Yemen Mobile PDSN Unified PS (GW) Technical Specification

Introduction

Yemen Mobile Company is developing towards the new advanced integration of multiple services and multiple networks. However service platforms built by most operators are still independent which leads to complicated networking facilities, redundant construction of the public parts of many platforms, expansion and technological update, and hence a waste of human resource. Yemen Mobile main target is to offer a new advanced PS (GW) equipment as a unified PS platform which also working as Foreign Agent (FA), Home Agent (HA) and HSGW for CDMA network for the end user, while keeping control on the global incoming revenues.

Important Note: **All the following project components, services, functions, features, capacities and protocols are mandatory provided by software and required hardware, and it will introduce in the technical and financial proposal.**

Project Components:

Features and Functions	Description
PDSN/HSGW	Required unified PS Gateway must be designed in strict accordance with the 3GPP/3GPP2 specifications. PDSN and HSGW functions must be integrated together hardware and software in your offer. For guaranteeing continuity of existing CDMA services, it should include services and subscribers of CDMA,EVDO (Rev.0-Rev.A-Rev.B) and LTE at the same time using single Network Element. And resource sharing must be based on any 3G/LTE service ratio.
HA	This PS (GW) also must be designed to work as Home Agent logically or physically to provide MIP and handover between this PDSN and other PDSNs that are provided by any vendor.
Simple IP	PS (GW) includes simple IP access function. When an MS launches a packet service, the PDSN assigns an IP address to the MS when a Point-to-Point Protocol (PPP) connection is

	set up. When the packet service is over, this IP address is released.
Mobile IP	PS (GW) obeys the regulation of RFC2002, RFC3344 and 3GPP2. It is capable of FA and HA functions, and provides mobile IP service of mobile IP terminal users. The mobile IP (MIP) is a solution for providing mobility on the IP networks. The MIP enables a node to keep its ongoing communication free of interruption even if the node switches from one network to another. A home address is used as a permanent address to connect to any other network.
Proxy Mobile IP **PMIP**	PS (GW) should include bearing PMIP function, which provides proxy mobile IP function for users who use simple IP terminal, and keeps service continuity of **inter-PDSN/FA** handover during the mobility. The Proxy Mobile IP (PMIP) function of the PDSN is integrated with the PPP function so that the PDSN, instead of the MS, can perform registration, update, and maintenance of the MIP. Therefore, the MS software does not need to support the MIP function.
Handoff Management	PS (GW) also should handle handoff between FAs of mobile IP users. The IP address remains the same in the handoff process. PDSN supports PCFs handoff under activation and dormancy situation. In the handoff process, PPP session and IP address of the user are not changed to keep session continuity and ensure user service experience.
Reliability	Considering high reliability in terms of : Hardware (Board and Module, Data Channel and Power) Software (Distributed System Architecture, Hot Backup, Overload Control, Fault Location and Lock Mechanisms) Networking (Physical Interface, Routing and Disaster Tolerant) Provide excellent disaster redundancy standby solution for packet domain, and highly-reliable network architecture and service security.
Security	PS (GW) should include ACL, Source Address Filtering security mechanism and IP Security (IPSec) protocol, which provides IP packets with high-quality, interoperable, and cryptology-based

	security. Also includes control policies that can be configured according to source IP, destination IP, source port, destination port, protocol type, etc. PDSN controls packets according to these control policies.
Large Capacity	PS (GW) should be based on the self-developed high performance router platform. Based on the advanced hardware platform and technology, with the modular design, large capacity and high integration are featured. Processing of signaling/control should consist of multiple universal processors that are of high performance. Also the data processing should consist of multiple network processors that are of high performance and high forwarding capability.
RADIUS Client	This function to enable PS (GW) sends RADIUS authentication request packet that is made up of user name and password provided when the user accesses to the external RADIUS server for authentication. Both PAP and CHAP authentication modes are supported. This module also provides RADIUS charging function. Remote Authentication Dial In User Service (RADIUS) client is a feature that enables the PDSN to provide the following functions: Functioning as an authentication client Functioning as an accounting client Striping a domain name from a user name Using configurable port numbers to communicate with the authentication, authorization and accounting (AAA) server. PDSN sends RADIUS authentication request packet, which consists of user name and its password provided when the user accesses to the external RADIUS server for authentication. Both PAP and CHAP authentication modes are supported. This module also provides RADIUS charging function.
IP Routing	The new System should include routing function with at least : IPv4/IPv6 Static Route and Default Route IPv4v6 Dual Stack Routing Policies Route Backup

