-roaming clients.

3.3.5 It is necessary that the payload from customers is delivered to the Internet as close to the user as possible. This could be at the Wi-Fi Hotspot depending on its capabilities and traffic requirements.

3.3.6 Different types of client devices shall be supported such as Laptops (with and without admin access), PDAs, WLAN phones etc. and client devices having different settings or zero client configurations.

3.4 The offered solution for Wi-Fi shall provide the following functionalities as given below.

3.4.1 **Remote monitoring -**All the network elements including the IEEE Access points and the CPEs shall be able to be monitored through the NOC for their healthy operation and other parameters such as currently authenticated users, network traffic parameters, and other configuration information.

3.4.2 **Allow secure and un-secure access to end-users -**Standards based security measures conforming to IEEE 802.1x/ EAP and IEEE 802.11i/WPA-2 shall be implemented in all the network components in the offered solution to offer secure connectivity to the end users, through the AAA solution at the Central NOC. It shall also be possible to simultaneously provide end-users not supporting any security mechanisms if so configured in NOC.

3.4.3 **QoS based services to end-users-**The System shall allow wireless bandwidth to be segmented and metered out on a per-user/per-location/per-SSID basis at each wireless location. The QoS levels can be mapped to specific service plans. For example, commercial users can be given a dedicated, high-priority portion of the total bandwidth while all public users share the remaining bandwidth at a lower priority. Connectivity for all users shall be able to be monitored from the NOC.

3.4.4 **Multiple Authentication Mechanisms -** The solution shall support multiple authentication mechanisms for end-customers in addition to RADIUS based authentication as configurable from the NOC. This shall include MAC, OTP/SMS, Username/Password via Portal and SIM based authentications. Prepaid voucher based authentication and access should also be possible. The system should support authentication of users from passwords on pre-printed vouchers, so users without means to pay online can use the pre-printed vouchers to gain access to the Wi-Fi network. The authentication of users for such purposes (buying vouchers) should be as per detailed in Clause 3.8.4.

3.4.5 **Branding, Content & Billing (Optional)-**Each Wireless access location shall be

able to present a uniquely branded user interface when the wireless client device connects to the wireless access location. The interface may also include a Web 'portal' through which users may access location-specific information and other services without requiring authentication to the Wireless LAN network. The custom interfaces are managed and updated centrally from the NOC and shall be able to billed at rates specifically defined for the location.

3.4.6 **Roaming-**The solution shall provide wireless access to roaming clients. Support for WISPr and UAM modes of authentication for in and out roaming clients.

3.4.7 **Support for data offload (optional)-** Provision in the network elements like Wi-Fi Access Point etc. to support data offloading from mobile networks should be present and should be compliant with the functionalities related to data offloading detailed in the respective network element specification (GR/IR). There should also be support to connect the mobile network HLR/HSS etc. servers to the Wi-Fi Hotspot network for authentication purposes in case of data offloading.

3.5 Requirements for NOC:

3.5.1 A Central Network Operations Centre shall be established for the complete operations, management, provisioning, authentication, billing and customer care.

3.5.2 The required NOC functionality includes the following:

a. AAA, DHCP & DNS for Authentication, Authorization & Accounting, client provisioning and DNS functions.
b. Web Portal & Web based customer Self-Management System.
c. Billing of end users.
d. Other Application Servers for SMS based authentication, Location based branding etc.
e. LAN Switch as specified under Clause 3.5.9.
f. Firewall System as specified under Clause 3.5.11.
g. Router as specified under Clause 3.5.10 for providing connectivity to the NOC components through the Internet.

3.5.3 An element Management System (eMS) shall be for operation, maintenance, configuration and firmware upgrades of respective network elements. This shall be collocated at the NOC.

3.5.4 The hardware and software of all NOC components and their databases including Billing, AAA, DHCP, DNS, Application Systems, eMS for respective packages, etc. shall be properly dimensioned for meeting requirements.

3.5.5 All systems shall be configured in the NOC so that there is no single point of failure in the network, leading to non-availability of services.

3.5.6 **Operator creation and access rights management:**

a. Network manager shall be able to create operators with user IDs and passwords for management of the NOC. He shall also be able to control and limit operators' authorization, rights and privileges. Network manager is an account with full control, rights and privileges.

b. Access control procedures shall allow classification of operators groups with common access rights characteristics with possibilities to restrict and extend the common access rights for single operators.

c. Restriction of access to network elements and/or to logs shall be possible.

d. All messages related to configurational changes in the network/network elements between NOC and the NEs shall be logged.

e. It shall be possible to identify the Operator, who initiated the message.

f. The system shall block the access from a local or remote terminal after receipt of consecutive failure attempts.

