MOBILE
ISSUE: FEB. 2004

PACKET CORE NETWORK FOR CDMA 2000 1X SYSTEM

GENERIC REQUIREMENTS
NO. GR/PCN.01/01 FEB 2004

TELECOMMUNICATION ENGINEERING CENTER
KHURSHID LAL BHAWAN, JANPATH
NEW DELHI – 110 001
INDIA

Generic Requirements
for
Packet Core Network for CDMA 2000 1x System

GENERIC REQUIREMENTS
GR No. GR/PCN.01/01 FEB.2004

History Sheet

SI. No.	Title	GR No.	Remarks
1	**Packet Core Network for CDMA 2000 1x System**	GR/PCN-01/01 FEB.2004	Issue 01

Table of Contents

CHAPTER-1

1. INTRODUCTION

1.1 This document contains the Generic Requirements (GR) of Packet Core Network (PCN) for cellular/WLL system based on the CDMA 2000 1x standards (TIA/EIA/ IS-2000) to provide packet data services to the customers of Bharat Sanchar Nigam Limited (BSNL)/ Mahanagar Telephone Nigam Limited(MTNL). The CDMA 2000 1x standards are based on TIA/EIA (Telecom Industry Association/Electronic Industry Association, USA) standards, 3GPP2 (Third Generation Partnership Project 2) standards and ITU-R Recommendation M-1457.

The tendering authority, at the time of tendering should review the versions of all the documents mentioned in this GR and update them if necessary.

1.2 Applications of such a system could be in urban and rural area with fixed and mobile wireless terminals in zero mobility, limited mobility or full mobility environment. It shall be possible to limit mobility in the system in a limited mobility scenario as per the definition of limited mobility as specified by the DOT.

1.3 This Packet Core Network shall be required to work with the Radio Network (RN) as specified in TEC GR No. GR/WLL-04 and MSC based core Network as specified in TEC GR No. GR/MSC-01.

1.4 Network architecture

The following paras describe the various components of the Packet Core Network under the purview of this GR. The various subsystems of the Packet Core Network are given in block schematic in figure 1.

(i) **Packet Data Serving Node (PDSN)-** PDSN provides the gateway between the cellular systems and the wire-line Internet Protocol(IP) Packet Data network. It interfaces between transmission of the packet data in the fixed network and its transmission over the air interface. One PDSN can be connected to multiple BSCs (PCF)and one BSC (PCF) can connect to multiple PDSNs. It also acts as a client for AAA servers. The Core PDSN functions along with Incremental PDSN functions to support Simple IP and Mobile IP Service shall be as per 3G PP2 standard P. S 0001 (latest version)

(ii) **Authentication, Authorization and Accounting (AAA) Server** –The AAA server provides the functions of Authentication, Authorization and Accounting. It interacts with the PDSN to perform AAA functions in support of the PDSN for requesting Remote Stations. It also generates the Usage Data Records (UDRs) for IP services. The AAA Server functions to support Simple IP and Mobile IP Service, shall be as per 3G PP2 standard P. S 0001 (latest version)

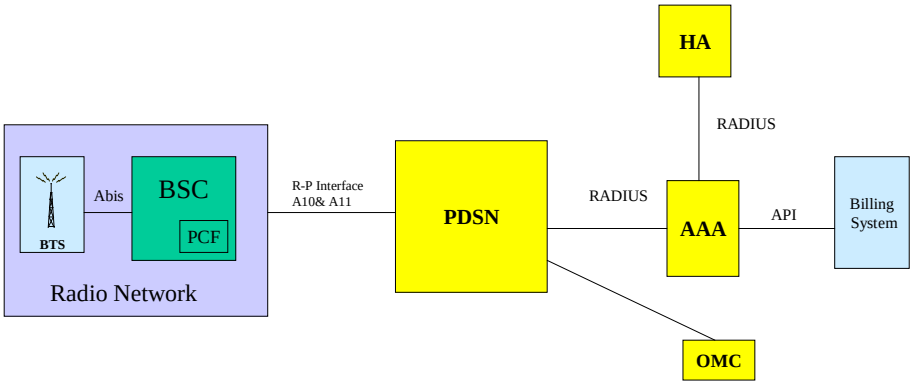


Figure 1. Block schematic figure of PCN

(iii) **Home Agent (HA)** - This network element enables mobility management for Mobile IP subscribers. HA is required for authenticating Mobile IP registrations from the RS and maintaining the current location information. It maintains the location of the mobile through mobile registrations and forwards datagram to the Foreign Agent where the mobile is currently registered. The HA functions to support Mobility IP Service shall be as per 3G PP2 standard P. S 0001 (latest version)

(iv) **Operations and Maintenance Centre (OMC)**
The Operations and Maintenance Centre (OMC) allows the centralized operation of the various units in the system and the functions needed to maintain the sub systems. The OMC provides the dynamic monitoring and controlling of the network management functions for operation and maintenance.

CHAPTER-2

2. GENERAL REQUIREMENTS

2.1 **Standards Compliant & Multi-Vendor Support** –Packet Core Network (PCN) shall conform to the Wireless IP Network Standard – 3GPP2 P.S0001 (latest version) and the PCN architecture shall be as per 3G PP2 standard P.R 0001 (latest version). The roadmap for implementation of TSG-X specifications of 3GPP2 in future may be provided. The equipment shall be supported by multiple vendors.

2.2 **Field Proveness and interoperability** - The equipment shall be fully solid state, field proven and shall adopt latest state-of-art technology. The equipment should have been field deployed commercially across multiple countries and networks and for a reasonable period of time. Tendering authority may indicate the extent of deployment and its duration as a criteria for ensuring field proveness. Tendering authority may also specify the various technologies / vendors of Radio Networks (RN), MSC based Core Network, Packet Core Network (PCN) and associated sub systems with which this system has to interoperate

2.3 **Types of Remote Stations:** The Packet Core Network shall support Remote Stations (RS) as specified in the TEC GR No. GR/WLL-04 "Radio Network (Base Station Controller & Base Transceiver Station) of WLL systems based on CDMA 2000 1x standards".

2.4 **Dimensioning** – The equipment supplier shall provide engineering rules/guidelines for dimensioning the capacity of the network components.

2.5 It shall be possible to upgrade the system (through software upgrades) to support CDMA 2000 1x Ev DO. Capability to support CDMA 2000 1x Ev DV in future may be indicated.

2.6 The system shall optionally allow voice (or circuit data service) and packet data service to operate concurrently (within the limits of the air interface system capacity) and support a Quality of Service (Q.O.S) control mechanism to balance the varying Q.O.S. requirements of multiple concurrent services.

2.7 **Quality of Service** : The IP entities shall be able to provide Quality of Service based on Differentiated Services (Diff Serv) as per standard 3G PP2 P. S 0001 (latest version).

2.8 The system shall have the capability to support all the registration methods specified in the IS 2000 standard. The tendering authority, at the time of tendering, should specify the registration methods required to be supported in the equipment.

2.9 The system shall support the architecture of the CDMA 2000 1x system in terms of different layers for specific functions conforming to the following 3GPP2 standards: -

-	Physical layer	-	C.S0002
-	Link layer-MAC sub-layer	-	C.S0003
-	LAC sub-layer	-	C.S0004
-	Upper layers	-	C.S0005

2.10 It shall be possible to integrate the system with the National Internet Backbone (NIB) Phase I (as defined in TEC GR No. G/NIB.01) and NIB Phase II (as defined in TEC GR No. GR/VPN-01 and other related GRs/IRs of narrowband and broadband access). The tendering authority may indicate the type of interfaces required to be supported and associated hardware/ software required for integration may be specified by the supplier.

2.11 Possibility to upgrade the system to support IPv6 protocol in future shall be indicated.

2.12 Dimensions/Weight - Dimension and weight of each of the equipment shall be indicated by the equipment supplier. The equipment shall be of self-supported cabinet or rack type. Maximum height of rack shall be restricted to 2100mm. To have greater flexibility for operations, front-only serviceable racks are preferred.

2.13 Cooling Arrangement - The equipment shall have necessary self cooling arrangement with or without in-built fan. The fan, if used, shall be a D.C. fan and shall be used in redundant configuration. The MTBF of the fan shall be at least 80,000 hours. It shall have a provision to report the fan failure event to the OMC.

2.14 Ease of Expansion - Expansion techniques of the system shall be easy, economical and shall not interrupt a working system. Expansion shall be required when the number of subscribers (capacity) in the area is increased or when the geographical coverage is increased. The equipment shall be modular in construction permitting expansion, without any major hardware changes by simply adding shelves and modules.

2.15 Power Consumption - The equipment shall have low power consumption.

2.16 Power Supply - The power supply unit shall form an integral part of the equipment and shall have protection against output over voltage, short circuit, input reverse polarity protection & shall have visual indication for output under voltage. The power supply shall be fully redundant and load sharing in order to avoid single point of failure. The power supplies shall also be hot swappable and should allow insertion and removal of power supply units without having to shut down the PDSN, HA and associated elements.