	IP Policy Based Routing RIPv1/v2 OSPFv2 BGP-4 IS-IS IP MPLS Static User Downlink Route Distribution
QoS Management	The new System should include Quality of Service (QoS) which is a basic function that allows operators to optimize the use of network resources and accommodate traffic for satisfying the needs of end-user. Also, QoS management makes it possible for operators to offer a richer variety of services and a higher level of service personalization. In other words the multiple QoS implementation technologies feature enables the PDSN to implement QoS technologies such as traffic classification, resource monitoring, traffic policing, congestion management, and congestion avoidance.
Charging	The new System should have both prepaid and postpaid charging. As the Radius client, PDSN is responsible for collecting the charging information about the MS and sending it to the AAA through the RADIUS message. As a pre-paid client, PDSN obtains the traffic quota and traffic threshold from CBS through the Diameter message. Packet prepaid is a type of prepaid service that allows subscribers to purchase credit in advance of service use. For prepaid data service, credit refers to a certain period of time or traffic volume. The usage of credit (time or volume) by subscribers is traced and the used credit is deducted from the account balance in real time.
DPI Function	DPI (Deep Packet Inspection) engine should be embedded to parse the packets from layer 3 to layer 7. Source IP address, port, destination IP address, port, URL, character string and application event are used to identify the traffic. Thus, user information such as duration, data volume and event of different service could be extracted to implement refine charging and service analysis. PDSN acquires dynamic control and charging

	policies by local DPI identification protocol and application type, and performs multi-dimensional control and charging according to user, service, location, time, access mode, usage, etc.
PCEF Function	PCEF (Policy and Charging Enforcement Function) should be embedded in this PDSN as required part to acquire dynamic control and charging policies by local DPI identification protocol and application type, and performs multi-dimensional control and charging according to user, service, location, time, access mode, usage, etc to enable the system manage and control the user bandwidth.
O&M Center Management	The Operation and Maintenance Center shall allow fault management, performance monitoring, configuration management, load management, security management, user management, system management, log management, report management, CPU monitoring, memory monitoring, buffer monitoring ,license /speed by account level monitoring, and O&M tools. The performance management feature in new system enables the Network Management System or the local maintenance terminal to monitor, collect, and store the performance data about the PDSN. This New PDSN GW and its surrounding networks are monitored.
Tracing and Monitoring	Subscriber and Interface tracing are features that enable the PDSN to trace and parse signaling and data packets based on network access identifiers of subscribers and interface IP, and display the results on the local maintenance terminal .Also PDSN performs real-time performance monitoring.

Interfaces and Protocols	Description
Between PDSN(GW) and other FAs	MIP Signaling Interface that works with any standard encapsulations (GRE-IP-in-IP…) PDSN GW can be connected to FAs that are provided by any vendor.
Between PDSN(GW) and AAA	Radius Interface compliant with any standard protocols as RFC2865, RFC2866, and RFC2869 with Pi interface.

