System Release 7.17.2

ASTRO® 25

INTEGRATED VOICE AND DATA

Packet Data Gateways

Feature Guide

NOVEMBER 2017

MN004402A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN004402A01-A	Original release of the *Packet Data Gateways Feature Guide*	November 2017

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Packet Data Gateways Feature Guide

This manual includes procedures for installation and configuration of the Packet Data Gateway (PDG) and is intended to be used by field service managers and field service technicians.

The Motorola Packet Data Gateway (PDG) is designed to link a customers data network to the customers radio network. The Packet Data Service is a bearer service to connect two parties in a communication system with the IP protocol.

The PDG consists of two primary software application components, the Packet Data Router (PDR) and the Radio Network Gateway (RNG). The PDR provides an interface between the GPRS Gateway Support Node (GGSN) router and the Radio Network Gateway (RNG). The RNG provides an interface between the local Radio Frequency (RF) resources and the PDR to support data communication with subscriber radios.

What Is Covered in This Manual?

This manual contains the following chapters:

- Packet Data Gateway Description on page 39 provides a high-level overview of the Packet Data Gateway (PDG) and how it fits into the system.
- Trunked IVD and HPD PDG Theory of Operations on page 41 provides a detailed overview of the Trunked IV&D and HPD PDG and how it works internally and within the system.
- Conventional IVD M Core and K Core PDG Theory of Operations on page 47 provides a detailed overview of the Conventional IV&D M core and Conventional IV&D K core PDG and how it works internally and within the system.
- Trunked IVD and HPD PDG Installation on page 55 provides the requirements for installation and the detailed hardware installation instructions for the Trunked IV&D and HPD PDG.
- Conventional IVD M Core and K Core PDG Installation on page 73 provides the requirements for installation and the detailed hardware installation instructions for the Conventional IV&D M core and Conventional IV&D K core PDG.
- PDG Local Configuration for Trunked IVD and HPD on page 95 provides the configuration requirements and procedures necessary to configure the Trunked IV&D and/or HPD PDG.
- PDG Local Configuration for Conventional IVD M Core and K Core on page 129 provides the configuration requirements and procedures necessary to configure the Conventional IV&D M core and/or Conventional IV&D K core PDG.
- Trunked IVD and HPD PDG Operation on page 161 provides the user operation procedures for working with the Trunked IV&D and/or HPD PDG.
- Conventional IVD M Core and Conventional IVD K Core PDG Operation on page 175 provides the user operation procedures for working with the Conventional IV&D M core and/or Conventional IV&D K core PDG.
- Packet Data Gateway Maintenance on page 195 describes the necessary procedures for the periodic maintenance of the PDG.
- Trunked IVD and HPD PDG Troubleshooting on page 197 provides the troubleshooting information for the Trunked IV&D and/or HPD PDG, including tools, LEDs, and specific problems.
- Conventional IVD M Core and K Core PDG Troubleshooting on page 219 provides the troubleshooting information for the Conventional IV&D M core and/or Conventional IV&D K core PDG, including tools, LEDs, and specific problems.

- Packet Data Gateway FRU/FRE Procedures on page 241 provides the PDG FRU/FRE replacement procedures necessary in case of equipment failure.
- Packet Data Gateway Reference on page 247 contains supplemental reference information relating to the PDG Light Emitting Diodes (LEDs).
- Packet Data Gateway Disaster Recovery on page 249 provides the recovery sequence for the PDG hardware.
- Conventional IVD K Core PDG Configuration on page 261 provides an overview of the Conventional IV&D K core PDG configuration.
- Conventional IVD K Core PDG Configuration – Command Reference on page 265 provides information necessary to configure the system parameters for the Conventional IV&D K core PDG.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

For associated information about the radio system, see the following documents:

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the *R56* manual. This manual may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Documentation Overview Reference Guide	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Dynamic System Resilience Feature Guide	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature that adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Virtual Management Server Hardware User Guide	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in an ASTRO® 25 system.
Virtual Management Server Software User Guide	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.
Trunked Data Services Feature Guide	Describes the implementation and use of data services on ASTRO® 25 systems, specific to the Classic Data (IV&D) and Enhanced Data functionalities, and the High Availability for Trunked IV&D and HPD feature.
Conventional Data Services Feature Guide	Provides descriptive and procedural content relating to the ASTRO® 25 conventional data feature and its components, as

Table continued…

Related Information	Purpose
	well as information regarding data call and data messages processing, including installation, configuration, operation, and troubleshooting procedures.
Master Site Infrastructure Reference Guide	Covers site-level information required to install and maintain equipment at the ASTRO® 25 IV&D system master site.
Unix Supplemental Configuration Setup Guide	Provides additional procedures that an organization may require for Solaris-based and Linux-based devices, including procedures for configuring password aging and welcome banners.
Securing Protocols with SSH Feature Guide	Provides information relating to the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in an ASTRO® 25 system. Includes configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
Unified Network Configurator User Guide	Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers, and base radios, and is used to set up sites for the ASTRO® 25 IV&D system. UNC has two components: VoyenceControl and Unified Network Configurator Wizards (UNCW).
Provisioning Manager User Guide	Provides a description of the Provisioning Manager application, including information on how to tailor this application for system use and how to provision ASTRO® 25 systems with various system-level, user-level, and device-level configuration parameters.
SNMPv3 Feature Guide	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems.
Authentication Services Feature Guide	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.
Centralized Event Logging Feature Guide	Provides information relating to the implementation and management of the Centralized Event Logging feature available for ASTRO® 25 systems. This feature enables capturing operating system events generated by most devices in ASTRO® 25 systems. This manual includes information about the server and client function required for the feature.
Unified Event Manager User Guide	Covers the use of Unified Event Manager (UEM) that provides reliable fault management services for devices in ASTRO® 25 systems.
Network Time Protocol Server Feature Guide	Provides an introduction to the components that comprise the Network Time Protocol (NTP) server, including detailed procedures for the TRAK 9100 NTP server installation and configuration and for the Field Replaceable Units (FRUs) replacement.

Table continued…

Related Information	Purpose
Private Network Management Servers Feature Guide	Describes how to install, configure, and manage the Private Network Management (PNM) client, a PC workstation which system administrators and technicians use for a variety of system-related tasks, such as viewing equipment operational status, monitoring network utilization and performance, or viewing alarms generated by system equipment.
CAI Data Encryption Module Feature Guide	Describes data encryption services provided by the CAI Data Encryption Module (CDEM) for ASTRO® 25 Conventional IV&D applications. The CDEM is an optional component of the Conventional IV&D feature, located with the Conventional IV&D PDG.
Key Management Facility User Guide	Provides descriptive and procedural information about the Key Management Facility (KMF) including a description of where the KMF can be found, a description of KMF encryption key management, as well as procedures on installation, configuration, operation, troubleshooting, and FRU/FRE replacement.
Configuration Manager for Conventional Systems User Guide	Covers the use of the Configuration Manager application to set up the Conventional system parameters for consoles, channels, user objects, and integrated data services in K Core ASTRO® 25 systems.
ASTRO 25 vCenter Application Setup and Operations Guide	Provides a description of the VMware vCenter application used to provide VMware fault tolerance and VMware high availability for virtual machines and includes process and procedures to support setup and operations for the VMware vCenter application in an ASTRO® 25 system.

Chapter 1

Packet Data Gateway Description

This chapter provides a high-level description of the Packet Data Gateway (PDG) and the function it serves on your system.

1.1

Packet Data Gateway

The Motorola Solutions Packet Data Gateway (PDG) is designed to link a customer data network to their radio network. It is placed at the junction of the wire line network and the Radio Frequency (RF) data network. It provides the interconnection between the two networks through its routing, translation, fragmentation, and error reporting services. The PDG employs Internet Protocol Version 4 (IPv4) routing. A multizone system requires one PDG per zone for seamless system-wide packet data service operation.

The Packet Data Service is a bearer service that connects two parties in a communication system with the IP protocol. One party is either a subscriber or a mobile terminal connected to the subscriber, and the other is an application in the CEN.

The PDG platform supports the following system types:

- **Conventional Integrated Voice and Data (IV&D) PDG**
  - within M core zones
  - within K core zones

    NOTICE: The Conventional IV&D K core PDG is functionally equivalent to the Conventional IV&D M core PDG, but is configured to operate in the K core without core services such as Authentication Services, Domain Name Server, Network Time Protocol Server, and the full centralized Network Management.
- **Trunked Integrated Voice and Data (IV&D) PDG**
  - within L core zones
  - within M core zones
- **High Performance Data (HPD) PDG**
  - within M core zones

IMPORTANT: Each type of data service requires a separate PDG.

For Trunked IV&D and HPD, the Packet Data Service is an implementation of the APCO 25 Common Air Interface (CAI) and the Standard Subnetwork Dependence Convergence Protocol (SNDCP) to provide IP datagram exchange between applications on mobile subscriber units and Fixed Network Equipment (FNE). To support High Availability for Trunked IV&D and HPD (HA Data), redundant PDGs, GGSNs, and CNI path equipment (data network transport devices) can be implemented in the L2, M2 and M3 zone cores. For a detailed description of the HA Data feature, see the *Trunked Data Services Feature Guide*.

For Conventional IV&D, the Packet Data Service is an implementation of the APCO standard SCEP (Simple CAI Encapsulation Protocol) air interface to provide IP datagram exchange between applications or attached to mobile subscriber units and Fixed Network Equipment (FNE).

The PDG is installed as a virtual machine on an HP DL380 server. For the description of the server, see the *Virtual Management Server Hardware User Guide*. To support High Availability for

Conventional IV&D, redundant PDGs, GGSNs, and CNI path equipment (data network transport devices) can be implemented in the M2 and M3 zone cores. For a detailed description of the HA Data feature, see the *Conventional Data Services Feature Guide*.

The virtual appliance of the PDG includes the following components:

- **Linux Operating System**
- **Packet Data Router (PDR) application**: The PDR provides a logical interface between the GPRS Gateway Support Node (GGSN) router and the Radio Network Gateway (RNG). The PDR forwards outbound data traffic to the RNG.
- **Radio Network Gateway (RNG) application**: The RNG provides a logical interface between the local Radio Frequency (RF) resources and the PDR to support data calls to subscriber radios.

Chapter 2

Trunked IVD and HPD PDG Theory of Operations

This chapter explains how the Trunked IV&D and HPD Packet Data Gateway (PDG) works in the context of your system.

2.1 Trunked IVD and HPD PDG Components and Architecture

The Packet Data Gateway (PDG) provides the interface between the Customer Enterprise Network (CEN) and packet data users in the system. The PDG performs registration services for packet data users, maintains user permissions and mobility information, as well as provides routing of traffic to the radio network or the GPRS Gateway Support Node (GGSN) router.

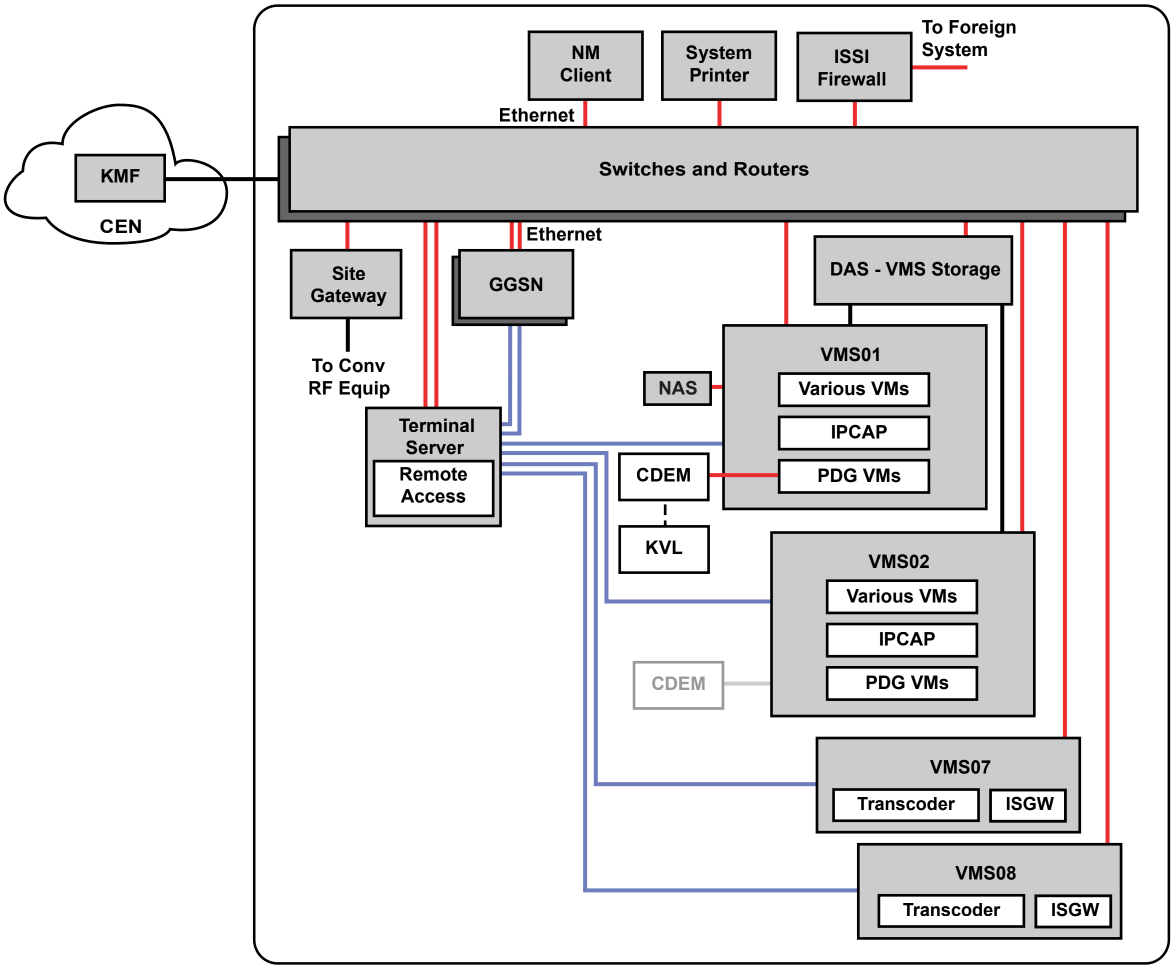
The main software components of the PDG are the Packet Data Router (PDR) and the Radio Network Gateway (RNG).