2.17 Hardware

2.17.1 General

(i) Compact and high-performance state-of-the-art hardware shall be used.
(ii) All components used shall be of rugged construction and shall be suitably designated by a label or sign-writing.
(iii) All modules in the system should be hot swappable and failure of any modules shall not result in complete system failure or adversely affect service delivery. All necessary hardware and software required for redundancy shall be provided.
(iv) The system hardware shall be modular in design to permit growth in small steps.
(v) The system shall use fully digital techniques for switching.
(vi) The variety of hardware modules and components used in the system shall be minimum.
(vii) Design precautions shall be taken to minimise the possibility of equipment damage arising from the insertion of an electronic package into the wrong connector or the removal of any package from any connector.

(viii) All components shall be rated for continuous operation of the system under the normal operating conditions. The circuits must also be designed so as to prevent damage to the other equipment under any condition of operating or any conditions of fault.

(ix) All the components used are to be approved and qualified as per the procedures of the QA wing of BSNL. The source of procurement of components is also required to be submitted by the manufacturers.

2.17.2 Processors

(i) Adequate backup memory shall be provided. Direct memory access, with suitable safeguards, is preferred for information flow between the backup memories on the one and the main memories and the input/output devices on the other.

(ii) Provision shall be made to prevent the loss/alteration of memory contents due to power failures, improper operating procedures and the procedures for restoring the system to its normal state, etc.

(iii) Dimensioning standards shall be evolved for the various types of memories used. This shall also include standards for provisioning of the required spare memory capacity.

(vi) The system shall support hard-disk (in duplicate) of suitable capacity, to provide storage of charging information, detailed billing information, traffic statistics, command log, system software, office data etc.

2.17.3 Input-Output devices

(i) The communication facilities provided for exchange of information between the system and the maintenance and operating personnel shall include facilities for a system test and control and alarm indication.

(ii) Input/output terminals shall be capable of transmitting/receiving characters of a subset of the Alphabet No.5 as specified in ITU-T recommendation Z.314. The printing/display device shall print/display different graphic symbols for the digit zero and the capital letter O. The Input/Output terminal shall have the English Keyboard. Capabilities of visual display terminals shall be as per ITU-T Recommendation Z-322. Terminal emulation software and any standard operating system shall be available in the PC.

(iii) Adequate number of man-machine interfaces shall be available to facilitate various types of system administrations listed.

(iv) If provision is made for monitoring from a remote terminal, it shall be ensured that the data links conform to the ITU-T Recommendation Q.513. Care shall be taken that the reliability of the data links does not, in any way affect the reliability of the system system. Special provision shall also be made for transmission of a failure signal even when the system is unable to transmit an output message.

(v) A suitable alarm and display system shall be provided for a continuous indication of the system status. The alarm system shall also provide an alarm to indicate the failure of power supply to the alarm circuits themselves. Provision shall be available to extend indications to a centralised place.

(vi) On a fault condition the system shall identity the faulty sub-system automatically and takes it out of service. This shall automatically bring in the diagnostic programmes for diagnosis. In such cases the details of the sub-systems taken out for executing diagnostic programmes shall be printed out. Availability of

Intelligent terminal (PC) to display the location of bay, shelf, PCB on the screen would be desirable. The dimensioning of processing capacity shall be such that the normal call processing is not effected due to invocation of any diagnostic program.

2.17.4 Equipment practice

(i) All cards of the same type and design shall be interchangeable without necessitating special adjustments.

(ii) All metal parts of frames, supports, etc. shall be mechanically rugged and constructed of corrosion resistant material or treated with anti-corrosive finish. All equipment shall have a tropical finish.

(iii) Suitable test access points and displays shall be provided for facilitating maintenance. Test access points shall preferably be located on the front side of the bay. All visual display devices shall be located in a position attracting immediate attention of the operating and maintenance personnel. Suitable extension boards shall be provided to facilitate access to components on a printed card.

(iv) The material used for all printed boards shall be expoxy or equivalent (FR4). It shall not buckle due to a load of the assembled board or due to temperature changes occurring under normal circuit operations.

(v) The supplier shall indicate whether printed board connectors are of edge type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.

(vi) All components and material used in the equipment shall be non inflammable or in absence of it, self-extinguishable. They shall be fully tropicalised.

(vii) The supplier shall indicate the various types of cables and wires used in the system. Detailed particulars of any special wires and cables like standardized coaxial, screened cable, etc. shall be furnished with their actual usage in the system.

(viii) The buses, if any, shall be suitably protected against electrical and magnetic interference from neighbouring systems (like electromechanical systems, fluorescent tubes, motors, etc). The supplier shall indicate the care taken in the design and location of the bus system for such interference.

(ix) The points for connecting the power supplies to the different plug-in cards shall be standardized and mechanically interchangeable. Otherwise suitable mechanical safeguards shall be provided to prevent damage due to accidental inter-change of cards.

(x) The supplier shall indicate the requirement at the external interface against induced voltages and currents due to lightning, high power system, etc.

(xi) The system shall provide for isolation and protection from accidental high voltage power contact.

2.18 Markings

(i) Equipment on the bay, whether of fixed or plug-in type, shall be suitably marked. Identification of type of cards in its connector shall be possible without necessitating its removal. Any plug-in component shall be marked with sufficient information for its complete identification.

(ii) The marking on the equipment and the cables shall be the same as that used on the schematic drawings, cabling lines etc., in the documentation supplied with the equipment.

(iii) All instructions, labels, or any other marking on the equipment shall be perfectly legible and in the English language.

(iv) Colour code used for power feeding bus-bars/cables and earth shall be identical for a given voltage throughout the equipment.

(v) Fuses shall have a suitable marking for the different ratings to enable easy identification and replacement.

(vi) Marking shall ensure easy traceability.

(vii) The plug-in units whose removal or insertion (while the equipment is in operation) might endanger the reliability or performance of the equipment - shall have suitable protection and caution marking.

(viii) Each sub-assembly shall be clearly marked to show its functions and circuit reference so that its complete description can be located in the handbook.

(ix) The components shall be marked with their schematic references so that they are identifiable from the component layout diagram in the handbook.

(x) All controls, switches, indicators etc. shall be clearly marked to show their circuit designations and functions.

(xi) Each terminal block and terminal shall be marked with an identifying code.

2.19 Software

2.19.1 General

(i) The software shall be modular and structured.

(ii) The design of the software shall be such that the system is easy to handle both during installation and day-to-day operations as well as during expansions.

(iii) The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.

(iv) The architecture of the software shall be open ended so that the growth and addition of new features can be handled in practice without any need of redesign of the software.

(v) Adequate flexibility shall be available to easily adopt changes in service features and facilities and technological evolution in hardware.

(vi) The design shall be such that propagation of software faults is contained.

(vii) The software shall provide sufficient checks to monitor the correct functioning of the system.

(viii) Test programs shall include fault tracing for detection and localisation of system faults.

(ix) The normal operation of the system should not be adversely affected while undertaking :

- (a) Extension to system (Hardware expansion)
- (b) Enhancement of system facilities.
- (c) Correction to programs or functional blocks.

(x) The software supporting documentation shall be in English. Any update in the software at a later stage to overcome deficiencies of the system due to bugs, compatibility etc., shall be provided free of cost by the equipment supplier.

(xi) The equipment supplier shall undertake to supply on continuing basis all software updates. These updates may include new features and services and other maintenance updates. The software up-gradation shall be possible with minimum interruption to the service. The tendering authority shall indicate the services and features required by it in future along with commercial terms for the same.

(xii) The equipment supplier shall provide any software modification necessary due to modification of software in the inter-working with other network elements.

2.19.2 Diagnostic programs to localise hardware faults

(i) On a faulty condition, the software shall provide for isolating the faulty sub-system and then automatically bring in the diagnostic programs for diagnostic purposes.

(ii) It shall preferably be possible to diagnose to single PCB level in atleast 95% of the types of PCBs.

2.19.3 Software of charge records

(i) Arrangements shall exist for dumping the charging information to non-volatile backup memories automatically at periodic intervals.

(ii) Facility shall be available for changing this interval by a Man-Machine Command.

(iii) The charging information records shall be sufficiently protected against modifications by man-Machine Commands.

2.19.4 Right to use

There shall be no imposition of any sort of precondition on the 'Right to Use' of software.

2.20 Man-Machine Communication

2.20.1 Man-Machine Language (MML)

(i) Man-machine interface language shall be based on ITU-T Recommendations Z 301 to Z 341.

(ii) The man-machine language shall be in English. Commands shall be English based and responses shall be in English.

(iii) The MML shall be easy to learn and to use, easy to input commands and to interpret outputs.