	PDSN GW can be connected to AAAs that are provided by any vendor.
Between PDSN(GW) and CBS	DIAMETER Protocol and Gy interface. PDSN GW can be connected to Billing System that is provided by any vendor.
Between PDSN(GW) and PCFs	R-P interface which referred to as A10 / A11 interface in the specification 3GPP2 A.S0001 .PDSN GW can be connected to PCFs and BSCs that are provided by any vendor.
PDSN(GW)/LAC and LNS	To support the data VPN service uses the L2TP protocol.
Between PDSN(GW) and LIC/LEA	LIG (Lawful Interception Gateway) is used to provide H1, H2, and H3 interface to LIC/LEA
Between PDSN(GW) and PDN	Standard IP protocol
Between PDSN(GW) and NTP	NTP (Network Time Protocol) for PDSN (GW) to obtains standard time from an external NTP server provided by any vendor.
Between PS(GW) and PCRF	Gx interface that is used based on Diameter protocol. PDSN GW can be connected to PCRF that is provided by any vendor.
Between PS(GW) and LTE Core Network	Should include all Standard LTE interfaces (such as S103, S2a…etc) and their related Protocols that enable this PDSN (GW) to work as HSGW and smoothly connect to LTE Core Network (P-GW,S-GW….).which is provided by any vendor.

Software Capacities	Description
Number of proxy mobile IP users	5.000 users.
Data forwarding throughput	1000 Mbps.
Number of PPP connections activated	100,000 sessions.

at the same for different services.	
Number of packet prepaid subscribers	100,000 subscribers.

Hardware Capacities	Description
Number of mobile IP users	HW must handle the minimum number of mobile IP users supported not less than 1 million.
Number of proxy mobile IP users	HW must handle the minimum number of proxy mobile IP users supported not less than 1 million.
Data forwarding throughput	HW must handle the minimum number of Data throughput not less than 30Gbps.
Number of PPP connections activated at the same for different services.	HW must handle the minimum number of ppp sessions not less than 1,000,000.
Number of packet prepaid subscribers	HW must handle the minimum number of prepaid subscribers not less than 1,000,000.
The main processing unit	Should be N+1 and working as load sharing .Processing units should meet all required capacities and features mentioned.
Network Equipments	HW should include all network equipments like firewalls and Lan-switches that are necessary to connect and protect the system internally and externally.
Spare Parts	HW should include all the spare parts necessary for the main units in the system.

1. PDSN (GW) as HSGW

This PDSN (GW) is required to be implemented with HSGW (HRPD Serving Gateway) function in order to:

- Enables Inter-Technology Handoff Between LTE and EV-DO Networks
- Enables Roaming For LTE Subscribers On EV-DO Networks

– Leverages Existing EV-DO Network Coverage When Deploying LTE

– Enables common applications to be used across EV-DO & LTE Access.

So this PDSN(GW) Should include all Standard LTE interfaces (such as S103, S2a…etc) and their related Protocols that enable this PDSN (GW) to work as HSGW and smoothly connect to LTE Core Network (P-GW,S-GW….).

2. PDSN(GW) as HA

HA and FA perform mobile IP users packet data session access service to Intranet and

Internet. Mobile terminals could be used with its home IP address in any roaming place. HA provides data services forward to home location for wireless packet data users, and receives data services sent to mobile IP users, provide data forward tunnel to FA for Mobile IP users. In our case we need HA system to perform PMIP (Proxy mobile IP) solution which will be used to solve the problem caused by the shortage of commercial MIP client software. The Proxy Mobile IP (PMIP) function of the PDSN is integrated with the PPP function so that the PDSN, instead of the MS, can perform registration, update, and maintenance of the MIP. Therefore, the MS software does not need to support the MIP function.

3. Multi-vendor Support:

Standard compliant & Multi-vendor Support: System shall be based on standards mentioned in Standards Requirements.

New PDSN GW should be imbedded with standard interfaces and protocols to connect to other Systems such as PDSN FAs, AAA System, Billing System, PCFs in BSCs, PCRF, NTP and any Systems (such as LTE System) that will be connected to PDSN GW either these systems are provided by the same vendor or different vendors. IOT test report with current vendor systems (Huawei BSCs, PDSN FA, AAA System and ZTE BSC).

4. Simple IP

When an MS launches a packet service, the PDSN (GW) assigns an IP address to the MS when a Point-to-Point Protocol (PPP) connection is set up. When the packet service is over, this IP address is released.