3.5.7 **Support to existing prepaid ISP customers:** Existing prepaid subscribers shall also be able to use the WLAN service. The NOC components (AAA etc) shall send authentication requests to existing AAA servers' infrastructure and generate customized CDRs for billing & authentication of such customers.

3.5.8 **Specifications for the Billing, AAA, DHCP and eMS servers:**

a. The Servers shall be Multi-server based with each server as multiprocessor The dimensioning of the servers shall be as per the deployment requirement and shall be specified by the procurer.

b. All servers shall be deployed in at least 1+1 redundant configuration. The server will operate in high availability cluster mode, on load sharing basis. The procurer may specify the requirement for N+1 redundant configuration requirement.

c. The system disk and storage size on the servers shall be dimensioned as per the deployment requirement and shall be specified by the procurer. Disk/Storage shall be RAID controlled with RAID 1 for servers that have mostly read operations (80% read, 20% write during peak load), RAID 1+0 or RAID 5 for servers that have mixed read/write load.

d. The system shall have provision for loading of software and configuration.

e. All common interfaces such as Ethernet interfaces etc shall operate in 1+1 redundancy.

f. At least 1+1 redundancy for Control module, Disk and Power supply and LAN interface in each of the servers. The power supply shall operate in load sharing and redundant mode. The procurer may specify the requirement for N+1 redundant configuration requirement.

3.5.9 **LAN Switch Specifications:** The LAN switch shall be used to inter-connect the various components such as Servers, Firewalls, Billing platform, and client terminals. Connectivity to servers shall be provided only through the Firewall. The minimum specifications for LAN Switch are as under:

a. For Hotspot location: Category IV LAN Switch and Interface Requirements as per clause no. 4.4 (i) and (iv) of TEC GR No. - TEC/GR/IT/LSW-01/05/MAR 2014. Outdoor switch shall be IP-65 Compliant.

b. For NOC location: Category III LAN Switch and Interface requirements for LAN switch shall be as per clause no. 4.3 (i), (ii), (iv) (TX/LX/SX option should be optional and specified by procurer) of TEC GR No. - TEC/GR/IT/LSW-01/05/MAR 2014.

Note: The capacity requirements and dimensioning of the LAN Switch used at Hotspot or NOC location shall be as per procurer's requirement and shall supersede the requirements of the referred GR.

3.5.10 Router Specifications:

a. Type I Router: The Type I Router shall be deployed at some of the Hotspot locations for providing backhaul connectivity of the Access Points to the Internet. The specifications shall be as per TEC GR Number TEC/GR/I/TCP-001/04 MAR-12 for Edge Routers as per Clause 1.4 of the TEC GR.

b. Type II Router: The Type II Router shall be used at the Central NOC for providing Internet connectivity to the NOC components through a Firewall. The specifications shall be as per TEC GR Number TEC/GR/I/TCP-001/04 MAR-12 for Intranet / Internet Access routers - Low range as per Clause 1.3e and related clauses of the TEC GR.

Note: The capacity requirements and dimensioning of the Router used at Hotspot or NOC location shall be as per procurer's requirement and shall supersede the requirements of the referred GR.

3.5.11 Firewall System:

a. The Firewall system shall be dual redundant hardware based.

b. The Firewall system could be deployed at:

   i. Hotspot location for the local break-out

   ii. NOC location for providing security to the various servers including eMS & Billing system at the NOC and also for breaking out the traffic towards Internet at centralized NOC location.

c. The Firewall System shall be as per TEC GR No. TEC/GR/IT/FWS-001/04/MAR-14.

d. The Firewall System(FWS) shall be dimensioned as per procurer's specified values of the following capability of handling a i) concurrent session ii) number of users.

e. The firewall shall be based on state-full connection-oriented fire walling and shall be appliance/hardware based.

Note: The capacity requirements and dimensioning of the Firewall used at Hotspot or NOC location shall be as per procurer's requirement and shall supersede the requirements of the referred GR.

3.6 Requirements from the AAA components

3.6.1 The AAA, in the NOC shall provide multiple authentication mechanisms for end-user and shall be able to record the end-user details as per, but not limited to, the attributes listed below for every user session, and the options shall be configurable from the NOC, on a per Access Point/ end user basis:

a) Unique user identifier
b) The calling IP address allotted by the RADIUS
c) Start time and date
d) End time and date
e) Volume of data transmitted and port type
f) MAC Address

Unique user identifier could be either of the following:

a) an alpha-numeric user-id associated with the user,
b) an MSISDN used for by a walk-in user for OTP based authentication,
c) any other identifier that could be used for unique identification of the user whilst Wi Fi access and even later for any Lawful Interception purposes.