(iv) The Man-Machine Language shall contain Man-Machine Commands (MMC), outputs, control actions and procedures sufficient to ensure that all relevant functions for the operation, maintenance, installation and testing of the system can be performed.

(v) The MML shall have an open-ended structure such that any new function or requirement added will have no influence on the existing ones. The language structure shall be such that subsets can be created.

(vi) The character set used in the MML shall be a sub-set of the ITU-T alphabet No. 5 as recommended in ITU-T Z.314.

(vii) The command codes shall be function oriented. There shall be only one command per function. The codes shall be mnemonic. All the command codes in a particular application shall preferably consist of the same number of characters.

(viii) The output in response to input commands shall have the same format and use the same identifiers, codes, and labels, as the corresponding input command.

(ix) The MML shall provide facilities for cancelling and aborting the execution of commands.

(x) The MML shall provide facilities for inputting the parameters, for a command, in any sequence and the optional parameters need to be inputted only when they are required. Screen editing facilities for modifying the commands and parameters shall be available.

2.20.2 Input/Output

(i) The input and output information shall be presented in a compact form.

(ii) The automatic output, not made in response to an input command shall:

a. Include the time and date.

b. Use standard telephone terminology. It is preferred if the automatic output is differentiated by colour or special characters from the output in response to an input command.

(iii) To facilitate filling and retrieval of recorded information in MML; the information shall be recorded on forms or pages with an identification header on top of each page with the date and time.

(iv) Special information shall be provided on priority printouts indicating emergent situations.

2.20.3 Man-machine dialogue

(i) The MMC shall offer the facility for a conversational mode of operation.

(ii) The MMC shall have facility for restricting the use of certain commands or procedures to certain staff/terminals.

(iii) Where several man-machine terminals are in use on a single system, a mechanism shall be available to avoid clashes.

(iv) The execution of any command shall not result in malfunctioning and/or over loading of the system. It shall also be ensured that the operator is not locked out by the system.

(v) The MMC shall be implemented in such a way that errors in commands or control actions shall not cause the system to stop or unduly alter the system configuration.

(vi) Command errors detected by the system shall be indicated by the output of error messages.

(vii) Possibility of priority messages to interrupt an input or output message of lower priority is desirable.

2.20.4 Checks and safeguards

Sufficient checks and safeguards shall be built into the implementation of the MMC so as to ensure reliable operation of the system.

2.21 Diagnostics/Testing – The equipment shall support diagnostic capabilities (which will run as background tasks) to verify the equipment's proper operation within the network. Built-in test capabilities shall be provided which will run at specific events or on demand. Health monitoring signals shall be continuously passed between the various modules to ensure the detection of any failure in a module.

2.22 The system hardware and software shall not pose any problem, due to changes in date in time caused by events such as changeover of leap year etc., in the normal functioning of the system.

2.23 Maintenance Aspects:

(i) Maintenance philosophy is to replace faulty units after quick analysis of monitoring and alarm indications. Actual repair will be undertaken at a repair centre. The supplier shall ensure the repair of faulty equipment during and after warranty period.

(ii) It shall be possible to isolate Interface points for testing purposes.

(iii) The equipment shall have easy access for servicing and maintenance.

(iv) All important switches/controls on front panel shall be provided with suitable safeguards such as interlock system to avoid accidental operation by the maintenance personnel.

(v) Procedure for repair of equipment giving full details of testing instruments shall be provided by the equipment supplier. Test jigs, fixtures required for maintenance/repair shall also be provided.

(vi) Extensive facilities for testing, supervision and monitoring functions shall be provided for quick isolation and rectification of faults. These functions shall be performed by OMC. Any additional instruments required shall be provided by the equipment supplier with details.

(vii) The supplier shall provide information regarding the failure rate of the PCBs and accordingly supply number of spare cards depending on the size of the system, for a period of three years or for a period as specified by the tendering authority

(viii) The maintenance spares supplied shall take into account the MTTR. At least one spare PCB of each type shall be supplied.

2.24 Electromagnetic Compatibility (EMC)

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished by the supplier:-

a) Conducted and radiated emissions: - To comply with Class B of CISPR 22 {2003} "Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment";

b) Electrostatic discharge:- To comply with IEC 61000-4-2(2001) "Testing and measurement techniques of Electrostatic discharge immunity test" under following test levels:
   Contact discharge level 2 {$\pm$ 4 kV};
   Air discharge level 3 {$\pm$ 8 kV};

c) Fast transients common mode (burst):- To comply with IEC 61000-4-4 {1995 with Amendment 1 (2000) and Amendment 2 (2001)} "Testing and measurement techniques of electrical fast transients/burst immunity test" under Level 2 {1kV for DC power lines; l kV for signal control lines};

d) Immunity: IEC 61000-4-3{2002} "Radiated RF Electromagnetic Field Immunity test under test level 2 (test field strength 3 v / m) for general purpose in frequency range 80 MHz to 1000 MHz and under test level 3 (10 v/ m) for protection against digital radio telephones in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 2.0 GHz";

e) Surges Common and differential mode :- To comply with IEC 61000-4-5 {2001} "Test & Measurement techniques for Surge immunity tests" under test levels of 0.5kV for differential mode and 1 kV for common mode;

f) Radio frequency common mode: To comply with IEC 61000-4-6 {2001} "Immunity to conducted disturbances induced by radio frequency fields" under the test level 2 {3 V r.m.s.}; clamp injection method for DC lines and Signal Control lines.

[**Note: -** For tests for checking compliance to above EMC requirements, the method of measurement shall be in accordance with TEC Standard No.SD/EMI-02/02.SEP.2001 and the references mentioned therein.]

2.25 Safety Requirements

a. The operating personnel shall be protected against shock hazards as per IS 8473 (1993) – Guide on the effects of current passing through the human body (equivalent to IEC publications 479-1 (1984).

b. The equipment shall conform to IS 13252 (1992) – Safety of information technology equipment including electrical business equipment (equivalent to IEC publication 95 (1986) and IEC 215 (1987) Safety requirements of radio transmitting equipments (for Radio equipments only)

The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.

2.26 Documentation

2.26.1 Hard & soft copy of all documents shall be provided in English by the equipment supplier. The documents shall comprise of:

(i) System Description Documents

The following system description documents shall be supplied along with the system:

(a) Overall system specification and description of hardware and software.
(b) Installation manuals and testing procedures. Installation manuals to be provided shall contain step by step process of installation of system.
(c) Equipment layout drawings
(d) Cabling and wiring diagrams
(e) Detailed specification and description of all I/O devices.
(f) Adjustment procedures, if there are any field adjustable units.
(g) Spare parts catalog including information on individual component values, tolerances etc. enabling procurement from alternate sources.
(h) Detailed description of software describing the principles, functions, interactions with hardware, structure of the program and data.
(i) Programming language (s) manual.
(j) Planning and system engineering documents.

(ii) System Operation Documents

The following system operation documents shall be provided by the equipment supplier : -

a) Operating manual of the system
b) Maintenance manual.
c) Man-machine language manual.
d) Operation and maintenance manual for all I/O devices and auxiliary equipments.
e) Faulty location and trouble shooting instructions including fault dictionary.
f) Test procedures with auxiliary test equipments.
g) Emergency action procedures and alarm dictionary.

(iii) Training documents

Training manuals and documents necessary for 0rganizing training in installation, operation and maintenance and repair of the system shall be made available.

2.26.2 In addition to the printed documentation, all documents shall be provided in CD-ROM alongwith suitable means of retrieval i.e. IBM PC compatible machine with CD-ROM drive for each site.

2.26.3 Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be supplied immediately following the issue of such updates.

2.26.4 The structure and scope of each document should be clearly described.

2.26.5 The documents should be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

2.26.6 All diagrams, illustrations and tables shall be consistent with the relevant text.

2.27 For all documents/ standards referred in this GR, only the latest version shall be applicable. The tendering authority, at the time of tendering may review the versions of all the documents mentioned in this GR and update them if necessary.

CHAPTER -3

3. QUALITY REQUIREMENTS

3.1 Components

(a) All the components used shall have to be approved and qualified as per procedure specified in QA document no. QM-324. The source of procurement of components shall also be submitted by the manufacturers. Alternatively, the bidders may indicate whether the components are approved by any international authority.

(b) List of all the components for which second source is not available, shall be provided.

3.2 Quality Standards

(a) The equipment shall be manufactured in accordance with the International Quality Standard ISO-9001:2000 for which the manufacturer shall be duly accredited. The quality plan describing the quality assurance system followed by the manufacturer shall be submitted.

(b) The equipment shall be manufactured as per the latest BSNL QA Guidelines indicated in Quality Manuals 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 Boards Assemblies}, QM 210 {Guidelines for Standard of Workmanship for Surface Mounted Devices} and QM 301{Transmission Equipment General Equipment}.