It is easy to enable the simple IP access mode. The IP address is assigned only when it is needed. Thus the demand for the amount of IP addresses is relatively small. The simple IP mode, however, only supports packet services initiated by an MS. If the MS switches from one PDSN to another, it must interrupt the current packet service and set up a PPP connection with the new PDSN.

The simple IP mode involves two network elements (NEs), the PDSN and the AAA server.

The basic service flow of the simple IP mode performed by the PDSN is described as follows:

An MS launches a packet service request. A PPP link is set up between the MS and the PDSN through the radio access network (RAN).

The PDSN communicates with the AAA server for authentication of the MS.

After the authentication, an address is assigned by the PDSN or from the AAA server at the request of the PDSN.

The PDSN then connects the MS to the external public data network (PDN) in IP mode. The PDSN collects the charging information and sends it to the AAA server.

If the user initiatively exits from the network or performs no operation for a long time, the PDSN launches a flow to release the IP address of the MS.

PDSN supports CDMA2000 simple IP access function

When user is accessing, PDSN performs PPP session negotiation with user, and sends user authentication and function authorization to AAA, allocates IP address and related resources for user. After user is successfully accessing, PDSN performs volume and duration accounting statistics.

5. Mobile IP

The mobile IP (MIP) is a solution for providing mobility on the IP networks. The MIP enables a node to keep its ongoing communication free of interruption even if the node switches from one network to another. A home address is used as a permanent address to connect to any other network.

The simple IP mode supports only the packet data services that are started by the MS. When the MS moves from one link to another (when the MS switches from one PDSN to another), the current packet service must be interrupted and the IP address must be reassigned or renegotiated. To solve the problem of increasingly frequent MS mobility, the CDMA2000 packet service solution has enabled the MIP.

That is, with the MIP technology, when an MS switches from one PDSN to another, the current IP address and the ongoing session remain as they are and the data service is not interrupted.

In MIP mode, apart from the PDSN and the AAA server, the HA is also one of the networking elements (NEs) of the core network packet-switched domain. At the same time, the PDSN also integrates the FA function.

The MIP service flow of the PDSN is as follows:

1. An MS launches a packet service request. A PPP link is set up between the MS and the PDSN/FA through the RAN.
2. The PDSN/FA sends agent advertisement messages to inform its FA services. Such a message carries a certain IP address of the PDSN/FA. This IP address serves as the foreign agent care-of address of the MS.
3. The PDSN/FA checks whether the MS is legal through the authentication messages between the PDSN/FA and the AAA Server. When the MS passes the authentication, the PDSN/FA forwards the registration request of the MS to the HA.
4. The HA checks whether the registration request is valid, assigns a home address for the MS. The address can be assigned through the local address pool or by the AAA sever. The HA creates a mobility binding table that shows the mapping between the home addresses and the foreign agent care-of addresses. The HA also sets up a tunnel to the

PDSN/FA, and then sends the registration reply message to the PDSN/FA. The PDSN/FA then forwards it to the MS.

5. The HA informs that the network prefix of the MS home address can be reached. Then, the packets destined to the MS home address are routed to the home network. The HA delivers these packets to the PDSN/FA through the tunnel. Then, the PDSN/FA obtains the original packets from the tunnel and forwards them to the MS.
6. In the reverse direction, the packets from the MS follow the simple IP forwarding flow and are delivered directly to the destination node on the PDN with the PDSN/FA as the default router rather than through the HA. If a reverse tunnel is used, the packets can reach the HA through the reverse tunnel between the PDSN/FA and the HA, and then be forwarded by the HA.

6. Proxy Mobile IP

The Proxy Mobile IP (PMIP) function of the PDSN is integrated with the PPP function so that the PDSN, instead of the MS, can perform registration, update, and maintenance of the MIP. Therefore, the MS software does not need to support the MIP function.

The PMIP solution can be used to solve the problem caused by the shortage of commercial MIP client software. Thus, the PMIP feature is a substitute of the MIP solution.