3.6.2 RADIUS and database storage servers shall be dimensioned for customer base as per the procurer's requirement.

3.6.3 Irrespective of the mode of access, it shall centrally manage the authentication of all users / customers – both locally via proxy RADIUS – and deliver appropriate level of service to each customer.

3.6.4 It shall integrate with all aspects of NOC, from the database of customer information to back – office provisioning and billing systems. It shall be able to implement usage–based premium services (prepaid and Postpaid), and bill customers according to actual service usage.

3.6.5 The server shall implement IETF standard RADIUS (Remote Authentication Dial – In User Service) protocols, and shall be a full– function AAA, (Authentication, Authorization, and Accounting) server.

3.6.6 Roaming Capabilities:

a) Both authentication and accounting request messages from the gateway to the home AAA, system shall be supported.

b) It is required that the visited AAA, systems keep a copy of the accounting records that were forwarded to the home network for settlement purposes. The AAA, server shall use the domain portion of the User-Name attribute to determine proxy routing destinations.

c) The home network of a subscriber will be determined by the NAI of the subscriber as recorded in the User-Name RADIUS attribute.

3.6.7 It shall provide standards based security measures conforming to IEEE 802.1x/ EAP and IEEE 802.11i/ WPA2 so as to secure the Wireless link to offer secure connectivity to the end users. It shall also be possible to simultaneously provide end-users not supporting any security mechanisms if so configured in NOC. It shall have full support for Extensible Authentication Protocol (EAP) and atleast the EAP-PEAP, EAP-SIM types of EAP authentication 5 for compatibility with wireless LAN access Points and hot spots.

3.6.8 It shall simplify the process of managing service delivery to customers. It shall allow user defined profiles to easily assign a set of connection attributes to a user or group of users. It shall also make it easy to standardize profiles across different types of network access equipment so that it can deliver the appropriate level of service to all customers, regardless of which network access equipment they connect to.

3.6.9 It shall have the capability to integrate with a WAP gateway or other Internet server to provide subscriber connection details, including each user's credentials and currently assigned IP address. With this information, the Internet server is able to deliver the appropriate level of service to each subscriber.

3.6.10 Carrier-Grade Reliability: It shall allow stringent uptime requirements with state-of-the-art reliability features, including load balancing and redundancy across authentication and accounting systems. It shall also offer complete scalability.

3.6.11 Broad Multi-vendor Support and Integration:

a) It shall work in any network environment.
b) It shall be access agnostic.
c) It shall support the most commonly used back-end authentication databases, for instant compatibility with the authentication, provisioning, and billing schemes.
d) It shall provide flexibility in interoperating with other RADIUS servers, to easily communicate with other service providers and enterprise customers.
e) Flexible Authentication Methods: It shall be able to authenticate remote user names and passwords against a wide range of back-end authentication databases.

3.6.12 Support to LDAP Directories (Optional):

a) It shall support interfacing with LDAP-based authentication, billing, and provisioning systems.
b) It shall fully support authentication against credentials stored in LDAP directories and SQL databases and any ODBC-compliant database.
c) It shall work with any SQL table structure or LDAP schema; no database redesign shall be necessary.
d) It shall be able to authenticate against one or more SQL or LDAP databases, even if they're from different vendors.
e) It shall run any LDAP filter or SQL query specified, for flexibility in retrieving information.
f) It shall load balance authentication requests between several SQL or LDAP databases, to eliminate the risk of a single point of failure, and increase performance on busy networks.
g) It shall support concurrent access limits for users set up in SQL or LDAP.
h) It shall be able to retrieve stored RADIUS attributes and Profiles from the SQL database or LDAP directory to return to the network access equipment.