The PDG is installed on the virtual server, which interfaces directly with the Ethernet LAN switch. For the description of the hardware components, see the *Virtual Management Server Hardware User Guide*.

Figure 1: Data Subsystem – Trunked IV&D and HPD PDG – M3 Zone Core

The following diagram shows the Trunked IV&D and HPD PDG in an M3 zone core employing the VMS host server architecture.

NOTICE: The virtual machine (VM) for the PDG can be incorporated with other VMs on a VMS host.



S_A717_M3_conv_CSA_config_A

Table 1: Trunked IV&D and HPD PDG Components

Component	Description
RNG	The RNG is a software component which interfaces with the remote sites to handle inbound/outbound packet data traffic between the remote sites and the PDR. The RNG provides a logical connection to the sites, and facilitates delivery of traffic between the PDR and the remote sites. In Outbound direction, RNG supports fragmentation of IP datagrams received from PDR and formats them to Logical Link Control (LLC) packets. Then, it forwards the packets to the subscriber in the zone through the local site of the subscriber. In inbound direction, LLC assembles LLC packets and converts them to IP Packets before forwarding them to PDR. The RNG also communicates with the zone controller and maintains a packet data visitor location register (PD-VLR).
PDR	The PDR is a software component which provides tunneling of packet data traffic to the GGSN router, which then routes the traffic to the Customer Enterprise

Component	Description
	Network (CEN). The PDR hosts the Packet Data Home Location Register (PD-HLR), tracks mobility of mobile subscribers on the network, and controls access to the GGSN and CEN.

2.2 Trunked IVD and HPD PDG Connections

A Packet Data Gateway (PDG) in IV&D and HPD configurations has two virtual network interfaces, eth0 for PDR and eth1 for RNG. Eth0 and eth1 map to the same physical network port on the HP DL380 server. They also map to a redundant network port. The ports are connected to the LAN switch. The connection to the PDR supports the routing of traffic through a GPRS tunnel to the GGSN router, and Network Management communication with Unified Network Configurator (UNC) and Unified Event Manager (UEM) using SNMPv3. The PDR also communicates with RNGs in other zones to support InterZone packet data activity, as well as with the Zone Controller for the HLR, and peer PDRs for operational health messages. The connection to the RNG supports the logical connection to the packet data subscribers and supports connection to the zone controller for visitor location register updates. All traffic for the PDG is routed through the gateway router.

To support High Availability for Trunked IV&D and HPD (HA Data), two PDGs on separate virtual servers interface to the LAN switch and two GGSN routers support data network transport. See the *S6000 and S2500 Routers Feature Guide* for details regarding the GGSN.

2.3 Trunked PDR and RNG Features

PDR features include:

- Packet data registration
- InterZone Mobility Management
- IP Bearer Services
- GTP Tunneling of IP Messages
- SNMP Fault Management
- SNMP Configuration Management, allowing the Network Manager to configure the PDR remotely
- Local configuration
- Local (Co-Resident) RNG Management
- Security
- Message overload protection
- Context Activation/Deactivation
- Maintenance of persistent context activation of subscribers
- Automatic context renewal of all registered subscribers on a restart recovery request from the GGSN

RNG features include:

- Fragmentation of IP datagrams into Common Air Interface (CAI) protocol data units
- Fragmentation of IP datagrams into Wideband Air Interface (WAI) protocol data units
- Retransmission of RF message segments through LLC Selective Automatic Retry Request (SARQ) (This feature applies to the HPD PDG only.)
- Site Level Mobility Management

- Link Status to track and report Base site link status and Zone Controller Link status to the home PDR.
- Statistics to track and report various statistics to the home PDR, which forwards them to network management applications upon request
- Message overload protection

2.4 Trunked IVD and HPD PDG Interfaces

The Trunked IV&D and HPD Packet Data Gateway (PDG) has the following interfaces:

- PDG Administration User interface
- Radio Network interface
- GGSN services
- Zone Controller interface
- Remote Network Management interface
- PDR Peer interface for DSR

PDG Administration User Interface

The PDG Administration User interface provides a menu-driven, character-based interface that can be used to perform all common administrative tasks. The menu structure is common to all ASTRO® 25 servers, so that common administrative tasks are accessed the same way on all servers.

Radio Network Interface

The PDG communicates with the subscribers through the Data Site Controller (DSC), which is responsible for managing the RF resources. DSC communication is conducted through the UDP/IP and the Link Access Protocol-D channel (LAPD) over the UDP/IP.

GGSN Services

The PDG communicates with the Gateway General Packet Radio Service (GPRS) Support Node to provide mobile subscriber users access to the Public Data Network (PDN) or specified customer networks. The communication protocol for the Gateway GPRS Support Node (GGSN) services is GTP over UDP/IP.

Zone Controller Interface

The PDG communicates with the zone controller to obtain location information of the individual subscribers. The communication is multicast over UDP/IP.

Remote Network Management Interface

The PDG communicates with the Network Manager to obtain configuration, alarms, failures, and statistics information regarding subscribers, Site configuration, and Zone information. The communication is conducted using SNMPv3.

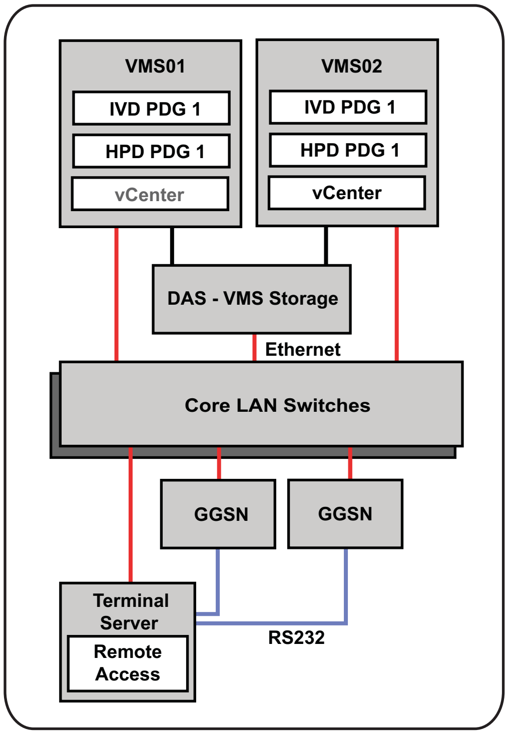
PDR Peer Interface for DSR

See PDG – DSR System Architecture on page 45.

2.5 PDG – High Availability System Architecture

The High Availability for Trunked IV&D and HPD (HA Data) feature provides a high availability data solution within a single zone core by establishing two Packet Data Gateways (PDGs) on separate virtual servers, two GGSN routers, and redundant CNI path devices at a zone core to support trunked data services. A redundant PDG is established by enabling the Fault Tolerance feature of the VMware vCenter application for the primary PDG. vCenter provides automatic or user-initiated PDG to PDG switchover in case of a hardware failure. To implement the HA Data feature for a non-DSR zone core, the HA Data equipment configuration would exhibit the following:

Figure 2: Data Subsystem – HA Data – Non-DSR



High_Avail_Data_Option_NonDSR_B

For information regarding the implementation of HA Data in a DSR system architecture, see PDG – DSR System Architecture on page 45.

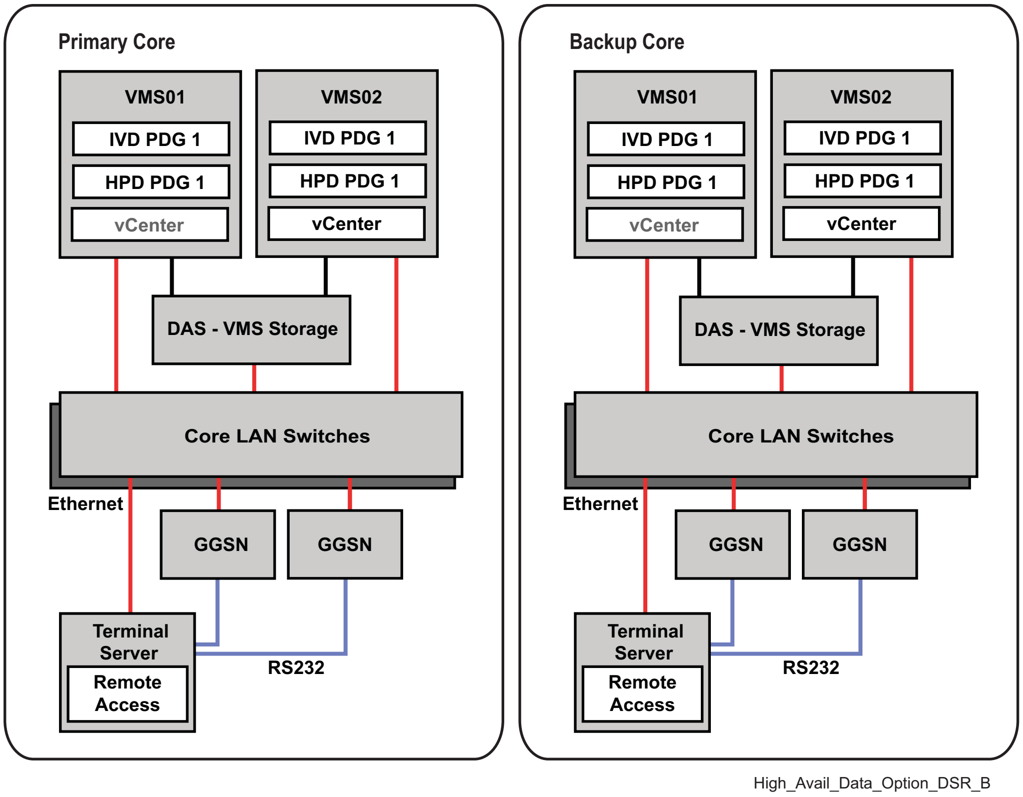
For more information regarding the High Availability for Trunked IV&D and HPD (HA Data) feature, see the *Trunked Data Services Feature Guide*.

2.6 PDG – DSR System Architecture

Dynamic System Resilience (DSR) is a system architecture feature that provides redundant zone core equipment by establishing a primary zone core and a backup zone core usually at two different master site locations.

In a system implementing DSR, the High Availability for Trunked IV&D and HPD (HA Data) feature is supported by establishing two Packet Data Gateways (PDGs) on separate virtual servers, two GGSN routers, and redundant CNI path devices for high availability of trunked data services at the primary zone core as well as the backup zone core. To implement the HA Data feature in a DSR system architecture with a primary zone core and backup zone core, the HA Data equipment configuration would exhibit the following:

Figure 3: Data Subsystem – HA Data – DSR



For more information regarding the DSR system architecture, see the *Dynamic System Resilience Feature Guide*.

For more information regarding the High Availability for Trunked IV&D and HPD (HA Data) feature, see the *Trunked Data Services Feature Guide*.

2.7 Direct Attached Storage (DAS)

In Common Server Architecture (CSA) systems, the Virtual Management Server (HP DL380 Gen8 or Gen9 with ESXi OS) hosting the PDG and other virtual machines uses Direct Attached Storage (DAS) to store software and data for the virtual machines. DAS is an external storage solution used instead of a local drive. See the *Virtual Management Server Hardware User Guide* for more details regarding the DAS hardware and the *Virtual Management Server Software User Guide* for installation and configuration procedures relating to DAS.

NOTICE: An internal hard drive is used instead of DAS for the Conventional IV&D K core PDG.

Chapter 3

Conventional IVD M Core and K Core PDG Theory of Operations

This chapter explains how the Conventional IV&D M core and K core Packet Data Gateway (PDG) work in the context of your system.

3.1 Conventional IVD PDG Components and Architecture

The Packet Data Gateway (PDG) provides the interface between the Customer Enterprise Network (CEN) and packet data users in the system. The PDG performs registration services for packet data users, maintains user permissions and mobility information, as well as provides routing of traffic to the radio network or the GPRS Gateway Support Node (GGSN) router.