The PMIP service flow realized by the PDSN is described as follows:

1. The PDSN generates the authentication request of the MS and then forwards it to the AAA server for authentication.
2. If the authentication result shows that the MS is a PMIP user, go to 3. If the PDSN/FA cannot determine whether the MS is a PMIP user based on the authentication result, it determines based on the configuration information of the domain to which the MS belongs. If the PMIP flag of the domain is enabled, the MS is a PMIP user. Go to 4.
3. If the MS is successfully authenticated to use the PMIP service provided by the PDSN/FA, the AAA server returns the registration data of the MS and the address of the HA.

4. The PDSN/FA searches the registration data and the HA address that are bound with the domain to which the MS belongs.
5. The PDSN/FA uses this information and other data to send a registration request (RRQ) message to the HA for the MS.
6. If the registration is successful, the HA sends a registration reply (RRP) message that contains the IP address to the PDSN/FA.
7. The PDSN/FA assigns the IP address obtained from the RRP to the MS through the IP over PPP (IPCP).
8. Between the HA and the PDSN/FA, a tunnel is set up for transmitting the uplink and downlink packets of the MS.

7. High Reliability

This describes the high reliability feature of the PDSN (GW). Reliability is crucial for both operators and end users. Therefore, the PDSN (GW) is designed by considering reliability in terms of hardware, software, and networking to ensure normal running.

- The hardware adopts comprehensive double-star redundancy structure, and supports board redundancy backup mechanism, provides reliability for data and control tunnel, and provides protect mechanism such as Anti-jamming power and Anti-lightning, etc.
- The software adopts distributed redundancy backup mechanism, and provides overload control, flow control, hot backup, hot patch, Local UDRs Storage, etc. The system provides perfect operational monitoring mechanism so as to assure system smooth running and prevent user information and bill file from losing.
- Network organization adopts perfect dual-networking and dual-plane structure, provides interface backup mode and route backup mode, and supports Disaster Tolerance mechanism.
- Provide excellent disaster redundancy standby solution for packet domain, and highly-reliable network architecture and service security.

8. Security

PDSN (GW) should include ACL and Source Address Filtering security mechanism:
Some control policies are configured in PDSN (GW), according to source IP, destination IP, source port, destination port, protocol type, etc. PDSN (GW) will control packets according to control policies.
PDSN (GW) supports to filter source IP address for MS.

This describes the security feature of the PDSN (GW). The requirements for security are taken into consideration for the design of the PDSN (GW) and multiple measures are adopted to protect profits of operators and end users.

The same as reliability, security is concerned by operators and end users. The requirements or security is fully considered for the design of the PDSN (GW) and the following measures are taken:

- Strict verification of operator identity
- Point-to-Point Protocol (PPP) security verification by the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) modes
- Packet filtering and access control list (ACL) mechanism to filter packets based on preset conditions
- Pi interface redirection function, which can offer defense against attacks that are based on protocol packets between mobile users in one PDSN
- IP Security (IPSec) protocol, which provides IP packets with high-quality, interoperable, and cryptology-based security

9. O&M Centre Management

The Operation and Management Center shall allow fault management, performance monitoring, configuration management, load management, security management, user management, system management, log management, report management, CPU monitoring, memory monitoring, buffer monitoring ,license /speed by account level monitoring, and O&M tools.

9.1 Performance and Fault Management

The administration interface shall show the status of each part of the System:
running
stopped
failed
overloaded (in case of insufficient resources)
Alarms on the different components.

The supplier shall provide a solution to supervise and administrate remotely the System. The Tender should describe the interfaces that are available for Monitoring of the System from operator's OSS.

9.2 Configuration and Other Management tools

Allow globe service configuration tasks by performed both via a GUI (Graphical User Interface) and BI (Batch Interface) also it could be performed by Command Line Interface.

9.2 Backup & Recovery Solution

A reliable solution for storage and backing up of data (user data, and configurations) including data recovery for the Node after system error/failure.
The Tender should describe the own backup solution.

9.3 High availability and Redundancy

The requirements in terms of redundancy are listed below:
Redundant components in all servers: CPUs, RAMs, Ethernet cards…etc.
All databases should work in clustered mode (2N), where the backup node automatically takes over when the active one fails.
Traffic is load shared on main process units.