3.6.13 Advanced Proxy RADIUS Capabilities:

a) It shall include advanced proxy RADIUS support. It shall be able to act as a proxy target server, and can forward proxy requests to other RADIUS servers. It shall be able to set up Proxy Radius user by:
    - Specifying a user-name decorator to indicate a proxy target
    - Configuring proxy by Called-Station-Id RADIUS Attribute in the Authentication or Accounting request
    - Directing incoming proxy requests to a specific authentication or accounting method based on user name decoration or Called-Station-Id RADIUS Attribute.
b) It shall also be able to forward proxy RADIUS requests to multiple target servers. This capability would let back-up target servers within a site, introduce redundancy into the network, and eliminate the risk of service interruption.
c) It shall also provide proxy packet filtering. With filtering, it shall setup rules that govern how to handle packets that are forwarded to or received from target servers.
d) In a roaming context, the RADIUS client shall request authentication from the visited AAA, server for the opaque credentials that were returned to the visited network. The RADIUS client shall communicate the authentication response messages received from the home network operator AAA, system to the appropriate network elements in the visited network operator network for implementation. If the opaque credentials fail RADIUS authentication of the visited network shall deny the subscriber access to service.

3.6.14 Easy Tunnel Management: It shall be able to centralize the management and administration associated with VPN/tunnel access. It shall support:

a) All standard RADIUS tunneling attributes, as well as the vendor-specific attributes.
b) Tunnel authorization based on username format (user@tunnel,

tunnel#user), or the dialed number ((Called-Station-Id RADIUS Attribute)

3.6.15 **Reliable, Real-Time Accounting**: RADIUS accounting log files shall easily be exported to spreadsheets, databases, and specialized billing software. It shall also be possible to log accounting data directly to a single SQL database, or specify multiple SQL target servers. In addition, it shall have the capability to be configured to spool accounting data from distributed RADIUS servers to a central billing system, thereby guaranteeing delivery in the event of a system failure.

3.6.16 **Centralized Administration**: It shall streamline administration by:

a) Reporting activity and system problems via SNMPv2 or higher, and support RADIUS client authentication and accounting MIBS, enabling proxy RADIUS activity to be reported to standard SNMP management consoles.
b) Being configurable from the GUI or the command line.

3.6.17 **LDAP (Directory Server) Specifications, if used:**

a) Shall be LDAP v3 Compliant
b) Shall support procurer specified number of read-only consumers for authentication queries.
c) Shall support XML for integration with external applications.
d) Shall support the e-mail servers in default mode.
e) Shall support servers in Master - Slave configuration.
f) Shall be able to replicate data between servers and support cascading replication using replication hubs if required, to optimize performance.
g) Shall support multiple modes of deployments (eg. write or read-only).
h) Shall support the SNMP v2 protocol to enable management centrally.
i) Shall support Class-of-service and Role based mechanism.
j) Shall support Access Control Lists (ACLs).
k) Shall support Chaining and Referrals to aid the client query process.
l) Shall support controlling access to the directory, a subtree, entries, attributes by setting permissions for users, groups, roles and location information like IP addresses.

m) Shall support Authenticated and encrypted LDAP operations using SSL encryption.

n) Shall support User authentication through userID/password, X.509v3public-key certificates, or Anonymous authentication

o) Shall support Password Hashing.

p) Development tools using Java and C/C++ must be available to enable customizing and extending Directory functionality.

q) Shall support LDAP search filters, including presence, equality, inequality, sub string, approximate("soundslike"), and the Boolean operators and(&), or(|), and not (!)

r) Shall provide Transaction Logging on the file system.

s) Shall support Account inactivation to provide flexibility to temporarily disable user access.

t) Shall support storage of Digital Certificates.

u) Shall support PKCS#11 hardware acceleration to aid system performance.

v) Shall Support for online backups, configuration changes, schema updates, and indexing.

w) Shall Support for Industry standards: LDAP version 3, XML, Simple Authentication and Security Layer SASL RFC 2222, UTF-8 String Representation of Distinguished Names RFC 2253, The LDAP Data Interchange Format RFC 2849.

3.7 DHCP Requirements

3.7.1 DHCP will be used to automatically configure network parameters on client computer systems. This will allow a client computer to connect to a WLAN without requiring the computer to be preconfigured for that particular network and without requiring user interaction. The use of DHCP in a WLAN also allows for more efficient use of IP address space on the network as IP addresses are only allocated to active subscribers.

3.7.2 The following parameters must be returned to the client via DHCP in order to allow them access to the wireless access network:

a) IP address
b) Subnet Mask
c) Default Gateway
d) DNS server IP address(es)

3.7.3 The DHCP lease time must be set longer than twice the idle-timer value in order to prevent fraud. If the DHCP lease timer is less than twice the idle-timer value, there is the potential that an IP address could be reassigned to a new subscriber before the previous session associated with that IP address is released.

3.8 Billing software functionality

3.8.1 The Wi-Fi hotspot solutions is required to provide a comprehensive Billing solution for Billing users on Prepaid & postpaid basis for both network users.