(c) The product shall conform to the QA requirements stipulated in QM-351 (QA Requirement for Switching equipment).

3.3 Lightning Protection - The equipment including OMC shall have adequate protection against lightning & power surges. All equipment shall have provision for grounding.

3.4 Redundancy - The Power Supply as well as the control equipment for all components of the Packet Core Network including the OMC shall be provided with 1+1 hot standby/ N +1 mode redundancy. Any other redundancy provided shall be indicated by the equipment supplier. The system shall reliability of 99.999.

3.5 Service Provisioning –Manual service provisioning capabilities shall be provided to facilitate optimal utilisation of network resources and real time service provisioning (limiting human involvement to a minimum). Once a service is provided to a customer, the provisioning system shall constantly monitor its availability and quality. During an outage, it shall be possible to re-provision or provide an alternative support to the customer. This feature shall be applicable for Simple IP as well as Mobile IP users.

It shall also support automated provisioning. However the tendering authority may specify at the time of tendering whether the hardware and software required for automated provisioning of services is required or not. Details shall be provided by the vendor with respect to the methodology procedures adopted for auto provisioning of service.

3.6 System Design Objectives – The system design objectives of the PCN (as defined in 3G PP2 P.R 0001) shall be to :

- Support a wide range of addressing configurations
- Provide seamless roaming
- Provide robust authentication and authorization services
- Provide QOS Support
- Provide accounting services

3.7 Grade of Service : The system shall have Grade of service of 0.5% for PCN-RN(BSC/PCF).

CHAPTER-4

4. OPERATIONAL REQUIREMENTS

4.1 Services as specified in Chapter 11 shall be supported.

4.2 Billing/Charging

4.2.1 PDSN shall provide support for packet accounting/charging function for the IP network specific parameters (packet accounting). It shall be able to receive the packet accounting/charging function for the radio specific parameters (usage time) from the PCF (an integral part of BSC).

4.2.2 The PDSN shall merge the Radio specific parameters (sent by PCF in messages called airlink records over R-P interface) and the IP network specific parameters (generated by PDSN) to form a Usage Data Record (UDR).

4.2.3 The UDRs generated by PDSN shall be as per 3GPP2 standard P.S0001 (latest release). The PDSN shall send the UDR to a local RADIUS Server or to a secondary RADIUS server if the primary RADIUS is unavailable or not responding.

4.2.4 The PDSN shall communicate with the AAA Server using the RADIUS Accounting and Authentication protocol as defined in RFC 2865 and RFC 2866. The PDSN shall send RADIUS Accounting messages to the AAA server as per the accounting trigger points defined in TIA/EIA/IS-835B (TR45.6). This occurs at the following points in a packet data call:

- Packet Data Session is opened - transition from idle to active mode.
- PDSN Interim Update Timer expires – The PDSN sends an Accounting Interim Update Message.
- In addition, the PDSN shall supports a configurable Time of Day Accounting. An Accounting Stop Message and then an Accounting Start Message are sent if Time of Day Accounting is invoked.

4.2.5 The UDRs generated by PDSN (and available at local RADIUS server) shall be capable of being transferred over X.25 or TCP/IP links to the billing centre of BSNL/MTNL using any standard file transfer protocol. In addition it shall also be possible to transfer the billing information i.e. the UDRs available at the RADIUS server to standard magnetic tapes / optical disc used by BSNL/ MTNL. Any additional hardware /software (if required) for retrieving the billing information from magnetic tape/ optical disc or for on-line transfer of billing information over X.25 / TCP/IP to the billing centre shall be provided by the equipment supplier.

4.2.6 The UDRs shall be capable of being used by the existing billing system of BSNL/MTNL as specified by TEC GR No. GR/BCS-01 or TD/CDR-01. The tendering authority may specify at the time of tendering if there is requirement for a mediation device for co-relation of CDRs and UDRs for packet data access and for applications from point of view of packet charging.

4.2.7 There shall be provision for generation of intermediate UDRs for long call with respect to time, charge etc.

4.3 Lawfully Authorized Electronic Surveillance (LAES) – The packet data architecture shall support LAES for all packet services for both access methods, namely simple IP and Mobile IP. The PDSN shall provide the access point to the user data stream identified for interception by HLR/VLR and tagged by the BSC/PCF. A duplicate stream of packets shall be sent to an authorized collection point. The packets shall be duplicated before any network level encryption is applied. It shall be possible to monitor or trace communication of any subscriber served by a PDSN. Call content and other associated data shall be deliverable to the proper legal authorities. This information must not be available or may not be reported to unauthorised personnel.

- The monitored packets shall be in assembled form to provide complete readable information transacted along with relevant header information, irrespective of routing of the information /packets.
- Monitored information shall contain call-related information (CRI) like sender address, destination address, date and time of forwarding the message, notification of successful delivery of message etc.
- Monitored packets/messages shall be transported on a pre-defined channel to the user agency in sequence and with correlated data where it should be stored in separate directory.
- The system shall provide facilities for printing, storing, transferring and concurrent/post storage analysis.
- It shall be possible to monitor the messages transacted simultaneously by multiple monitoring agencies.

The general requirements of lawful interception and monitoring shall be as per TEC GR No. GR/LIS-01 (latest version).

4.4 Mobility Management – The system shall support the following types of " hand-off" as per 3GPP2 P.S0001 (latest version) without having to make any modification in the Simple IP handset:

4.4.1 Inter PCF Intra PDSN (PCF to PCF) handoff

The link layer mobility management function shall be used to manage the change of the R-P session point of attachment while maintaining the PPP session and IP address. The R-P session point of attachment shall be the PCF. When a Remote Station moves from one PCF to another PCF, a new R-P session shall be set up for every Packet Data session.

4.4.2 Inter PCF Inter PDSN(PDSN to PDSN) handoff

The IP layer mobility management function, provided by Mobile IP, shall maintain persistent IP addresses across PDSNs. For Mobile IP Mobile Stations, in order to maintain persistent IP addresses, the Remote Station shall effect a PDSN to PDSN hand-off by registering with its Home Agent as per RFC 2002.

4.5 **Supervision** – Supervision of complete network shall be both automatic and operator controlled and centralized at OMC.

4.6 **Alarm Indications** – In case of all major alarms (any event that leads to system switch-over or service disruption) both audio and visual alarm indications shall be provided. In case of minor alarms visual alarm indications shall be provided and provision of audio alarms is desirable. It shall be possible to define the major and minor alarm conditions and set the threshold values thereof. The OMC shall provide the flexibility to forward the alarm triggered by faulty operations to either a pager, a short message service system, an electronic mail or additional alarm windows on the OMC interface. The operator shall be able to redefine and configure the alarm forwarding destination. Facility shall exist for audio/visual alarm indication in the event of 'Route Busy', poor network performance in terms of under utilisation of BSC/PCF or too many blocked calls etc., or when the processor load exceeds a certain preset value. Alarm indication shall exist in the event of fan failure.

4.7 **Security** - The system shall provide confidentiality, subscriber authentication features and high security through special encryption techniques.

4.8 Power Supply

4.8.1 **Input supply** : The system shall work satisfactorily for nominal input supply of -48 V DC over the voltage range of –44.4 V to –56.4 V.

4.8.2 **Power consumption:** The power consumption of system shall be specified by equipment supplier.

4.8.3 **Protection** : The protection for input over voltage, under voltage, and short circuit protection shall be provided.

4.9 Environmental Specifications

(i) The system shall satisfy the pre-installation conditions specified under category 'A' of QA document QM-333 for environmental testing of Electronic Equipment for Transmission and Switching use.

(ii) The system shall be capable of working in an environment specified for category 'A' equipment in the QA document QM-333.

(ii) Extreme environmental conditions under which the system is capable of short-term emergency operation without permanent damage may be indicated.

4.10 Transportation & Storage : As per QM-333.

4.11 MTBF/MTTR : The MTBF and MTTR (predicted and observed values) figures shall be worked out by the equipment supplier as per QA document QM-115 and based on these figures, the maintenance spares for three years or for a period as specified by the tendering authority shall have to be specified by equipment supplier.

CHAPTER - 5

5. PACKET DATA SERVING NODE (PDSN)

5.1 Packet Data Serving Node (PDSN) shall support the CDMA 2000 1x based Radio Network (as per TEC GR/WLL-04) and Authentication, Authorization and Accounting Server, and the Home Agent (required for mobile IP support) as per relevant 3G PP2 standards.

5.2 The PDSN shall support multiple Home Agents and shall support secure encrypted tunnels and reverse IP tunneling between the PDSN and Home Agents over the public network as defined in the standards.