The Tender shall specify which are the main performance characteristics and describe the KPI's to measure the performance of the system.

The Tender shall specify the values for the system availability KPI's:

Availability

Mean time between failures per module.

Mean time to repair per module.

No part of the system shall be a single point of failure.

Tender shall elaborate on how the solution handles peak traffic bursts (overload on call setup requests), for instance New Years Eve and Holiday of Eid. Preferred method is to drop the latest incoming call-setups to the system maximum.

9.4 Alarm and Network Management Modules

All the service modules can connect to monitoring and management system through SNMP and current report alarms (U2000) from Huawei and performance data to it. Topology and View Management shall be supported in monitoring and management system through network topology status monitoring, view management, Please describe the detailed topology and view management modes.

The distributed hierarchical structure based on B/S shall be supported for unified alarms modules.

Alarm module shall be made up of collection layer, application layer and presentation layer. The application layer falls into alarm analysis, alarm query, alarm collection, alarm processing, alarm statistics, alarm reports, alarm configuration, and fault bills. Modules in Presentation layer can be customized according to users' operation habits.

Alarm information processing shall support information filtering, alarm confirmation, alarm clearance, alarm notification, alarm synchronization, alarm re-definition, and alarm processing Module functions

A friendly alarm information query interface and combined querying conditions shall be complied shall be supported. And the history information shall be queried.

Statistics results shall be displayed with tables and graphs, and shall be printed. Information statistics classified by module, type, etc are given in reports (period, times, etc).

Alarm management system shall conduct dependency analysis of received alarm information and then conducts location and diagnosis of faults that have occurred in the system, assisting users with troubleshooting and reducing impacts of system faults on the operation quality of the whole network.

Alarm setting shall be flexible and displayed in a visual way. The multiple alarm modes such as host visual & audio alarm prompt, alarm box prompt, email releasing, handset short message sending (releasing), etc shall be chosen by the users.
Fault bill generation mechanism shall be supported, please describe the detailed info.

10. Operation and maintenance Support Service Requirement:

The vendor must offer (24 months) warranty period and Operation and maintenance as follow:

Technical Support Service	Help Desk
	Telephone Support
	Remote Access
	On-site Troubleshooting
	Emergency Recovery
Software Support Service	Software Diagnosis and Correction
	Software Update
	First Node Implementation
Hardware Support Service	Repair and Return
Knowledge Database Service	Knowledge Database Service
Outsourced Products Service	Outsourced Products Service
Inspection Service	Inspection Service

11. Roadmap:

The bidder shall present the roadmap during the period 2014-2020 of his equipment highlighting for each release the following details:
-Changes in architecture (New network elements, concepts, etc.)
-Changes in hardware (Platform technology, Transport technology, etc.)
-Changes in features (New, altered and upgraded features) Detail optional and basic features.

***The vendor must provide the solution in detail (as optional) of the Hardware, Software and Features changes either in New PDSN GW or as separated solution to immigrate to LTE System.**

12. Implementation Requirements

This part of the document shall address the Implementation and Project Management requirements and responsibilities for both the operator and the provider, deemed essential towards the successful implementation of the Operator's Platform.

12.1 Site specifications

Hardware layout should be provided in the offer. Length, width, depth, height and square meters used should be given. The space needed above the system for height should be given. Hardware weight shall be provided in the offer.

Power consumption should be provided in the offer. The offer will provide the recommended power requirements; this will include peak and normal operation. Offer will also include grounding requirements and locations of power distribution cabinets in the floor plan. Redundancy power supply is mandatory. Power input: -48 VDC is preferred by the operator.

Environmental limits to be provided. This includes relative humidity and temperature needed, and the platform heat generation.

Auxiliary equipment should be provided in the offer. This includes needed access terminals. Offer shall provide the total space needed for the equipment and control

equipment (rack mountable console, monitors, etc.) and description of each hardware module.

Detailed technical design, defining the detailed specifications for the solution to be delivered and integrated in the Operator's network.