3.8.2 Billing solution for the standalone Wi-Fi Network shall be provided and customer database using pre-paid cards. The solution shall serve all Wireless access locations from a single server with centralized user management and centralized pre-paid card management.

3.8.3 The Billing solution shall have/ provide the following functionalities.

a) Product Pricing: Product usage can be charged according to a variety of units, schemes and rates. Pricing can be defined as transaction rates, period rates and 'annual' rates. The solution shall be able to have configurable packages and plans for accessing the system. Subscription based services including setup fees, recurring fees, usage fees and bonuses.
b) Flat & usage based billing: Duration & volume based.
c) Time based billing: Charge based on time of day /day of week.
d) Hotspot billing shall allow signing up subscribers instantly to Public

Wireless Access Network services through an on-line registration process.

e) Dealer Management- The Software supports creation of dealers through whom a service provider may offer services. It is possible to define commission/ incentive schemes for dealers against achievement of set targets such as the number of subscriptions sold, total spending of the subscribers belonging to the dealer etc.

f) Hotspot portal with web registration, web self-care and instant connection purchase. Bill view enquiry of charge details. Account shall be made invalid once it is exhausted.

g) Location based service offerings: It shall be possible to offer besides a common network wide offering of service plans, also location specific packages (branding + price plans + time of day).

h) Credit card clearing

i) Bill payment and Presentation to customers through a web based interface

j) Optionally, the pages that are served by the portal shall be multi-lingual and should support English and Hindi content based on user selection. The requirement for this shall be specified by the procurer.

3.8.4 **Prepaid Voucher Key Management (Vouchers):** The system shall be able to generate and manage prepaid vouchers allowing services to customers using pre-paid accounts and credit card payments. Prepaid cards shall either be able to be printed physically at the NOC or at any Hotspot location or transmitted electronically in case the customer makes payment through the credit card either through a portal or through SMS. The software shall provide and control all the prepaid voucher number related activities given below:

a) Generation & Administration.

b) Allocation.

c) Recharging the account.

d) The system shall also support cards of multiple denominations.

e) There shall be option to generate pre-paid card activation / deactivation,

expiry of cards, deletion of cards.

f) Pre-paid account balance management: Once a transaction is complete, the balance usage level in user account will be calculated based on business rules and the balance limit will be updated. The system helps the user to view the balance usage level for each subscriber. A follow-up scheme helps to define the course of actions to be taken whenever the usage level of a subscriber crosses user defined thresholds.

g) Generate and enable use of various types of pre-paid vouchers such as one-time password access, flexible validity periods of 1 hour, 24 hours, 1 week 1 month, 6 months etc. (from date or time of use).

h) The Billing shall be able to interface with other billing applications through APIs which shall be provided.

i) Reports- The comprehensive range of reports gives details of sale, usage, payment and accounting, dispute handling, statistics and allows different types of searches to retrieve information from the system. The software supports preview of reports, before printing.

j) Support for thermal hand-held printers to be able to print vouchers at the point of sale.

3.9 Web portal requirements

3.9.1 The Web portal is responsible for responding to client requests for the visited network login page. This initial login page or welcome page will present the user with login options and links to the roaming login pages of each partner network.

3.9.2 The Web Portal shall provide the following functionalities:

a) Automatic re-direct to a different Login & Payment page for end-users depending on subnet

b) Optional re-direct to external portal after authentication and/or payment

c) Centrally stored and managed Login & Payment pages

d) Provision for design of individual and unique Login & Payment pages and Pop-up windows for the service provider or local public hotspots

e) Unique set of Login & Payment pages and payment/pricing configuration per subnet

f) Multi-client browser support for different sets of Login & Payment pages based on `device type: laptop, smart phone, tablet, etc.

g) Pass-through (free sites and services) IP address possibility (“White list”)

h) Block-out (banned sites and services) IP address possibility (“Black list”)

i) Generate appropriate error pages to a subscriber and web based logout functions

j) Re-direct to customer configurable URL after successful login

k) Possibility to re-direct to URL after automatic login

3.9.3 This web portal server shall have the ability to retrieve opaque client credentials that are returned via an HTTP redirect URL. These opaque credentials will eventually be passed on to the RADIUS client functional unit of the gateway for authentication. Upon authenticating the opaque credentials, via RADIUS, from the home network, the visited network web server shall create a logout pop-up window. This pop-up window shall contain a logout button and a counter. The logout button allows a subscriber to signal an explicit logout request to the visited network. Upon receipt of this logout signal the visited network shall terminate the subscriber’s active session, return a RADIUS accounting STOP message to the home network operator with session usage information included and shall return the subscriber to the visited network welcome page.