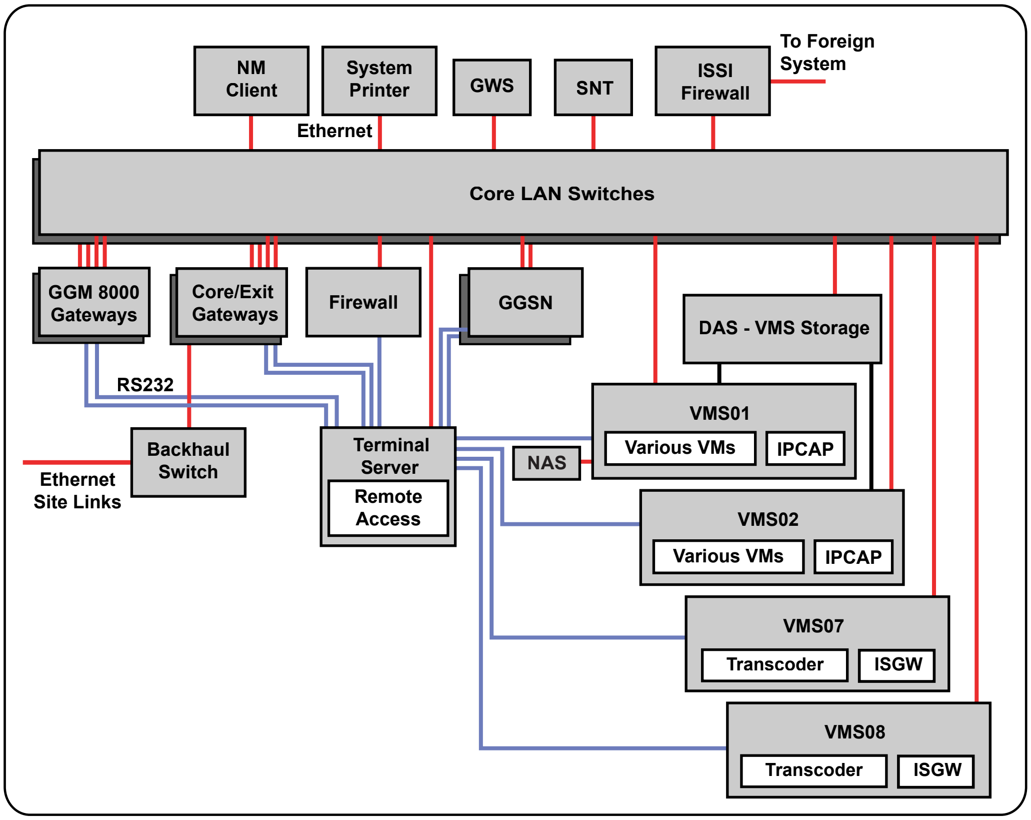
The main software components of the PDG are the Packet Data Router (PDR) and the Radio Network Gateway (RNG).

The PDG is installed on the virtual server, which interfaces directly with the Ethernet LAN switch. For the description of the hardware components, see the *Virtual Management Server Hardware User Guide*.

Figure 4: Data Subsystem – Conventional IV&D PDG – M3 Zone Core

The following diagram shows the Conventional IV&D PDG in an M3 zone core employing the VMS host server architecture.

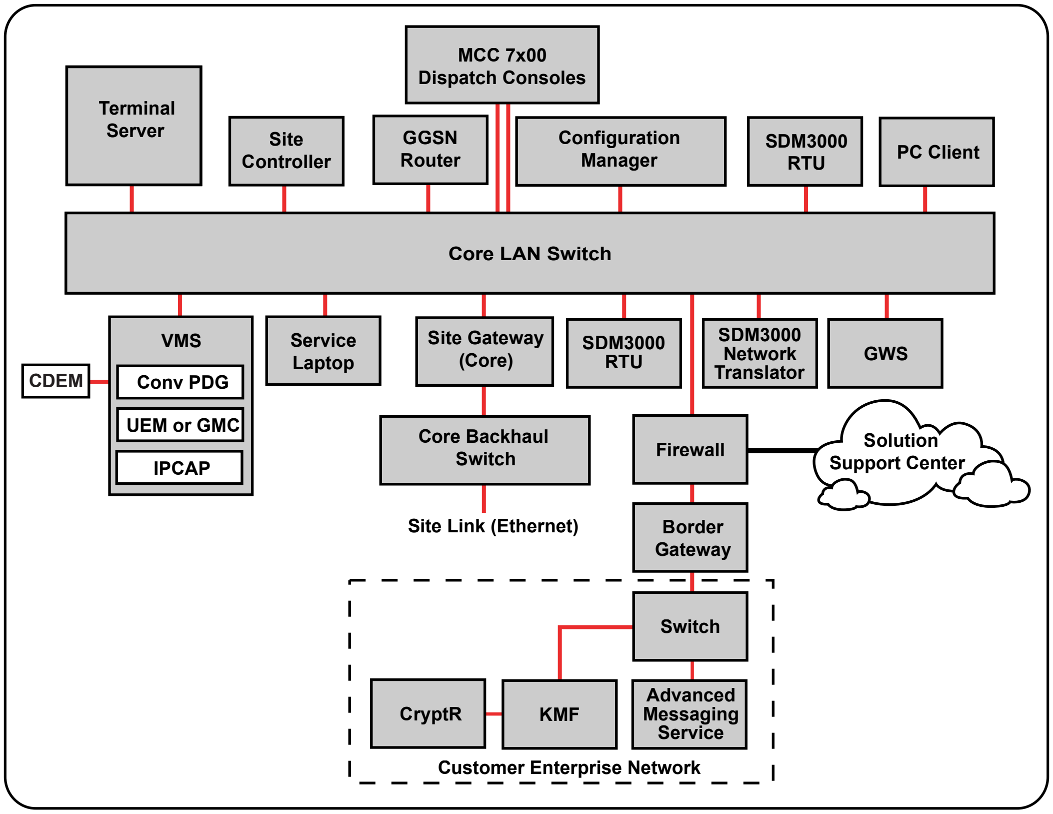
NOTICE: The virtual machine (VM) for the PDG can be incorporated with other VMs on a VMS host or it can be placed on a dedicated VMS host platform.



S_A717_M3_Primary_System_Zone_Core_Config_A

Figure 5: Data Subsystem – Conventional IV&D PDG – K1 Core

The following diagram shows the Conventional IV&D PDG in a K1 Conventional System.



S_K1_config_K

Figure 6: Data Subsystem – Conventional IV&D PDG – K2 Core

The following diagram shows the Conventional IV&D PDG in a K2 Conventional System.

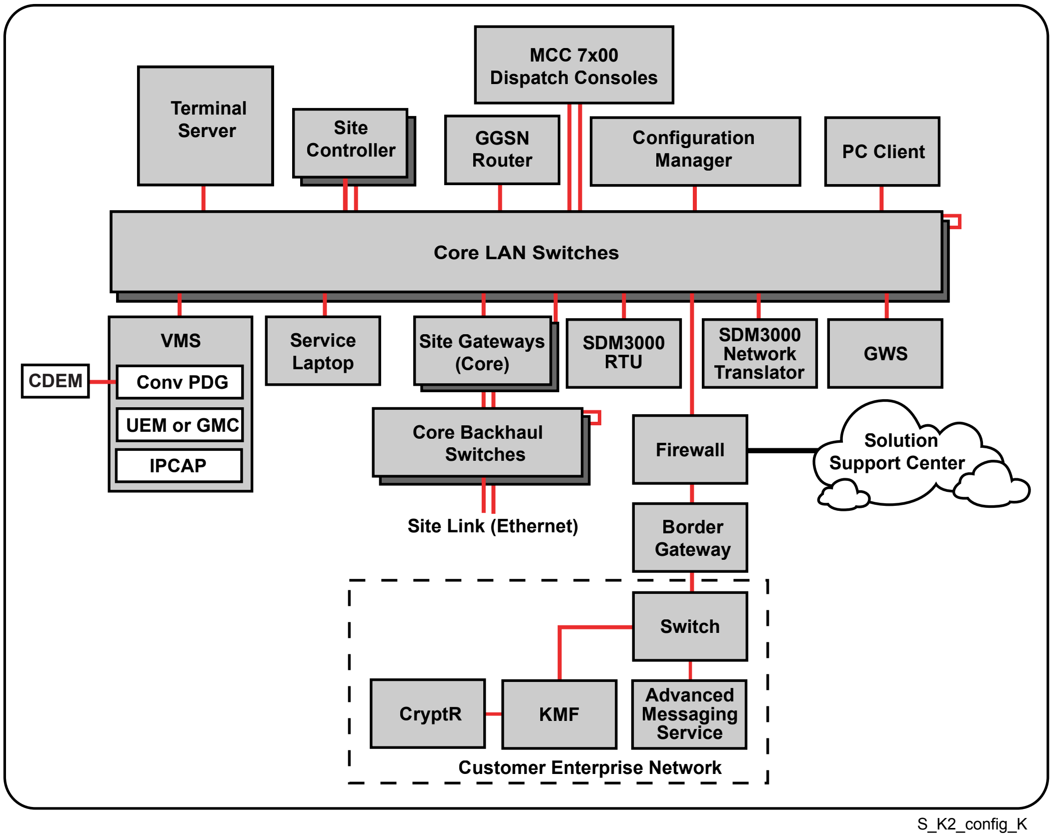


Table 2: Conventional IV&D PDG Components

Component	Description
RNG	The RNG is a software component which provides a link (CAI) layer termination point for all the Conventional Sites in that same zone. The RNG routes data packets over the infrastructure links to the Conventional Sites in the zone. The RNG receives packets from, and sends packets to, the PDR in the same zone. The RNG sends datagrams to the CDEM for encryption/decryption as needed before routing them to their ultimate destination. When key management of the CDEM is performed through OTEK, the RNG proxies the OTEK connection to the KMF on behalf of the CDEM.
PDR	The PDR is a software component which serves as the termination point for the GTP tunnel (the GGSN being the other termination point). The PDR also interacts with the local Radio Network Gateway (RNG). The PDR is responsible for managing Packet Data registrations and de-registrations, tracking subscriber location, interfacing with the Network Manager for configuration and fault management, proxying configuration and fault management messaging for the RNG and CDEM, and ensuring maintenance of persistent contexts. The PDR is also responsible for maintaining registrations for configured Broadcast Data Agencies.

3.2 Conventional IVD PDG Connections

A Conventional IV&D PDG has three virtual network interfaces, eth0 for PDR and eth1 and eth2 for RNG. Eth0 and eth1 map to the same physical network port on the HP DL380 server. They also map to a redundant network port. Eth2 maps to a single port. The ports are connected to the LAN switch. The connection to the PDR supports the routing of traffic through a GPRS tunnel to the GGSN router, and Network Management communication with the UNC and UEM using SNMPv3. The connection to the RNG supports the logical connection to the packet data subscribers. The RNG also connects through eth2 to the CDEM, which performs encryption and decryption of sent data.

3.3 Conventional PDR and RNG Features

PDR features include:

- Packet data registration
- IP Bearer Services
- GTP Tunneling of IP Messages
- SNMP Fault Management

  NOTICE: For the Conventional IV&D K core PDG, Fault Management is done through the local syslog.

- SNMP Configuration Management, allowing the Network Manager to configure the PDR remotely
- Local configuration
- Local (Co-Resident) RNG Management
- Security
- Message overload protection
- Proxy CDEM connection status and fault management
- Automatic Context Activation for all types of Conventional registrations
- Automatic Context Activation for broadcast agencies
- Context Activation of subscribers configured as data-triggered first time a data packet is received
- Maintenance of persistent Context Activation of subscribers

RNG features include:

- Creation of Common Air Interface Protocol Data Units for each IP datagram
- Site Level Mobility Management
- Link Status to track and report Base Site Link status to the PDR.
- Statistics to track and report various statistics to the PDR, which forwards them to network management applications upon request
- Message overload protection
- Encryption and decryption of messages through the CDEM.

3.4 Conventional IVD PDG Interfaces

The Conventional IV&D Packet Data Gateway (PDG) has the following interfaces:

- PDG Administration User interface

- GGSN services
- Remote Network Management interface
- CAI Data Encryption Module interface
- Site Gateway (Conventional Channel Interface)
- Command Line Interface (Conventional IV&D K core PDG only)
- PDR Peer interface for DSR

PDG Administration User Interface

The PDG Administration User interface provides a menu-driven, character-based interface that can be used to perform all common administrative tasks. The menu structure is common to all ASTRO® 25 servers, so that common administrative tasks are accessed the same way on all servers.

GGSN Services

The PDG communicates with the Gateway General Packet Radio Service (GPRS) Support Node to provide mobile subscriber users access to the Public Data Network (PDN) or specified customer networks. The communication protocol for the Gateway GPRS Support Node (GGSN) services is GTP over UDP/IP.

The PDG and GGSN routes data messages from the Fixed Host located in the Customer Enterprise Network (CEN) to the mobile clients connected to radios.

Remote Network Management Interface

The PDG communicates with the Network Manager to obtain configuration, alarms, failures, and statistics information regarding subscribers, Site configuration, and Zone information. The communication is conducted using SNMPv3.

NOTICE: For the Conventional IV&D K core PDG, the Site configuration and Zone information is provisioned locally through the Command Line Interface. For details, see Conventional IVD K Core PDG Configuration on page 261.

CAI Data Encryption Module Interface

The CDEM is an optional component that secures data encryption and decryption services for the ASTRO® 25 Conventional with Integrated Data feature. The CDEM is located in the Radio Network Infrastructure (RNI) and connects to the Radio Network Gateway (RNG) component of the Packet Data Gateway (PDG) virtual machine through an Ethernet crossover cable. When the PDG receives data from either the Customer Enterprise Network (CEN) or from a subscriber through the Conventional RF equipment, it passes that data to the CDEM, if secure services are required. The CDEM performs the desired encryption or decryption operation and sends the data back to the PDG for transmission to its final destination.

Site Gateway (Conventional Channel Interface)

The PDG interfaces with the Site Gateway (Conventional Channel Interface) to enable IP data connectivity between Conventional IV&D subscribers and the Customer Enterprise Network (CEN).