Implementation phase comprises the execution of the planned equipment deliveries, installation, integration, commissioning and pre-acceptance Platform integration.

Acceptance phase comprises the acceptance testing of individual Platform nodes, as well as of the end-to-end Platform proving (including interconnection and interworking tests to other Platforms).

12.2 Implementation Phase

The offer shall provide the Operator Contract Liaison with detailed Implementation Plans for each of the major Platform components included in proposed solution.

The Delivery-Installation-Commissioning sequence shall be shown clearly on each of resourced Implementation Plans and the overall degree of overlapping activities indicated on a Master Implementation Schedule.

A provisional Master Implementation Plan shall be submitted in the offer.

13.SPARES

13.1 Mandatory Spares

Mandatory spares (for operation and maintenance) must be provided for all Boards, sub-system, and equipment in warranty period.

Spares must be provided from the same manufacturing facilities/location from where the respective equipment, subsystems are offered. Unit rates for each spares required for operation and maintenance shall be provided.

Vendor must provide the address, contact person, fax, telephone no. of the manufacturer of the spare parts. The Vendor must warrant that spare part for the system would be available for minimum of 10 years after system commissioning (taking over). After this period if the Vendor discontinues the production of the spare parts, then he must give at least 6 months notice prior to such discontinuation so that Purchaser may order the requirements of spares in one lot.

The list of the required spares being supplied with unit cost and total cost should be attached along with the bid.

13.2 Commissioning spares

The commissioning spare must be decided between the Vendor to bring the requirement during installation, commissioning, site acceptance testing, trial run and warrantee period. These spares shall be readily available with the Vendor. These commissioning spares are different from mandatory spares and Vendor must not use mandatory spares as commissioning spares.

14. Training Requirement

The advanced training course must focus on the following Objectives (for 4 persons):

The training course is advanced course with these main topics:

1- General PDSN (GW) operation and Maintenance.

2- PDSN as Home agent (HA) operation and Maintenance.

3- HSGW operation and Maintenance.

4- MIP management and configuration.

5- PDSN Handover Management.

6- PMIP management and configuration.

7- DPI management and configuration.

8- PCEF management and configuration.

Annex 1

The Key Items for Evaluation of New PDSN (GW) System:

S	Item	Compliance	Remarks
1.	**Sources and Capacities**		
1.1	Proxy mobile IP (PMIP)		
1.2	Throughput		
1.3	PPP connections		
1.4	Packet prepaid subscribers		
1.5	The main processing unit		
2.	**Hardware/Software**		
2.1	Disk storage		
2.2	DDR3 RDIMM		
2.3	CPU		
2.4	Interfaces		
2.5	Monitoring		
2.6	Network Equipment (Switches-Firewalls…)		
3.	**Features and Functions**		
3.1	HSGW		
3.2	HA (Home Agent)		
3.3	Multi-vendor Support		
3.4	Simple IP		
3.5	Handoff Management		
3.6	Reliability		
3.7	Security		
3.8	RADIUS Client		
3.9	IP Routing		

3.10	QoS Management		
3.11	Charging		
3.12	DPI Function		
3.13	PCEF Function		
4	**Protocols:**		
4.1	Between PDSN(GW) and other FAs		
4.2	Between PDSN(GW) and AAA		
4.3	Between PDSN(GW) and CBS		
4.4	Between PDSN(GW) and PCF		
4.5	PDSN(GW)/LAC and LNS		
4.6	Between PDSN(GW) and LIC/LEA		
4.7	Between PDSN(GW) and PDN		
4.8	Between PDSN(GW) and NTP		
4.9	Between PDSN(GW) and PCRF		
4.10	Between PDSN(GW) and LTE Core Network		
5	**O&M Center Management**		
6	**Operation and maintenance Support Service Requirement:** The vendor must offer (24 months) warranty period and Operation and maintenance.		
7	**Spares**		
8	**Training Requirement** The advanced training course must cover PDSN (GW) features Objectives (for 4 persons)		