3.9.4 All communications between the visited network web server and the client web browser shall be secured using HTTPS.

3.9.5 It shall be possible to provide to provide landing page unique to a particular location or chain of locations and to set up and manage a walled garden for own products.

3.9.6 Self-Provisioning

a) Self provisioning is a method by which the subscriber can directly, with ease of use, and clear instructions obtain a password without talking to a call center representative. The following are the key self provisioning

methods to be supported.

- Web - customer must be able to request and receive a password - after sufficient validation of identity.
- SMS - customer must be able to request and receive a response via SMS with password for the service.

b) The system shall provide the following:

- Allow password change
- Bill payment and presentation through the Billing Platform
- Login history and session report
- Refill prepaid account.
- Trouble ticketing
- Email invoices and session reports through the Billing Platform
- User import utilities and batch CRM.
- CSR can post payments, credits and adjustments.
- Web based account activation and account refill using vouchers.
- Issue pre-paid vouchers that can be purchased online through a secure portal, with flexible validity periods of time.

3.10 Access Points- It shall be as per TEC GR no. TEC/GR/R/WiFi-002/02.DEC-15

3.11 Requirements in Managed Hotspot Services:

3.11.1 The Managed Hotspot Service shall provide all the functionalities specified in this document for the Network Operations Centre for managing Wi-Fi network including providing SMS based authentication for mobile customer and providing support for prepaid ISP customers.

3.11.2 The Managed Hotspot service shall include full operation and support of the Hotspot Management System including:

a) All software nodes (system) needed

b) System configuration and Service set-up, including all required start-up activities to put the service in operation

c) Operation of centralized servers for AAA, billing and service

management.

d) Support of service 24x7 including Service monitoring, alarm handling, statistic reporting, application maintenance and 2nd line support.

e) Pre-enabled payment methods such as Credit Card payments, User-ID & Password, Credit Card self-service portal, pre-paid Vouchers and Scratch Cards, Cash Cards, Global Roaming support etc.

3.11.3 It shall be possible to host all the servers required and as specified for the NOC in this document and include all the functionality needed for control, management and monitoring of the public WLAN as well as management and positioning of mobile end-users. The solution provides the day-to-day system management web- interface for the network administrator, in addition to several machine-to-machine interfaces for customer care systems, billing systems, mediation gateways and network management.

3.11.4 It shall be possible to provide overall solution architecture and network design connectivity for the Managed Service Package.

3.11.5 Managed Hotspot Service shall offer a wide range of end-user authentication and payments options to address both domestic and international customers. User-ID & Password, Credit Card payments, Global Roaming Provider support, pre-paid Vouchers and Scratch Cards and payments through Mobile Phone accounts.

3.11.6 Hotspot management solution shall provide a web based self-care interface that can be utilized for both individual end-users and corporate accounts

3.11.7 It shall be possible to provide Portal Management and Login Pages Roaming services as part of the Managed Service offering.

3.11.8 The Managed Hotspot Services must provide Wi-Fi Service Management administrator tools for day-to-day system management web-interface for the administrator to monitor and manage the hotspot and easily and instantaneously create or change service offerings for new and existing service bundles based on customer demands. Daily and weekly reports shall be made available on the Wi-Fi Service usages.

3.11.9 It shall provide a login right to the Managed services infrastructure so that it is possible to view and manage on its own also.

3.11.10 The Hotspot system having RADIUS, AAA, and DNS servers shall be able to interface through the CNS (Core Network Service) with the standard LIS / LIM equipment deployed in the operator's network and provide all functions and interfaces as required by the TEC GR for LIM / LIS.

3.12 eMS Specifications and functional requirements

3.12.1 An Element Management System (eMS) shall be provided.

a) The eMS shall follow the TMN architecture as per ITU M.3010 standard. The eMS shall provide all FCAPS functionality and web based management capabilities for the supplied solution as per the latest TEC GR for eMS- TEC/SD/IT/EMT-001/01/MAR2016.

3.12.2 The eMS shall have standard North bound interfaces such as ITU Q3/TMF-CORBA/ TCP / IP / CMIP / SNMP/XML etc and shall be capable of integrated with other standards based NMS systems. The interfaces towards/ from Network elements shall be SNMP ver2 or better.

3.12.3 The eMS system shall use Open APIs and standard interfaces. Details of interfaces and APIs will be furnished for enabling integration of the NMS/ Billing/ Accounting System.