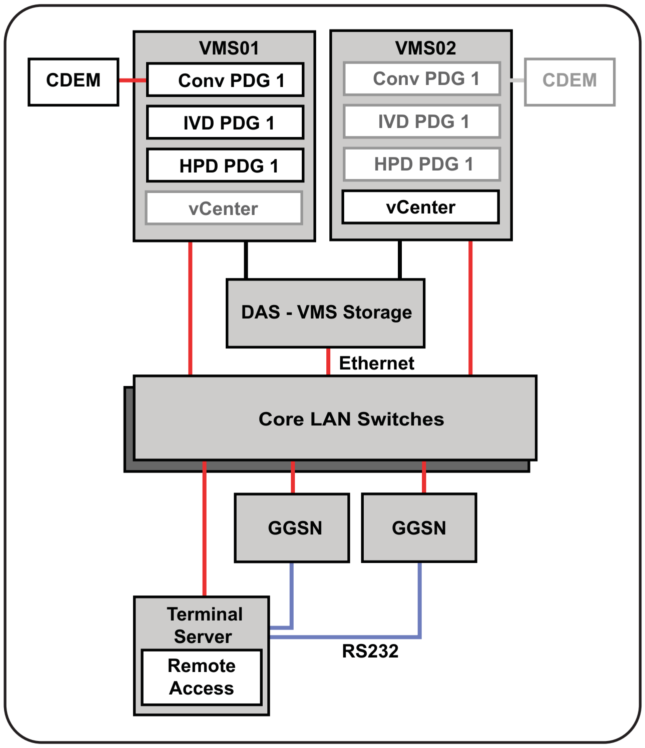
Command Line Interface

The Command Line Interface is used to configure system parameters on the Conventional IV&D K core PDG. For details, see Conventional IVD K Core PDG Configuration on page 261.

3.5 PDG – High Availability System Architecture

The High Availability for Conventional IV&D (HA Data) feature provides a high availability data solution within a single zone core by establishing two Packet Data Gateways (PDGs) on separate virtual servers, two GGSN routers, and redundant CNI path devices at a zone core to support conventional data services. A redundant PDG is established by enabling the Fault Tolerance feature of the VMware vCenter application for the primary PDG. vCenter provides automatic or user-initiated PDG to PDG switchover in case of a hardware failure. To implement the HA Data feature for a non-DSR zone core, the HA Data equipment configuration would exhibit the following:

Figure 7: Data Subsystem – HA Data – Non-DSR



Conv_High_Avail_Data_Option_NonDSR_A

For information regarding the implementation of HA Data in a DSR system architecture, see PDG – DSR System Architecture on page 53.

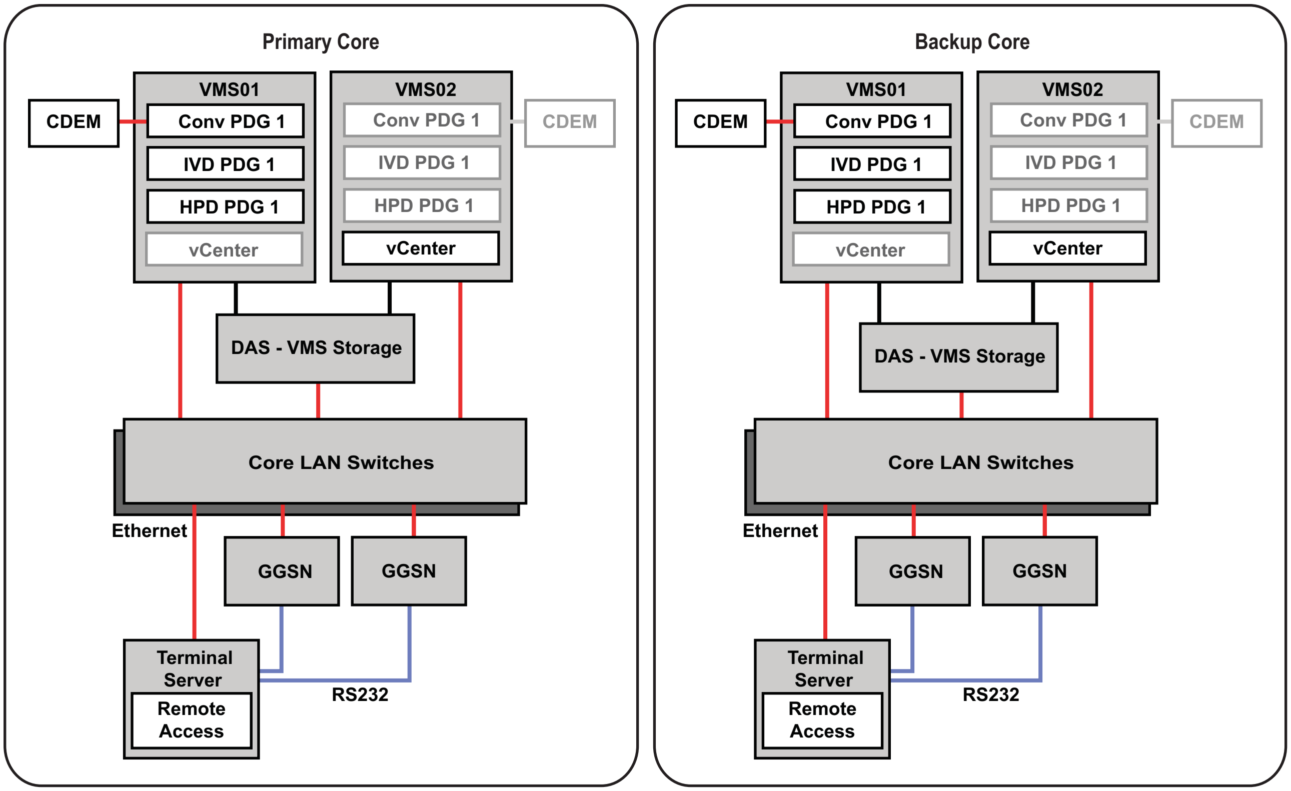
For more information regarding the High Availability for Conventional IV&D (HA Data) feature, see the *Conventional Data Services Feature Guide*.

3.6 PDG – DSR System Architecture

Dynamic System Resilience (DSR) is a system architecture feature that provides redundant zone core equipment by establishing a primary zone core and a backup zone core usually at two different master site locations.

In a system implementing DSR, the High Availability for Conventional IV&D (HA Data) feature is supported by establishing two Packet Data Gateways (PDGs) on separate virtual servers, two GGSN routers, and redundant CNI path devices for high availability supporting conventional data services at the primary zone core as well as the backup zone core. To implement the HA Data feature in a DSR system architecture with a primary zone core and backup zone core, the HA Data equipment configuration would exhibit the following:

Figure 8: Data Subsystem – HA Data – DSR



Conv_High_Avail_Data_Option_DSR_A

For more information regarding the DSR system architecture, see the *Dynamic System Resilience Feature Guide*.

For more information regarding the High Availability for Conventional IV&D (HA Data) feature, see the *Conventional Data Services Feature Guide*.

3.7 Direct Attached Storage (DAS)

In Common Server Architecture (CSA) systems, the Virtual Management Server (HP DL380 Gen8 or Gen9 with ESXi OS) hosting the PDG and other virtual machines uses DAS (Direct Attached Storage) to store software and data for the virtual machines. DAS is an external storage solution used instead of a local drive. See the *Virtual Management Server Hardware User Guide* for more details regarding the DAS hardware and the *Virtual Management Server Software User Guide* for installation and configuration procedures relating to DAS.

NOTICE: An internal hard drive is used instead of DAS for the Conventional IV&D K core PDG.

Chapter 4

Trunked IVD and HPD PDG Installation

This chapter details the installation procedures related to the Trunked IV&D and HPD Packet Data Gateway (PDG).

4.1 Deploying the Trunked PDG Virtual Appliance

The Packet Data Gateway (PDG) is installed on the virtual server. PDGs reside as virtual machines on an ESXi platform which has its own installation and configuration process.

For information concerning mechanical installation, power supply, hardware specifications, and physical specifications, see the *Virtual Management Server Hardware User Guide*. For information about the installation, security settings, and other, see the *Virtual Management Server Software User Guide*.

Prerequisites:
Review the entire software installation process and each supporting procedure before installing the PDG software.

Process:

1. Satisfy all appropriate requirements and review all appropriate installation considerations before installing the PDG software. See Trunked PDG Software Installation – Requirements and Considerations on page 56.
2. Deploy the Packet Data Gateway Virtual Appliance. Perform the appropriate procedure for your system configuration:
   - To deploy the Trunked PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 57.
   - To deploy the Trunked PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Trunked PDG as a VM on a Dedicated VMS Host Server (DL380) on page 60.
3. If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88
4. Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61.
5. Apply Virtual Machines Supplemental Configuration. See Applying Supplemental Configuration to Virtual Machines on page 63
6. If required by your organizations policies, disable password aging on the PDG. See “Disabling Password Aging for the Root Account” in the *Unix Supplemental Configuration* manual.
7. Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.
8. Perform initial configuration of the PDG. See Configuring the Trunked PDG after Installation on page 66.

9 Join the PDG to the Active Directory Domain. See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide*.

10 Apply the platform patch to the PDG. See Applying the Platform Patch on page 67.

11 If applicable, perform Linux OS patching on the PDG. Installation procedures for the MOTOPATCH are available at: https://sites.google.com/a/motorolasolutions.com/susmotopatch/

If you cannot open the link, this means that MOTOPATCH for RHEL v7 is not available yet. Skip this step.

12 If required by your organization’s policies, configure the PDG for SNMPv3 and SSH. For more information, see the *SNMPv3 Feature Guide* and *Securing Protocols with SSH Feature Guide*.

Ask your system administrator which procedures and/or commands you should use, depending on your organization’s policies.

13 Synchronize the PDG database. See Trunked PDG Database Synchronization on page 69.

14 Change the PDG state to active. Perform the appropriate procedure depending on your system architecture:

- For PDGs in DSR systems, see Setting the Trunked PDG to the Active State (DSR) on page 162
- For PDGs in non-DSR systems, see Changing the Trunked PDG State to Active in Non-DSR Systems on page 68.

15 Back up the SSH configuration and keys on the PDG using commands that are common to the Linux devices in an ASTRO® 25 system. See the *Securing Protocols with SSH Feature Guide* manual.

16 If your system supports DSR, perform the procedures in Dynamic System Resilience Configuration on page 69.

17 If your system supports the High Availability for Trunked IV&D and HPD (HA Data) feature, perform the procedures in the *ASTRO 25 vCenter Setup and Operations Guide*.

4.1.1 Trunked PDG Software Installation – Requirements and Considerations

The following table lists the requirements and considerations for Packet Data Gateway (PDG) software installation. Review each topic to ensure that you are able to perform a successful software installation of the PDG.

Table 3: Requirements and Considerations for Trunked PDG Software Installation

Requirement or Consideration	Description
Backup and Restore Considerations	There is no data to back up or restore in a new installation. If you want to reinstall the software and there is an existing database, then the PDG data must be backed up before reinstalling the software. Once the installation is completed, conduct a data restore to the PDR.
Reinstallation or Upgrade Considerations	To ensure that the PDG software installation is successful, reinstalling, or upgrading the operating system as a separate procedure is not supported.
Network Management Support	The Unified Network Configurator (UNC) plays an important supporting role in installing the PDG software. Unless

Table continued…

Requirement or Consideration	Description
	specified, the processes and procedures in this manual assume that the UNC and other network manager applications are installed and running in the X-zone network when installing PDG software.
Resetting and Shutdown Considerations	Do not shut down by pressing the power button or disconnecting the power cord, if it can be avoided. For PDR, RNG and all PDG resets and shutdowns, it is recommended that you use options from the **admin_menu**.
AAA Server	The AAA server plays an important supporting role in installing and operating the PDG software.

4.1.1.1 Trunked PDG Access

Access the Packet Data Gateway (PDG) console for maintenance tasks, such as installing software, configuration, or monitoring by connecting to the virtual server through the network from the VMware Sphere Client application, which should be installed on a Windows-based machine.

4.1.2 Domain User Names and Domain User/Root Account Passwords Data Value Requirements and Criteria for the Trunked PDG

- See “Changing Root Account Passwords for Linux-Based Devices” in the *Unix Supplemental Configuration Setup Guide* for the root account password criteria.
- See “User/Group Name Restrictions” in the *Authentication Services Feature Guide* for Domain User names criteria.
- See “User Input Requirements for Server Installation/Configuration” in the *Authentication Services Feature Guide* for Domain User account passwords criteria.

4.1.3 Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380)

Perform this procedure when installing the Packet Data Gateway (PDG) virtual machine (VM) in a system employing the Common Server Architecture where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380).

Prerequisites:
Obtain the following from your system administrator:

- Motorola Virtual Appliance media (contains the PDG virtual machine files)
- Virtual Server host (ESXi-based server) IP address
- ESXi-based server root account password
- Hostname for the PDG
- Zone network for the PDG virtual machine

For more information on installing and configuring virtual machines on an HP DL380 server, see the *Virtual Management Server Software User Guide*.

When and where to use: Use this procedure only for a *trunked* IV&D or HPD PDG. For a conventional PDG, use Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75.

Procedure:

1. Launch the VMware vSphere Client from the Windows-based device where it resides.
2. At the login prompt, log on to the ESXi server where the PDG is being deployed with root credentials.

   The **vSphere Client Inventory** window appears.

3. Insert the PDG install media to the optical drive of the Windows-based device where the vSphere client was launched.
4. Select **File** → **Deploy OVF Template**.
5. In the **Deploy OVF Template – Source** window, select the source of the PDG OVF template:
   - **a** Click **Browse**.
   - **b** Select the PDG OVF template.
   - **c** Click **Next**.
6. In the **Deploy OVF Template – OVF Template Details** window, verify the OVF template details. Click **Next**.
7. In the **Deploy OVF Template – Name and Location** window, type the name for the PDG. Click **Next**.
   - For an IV&D PDG, type: `pdr` ***<X>***`.zone`***<Y>***
   - For an HPD PDG, type: `hpdpdr` ***<X>***`.zone`***<Y>***

   where:
   <X> represents the core type (`01` for a primary core or `02` for a backup core).
   <Y> represents the zone number (ranging from 1 to 7).