5.3 The PDSN shall support forward and reverse tunneling of traffic and signalling between the FA and HA (where applicable) using IP-in-IP encapsulation and optional encryption. In a Mobile IP VPN scenario, all packets sent to and received from the mobile node shall be tunneled between FA and HA and shall permit use of private IP addressing by the home networks. For the non-encrypted case, data packets shall be tunneled between the FA and HA using IP in IP encapsulation. For encrypted Mobile IP VPN, all control and data packets between the FA and HA shall be encrypted using IPSec in addition to being tunneled using IP-in-IP encapsulation.

5.4 The PDSN shall support the static routing protocol and dynamic routing protocols such as Routing information protocol-2 (RIP-2), Open Shortest Path First (OSPF) and the Interior Gateway Routing Protocol (IGRP). Support of exterior routing protocols such as BGP4 etc. may be optionally provided. The tendering authority at the time of tendering may indicate whether the support of BGP4 is required.

5.5 The PDSN shall support 3GPP2 A.S0001 (latest version) Access Network Interfaces Interoperability Specification (IOS 4.0 or later). The PDSN shall support open RP interface as defined by standards bodies such that it can inter-operate with third party PCFs in a multi vendor environment. The tendering authority may specify the BSC/PCF vendors for which the PDSN shall be required to interoperate.

5.6 The PDSN shall act as a client for AAA Server and shall interact with the RADIUS server for Authentication, Authorisation, and Accounting functions using the RADIUS protocol. The PDSN shall support interim accounting updates to the AAA server and accounting attributes as per 3GPP2 document P.S0001 (latest version).

5.7 The PDSN shall be scalable and in fully redundant configuration.

5.8 Interfaces

5.8.1 One PDSN shall be able to be connected to multiple PCFs .The maximum number of PCF that can be connected shall be specified.

5.8.2 The PDSN shall have standard ethernet or fast ethernet interfaces for the IP network.

5.8.3 The PCF and PDSN communicate with each other using a standard interface known as the R-P interface (defined as A10 and A11 interfaces in 3G PP2 standard). It has two components: the A11 interface used for control messages and the A10 interface used for user data. R-P interface is also referred to as the Aquater interface or A10/A11 interface. It shall meet the requirements as indicated in 3G PP2 standard P.S 0001.

5.9 PDSN shall have capabilities offering following features :

- Minimize inter-PDSN handoffs
- Load Balancing - Balance subscriber call load across PDSNs
- Redundancy - Provide service recovery due to a failed or out-of-service PDSN

5.10 The PDSN shall be capable of supporting the following features :

a) Simple IP and Mobile IP as per 3GPP2 standard P.S0001.

- **Simple IP**
  Support for mobility within the coverage area of a single PDSN Cluster i.e. no inter-PDSN handoffs (Mobile does not have a Mobile IP client.)
- **Mobile IP**
  Support for subscriber devices (with Mobile IP client) that allow an IP address to be retained even when handoff results in the client moving to a different PDSN.

  In addition to above, the support for Mobile IP type service with Simple IP mobiles (without a Mobile IP client) where the Mobile IP client is located with the FA, may optionally be provided through support of Proxy Mobile IP.

b) RFC 1918 for dynamic IP address assignment for Private Internets
c) RADIUS client

5.11 PDSN shall support the following Link layer protocols:

(i) PPP (RFC-1661)
(ii) PPP Asynch HDLC (RFC-1662)
(iii) PAP Authentication (RFC-1334)
(iv) CHAP Authentication (RFC-1994)
(v) IPCP (RFC-1332)
(vi) PPP compression negotiation between the subscriber device and the PDSN (RFC-1962)
(vii) PPP compression protocols between the subscriber device and the PDSN:
- Stac-LZS (RFC-1974) -optional
- Microsoft Point-To-Point Compression Protocol compression (RFC-2118)
- Deflate (RFC 2394) - optional

(viii) Virtual Private Network (VPN)
- L2TP
- PPTP

5.12 PDSN shall support the following Network Layer protocols :

(i) IP (RFC-791)
(ii) Mobile IPv4 (RFCs 2002, 2003, 2005, and 2006)

(iii) Mobile Ipv4 Challenge/Response Extensions, RFC 3012
(iv) Reverse Tunneling (RFC-2344)
(v) Reverse Tunneling for Mobile IP (RFC-3024)
(vi) Van Jacobson TCP/IP Header Compression (RFC-1144)
(vii) IP in IP encapsulation (RFC-2003).
(viii) Generic Route Encapsulation (GRE) (RFC-1701)
(ix) The Definitions of Managed Objects for IP Mobility Support Using SMIv2(RFC 2006)
(x) Mobile NAI Extension (RFC 2794)
(xi) Capability for constructing a properly formed NAI based on the MSID of the mobile station (RFC 2486)
(xii) GRE Key and Sequence Number Extensions (RFC 2890)

5.13 Quality of Service

PDSN shall support the differentiated services as defined in:

- Definition of the Differentiated Service Field (DS field) in the IPv4 and IPv6 Headers (RFC 2474).
- An Architecture for Differentiated Services (RFC 2475)
- An Expedited Forwarding PHB (RFC 2598)
- Assured Forwarding PHB Group (RFC 2597)
- Traffic prioritization based upon Diffserv field

(Differentiated service is a service model that can satisfy differing QoS requirements. For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet).

5.14 The PDSN shall support Foreign Agent (FA) functionality in case of mobile IP support.

5.15 The PDSN shall support packet filtering based upon IP headers.

5.16 The PDSN shall support both GUI and Command Line Interfaces for management. Web based interface for management is highly desirable.

5.17 The PDSN shall have adequate security measures and shall support multi level administration, access control lists and protection against denial-of-service attacks and spoofing.

5.18 The PCN shall implement a load balancing mechanism to enable an optimum PDSN to be selected for each arriving call by analyzing the availability and load of each of its PDSNs.

5.19 The PCN shall implement a redundancy and overload protection mechanism to enable monitoring of status of PDSNs such that failed /overloaded PDSN is marked as "unavailable" and new calls are routed to other available / less loaded PDSNs in the network**.**

CHAPTER - 6

6. AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA) SERVER

6.1 AAA Server shall authenticate and authorize the mobile client, provide user profile and Quality of Service (QoS) information to the PDSN and store accounting data. This shall conform to the requirements as per 3GPP2 document P.S0001(latest release).

6.2 It shall support the Authentication, Authorization and Accounting services specified in 3GPP2 standard P.S0001, TR45.6 accounting for PDSN standards, RFC 2865 for RADIUS Authentication and Authorization and RFC 2866 for RADIUS accounting.

6.3 The AAA Server shall support the following : -

- Remote Authentication Dial In User Service (RADIUS) as per RFC 2865 and 2866.
- RADIUS proxy servers and RADIUS brokers shall be supported.
- The local RADIUS Server shall also support the Interim Accounting Record and accounting attributes as per 3GPP2 document P.S0001.
- The local RADIUS Server shall also support the Differentiated Services Class attribute as given in 3GPP2 document P.S0001.

6.4 To support Mobile IP, the local RADIUS server shall also support the following attributes specified in 3GPP2 document P.S0001.

- IKE Pre-shared secret request attribute
- Security Level Attribute
- Reverse Tunnel Specification
- Differentiated Service Class Attribute
- Pre-shared Secret Attribute
- Correlation ID Attribute
- Home Agent Attribute
- Key ID Attribute

6.5 It shall support the following link layer protocols:

- PAP Authentication
- CHAP Authentication
- IMSI Authentication - Authentication using the IMSI as the username and common password.

6.6 It shall support the following Network Layer protocols :

- IP
- Mobile IPv4
- Reverse Tunneling
- NAI Extensions for mobile IP (Optional)
- IPSEC/IKE
- Van Jacobson TCP/IP Header Compression

6.7 It shall support the following Simple IP Access Methods

- MSID based simple IP routing access without PPP CHAP/PAP.
- Simple IP routing access based on the user name/NAI provided during CHAP/PAP.
- L2TP (Layer 2 Tunneling Protocol)
- Simple IP VPDN access based on the NAI provided during PPP CHAP/PAP.

6.8 It shall support the following Simple IP Services

- Static private and public IP address.
- Dynamic private and public IP address
- Accounting - TR45.6 accounting model shall be supported.
- Packet filtering through access lists.
- Automatic Ingress filtering as defined in TR45.**6.**
- Limited mobility (PCF hand-offs)

6.9 It shall support the following Mobile IP features*:*

- Static private or public IP address.
- Dynamic private or public IP address.
- Generic Route Encapsulation (GRE)
- Reverse Tunneling
- NAI extension
- Proxy mobile IP client (Optional)
- Multiple IP flows over the single session through unique NAIs.

6.10 Accounting

Packet Accounting parameters are divided into radio specific parameters collected by the PCF (Radio Network) and IP network specific parameters collected by the PDSN. The PDSN merges the radio specific parameters sent by PCF (RN) in messages called air link records across R-P interface for a given user session with the IP network specific parameters to form a Usage Data Record (UDR). After merging, the PDSN shall send the UDR to a local AAA RADIUS server. The RADIUS server shall maintain the UDR until the record is removed by the operator billing system.