3.12.4 Device management: The offered solution shall provide the following functionalities:

a) Automatic or manual device discovery of all Network Elements (NEs) such as Wi-Fi Access Points etc.

b) Web-based or GUI based graphical view with context sensitive on-line help and information about distributed Network Elements.

c) Topology generation of Layer 2 &layer 3 network elements with graphical displays of connected network devices giving a complete view of the network without physically checking each device at remote sites. A real-time Physical Network Map containing all the different network elements with drill-down to individual card-level view which are being managed shall

be provided. Coloured icons shall be used for network elements showing their alarm state. e.g. the red icon displays an alarm of the network element. Graphical maps shall represent the topology of the managed network, organised in a hierarchical manner. The map symbols shall be dynamic i.e. their appearance on the screen shall change according to the status change of the network elements.

d) Device status polling feature.
e) Ability to set a device to be managed and unmanaged.
f) Dynamic status, statistics and comprehensive configuration information for managed devices.

3.12.5 Configuration management: Menu driven hierarchy based operations on the Network elements through all necessary commands or operations to configure network components shall be provided. Tasks shall be able to be characterized by either single command or scripts that combine a sequence of commands to one compound task.

3.12.6 Software Management: For remote Installation, Upgrade & Correction of the NEs, including downloading of Patch application for software corrections in the network and backup on a monthly basis.

3.12.7 Alarm and Event Handling: All alarms from all network elements being managed shall be received and logged. The alarms shall be visible in various ways e.g. displayed in alarm lists on the screens of defined operators; alarm list can be exported for further treatment.

3.12.8 Performance Management: Performance management of NEs Wi-Fi Hotspots sites: Load over NEs/ sites/ zones, number of active user connections, sessions, session terminations, Access Point restarts, positioning events, access denied, Online site usage monitoring etc.

3.12.9 Report Generation: The eMS shall be capable of providing the following reports:

a) Inventory reports, including current version and status
b) Performance reports, by different time cuts (hour, day, week, month, etc.)

3.12.10 System administration: Includes all eMS operator related system and account management tasks such as:

a) Addition/change/configuration/removal of accounts (username/password, etc.) into the database
b) Addition/change/configuration/removal of NEs
c) Addition/change/configuration/verification/removal of “Sites”/ “Hotspots”

3.12.11 Operator creation and access rights management:

a) Network manager shall be able to create operators with user’s ID and passwords. He shall also be able to control and limit operators’ authorization, rights and privileges. Network manager is an account with full control, rights and privileges.
b) Access control procedures shall allow classification of operators groups with common access rights characteristics with possibilities to restrict and extend the common access rights for single operators.
c) Restriction of access to network elements and/or to logs shall be possible.
d) All management messages between eMS and the NEs shall be logged.
e) It shall be possible to view the changes done by the Operator, who initiated the message.
f) The system shall block the access from a local or remote terminal after receipt of consecutive 5 wrong logins/ passwords and unauthorized commands.

4.0 EMI/EMC Requirements

The equipment’s in the Wi-Fi Hotspot system shall conform to the EMC requirements laid down in the respective equipment specification (IR/GR). If no TEC specification for a particular network element used in the Wi-Fi Hotspot system exists, then that particular network element must conform to TEC SD No. TEC/SD/DD/EMC-221/05/OCT-16

5.0 Safety Requirements

5.1 The equipments in the Wi-Fi Hotspot system shall conform to IS 13252 part 1: 2010 “Information Technology Equipment –Safety- Part 1: General Requirements” [equivalent to IEC 60950-1 {2005} “Information Technology Equipment –Safety- Part 1: General Requirements”] and IS 10437{1986} “Safety requirements for radio transmitting equipments” [equivalent to IEC 60215].

6.0 Other Requirements:

6.1 The system hardware and 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.

6.2 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.

6.3 Power Supply: The equipment power supply requirements are given for each of the category. In addition, it shall meet the following requirements:

a) The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance.

b) The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.

c) The power supply for the equipment is as per the requirement specified in the specification referred to. For the remaining equipment, it shall be powered from a voltage source having nominal voltage of –48 volt. D.C. with a voltage variation of –40 to –60 volt.

d) For equipment requiring AC mains, nominal AC voltage for Single Phase shall be 230V with variation of -15% to +10%, at 50 ± 2Hz without any degradation in the performance.

e) The derived DC voltages shall have protection against short circuit and overload.

f) Support for Solar power option shall also be available for outdoor sites. The procurer shall specify the requirement for the same.