8. In the **Deploy OVF Template – Storage** window, select the storage location:
   - **a** Select **z00*<X>*das0*<Y>*_datastore1**.

     where:
     <X> is the zone number.
     <Y> is the instance number of the DAS that the VMS the PDG is being installed upon is connected to.
   - **b** Click **Next**.
9. In the **Deploy OVF Template – Disk Format** window, select the disk format:
   - **a** Select **Thick Provision Eager Zeroed**.

     If this option is not available, select **Thick Provision**.
   - **b** Click **Next**.
10. In the **Deploy OVF Template – Network Mapping** window, select the **Destination Network** for each **Source Network**:
    - **a** For **data0**, select **data0**.
    - **b** Click **Next**.
11. In the **Deploy OVF Template – Ready to Complete** window, confirm the values displayed are correct. Click **Finish**.

IMPORTANT: Do not check **Power on after deployment**, because additional modifications to the PDG VM are necessary after deployment, and these modifications require the PDG VM to be powered off.

The deployment status bar appears.

12 When the deployment has been completed successfully, click **Close**.

The deployed PDG is now present in the vSphere client.

13 In the **vSphere Client Inventory** window, perform the following actions:

a Right-click the newly deployed PDG VM.

b Select **Edit Settings**

c Click the **Options** tab.

d In the left pane, under **Advanced**, click **General**.

e In the right pane, click **Configuration Parameters**.

14 In the **Configuration Parameters** window, perform the following actions:

a Click **Add Row**.

A new row appears at the bottom of the list.

b In the **Name** column for that row, type: `ethernet0.coalescingScheme` and press TAB.

c In the **Value** column for that row, enter: `disabled`

d Click **Add Row**.

A new row appears at the bottom of the list.

e In the **Name** column for that row, type: `ethernet1.coalescingScheme` and press TAB.

f In the **Value** column for that row, enter: `disabled`

g *Optional:* Click **Add Row**.

A new row appears at the bottom of the list.

h *Optional:* In the **Name** column for that row, type: `ethernet2.coalescingScheme` and press TAB.

i *Optional:* In the **Value** column for that row, enter: `disabled`

j Click **OK**.

The **Configuration Parameters** window closes.

15 In the **Resources** tab, reserve CPU resources for the PDG:

a In the left pane, click **CPU**.

b In the right pane, in the **Reservation** text box, enter the value that corresponds to the type of server used in your system.

- For a Gen8 server, type: `1296 MHz`
- For a Gen9 server, type: `1248 MHz`

c Click **OK**.

4.1.4 Installing the Trunked PDG as a VM on a Dedicated VMS Host Server (DL380)

Use this procedure to install the Packet Data Gateway (PDG) as a virtual machine on a dedicated VMS Host Server (DL380).

Prerequisites: Obtain the following from your system administrator:

- Motorola Virtual Appliance media (contains the PDG virtual machine files)
- Virtual Server host (ESXi-based server) IP address
- ESXi-based server root account password
- Hostname for the PDG
- Zone network for the PDG virtual machine

When and where to use: For more information on installing and configuring virtual machines on an HP DL380 server, see the *Virtual Management Server Software User Guide*.

Procedure:

1. Launch the VMware vSphere Client from the Windows-based device where it resides.
2. At the login prompt, log on to the ESXi server where the PDG is being deployed with root credentials.

   The **vSphere Client Inventory** window appears.
3. Insert the PDG install media to the optical drive of the Windows-based device where the vSphere client was launched.
4. Select **File** → **Deploy OVF Template**.
5. In the **Deploy OVF Template – Source** window, select the source of the PDG OVF template:
   - **a** Click **Browse**.
   - **b** Select the PDG OVF template.
   - **c** Click **Next**.
6. In the **Deploy OVF Template – OVF Template Details** window, verify the OVF template details and click **Next**.
   - For an IV&D PDG, enter: `pdr` ***<X.>***`zone`***<Y>***
   - For an HPD PDG, enter: `hpdpdr` ***<X.>***`zone`***<Y>***

   where:
   - ***<X>*** represents the core type (`01` for a primary core or `02` for a backup core).
   - ***<Y>*** represents the zone number (ranging from `1` to `7`).
7. In the **Deploy OVF Template – Storage** window, select the storage location:
   - **a** For all system configurations, select **z00Xvms0Y_datastore1**.
   - **b** Click **Next**.
8. In the **Deploy OVF Template – Disk Format** window, select the disk format:
   - **a** Select **Thick Provision Eager Zeroed**. If this option is not available, select **Thick Provision**.
   - **b** Click **Next**.
9. In the **Deploy OVF Template – Network Mapping** window, for each **Source Network**, select the **Destination Network**:

a For **data0**, select **data0**.

b Click **Next**.

10 In the **Deploy OVF Template – Ready to Complete** window, confirm the values displayed are correct and click **Finish**.

IMPORTANT: Do not check **Power on after deployment**, because additional modifications to the PDG VM are necessary after deployment, and these modifications require the PDG VM to be powered off.

The template is being deployed and the deployment status bar appears.

11 When the deployment has been completed successfully, click **Close**.

The deployed PDG is now present in the vSphere Client.

12 Reserve CPU resources for the PDG:

- For a Gen8 server, perform the following actions:
  1 Right-click the newly deployed PDG VM.
  2 Select **Edit Settings**.
  3 Click the **Resources** tab.
  4 In the left pane, click **CPU**.
  5 In the right pane, in the **Reservation** text box, type `1296 MHz` for a Trunked IV&D/HPD PDG.
  6 Click **OK**.
- For a Gen9 server, perform the following actions:
  1 Right-click the newly deployed PDG VM.
  2 Select **Edit Settings**.
  3 Click the **Resources** tab.
  4 In the left pane, click **CPU**.
  5 In the right pane, in the **Reservation** text box, type `1248 MHz` for a Trunked IV&D/HPD PDG.
  6 Click **OK**.

4.1.5 Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) host are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS host, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

2 Log on to the server as a user with root privileges.

3 On the upper left side of the **vSphere Client Inventory** window, select the ESXi server that serves as the VMS host.

4 On the right side of the window, select the **Configuration** tab.

The window displays information about the configuration of the selected server.

5 In the **Software** section, select **Virtual Machine Startup/Shutdown**.

6 On the right side of the main window, select **Properties**.

7 In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.

8 In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.

9 In the **Default Shutdown Delay** area, select **Shutdown Action** → **Guest Shutdown**.

10 Set the boot order for the virtual machines hosted on the server:

- **a** In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.
- **b** Using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

  To determine the correct ordered slot for each virtual machine hosted on the server that you are configuring, see Zone Core Virtual Machine Boot Order on page 62.
- **c** Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.

11 Click **OK**.

The **Properties** window closes.

4.1.5.1
Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the Graphical Master Computer (GMC) for MOSCAD Network Fault Management (NFM) can be on the server.

If the Unified Network Configurator Database Server (UNCDS is present, three instances of the UNCDS are on the server.

Table 4: Zone Core Virtual Machine Boot Order

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	ZC	Enabled	Use Default	Use Default	Use Default
2	Transcoder	Enabled	Use Default	Use Default	Use Default
3	ISGW	Enabled	Use Default	Use Default	Use Default
4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
7	License Manager	Enabled	Use Default	Use Default	Use Default
8	ATR	Enabled	Use Default	Use Default	Use Default
9	DC-System	Enabled	Use Default	Use Default	Use Default
10	DC-Zone	Enabled	Use Default	Use Default	Use Default
11	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order	AuC	Enabled	Use Default	Use Default	Use Default
	BAR	Enabled	Use Default	Use Default	Use Default

Table continued…

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
	CSMS	Enabled	Use Default	Use Default	Use Default
	InfoVista	Enabled	Use Default	Use Default	Use Default
	FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
	GDG	Enabled	Use Default	Use Default	Use Default
	GMC	Enabled	Use Default	Use Default	Use Default
	NM Client	Enabled	Use Default	Use Default	Use Default
	UCS	Enabled	Use Default	Use Default	Use Default
	SSS	Enabled	Use Default	Use Default	Use Default
	Syslog	Enabled	Use Default	Use Default	Use Default
	UEM	Enabled	Use Default	Use Default	Use Default
	UNC	Enabled	Use Default	Use Default	Use Default
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

4.1.6
Applying Supplemental Configuration to Virtual Machines

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) may require supplemental configuration to improve their security settings, depending on the security requirements of your organization. Users apply the supplemental configuration by running a script stored on the configuration media listed in the Prerequisites to this procedure.

Prerequisites:

- Obtain the *VMware vSphere Configuration Media*.
- Install the VMware PowerCLI application on the Windows-based device. See Installing VMware PowerCLI on page 65.

When and where to use:
Perform this procedure on a Windows-based device, such as a Network Management (NM) client, dispatch console, or service computer or laptop.

During an upgrade, you must run the script specifically on the newly imported virtual machines if the virtual machines were imported after the VMS host was updated.

Procedure:

1. Insert the *VMware vSphere Configuration Media* into the optical drive of the Windows-based device.
2. Open the PowerShell command prompt as administrator, using the actions that apply to the Windows operating system version that is present on the device.
   - For Windows 7 or Windows Server 2008, perform the following actions:
     1. From **Start**, in the **Search programs and files** field, enter: `Command Prompt`

    2 Right-click **Command Prompt** and select **Run as administrator**.
    3 If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see.
    4 If you are not logged on with an administrative account, enter the domain admin credentials.
    5 At the command prompt, enter: `powershell`

- For Windows 10 or Windows Server 2012, perform the following actions:
    1 From **Start**, click **Search**.
    2 In the search field, type in `powershell`
    3 Right-click **Windows PowerShell**, and select **Run as administrator**.
        - If the **User Account Control** window appears, click **Yes**.
        - If you are not logged on with an administrative account, enter the domain admin credentials.

3 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* followed by a colon.

Step example: `E:`

The directory is changed to the root directory of the *VMware vSphere Configuration Media*.

4 At the PowerShell prompt, enter: `cd common\bin`

The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media*.

5 At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`

6 At the ESXi host IP prompt, enter the IP address of the VMS host.

7 At the user name prompt, enter the user name for an administrative account on the VMS host.

8 At the password prompt, enter the password for the account used in step 7.

9 At the PowerShell, prompt, enter the name of the virtual machine for which you want to update the configuration. Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the VMS host.

10 If the PowerShell prompt appears, perform one of the following actions:

- To apply supplemental configuration to all virtual machines on the VMS host, enter: `All`
- To apply supplemental configuration to a single virtual machine, enter the name of the particular virtual machine. Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the VMS host.

11 When the script output appears, verify that no messages stating `[FAILED]` appear in the output of the script.

12 At the PowerShell prompt, enter: `exit`

13 At the Windows command prompt, enter: `exit`

4.1.6.1 Installing VMware PowerCLI

This procedure installs and configures the PowerCLI utility from the *VMware vSphere Configuration Media* disc onto a Network Management (NM) client, dispatch console, or service laptop.

Prerequisites:

- Log on as administrator.
- Ensure that any existing vSphere client instances are closed.
- Obtain the *VMware vSphere Configuration Media*.

When and where to use: Perform this procedure only if **vSphere VMWare PowerCLI** does not appear in the Windows **Start** menu or does not have contents.

Procedure:

1. Insert the *VMware vSphere Configuration Media* into the optical drive of the Windows-based device that hosts the vSphere Client.
2. On the *VMware vSphere Configuration Media*, navigate to the `WMware vSphere PowerCLI` folder and launch `VMware-PowerCLI.exe`.
3. If a pop-up window appears, click **Continue** or **Yes**.
4. In the **VMware PowerCLI Installation Requirements** window, click **Install**.
5. In the **VMware Remote Console Plug-In** installation welcome screen, click **Next**.
6. In the **Ready to Insstall VMware Remote Console Plug-in** components window, click **Install**.
7. In the **Installation Wizard Completed** window, click **Finish**.
8. In the **VMware VIX** installation welcome window, click **Next**.
9. Follow the on-screen instructions to complete the installation.
10. In the **VMware VIX License Agreement** screen, select **I accept the terms in the license agreement**. Click **Next**.
11. In the **Destination Folder** window, click **Next**.
12. In the **Ready to Install the Program** window, click **Install**.
13. In the **Installer Completed** window, click **Finish**.
14. If a pop-up warning appears, click **Continue**.

    The **VMware vSphere PowerCLI** installation welcome screen appears.

15. At the **Welcome to the InstallShield Wizard** window, click **Next**.
16. On the **License Agreement** window, select **I accept the terms in the license agreement**. Click **Next**.
17. On the **Custom Setup** window, click **Next**.
18. On the **Ready to Install the Program** window, click **Install**.
19. On the **InstallShield Wizard Completed** window, click **Finish**.
20. On the computer/laptop, select **Start**.
21. In the **Search programs and files**, enter: `command`.

    The **Command Prompt** appears in the list of available programs and files.

22. Right-click **Command Prompt** and select **Run as administrator**.
23. At the command prompt, enter: `powershell`

24 At the PowerShell prompt, enter: `set-executionpolicy remotesigned`

25 At the PowerShell prompt, enter: `new-eventlog Application -Source esxiconfig`

If the following message appears, it can be safely ignored.

```
new-eventlog : The 'esxiconfig' source is already registered on the
"localhost" computer.
```

26 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* followed by a colon. Press ENTER.

Step example: `E:`

The directory changes to the root directory of the *VMware vSphere Configuration Media*.

27 At the PowerShell prompt, enter: `cd “VMware vSphere PowerCLI”`

The directory changes to the VMware vSphere PowerCLI directory.

28 At the PowerShell prompt, enter: `.\disableCeip.ps1`

The Customer Experience program is disabled, and installation is complete.

29 Close the **Command Prompt** window.

4.1.7 Configuring the Trunked PDG after Installation

Perform this procedure to configure the Packet Data Gateway (PDG) after powering on a new PDG server virtual machine for the first time. The purpose of this required initial configuration is to set the correct zone number and type of the PDG. Use this procedure for initial configuration only. Do **not** use the procedure to reconfigure the PDG for a different type or zone.