The different types of Airlink Records and the fields in the various Airlink records generated by the PCF (BSC) shall be as per 3GPP2 standard P.S0001.The Radio Network parameters transmitted across the R-P interface shall follow the RADIUS format as defined in RFC 2865 and 2866. The format of the UDR generated by PDSN shall be as per 3GPP2 standard P.S0001.

CHAPTER – 7

7. HOME AGENT (HA)

7.1 This network entity is required to support Mobile IP. Mobile IP is intended to provide for ubiquitous internet connectivity to user while on the move irrespective of whether they are located within their own IP sub-network or another IP sub-network Mobile IP enables to have the same IP address even while the mobile node changes its point of attachment to the internet. The HA is responsible for attracting traffic destined for the mobile node and for tunneling it to the CoA (care of address) associated with a given mobile node for further delivery to mobile node. The care of address is an indirect pointer to the mobile node and represents the topologically correct and reachable IP address that corresponds to the mobile node's current network attachment, so that the home agent can tunnel packets to mobile node (Mobile IP device). Home Agent authenticates Mobile IP registrations from the Mobile station, maintains current location information for RS and redirects packets to the Foreign Agent.

7.2 Home Agent shall support reverse and forward tunneling and support IP-in-IP encapsulation, IPSec protocols for all communication between the HA and FA.

7.3 The HA shall support RADIUS protocol for AAA as in case of PDSN.

7.4 The HA shall support Diffserv coloring.

7.5 HA shall have following features:

7.5.1 Support for static IP Address assignment
- Public IP addresses
- Private IP addresses

7.5.2 Support for dynamic IP Address assignment
- Public IP addresses
- Private IP addresses

7.5.3 Multiple flows for different NAIs using static or dynamic addresses

7.5.4 Multiple flows for the same NAI using different static addresses

7.5.5 Foreign Agent Challenge extensions as specified in RFC 3012
- Mobile IP Agent Advertisement Challenge Extension
- MN-FA Challenge Extension
- Generalized Mobile IP Authentication Extension, which specifies the format for the MN-AAA Authentication Extension

7.5.6 Mobile IP Extensions specified in RFC 2002
- MN-HA Authentication Extension
- FA-HA Authentication Extension

7.5.7 Reverse Tunneling as specified in RFC 2344

7.5.8 Mobile NAI Extension as specified in RFC 2794

7.5.9 Multiple tunneling Modes between FA and HA
- IP-in-IP Encapsulation as specified in RFC 2003
- Generic Route Encapsulation as specified in RFC 2784

7.5.10 Binding Update message for managing stale bindings

7.5.11 Home Agent redundancy support

7.5.12 Mobile IP Extensions specified in RFC 3220

- Authentication requiring the use of SPI (Security Parameter Index)

7.5.13 Support for Packet Filtering

- Input access lists
- Output access lists

7.5.14 Support for proxy and gratuitous Addressed Resolution Protocol (ARP)

7.5.15 Mobile IP registration replay protection using timestamps.

7.5.16 Network Time Protocol (NTP) as per RFC 1305.

7.5.17 The Home Agent may optionally support VLAN tagging such that a common HA can be used for terminating multiple subscriber FA – HA tunnels.

CHAPTER - 8

8. Operations and Maintenance Centre (OMC)

8.1 The OMC allows the centralized operation of the various units in the system and the functions needed to maintain the sub systems. The OMC provides the dynamic monitoring and controlling of the network management functions for Operation and Maintenance (O&M). The OMC shall support Graphical User Interface (GUI) for operation and standard TMN interfaces as specified in ITU-T Rec. M-3010 & M-3020.

8.2 The overall objective of OMC is that neither equipment failure nor human error in the OMC implementation should render the OMC and /or the part of the network it supervises, out of service.

8.3 OMC shall be a carrier grade system with full redundancy and scalability. It shall be possible to have remote workstations with the OMC, with complete GUI tools for O & M of the system at the remote locations. It shall support north-bound interface like SNMP, Corba, TCP / IP, CMIP etc., to enable it to work with a remote NMS. The tendering authority, at the time of tendering may specify the type of NMS with which the OMC would be required to interface with and accordingly any additional hardware / software, (if required) shall be provided for interfacing with the NMS.

8.4 The Operation & Maintenance Centre (OMC) shall be capable of performing the following functions: -

(i) Event/Alarm Management: Alarms shall be presented to the operator via software programs and tools for easy presentation and interpretation, for easy maintenance and to locate faults of all managed elements of the network. Events shall be logged for future use. The following events/alarms shall be supported :

a. Memory threshold
b. User Authentication fails on the Registration Request message (for individual AAA servers)
c. PDSN/HA does not receive a response from the AAA after a configured number of retrials
d. PDSN has successfully established a PPP connection
e. PDSN/HA disconnects a PPP connection
f. Network Time Protocol Server connection failure
g. Authentication server fails to respond after a pre-defined number of retrials.
h. PDSN/HA is rebooted or restarted
i. Exhaustion of RADIUS message re-transmit
j. Amount of session, active sessions & failed sessions when an alarm is generated /cleared.
k. Amount of R-P packet throughput when an alarm is generated /cleared.

(ii) Configuration Management : OMC shall provide real time configuration database access to manage the software loading and version tracking, support for addition, deletion and change of network element parameters.

(iii)Performance Management: OMC shall provide tools for the collection of statistics and call information into a database and logging file. Data shall be viewed using tabular or graphical reports on the GUI terminal.

(iv) Security Management : OMC shall provide password and login access to the system to prevent any unauthorized access to the system.

(v) Fault Management : OMC shall provide capability to query and change device states and provide control for system diagnostics. It shall be possible to monitor different protocols in real-time using command line interface of the PDSN/HA in order to be able to identify and trouble-shoot user problems and network problems. The PDSN/HA shall be able to monitor the following protocols in real time:

a. A10/A11 messages on the R-P interface of the PDSN
b. PPP – LCP, IPCP and Authentication protocols (PAP/CHAP)
c. RADIUS
d. L2TP, PPTP
e. Pi Interface messages

(vi) Network statistics – OMC shall provide data related to channel occupancy, rejected calls etc. with visual display of faulty elements of the network. The OMC shall provide atleast the following statistics:

a. Mobile IP Statistics:

i. Number of Packets & Bytes Transmitted and Received per Mobile IP session
ii. Total Number of Current Mobile IP sessions
iii. Total Duration (length of time) of all Mobile IP sessions
iv. Total Duration of (length of time) completed Mobile IP sessions
v. Total number of RRQ denied by PDSN for missing NAI, missing Home Agent, reverse tunnel mandatory etc.

b. PPP statistics such as call setup, connect and release

i. Connection failed at LCP
ii. Connection failed at IPCP
iii. Connection failed at Authentication

c. Session Statistics:

i. Number of Active Sessions at any given instance
ii. Number of Dormant Sessions at any given instance
iii. RP connections Setup
iv. RP connections Released
v. RP Connections De-Registered
vi. RP Connections Life Time Expired
vii. RP Connections released other reasons

viii. Total Number of Registration Requests Received, Accepted, Denied, Discarded
ix. Initial Registration Requests Accepted & Denied
x. Re-Registration Requests Accepted and Denied
xi. De-registration Requests Accepted and Received
xii. Total GRE Packets Received & Sent
xiii. Total GRE Bytes Received and Sent
xiv. GRE Throughput

CHAPTER-9

9. TECHNICAL REQUIREMENTS

The performance specifications of different sub-systems of the Packet Core Network shall be as given below. The performance parameters are given for a typical call model and these values may be reviewed by the tendering authority taking into consideration the actual traffic/call model and expansion envisaged

9.1 PDSN : The PDSN shall be of two types namely Type 1 (High capacity) and Type 2 (Low capacity) with minimum specification as given below :-

Type 1

i	Number of simultaneous active PPP sessions	: 2,40,000
ii	Number of PPP sessions which can be enabled for header or payload compression without any adverse effect	: 50% of above
iii	Throughput assuming packet size of 512 byte	: 1Gbps
iv	Number of call setups and tear downs per second	: 2,500
v	Number of simultaneous VPN tunnels using L2TP or PPTP Protocols with encryption disabled	: 32,000
vi	Number of simultaneous VPN tunnels using L2TP or PPTP Protocols with encryption enabled	: 3,200
vii	Number of simultaneous PDSN-HA tunnels (Mobile IP sessions)	: 1,20,000

Type 2

i	Number of simultaneous active PPP sessions	20,000
ii	Number of PPP sessions which can be enabled for header or payload compression without any adverse affect	50% of above
iii	Throughput assuming packet size of 512 byte	50 Mbps
iv	Number of call setups and tear downs per second	300
v	Number of simultaneous VPN tunnels using L2TP or PPTP Protocols with encryption disabled	3,000
vi	Number of simultaneous VPN tunnels using L2TP or PPTP Protocols with encryption enabled	2,000
vii	Number of simultaneous PDSN-HA tunnels (Mobile IP sessions)	10,000

9.2 Home Agent - The HA shall be able to support atleast:

i	Number of user bindings	: 1,20,000
ii.	Number of user bindings per second or session set up rate	: 5,000
iii.	Throughput	: 500 Mbps
iv.	Number of FA-HA tunnels	: 1,20,000
v.	Number of PDSN-HA tunnels to support VPNs with IPSec	: 3,000

9.3 AAA server – The server shall be able to support atleast:

(i) 5,00,000 simultaneous active sessions when configured for maximum capacity
(ii) 4 million subscribers handling 2,000 transaction per second (TPS) at 70% loading
(iii) Definition of 2.5 million subscribers in less than 90 minutes
(iv) Maximum response time of 180 milliseconds per RADIUS message at maximum load for at least 90 % messages

CHAPTER - 10

10. INTERFACES

10.1 Full Technical details regarding implementation of interfaces (at each standard reference point)amongst different network elements as well as with other networks shall be provided and no interface shall be proprietary in nature. The block schematic showing the network and interfaces is at annex1.