7.0 Documentation

7.1 Complete documentation including technical literature in English with detailed block schematic diagram of various sub-assemblies shall be provided. All aspects of installation, operation, testing, maintenance and repair shall also be covered in the handbook.

7.2 Procedure for repair giving full details of test setup shall be indicated. Test jigs and fixtures if any, required for maintenance and repair shall also be indicated. The manufacturer shall indicate the repair philosophy.

7.3 The necessary flow charts for probable faults and the remedial actions shall be provided in the repair manuals.

7.4 Each sub-assembly and component shall be clearly marked with schematic reference to show its function so that they are identifiable from the component layout diagram in the handbook.

7.5 All documentation and training manuals provided shall be of the latest version.

CHAPTER-2

8.0 Information for the procurer of product

8.1 The procurer shall specify the requirements for clauses

i. 3.1.1(b) for interconnection of Access Points.
ii. 3.2– Parameters for dimensioning the Hotspot network.
iii. 3.4.5 for Branding and content for user interface or web portal.
iv. 3.4.7 for support of data offload.
v. 3.5.8 for Dimensioning, redundancy etc. requirements for servers.
vi. 3.5.9- Capacity requirements for LAN Switch
vii. 3.5.10- Capacity requirements for Router
viii. 3.5.11- Capacity requirements for Firewall system.
ix. 3.6.12- Support for LDAP directories.
x. 3.6.17- Requirement of LDAP directory server (to be used or not)
xi. 3.8.3(j)- Requirement as per this clause.
xii. 6.3(f)- Requirement for solar power option for power supply.

8.2 The procurer shall specify the requirements for more advanced protocols that RADIUS like DIAMETER for AAA functionalities.

9.0 Information to be mentioned on the TEC Type Approval Certificate

Following items shall be mentioned in the TEC Type Approval certificate:

9.1 Access Point – Type A or Type B

9.2 LAN Switch – For Hotspot, NOC Location

9.3 Router - For Hotspot, NOC Location

9.4 Firewall System- For Hotspot, NOC Location

9.5 Hardware and Software used in NOC

ABBREVIATIONS

AAA	Auhenticaion, Authorisation and Accounting
ACL	Access Control List
AP	Access Point
API	Application Program Interface
CAT	Category
CD	Compact Disc
CDR	Call Details Records
CISC	Complex Instruction Set Computer
CISPR	Committee International Special des Perturbations Radioelectriques
CPE	Customer Premises Equipment
CRM	Customer Relations Management
CSR	Customer Service Representative
DAT	Digital Audio Tape
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DNIS	Dialled Number Identification Service
DNS	Domain Name Service
DVD	Digital Video Disc
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol - Authentication and Key Agreement
EAP-SIM	Extensible Authentication Protocol -Subscriber Identity Module
EAP-TLS	Extensible Authentication Protocol -Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
eMS	element Management System
EPC	Electronic Product Code

FCAPS	Fault Configuration Accounting Performance Security
FWS	Firewall System
FTP	File Transfer Protocol
GB	Giga Byte
GHz	Giga Hertz
GR	Generic Requirement
GRIC	Global Reach Internet Connection
GUI	Graphic User Interface
HDD	Hard Disk Drive
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification Data
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standards Organisation
ITU	International Telecommunication Union
IVR	Interactive Voice Response
LAN	Local Area Network
LCI	LDAP Configuration Interface
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LIM	Lawful Interception Monitoring
LIS	Lawful Interception System
MAC	Media Access Control
MIB	Management Information Base
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MTBF	Mean Time Between Faults

MTTR	Mean Time To Restore
mW	Milli watts
NAI	Network Access Identifier
NAS	Network Access Server
NAT	Network Address Translator
NE	Network Element
NMS	Network Management System
NOC	Network Operation Centre
OS	Operating System
OTP	One Time Password
PAP	Packet Authentication Protocol
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PKCS	Public-key cryptographic standard
POP	Post Office Protocol version
PPP	Point-to-Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
QA	Quality Assurance
QM	Quality Manual
QoS	Quality of Service
QR	Quality Requirements
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Desks
RAM	Random Access memory
RDBMS	Relational Database Management System
RFC	Request For Comment
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RP	Radio Paging

SASL	Simple Authentication Security Layer
SDK	Software Development Kit
SIM	Subscriber Identity Module
SMPP	Short Message Peer to Peer Protocol
SMS	Short Message Service
SMSC	Short Message Service Centre
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set identifier
SSL	Secured Socket Layer
TCP	Transmission Control Protocol
TEC	Telecom Engineering Centre
TMN	Telecommunication Management Network
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

======== End of the document ========