Prerequisites:
Upgrade VMware Tools.

Obtain the following information from your system administrator:

- User name and password for the account with root access to the Packet Data Gateway (PDG) server
- Zone number for the PDG server
- Location of the PDG server (zone core)
- Role of the PDG server in the system (primary or backup server)
- Time zone, which you can find in the following location: `/usr/share/zoneinfo/zone.tab`

Procedure:

1 After powering on the PDG server virtual machine, click the PDG virtual machine (VM) in the navigation pane on the left side of the screen. Click the **Console** tab on the right side of the screen.

2 Activate the console by clicking anywhere in the console window. If the user prompt does not appear, right-click the VM in the left pane. Click **Open Console** or restart the VM client.

3 At the login prompt, log on as a user with root privileges.

4 At the root command prompt, enter: `admin_menu`

5 In the server administration **Main Menu**, enter the number associated with **OS Administration**.

6 In the **OS Administration** menu, enter the number associated with **Manage Platform Configuration**.

7 In the **Manage Platform Configuration** menu, enter the number associated with **Set Identity**.

8 At the DSR configuration prompt, perform one of the following actions:
   - If the system is configured for DSR, enter: `y` and go to step 9.
   - If the system is not configured for DSR, enter: `n` and go to step 10.

9 At the DSR core prompt, perform one of the following actions:
   - If the server is in the Primary Zone Core, enter: `0`
   - If the server is in the Backup Zone Core, enter: `1`

10 At the Zone ID prompt, enter the appropriate zone number from 1–7.

11 At the application ID prompt, enter the appropriate number for your application:
   - For an IV&D PDG in the Primary Zone Core, enter: `1`
   - For an IV&D PDG in the Backup Zone Core, enter: `5`
   - For an HPD PDG in the Primary Zone Core, enter: `2`
   - For an HPD PDG in the Backup Zone Core, enter: `6`

12 At the Centralized Syslog Server prompt, perform one of the following actions:
   - If there are Centralized Syslog Servers installed in this configuration, enter their IPs and hostnames in a list separated by colons.
   - If there are no Centralized Syslog Servers, press ENTER.

13 At the summary, perform one of the following actions:
   - To confirm that the data is correct, enter: `y`
   - To reject and re-enter the data, enter: `n` and go to step 8.
   - To exit this operation, enter: `q`

   The identity configuration is applied and the PDG virtual machine is restarted.

4.1.8
Applying the Platform Patch

You must update the virtual machine by applying the platform patch.

Prerequisites: Obtain the *PLATFORM PATCH* DVD or ISO for the current system release.

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

2 Log on to the ESXi server.

3 Verify whether the following path appears on the toolbar: **Home** → **Inventory** → **Inventory**.

4 In the left pane, navigate to the virtual machine that you want to update.

5 In the right pane, click the **Console** tab.

6 Connect the virtual machine to the local DVD drive or ISO:
   - If you have the DVD, perform the following actions:
     1 Insert the DVD in the drive of the Windows-based device.
     2 In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to *<drive_letter>*:**

       where *<drive_letter>* represents the drive with the DVD.

- If you have the ISO, perform the following actions:
  1. Upload the ISO image to the Windows-based device.
  2. In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1 → Connect to ISO image on local disk**.

7. Navigate to the location of the patch ISO and select it. Click **Open**.
8. Click anywhere in the **Console** tab and log on to the virtual machine as the root user.
9. Enter: `systemctl start autofs`

   If messages appear about the autofs service already running, ignore them.
10. Enter: `ls /media/cdrom0/`

    If the drive contains the updater script, the update directory appears.
11. If the update directory does not appear, enter: `ls /media/cdrom1/`
12. Enter one of the following commands:
    - If the updater script is on cdrom0, enter: `/media/cdrom0/update/updater`
    - If the updater script is on cdrom1, enter: `/media/cdrom1/update/updater`
13. Change the directory to root by entering: `cd /`
14. Enter: `admin_menu`
15. Select **Software Administration → Eject CD/DVD → Eject All**.
16. Remove the DVD or ISO:
    - **a** Disengage the cursor from the console by pressing left CTRL + ALT.
    - **b** In the VMware vSphere Client, click the disc icon on the top toolbar and disconnect the DVD or ISO from the virtual machine.
    - **c** If prompted, confirm the operation.
17. Click anywhere in the **Console** tab.
18. Press ENTER.
19. Enter: `q`
20. Enter: `exit`

4.1.9 Changing the Trunked PDG State to Active in Non-DSR Systems

The Redundancy Configuration menu exists also on Packet Data Gateways (PDG) in systems without Dynamic System Resilience (non-DSR).

When and where to use: After installing and configuring the PDG, change the PDG state to active.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, select **Application Administration** and press ENTER.
3. In the **Application Administration** menu, select **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, select **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** menu, select **Redundancy Configuration** and press ENTER.

6 In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration** and press Enter.

PDG redundancy states are displayed. The initial default PDG state is user requested standby.

7 In the **Modify Redundancy Configuration** window, perform the following actions:

a Select **Active** using arrow keys. Press Enter.

b Select **Submit** using arrow keys. Press Enter.

A warning appears, informing that the next action will enable automatic switchover and may enable the PDG for data service.

8 To proceed, select **Yes** and press Enter.

A message appears, confirming that the PDG redundancy state has been set to active.

9 To exit the **PDG Local Configuration** menu, perform the following actions:

a Enter: `q`

b Enter: `y`

The **Application Specific Management and Operations** menu appears.

10 To exit the **Main Menu**, enter: `q` and press Enter.

The user's command prompt appears.

4.2 Trunked PDG Database Synchronization

You have to synchronize the PDG database with the network management database to perform other configuration and to enable data services on the PDG. The Database Synchronization Interface allows you to synchronize the PDG database with the network management database and download the database to the PDR. For the procedures, see “PM Data Sync State” in the *Unified Network Configurator User Guide*.

IMPORTANT: After the PDG database is synchronized, you have to perform a force initialization. For details, see “Distributing Full Configuration (Force Initialize Configuration)” in the *Provisioning Manager User Guide*.

4.3 High Availability Configuration

To enable the High Availability for Trunked IV&D and HPD (HA Data) feature for the PDG, perform the installation and configuration procedures in the *ASTRO 25 vCenter Setup and Operations Guide*. To learn more about the HA Data feature, see the *Trunked Data Services Feature Guide*.

4.4 Dynamic System Resilience Configuration

If your system supports Dynamic System Resilience (DSR), perform the procedures in this section. To learn more about the DSR feature, see the *Dynamic System Resilience Feature Guide*.

IMPORTANT: The DSR configuration procedures described in this section are only applicable if your system supports the DSR feature. For more information, contact your system administrator.

4.4.1 Setting Heartbeat Key on the Trunked PDG

The primary core Packet Data Router (PDR) and backup core PDR exchange authenticated heartbeats. The heartbeat message contains the number of sites connected to the Radio Network Router (RNG) and the operational health of the PDR itself.

Prerequisites: Ensure that PDR is running. If the PDR service is not running, perform the Starting the Trunked PDR on page 168 procedure before starting this procedure.

When and where to use: Perform this procedure on both the primary and the backup PDR and enter the same key on both.

Procedure:

1. Log on to the PDG and invoke the Main Menu (see Logging On to the Trunked PDG and Invoking the Main Menu on page 161).
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations** and press ENTER.
5. In the **PDR Specific Management and Operations** menu, type the number associated with **Heartbeat Key Setting** and press ENTER.
6. In the **Set Heartbeat Key** menu, perform one of the following actions:

   IMPORTANT: Before performing this step, verify that the backup PDG is in the User Requested Standby (URS) state. Otherwise, the HA link goes down, and the peer (backup) PDG goes active. See Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

If…	Then…
If you want to set an ASCII-based key,	perform the following actions: **a** Type `1` and press ENTER. **b** Type the 16-character ASCII key. **c** Retype the same 16-character ASCII key. A message appears, informing that the operation has been successful, and you return to the **PDR Specific Management and Operations** menu.
If you want to set a Hexadecimal based key,	**a** Type `2` and press ENTER. **b** Type the 32-character Hexadecimal Key. **c** Retype the same 32-character Hexadecimal Key. A message appears, informing that the operation has been successful, and you return to the **PDR Specific Management and Operations** menu.
If you want to exit,	type `q` and press ENTER.

4.4.2 Verifying the HA Link Status on the PDR

Prerequisites: Ensure that the PDR is running. If the PDR service is not running, then perform Starting the Trunked PDR on page 168 before starting this procedure.

When and where to use:
After you set Heartbeat Key on both the active and the backup PDR, perform the following procedure to verify the HA Link status on both active and backup PDR.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **Local Configuration** interface, select **Redundancy Configuration** and press ENTER.
6. In the **Redundancy Configuration** menu, select **View Redundancy Configuration** and press ENTER.

   In the **View Redundancy Configuration** menu, the HA link status can be **Link Up** or **Link Down**. In a normally operated Dynamic System Resilience (DSR) system, the HA link status is **Link Up**.
7. To exit the **View Redundancy Configuration** menu, type `q`, and then type `y`.
8. To exit the **Main Menu**, type `q` and press ENTER.

4.5 Trunked PDG Redundancy Configuration

In a Dynamic System Resilience (DSR) configuration, the Packet Data Gateway (PDG) is redundant in the backup core. In case of the primary PDG failure, an automatic switchover takes place and the backup PDG becomes active and minimizes loss of data services. In a non-DSR configuration, no backup core exists with a redundant PDG.

A PDG can be in one of the following three states:

- Active
- Standby
- User Requested Standby

Depending on your system configuration, set the PDG to active or standby state:

Table 5: PDG States in DSR and Non-DSR Systems

DSR System	Non-DSR System
Set the primary PDG to the active state. Set the backup PDG to the standby state.	Always keep the PDG in the active state.

Active State

In the active state, the PDR is capable of establishing a data session with a GGSN and RNG. Upon establishing a data session with a PDR, the RNG can accept connection requests from RF sites and a remote PDR in other zones. Upon establishing a data session with the PDR, the GGSN forwards outbound data for the radios that are currently context activated. To set the PDG to the active state, perform Setting the Trunked PDG to the Active State (DSR) on page 162.

Standby State

In the standby state, the PDR is capable of an automatic switchover. While a PDR is in a standby state, it suspends establishing a data session to the local RNG, remote RNG in other zones and GGSN. Without a connection to a PDR, the RNG does not accept link-up requests from RF sites or remote PDR in other zones. The GGSN does not forward any data to a PDR without a data session established. The PDR monitors heartbeat messages from the active PDR. If the PDR misses consecutive heartbeats or is informed that the other PDR can no longer remain active, it becomes active. To set the PDG to the standby state, perform Setting the Trunked PDG to the Standby State (DSR) on page 163.

User Requested Standby State

In the User Requested Standby state, the PDR disables the automatic switchover capability and remains in a User Requested Standby state until you change the state to standby or active. To set the PDG to the user requested standby state, perform Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

Chapter 5

Conventional IVD M Core and K Core PDG Installation

This chapter details the installation procedures related to the Conventional IV&D M core and K core Packet Data Gateway (PDG).

5.1

Deploying the Conventional PDG Virtual Appliance

The Packet Data Gateway (PDG) is installed on the virtual server. PDGs reside as virtual machines on an ESXi platform which has its own installation and configuration process.

For information about mechanical installation, power supply, hardware specifications, and physical specifications, security settings, and other, see the *Virtual Management Server Software User Guide*.

Prerequisites:
Review the entire software installation process and each supporting procedure before installing the PDG software.

To avoid damage during shipping, external system cables are often removed before packing and later connected during installation. Installation of a Conventional PDG on the server requires a cable connection to CDEM.

NOTICE: The Conventional IV&D K core PDG uses the Command Line Interface commands to configure the parameters for an M core that are configured in Unified Network Configurator (UNC). For more information, see Conventional IVD K Core PDG Configuration on page 261.

Process:

1. Satisfy all appropriate requirements and review all appropriate installation considerations before installing the PDG software. See Conventional PDG Software Installation – Requirements and Considerations on page 74.
2. Deploy the Packet Data Gateway Virtual Appliance. Perform the appropriate procedure for your system configuration:
   - To deploy the Conventional PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75.
   - To deploy the Conventional PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380) on page 78.
3. If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88
4. Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61.
5. Apply the supplemental configuration. See Applying Supplemental Configuration to Virtual Machines on page 63.
6. If required by your organizational policies, disable password aging on the PDG. See “Disabling Password Aging for the Root Account” in the *Unix Supplemental Configuration Setup Guide*.

7 Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.

8 Perform initial configuration of the PDG. See Configuring the Conventional PDG after Installation on page 84.

9 Join the PDG to the Active Directory Domain. See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide*.

> **NOTICE:** This step is not applicable to the Conventional IV&D K core PDG. On this type of PDG, perform authentication locally through the local Operating System facilities.

10 Apply the platform patch to the PDG. See Applying the Platform Patch on page 86.

11 If applicable, perform Linux OS patching on the PDG. Installation procedures for the MOTOPATCH are available at: https://sites.google.com/a/motorolasolutions.com/susmotopatch/

If you cannot open the link, this means that MOTOPATCH for RHEL v7 is not available yet. Skip this step.

12 If required by your organizational policies, configure the PDG for SNMPv3 and SSH. For more information, see the *SNMPv3 Feature Guide* and *Securing Protocols with SSH Feature Guide*.

Ask your system administrator which procedures and/or commands you should use, depending on your organizational policies.