10.2 **Interface between PDSN & BSC** (at the Aquater reference point) (R-P Interface): This interface shall be A10/A11 interface as defined in IOS ver. 4.0 .The bearer path shall be A10 connection and shall use Generic Route Encapsulation (GRE) to carry PPP bearer traffic over IP. The signaling path shall be A11 connection based on Mobile-IP with extensions over UDP/IP. It shall be implemented using E1 links, upgradable to E3/STM-I links. Support for Ethernet interface may also be optionally provided. E1 interface may be internal or external to PDSN. In cases where only Ethernet Interface is provided on the PDSN and the BSC and the PDSN are not co-located, provision shall have to be made to transport IP over WAN interfaces such as E1/E3/STM 1 by using a suitable router.

10.3 **Interface between PDSN and AAA** (RADIUS interface) - This interface shall be based on the RADIUS protocol defined by RFC 2865 and RFC 2866. The RADIUS client shall reside in the PDSN. The physical/link connection shall be via the Access Network using 100BaseT / 1 Gbps Ethernet. The PDSN shall pass UDR onto AAA via this interface.

10.4 **Interface between PDSN and HA/IP Network (Pi interface**) : This interface shall support registration submitted by the Mobile/Mobile Proxy agent for Mobile IP/Proxy Mobile IP operation. The physical/link connection is via the Access Network using 100BaseT /1 Gbps Ethernet.

The tendering authority, at the time of tendering may select, as per their requirement, the types of interfaces required as well as the number of such interfaces and ports.

CHAPTER - 11

11. SERVICES

11.1 Data Services :

It shall support packet switched High Speed Data Services Up to 144 Kbps – service options based on TIA/EIA/IS-707.

11.2 Prepaid Billing

PDSN shall support the prepaid billing solution based on the RADIUS (AAA) server and existing flow-based accounting functionality. It shall support real-time monitoring and rating of data calls for prepaid users. The prepaid billing feature shall provide the following services:

- Simple IP-based service metering in real time
- Undifferentiated Mobile IP service in real-time with support for multiple Mobile IP flows per user
- Rating based on per flow data volume, octet or packet count, and call duration.

The PDSN shall perform real time usage tracking on a per pre-paid user basis and compare the usage of that session against a prepaid account balance (measured in time or bytes) sent to the PDSN during call set up. When the usage for the current session depletes the account balances, the PDSN shall either kill the call or re-direct traffic to a registration server. Further the real time usage information must be transferred to the target PDSN during Inter-PDSN handoff to ensure continuation of pre-paid session and no revenue leakage.

11.3 WIN Services

The PCN shall be able to interwork with the Wireless Intelligent Network as described in the TEC GR No. GR/MSC-01 and details/status regarding implementation of the WIN services as specified in TEC GR No. GR/MSC.01 shall be indicated. In case of non-support of certain features, their roadmap for future support may be indicated.

The tendering authority, at the time of tendering may specify the services/ features required to be supported by the equipment.

CHAPTER – 12

12. TENDERING INFORMATION

12.1 The versions of all the documents mentioned in this GR may be reviewed and updated, if necessary. Refer clause 1.1 and clause 2.27.

12.2 Field Proveness and interoperability: The tendering authority may mention the requirement of equipment being deployed in multiple countries and networks and minimum period of deployment which may be atleast six months or any other period more than six months, as decided by the tendering authority. Tendering authority may also specify the various technologies / vendors of Radio Networks (RN), Packet Core Network (PCN) and associated sub systems with which this system has to interoperate Refer clause 2.2

12.3 The registration methods required to be supported in the equipment may be specified. Refer clause 2.8.

12.4 The tendering authority may indicate the type of interfaces required to be supported and obtain information from the vendor regarding associated hardware/ software required for integration to NIB Phase I and Phase II. Refer Clause 2.10

12.5 The tendering authority may indicate the software/hardware upgrades for services and features required in future along with the commercial terms for the same. Refer clause 2.19.1 (xi).

12.6 The tendering authority may specify the period for which the spares are required. Refer clause 2.23 (vii) and clause 4.11.

12.7 The tendering authority may specify at the time of tendering whether the hardware and software required for automated provisioning of services is required or not.. Refer clause3.5

12.8 The tendering authority may specify whether a mediation device for co-relation of CDRs and UDRs for packet charging for packet data access and for applications is to be provided or not. Refer Clause 4.2.6

12.9 The tendering authority at the time of tendering may specify whether for PDSN the support of exterior routing protocols like BGP4 is required. Refer Clause 5.4 and clause 7.5.

12.10 The tendering authority may specify the type of NMS (if at all) which the OMC of PCN would be required to interface with and accordingly any additional hardware/ software (if required), shall be provided by the vendor for interfacing with the NMS. Refer clause 8.3.

12.11 The type of interfaces as well as the number of such interfaces and ports may be indicated. Refer chapter 10 on ‘Interfaces’.

12.12 The tendering authority may specify the services/features required to be supported by the equipment. Refer Chapter 11.

12.13 The requirement of the test Instruments may be indicated.

Note: *TEC validation of the equipment is done under test/simulated conditions. Field Trial also is done with partially installed system and with limited number of test subscribers. It may not truly reflect the performance of the system in the filed. Hence, the network (of which the equipment covered under this GR is a part) should be retested for its performance after its complete commercial deployment under loaded condition, for a suitable time period. Accordingly, necessary provision may be made in the tender.*

CHAPTER - 13

REFERENCES

TEC Documents

GR/BCS-01	-	Billing and customer care system for cellular mobile system
GR/LIS-01	-	Requirements of switching systems for lawful interception and monitoring
GR/MSC-01	-	MSC based Core Network for CDMA 2000 1x system
G/NIB.01	-	National Internet Backbone (NIB)
GR/VPN-01	-	GR for BGP/MPLS Virtual Private Network –
GR/WLL-04	-	RN of WLL Systems based on CDMA 2000 1x Standards
TD/CDR-01	-	CDR based billing system for PSTN
SD/EMI-02	-	Electromagnetic compatibility standard for telecommunication equipment

QA Documents of BSNL

QM-115	-	Guidelines for Computing Reliability Figures.
QM-205	-	Guidelines for Standard of Workmanship for Printed Boards.
QM-206	-	Guidelines for Standard of Workmanship for Printed Board Assemblies.
QM-210	-	Acceptability of Printed Board Assemblies Containing SMDs.
QM-301	-	QA Requirements for Transmission Equipment.
QM-324	-	Guidelines for Computing Reliability Figures.
QM-333	-	Specification for Environmental testing of Sw. and Tx. Equipments
QM-351	-	QA Requirement for switching equipment.

.

ITU –T Standards

M-3010	-	Principles for a telecommunications management network (TMN)
M-3020	-	TMN interface specification methodology.
Q.513	-	Digital exchange interface for operations, administration and maintenance
Z.301 to Z.341	-	Specifications pertaining Man-machine Language (MML)
Z.314	-	Character set and basic elements of MML
Z.322	-	Capabilities of visual display terminals

ITU-R Standards

M-1457	-	Detailed specifications of the radio interfaces of IMT-2000.

Other standards

CISPR 22 (2003)	-	Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment"
IEC 215 (1987)	-	Safety requirements of radio transmitting equipments (for Radio equipments only)
IEC 61000-4-2 (2001)	-	Testing and measurement techniques of electrostatic discharge immunity test.
IEC 61000-4-3 (2002)	-	Radiated RF electromagnetic field immunity test.
IEC 61000-4-4 (1995) (with amendments 1&2)	-	Electrical fast transients/burst immunity test.
IEC 61000-4-5 (2001)	-	Test & Measurement techniques for Surge immunity tests.
IEC 61000-4-6 (2001)	-	Basic Immunity standard.

International Quality Standard

ISO-9001:2000	-	Quality Management System – Requirement

ANSI/EIA/TIA Standards

IS-707	-	Data Service Options for Spread Spectrum Systems
IS-835	-	Wireless IP Network
IS 8473 (1993)	-	Guide on the effects of current passing through the human body (equivalent to IEC publications 479-1 (1984).
IS 13252 (1992)	-	Safety of information technology equipment including electrical business equipment (equivalent to IEC publication 95 (1986)
TR45.6	-	Adjunct Wireless Packet Data Technology – Mobile & Personal Communications Standards.

3GPP2 Standards

A.S0001	-	Access Network Interfaces Inter-Operability Specifications (ISO)
C.S0002	-	CDMA 2000 System – Physical Layer
C.S0003	-	CDMA 2000 System – Layer 2 (Link Layer)[MAC sub-layer
C.S0004	-	CDMA 2000 System – Layer 2 (Link Layer)- LAC sub-layer
C.S0005	-	CDMA 2000 System – Upper Layers
P.R0001	-	Wireless IP Architecture Based on IETF Protocols
P.S0001	-	Wireless IP Network Standard

TSG-X - Specifications

X.S0011-001	-	CDMA2000 Wireless IP Network Standard (Introduction)
X.S0011-002	-	CDMA2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services
X.S0011-003	-	CDMA2000 Wireless IP Network Standard: Packet Data Mobility and Resource Management

X.S0011-004	-	CDMA2000 Wireless IP Network Standard: Quality of Service and Header Reduction
X.S0011-005	-	CDMA2000 Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs
X.S0011-006	-	CDMA2000 Wireless IP Network Standard: PrePaid Packet Data Service
X.S0016.340	-	MMS

IETF RFCs

RFC-791	-	Internet Protocol
RFC-1144	-	Van Jacobson TCP/IP header compression
RFC-1332	-	IPCP
RFC-1334	-	PPP Authentication Protocols
RFC-1661	-	PPP
RFC-1662	-	PPP byte oriented HDLC.
RFC-1701	-	Generic Routing Encapsulation
RFC-1918	-	Address Allocation for Private Internets
RFC-1962	-	PPP Compression Control Protocol (CCP)
RFC-1974	-	PPP Stac LZS Compression Protocol
RFC-1994	-	CHAP
RFC-2002	-	Ipv4 Mobility
RFC-2003	-	IP Encapsulation within IP
RFC-2005	-	Applicability Statement for IP Mobility support
RFC-2006	-	The Definitions of Managed Objects for IP Mobility Support
RFC-2118	-	Microsoft Point-to-point compression
RFC-2344	-	Reverse Tunneling for Mobile IP
RFC-2394	-	Deflate PPP compression
RFC-2474	-	Definition of Differentiated Services field
RFC-2475	-	Architecture for Differentiated Services
RFC-2486	-	NAI based on MSID of MS
RFC-2597	-	Assured Forwarding PHB
RFC-2598	-	An Expedited Forwarding PHB
RFC-2785	-	Methods for Avoiding the “Small-Subgroup” Attacks
RFC-2794	-	Mobile NAI Extension
RFC-2865	-	Remote Authentication Dial In User Service (RADIUS)
RFC-2866	-	RADIUS Accounting
RFC-2890	-	Key and Sequence Number Extension to GRE
RFC-3012	-	Mobile IP Foreign Agent Challenge/ Response Extension
RFC-3024	-	Reverse Technology for Mobile IP
RFC-3220	-	IP mobility support for Ipv4

Note: All references are w.r.t. the latest versions/releases along with all amendments/addendums.

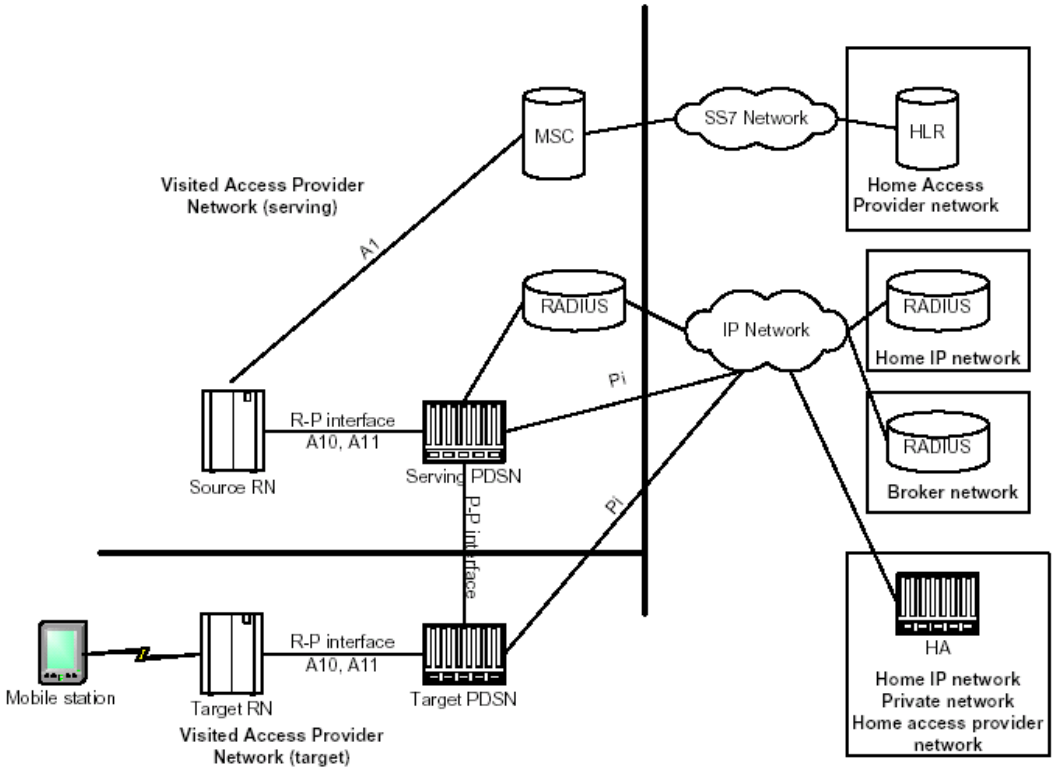
CHAPTER – 14

GLOSSARY

3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
BSC	Base Station Controller
BGP	Border Gateway Protocol
BSNL	Bharat Sanchar Nigarm Limited
CD-ROM	Compact Disc Read Only Memory
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter Domain Routing
CMIP	Common Management Information Protocol
CRI	Call Related Information
Diff Serv	Differentiated Services
DOT	Department of Telecommunications
DS	Differentiated Service
EIA	Electronic Industry Association
EMC	Electromagnetic Compatibility
FA	Foreign Agent
GR	Generic Requirements
GRE	Generic Route Encapsulation
GUI	Graphical User Interface
HA	Home Agent
HDLC	High-Level data Link Control
I/O	Input /Output
IEC	Internet Key
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Industry
IMSI	International Mobile Subscriber Identity
IPSEC	IP Security
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version4
Ipv6	Internet Protocol version6
IS	Interim Standards
ITU-R	International Telecommunication Union-Radio
ITU-T	International Telecommunication Union-Telecom.
L2TP	Layer 2 Tunneling Protocol
LAES	Lawfully Authorized Electronic Surveillance
LCP	Link Control Protocol
MMC	Man-Machine Commands
MML	Man-Machine Language
MN	Mobile Node
MSID	Mobile Station ID

MTBF	Mean Time Between Failure
MTNL	Mahanagar Telephone Nigam Limited
MTTR	Mean Time to Restore
NAI	Network Access Identifier
NIB	National Internet Backbone
NMS	National Management System
OMC	Operation and Maintenance Centre
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PCB	Printed Card Board
PCF	Packet Control Function
PCN	Packet Core Network
PDSN	Packet Data Serving Node
PHB	Per Hop Behavior
PPP	Point to Point Protocol
PPTP	Point-to-Point Tunneling Protocol
Q.O.S.	Quality of Service
QA	Quality Assurance Circle of BSNL
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RFC	Requests for Comments
RIP	Routing Information Protocol -2
R-P	RN-PDSN Interface
RRQ	Mobile IP Registration Request
RS	Remote Station
SMIv2	Structure of Management Information version 2
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
TCP/IP	Transmission Control Protocol/Internet Protocol
TEC	Telecom Engineering Centre
TIA	Telecom Industry Association
TMN	Telecom Management Network
TPS	Transaction Per Second
UDR	Usage Data Records
VPDN	Virtual Private Dialup Network
VPN	Virtual Private Network
WLL	Wireless in Local Loop

Annex-I



Network Reference Model for PCN (Ref. 3GPP2 P.S0001)

End of the Document