13 Synchronize the PDG database. Use the appropriate tools, depending on your PDG type:

- For the Conventional IV&D M core PDG, see Conventional IVD M Core PDG Database Synchronization on page 90.
- For the Conventional IV&D K core PDG, see Conventional IVD K Core PDG Configuration on page 261.

14 Change the PDG state to active. See Changing the Conventional PDG State to Active on page 87.

15 **Conventional IV&D PDG in K cores**: Back up the PDG database on a regular basis. See Backing Up a Conventional IVD PDG in a K Core on page 184.

> **NOTICE:** In M cores, the Backup and Restore (BAR) server backs up the Conventional IV&D PDG.

16 Back up the SSH configuration and keys on the PDG, using commands that are common to the Linux devices in an ASTRO® 25 system. See the *Securing Protocols with SSH Feature Guide*.

5.1.1
Conventional PDG Software Installation – Requirements and Considerations

The following table lists the requirements and considerations for PDG software installation. Review each topic to ensure that you are able to perform a successful software installation of the PDG.

Table 6: Requirements and Considerations for Conventional PDG Software Installation

Requirement or Consideration	Description
Backup and Restore Considerations	There is no data to back up or restore in a new installation. If you want to reinstall the software and there is an existing database, then the PDG data must be backed up before reinstalling the software. Once the installation is completed, conduct a data restore to the PDR.

Table continued…

Requirement or Consideration	Description
Reinstallation or Upgrade Considerations	To ensure that the PDG software installation is successful, reinstalling, or upgrading the operating system as a separate procedure is not supported.
Network Management Support (Conventional IV&D M core PDG only)	The Unified Network Configurator (UNC) plays an important supporting role in installing the PDG software. Unless specified, the processes and procedures in this manual assume that the UNC and other network manager applications are installed and running in the X-zone network when installing PDG software.
Resetting and Shutdown Considerations	Do not shut down by pressing the power button or disconnecting the power cord, if it can be avoided. For PDR, RNG, and all PDG resets and shutdowns, it is recommended that you use options from the **admin_menu**.
AAA Server (Conventional IV&D M core PDG only)	The AAA server plays an important supporting role in installing and operating the PDG software.

5.1.1.1
Conventional PDG Access

Access the PDG console for maintenance tasks, such as installing software, configuration, or monitoring by connecting to the Virtual server through the network from the VMware Sphere Client application, which should be installed on a Windows-based machine.

5.1.2
Domain User Names and Domain User/Root Account Passwords Data Value Requirements and Criteria for the Conventional PDG

- See “Changing Root Account Passwords for Linux-Based Devices” in the *Unix Supplemental Configuration Setup Guide* for the root account password criteria.
- See “User/Group Name Restrictions” in the *Authentication Services Feature Guide* for Domain User names criteria.
- See “User Input Requirements for Server Installation/Configuration” in the *Authentication Services Feature Guide* for Domain User account passwords criteria.

5.1.3
Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380)

Perform this procedure to deploy the Conventional Packet Data Gateways (PDG) in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380).

Prerequisites:
Obtain the following from your system administrator:

- Motorola Virtual Appliance media (contains the PDG virtual machine files)
- Virtual Server host (ESXi-based server) IP address
- ESXi-based server root account password

- Hostname for the PDG
- Zone network for the PDG virtual machine

For more information on installing and configuring virtual machines on an HP DL380 server, see the *Virtual Management Server Software User Guide*.

When and where to use: Use this procedure only for a *conventional* PDG. For a trunked IV&D or HPD PDG, use Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 57.

Procedure:

1 Launch the VMware vSphere Client from the Windows-based device where it resides.

2 Log on to the ESXi server where the PDG is being deployed with root credentials.

  The **vSphere Client Inventory** window appears.

3 Insert the PDG install media to the optical drive of the Windows-based device where the vSphere client was launched.

4 Select **File** → **Deploy OVF Template**.

5 In the **Deploy OVF Template – Source** window, select the source of the PDG OVF template:

  a Click **Browse**.

  b Select the PDG OVF template.

  c Click **Next**.

6 In the **Deploy OVF Template – OVF Template Details** window, verify the OVF template details and click **Next**.

7 In the **Deploy OVF Template – Name and Location** window, enter the name for the PDG:

  a For a Conventional IV&D PDG, type:
  `convpdr` ***<X>***`.zone`***<Y>***

  where:
  <X> represents the core type (`01` for a primary core or `02` for a backup core).
  <Y> represents the zone number (ranging from 1 to 7).

  b Click **Next**.

8 Click **Next**.

9 In the **Deploy OVF Template – Storage** window, select the storage location:

  a Use **z00*<X>*das0*<Y>*_datastore1**

  where:
  <X> is the zone number
  <Y> is the instance number of the DAS that the VMS the PDG is being installed upon is connected to.

  b Click **Next**.

10 In the **Deploy OVF Template – Disk Format** window, select the disk format:

  a Select **Thick Provision Eager Zeroed**. If this option is not available, select **Thick Provision**.

  b Click **Next**.

11 In the **Deploy OVF Template – Network Mapping** window, select the **Destination Network** for each **Source Network**:

  a For **data0**, select **data0**.

  b For **cdem**, select **cdem**.

c Click **Next**.

12 In the **Deploy OVF Template – Ready to Complete** window, confirm the values displayed are correct and click **Finish**.

NOTICE: Do not check **Power on after deployment** as there are additional modifications to the PDG VM to be done after deployment that requires the PDG VM to be powered off.

The template is being deployed and the deployment status bar appears.

13 When the deployment has been completed successfully, click **Close**.

The deployed PDG is now present in the vSphere Client.

14 In the **vSphere Client Inventory** window, perform the following actions:

a Right-click the newly deployed PDG VM.

b Select **Edit Settings**

c Click the **Options** tab.

d In the left pane, under **Advanced**, click **General**.

e In the right pane, click **Configuration Parameters**

15 In the **Configuration Parameters** window, perform the following actions:

a Click **Add Row**.

A new row appears at the bottom of the list.

b In the **Name** column for that row, type: `ethernet0.coalescingScheme` and press TAB.

c In the **Value** column for that row, enter: `disabled`

d Click **Add Row**.

A new row appears at the bottom of the list.

e In the **Name** column for that row, type `ethernet1.coalescingScheme` and press TAB.

f In the **Value** column for that row, type `disabled` and press ENTER.

g Click **Add Row**.

A new row appears at the bottom of the list.

h In the **Name** column for that row, type `ethernet2.coalescingScheme` and press TAB.

i In the **Value** column for that row, type `disabled` and press ENTER.

j Click **OK**.

The **Configuration Parameters** window closes.

16 In the **Resources** tab, reserve CPU resources for the PDG:

a In the left pane, click **CPU**.

b In the right pane, in the **Reservation** text box, enter the value that corresponds to the type of server used in your system.

- For a Gen8 server in any system, enter: `1296 MHz`
- For a Gen9 server in an M core or L core system, enter: `1248 MHz`
- For a Gen9 server in a K core system, enter: `1198 MHz`

c Click **OK**.

17 In the **vSphere Client**, right-click the **PDG VM** and select **Power** → **Power On**.

The newly deployed PDG VM is powered on.

5.1.4 Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380)

Perform this procedure to deploy the Conventional Packet Data Gateway (PDG) as a virtual machine on a dedicated VMS Host Server (DL380).

Prerequisites:
Obtain the following from your system administrator:

- Motorola Virtual Appliance media (contains the PDG virtual machine files)
- Virtual Server host (ESXi-based server) IP address
- ESXi-based server root account password
- Hostname for the PDG
- Zone network for the PDG virtual machine

For more information on installing and configuring virtual machines on an HP DL380 server, see the *Virtual Management Server Software User Guide*.

Procedure:

1 Launch the VMware vSphere Client from the Windows-based device where it resides.

2 At the login prompt, log on to the ESXi server where the PDG is being deployed with root credentials.

The **vSphere Client Inventory** window appears.

3 Insert the PDG install media to the optical drive of the Windows-based device where the vSphere client was launched.

4 Select **File** → **Deploy OVF Template**.

5 In the **Deploy OVF Template – Source** window, select the source of the PDG OVF template:

a Click **Browse**.

b Select the PDG OVF template.

c Click **Next**.

6 In the **Deploy OVF Template – OVF Template Details** window, verify the OVF template details and click **Next**.

7 In the **Deploy OVF Template – Name and Location** window, type the name for the PDG:

a For a Conventional PDG, type `convpdr` ***<x.>***`zone`***<y>***

where ***<X>*** represents the core type (`01` for a primary core or `02` for a backup core) and ***<Y>*** represents the zone number (ranging from 1 to 7).

b Click **Next**.

8 In the **Deploy OVF Template – Storage** window, select the storage location:

a For all system configurations, select **z00Xvms0Y_datastore1** .

b Click **Next**.

9 In the **Deploy OVF Template – Disk Format** window, select the disk format:

a Select **Thick Provision Eager Zeroed**. If this option is not available, select **Thick Provision**.

b Click **Next**.

10 In the **Deploy OVF Template – Network Mapping** window, select the **Destination Network** for each **Source Network**:

a For **data0**, select **data0**.

b Click **Next**.

11 In the **Deploy OVF Template – Ready to Complete** window, confirm the values displayed are correct and click **Finish**.

NOTICE: Do not check **Power on after deployment** as there are additional modifications to the PDG VM to be done after deployment that require the PDG VM to be powered off.

The template is being deployed and the deployment status bar appears.

12 When the deployment has been completed successfully, click **Close**.

The deployed PDG is now present in the vSphere Client.

13 Reserve CPU resources for the PDG:

If…	Then…
If you have the Gen8 server in an M or L core system,	Perform the following actions: **a** Right-click the newly deployed PDG VM. **b** Select **Edit Settings**. **c** Click the **Resources** tab. **d** In the left pane, click **CPU**. **e** In the right pane, in the **Reservation** text box, type `1296 MHz` for a Conventional IV&D PDG. **f** Click **OK**.
If you have the Gen8 server in a K core system,	Perform the following actions: **a** Right-click the newly deployed PDG VM. **b** Select **Edit Settings**. **c** Click the **Resources** tab. **d** In the left pane, click **CPU**. **e** In the right pane, in the **Reservation** text box, type `1296 MHz` for a Conventional IV&D PDG. **f** Click **OK**.
If you have the Gen9 server in an M or L core system,	Perform the following actions: **a** Right-click the newly deployed PDG VM. **b** Select **Edit Settings**. **c** Click the **Resources** tab. **d** In the left pane, click **CPU**. **e** In the right pane, in the **Reservation** text box, type `1248 MHz` for a Conventional IV&D PDG. **f** Click **OK**.

If…	Then…
If you have the Gen9 server in a K core system,	Perform the following actions: **a** Right-click the newly deployed PDG VM. **b** Select **Edit Settings**. **c** Click the **Resources** tab. **d** In the left pane, click **CPU**. **e** In the right pane, in the **Reservation** text box, type `1198 MHz` for a Conventional IV&D PDG. **f** Click **OK**.

14 In the **vSphere Client**, right-click the **PDG VM** and select **Power** → **Power On**.

The newly deployed PDG VM is powered on.

5.1.5 Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) host are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS host, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.
2. Log on to the server as a user with root privileges.
3. On the upper left side of the **vSphere Client Inventory** window, select the ESXi server that serves as the VMS host.
4. On the right side of the window, select the **Configuration** tab.

   The window displays information about the configuration of the selected server.
5. In the **Software** section, select **Virtual Machine Startup/Shutdown**.
6. On the right side of the main window, select **Properties**.
7. In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.
8. In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.
9. In the **Default Shutdown Delay** area, select **Shutdown Action** → **Guest Shutdown**.
10. Set the boot order for the virtual machines hosted on the server:

    a In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

    b Using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

    To determine the correct ordered slot for each virtual machine hosted on the server that you are configuring, see Zone Core Virtual Machine Boot Order on page 62.

    c Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.
11. Click **OK**.

    The **Properties** window closes.

5.1.5.1

Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the Graphical Master Computer (GMC) for MOSCAD Network Fault Management (NFM) can be on the server.

If the Unified Network Configurator Database Server (UNCDS is present, three instances of the UNCDS are on the server.

Table 7: Zone Core Virtual Machine Boot Order

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	ZC	Enabled	Use Default	Use Default	Use Default
2	Transcoder	Enabled	Use Default	Use Default	Use Default
3	ISGW	Enabled	Use Default	Use Default	Use Default
4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
7	License Manager	Enabled	Use Default	Use Default	Use Default
8	ATR	Enabled	Use Default	Use Default	Use Default
9	DC-System	Enabled	Use Default	Use Default	Use Default
10	DC-Zone	Enabled	Use Default	Use Default	Use Default
11	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order	AuC	Enabled	Use Default	Use Default	Use Default
	BAR	Enabled	Use Default	Use Default	Use Default
	CSMS	Enabled	Use Default	Use Default	Use Default
	InfoVista	Enabled	Use Default	Use Default	Use Default
	FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
	GDG	Enabled	Use Default	Use Default	Use Default
	GMC	Enabled	Use Default	Use Default	Use Default
	NM Client	Enabled	Use Default	Use Default	Use Default
	UCS	Enabled	Use Default	Use Default	Use Default
	SSS	Enabled	Use Default	Use Default	Use Default
	Syslog	Enabled	Use Default	Use Default	Use Default
	UEM	Enabled	Use Default	Use Default	Use Default
	UNC	Enabled	Use Default	Use Default	Use Default
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default

Table continued…

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

5.1.6
Applying Supplemental Configuration to Virtual Machines

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) may require supplemental configuration to improve their security settings, depending on the security requirements of your organization. Users apply the supplemental configuration by running a script stored on the configuration media listed in the Prerequisites to this procedure.

Prerequisites:

- Obtain the *VMware vSphere Configuration Media*.
- Install the VMware PowerCLI application on the Windows-based device. See Installing VMware PowerCLI on page 65.

When and where to use:
Perform this procedure on a Windows-based device, such as a Network Management (NM) client, dispatch console, or service computer or laptop.

During an upgrade, you must run the script specifically on the newly imported virtual machines if the virtual machines were imported after the VMS host was updated.

Procedure:

1. Insert the *VMware vSphere Configuration Media* into the optical drive of the Windows-based device.
2. Open the PowerShell command prompt as administrator, using the actions that apply to the Windows operating system version that is present on the device.
   - For Windows 7 or Windows Server 2008, perform the following actions:
     1. From **Start**, in the **Search programs and files** field, enter: `Command Prompt`
     2. Right-click **Command Prompt** and select **Run as administrator**.
     3. If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see.
     4. If you are not logged on with an administrative account, enter the domain admin credentials.
     5. At the command prompt, enter: `powershell`
   - For Windows 10 or Windows Server 2012, perform the following actions:
     1. From **Start**, click **Search**.
     2. In the search field, type in `powershell`
     3. Right-click **Windows PowerShell**, and select **Run as administrator**.
        - If the **User Account Control** window appears, click **Yes**.
        - If you are not logged on with an administrative account, enter the domain admin credentials.
3. At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* followed by a colon.

   Step example: `E:`
   The directory is changed to the root directory of the *VMware vSphere Configuration Media*.

4 At the PowerShell prompt, enter: `cd common\bin`

The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media*.

5 At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`

6 At the ESXi host IP prompt, enter the IP address of the VMS host.

7 At the user name prompt, enter the user name for an administrative account on the VMS host.

8 At the password prompt, enter the password for the account used in step 7.

9 At the PowerShell, prompt, enter the name of the virtual machine for which you want to update the configuration. Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the VMS host.

10 If the PowerShell prompt appears, perform one of the following actions:

- To apply supplemental configuration to all virtual machines on the VMS host, enter: `All`
- To apply supplemental configuration to a single virtual machine, enter the name of the particular virtual machine. Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the VMS host.

11 When the script output appears, verify that no messages stating `[FAILED]` appear in the output of the script.

12 At the PowerShell prompt, enter: `exit`

13 At the Windows command prompt, enter: `exit`

5.1.6.1
Installing VMware PowerCLI

This procedure installs and configures the PowerCLI utility from the *VMware vSphere Configuration Media* disc onto a Network Management (NM) client, dispatch console, or service laptop.

Prerequisites:

- Log on as administrator.
- Ensure that any existing vSphere client instances are closed.
- Obtain the *VMware vSphere Configuration Media*.

When and where to use: Perform this procedure only if **vSphere VMWare PowerCLI** does not appear in the Windows **Start** menu or does not have contents.

Procedure:

1 Insert the *VMware vSphere Configuration Media* into the optical drive of the Windows-based device that hosts the vSphere Client.

2 On the *VMware vSphere Configuration Media*, navigate to the `WMware vSphere PowerCLI` folder and launch `VMware-PowerCLI.exe`.

3 If a pop-up window appears, click **Continue** or **Yes**.

4 In the **VMware PowerCLI Installation Requirements** window, click **Install**.

5 In the **VMware Remote Console Plug-In** installation welcome screen, click **Next**.

6 In the **Ready to Insstall VMware Remote Console Plug-in** components window, click **Install**.

7 In the **Installation Wizard Completed** window, click **Finish**.

8 In the **VMware VIX** installation welcome window, click **Next**.

9 Follow the on-screen instructions to complete the installation.

10 In the **VMware VIX License Agreement** screen, select **I accept the terms in the license agreement**. Click **Next**.

11 In the **Destination Folder** window, click **Next**.

12 In the **Ready to Install the Program** window, click **Install**.

13 In the **Installer Completed** window, click **Finish**.

14 If a pop-up warning appears, click **Continue**.

The **VMware vSphere PowerCLI** installation welcome screen appears.

15 At the **Welcome to the InstallShield Wizard** window, click **Next**.

16 On the **License Agreement** window, select **I accept the terms in the license agreement**. Click **Next**.

17 On the **Custom Setup** window, click **Next**.

18 On the **Ready to Install the Program** window, click **Install**.

19 On the **InstallShield Wizard Completed** window, click **Finish**.

20 On the computer/laptop, select **Start**.

21 In the **Search programs and files**, enter: `command`.

The **Command Prompt** appears in the list of available programs and files.

22 Right-click **Command Prompt** and select **Run as administrator**.

23 At the command prompt, enter: `powershell`

24 At the PowerShell prompt, enter: `set-executionpolicy remotesigned`

25 At the PowerShell prompt, enter: `new-eventlog Application -Source esxiconfig`

If the following message appears, it can be safely ignored.

```
new-eventlog : The 'esxiconfig' source is already registered on the
"localhost" computer.
```

26 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* followed by a colon. Press ENTER.

Step example: `E:`

The directory changes to the root directory of the *VMware vSphere Configuration Media*.

27 At the PowerShell prompt, enter: `cd “VMware vSphere PowerCLI”`

The directory changes to the VMware vSphere PowerCLI directory.

28 At the PowerShell prompt, enter: `.\disableCeip.ps1`

The Customer Experience program is disabled, and installation is complete.

29 Close the **Command Prompt** window.

5.1.7 Configuring the Conventional PDG after Installation

Perform this procedure to configure the Packet Data Gateway (PDG) after powering on a new PDG server virtual machine for the first time. The purpose of this required initial configuration is to set the correct zone number and type of the PDG. Use this procedure for initial configuration only. Do **not** use this procedure to reconfigure the PDG for a different type or zone.

Prerequisites:
Upgrade VMware Tools.

Obtain the following from your system administrator:

- User name and password for the account with root access to the Packet Data Gateway (PDG) server
- Zone number for the PDG server
- Location of the PDG server (zone core)
- Type of the PDG in the system – Conventional IV&D M core or Conventional IV&D K core
- Time zone, which can be found in the following location: `/usr/share/zoneinfo/zone.tab`

Procedure:

1. After powering on the PDG server virtual machine, click the PDG virtual machine in the navigation pane on the left side of the screen. Click the **Console** tab on the right side of the screen.
2. Click anywhere in the console to activate it. If the prompt does not appear, right-click the VM in the left pane. Click **Open Console** or restart the VM client.
3. At the login prompt, log in as a user with root privileges.
4. At the root command prompt, enter: `admin_menu`
5. In the server administration **Main Menu**, enter the number associated with **OS Administration**.
6. In the **OS Administration** menu, enter the number associated with **Manage Platform Configuration**.
7. In the **Manage Platform Configuration**, enter the number associated with **Set Identity**.
8. At the DSR configuration prompt, perform one of the following actions:
   - If the system is configured for DSR, enter: `y` and go to step 9.
   - If the system is not configured for DSR, enter: `n` and go to step 10.
9. At the DSR core prompt, perform one of the following actions:
   - If the server is in the Primary Zone core, enter: `0`
   - If the server is in the Backup Zone core, enter: `1`
10. At the Zone ID prompt, enter the appropriate zone number from 1 - 7.
11. At the application ID prompt, enter the appropriate number for your application:
    - For a Conventional M core IV&D PDG (CIVD), enter: `9`
    - For a Conventional K core IV&D PDG (IVDE), enter: `10`
    - For a Conventional M core IV&D (CIVD) backup, enter `11`
12. At the Centralized Syslog Server prompt, perform one of the following actions:
    - If there are Centralized Syslog Servers installed in this configuration, enter them in a colon-separated list of IPs and hostnames and press Enter.
    - If there are no Centralized Syslog Servers, press Enter.
13. At the summary, perform one of the following actions:
    - To confirm that the data is correct, enter: `y`
    - To reject and re-enter the data, enter: `n` and go to step 8.

- To exit this operation, enter: `q`

The identity configuration is applied and the PDG virtual machine is restarted.

5.1.8

Applying the Platform Patch

You must update the virtual machine by applying the platform patch.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.
2. Log on to the ESXi server.
3. Verify whether the following path appears on the toolbar: **Home** → **Inventory** → **Inventory**.
4. In the left pane, navigate to the virtual machine that you want to update.
5. In the right pane, click the **Console** tab.
6. Connect the virtual machine to the local DVD drive or ISO:
   - If you have the DVD, perform the following actions:
     1. Insert the DVD in the drive of the Windows-based device.
     2. In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to *`<drive_letter>`*:**

        where ***`<drive_letter>`*** represents the drive with the DVD.
   - If you have the ISO, perform the following actions:
     1. Upload the ISO image to the Windows-based device.
     2. In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to ISO image on local disk**.
7. Navigate to the location of the patch ISO and select it. Click **Open**.
8. Click anywhere in the **Console** tab and log on to the virtual machine as the root user.
9. Enter: `systemctl start autofs`

   If messages appear about the autofs service already running, ignore them.
10. Enter: `ls /media/cdrom0/`

    If the drive contains the updater script, the update directory appears.
11. If the update directory does not appear, enter: `ls /media/cdrom1/`
12. Enter one of the following commands:
    - If the updater script is on cdrom0, enter: `/media/cdrom0/update/updater`
    - If the updater script is on cdrom1, enter: `/media/cdrom1/update/updater`
13. Change the directory to root by entering: `cd /`
14. Enter: `admin_menu`
15. Select **Software Administration** → **Eject CD/DVD** → **Eject All**.
16. Remove the DVD or ISO:
    a. Disengage the cursor from the console by pressing left CTRL + ALT.
    b. In the VMware vSphere Client, click the disc icon on the top toolbar and disconnect the DVD or ISO from the virtual machine.
    c. If prompted, confirm the operation.

17 Click anywhere in the **Console** tab.

18 Press ENTER.

19 Enter: `q`

20 Enter: `exit`

5.1.9 Changing the Conventional PDG State to Active

The Redundancy Configuration menu exists also on Packet Data Gateways (PDG) in systems without Dynamic System Resilience (non-DSR).

When and where to use: After installing and configuring the PDG, change the PDG state to active.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, select **Application Administration** and press ENTER.
3. In the **Application Administration** menu, select **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, select **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** menu, select **Redundancy Configuration** and press ENTER.
6. In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration** and press ENTER.

   PDG redundancy states are displayed. The initial default PDG state is user requested standby.

7. In the **Modify Redundancy Configuration** menu, perform the following actions:
   - **a** Select **Active** using arrow keys and press ENTER.
   - **b** Select **Submit** using arrow keys and press ENTER.

   A warning informing that the next action will enable automatic switchover and may enable the PDG for data service appears.

8. To proceed, select **Yes** and press ENTER.

   A message appears, confirming that the PDG redundancy state has been set to active.

9. To exit the **PDG Local Configuration** menu, perform the following actions:
   - **a** Type `q` and press ENTER.
   - **b** Type `y` and press ENTER.

   The **Application Specific Management and Operations** menu appears.

10. To exit the **Main Menu**, type `q` and press ENTER.

    The user's command prompt appears.

5.1.10 Modifying vCenter MotoMaster Password and Verifying Connection to vCenter

Perform this procedure to update the vCenter MotoMaster user's password on the Packet Data Gateway and to verify the connection is working.

Prerequisites: Conventional PDG installation is complete.

When and where to use: Perform these steps after installation of the PDG or after a change of the MotoMaster password on the vCenter. Without this procedure, conventional PDG communications to the vCenter may not work and unnecessary events could appear in the UEM.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, select **Application Administration** and press ENTER.
3. In the **Application Administration** menu, select **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, select **PDR Specific Management and Operations** and press ENTER.
5. Select **Modify vCenter Motomaster password** and press ENTER.

   The following message appears: `Please enter the updated password for vCenter MotoMaster user.`

6. Type the new password and press ENTER.

   The following message appears on successful update: `The value of property` ***`<mtmspwd>`*** `in application group` ***`<vcgrp xxx>`*** `was changed successfully.`

7. Retype the new password for validation and press ENTER.
8. Select **Verify connection to vCenter** and press ENTER.

   The following message appears: `PDG Connected to vCenter Successfully.`

   NOTICE: If a different message appears, indicating a failure, act according to the message to resolve the issue.

9. To exit the admin menu, type `Q` and press ENTER.

5.1.11 Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default High Availability (HA) cluster settings and modify the restart priority for the new virtual machines. After a Virtual Management Server (VMS) host fails, the virtual machines are restarted in the relative order determined by their restart priority.

When and where to use:

- This procedure applies only to systems where the vCenter application is installed.

- Perform this procedure only if an Open Virtualization Format (OVF) virtual machine was deployed after the vCenter was originally configured.

Procedure:

1. Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.
   - In the address field of the browser, enter the address in the following format: `https://`***`<vCenter_IP_address>`***`/vsphere-client`
   - Ignore or accept any warnings about the connection security or self-signed certificates.
2. In the dialog box, perform the following actions:
   - **a** Enter the user name in the following format:

     `administrator@z00`***`<Z>`***`vcs`***`<H>`***`.zone`***`<Z>`***
     `<Z>` is the zone number

     `<H>` is the vCenter instance number
   - **b** Enter the password for the administrator account.
   - **c** Click **Login**.

   The vSphere Web Client homepage appears.
3. In the left pane, click **Hosts and Clusters**.
4. Expand the tree and right-click the **Zone*<X>*** HA cluster

   where ***<X>*** is the zone number.
5. Select **Settings**.
6. In the **Settings** window, click **VM Overrides**.
7. Click **Add**.
8. Click the plus (**+**) button.
9. Select the check box for the virtual machine you are configuring. Click **OK**.
10. Depending on the virtual machine you are configuring, select the appropriate value for **VM Restart Priority**.
    - For the vCenter virtual machine, select **Medium**.
    - For virtual machines that are monitored under Fault Tolerance, select **High**.
    - For virtual machines that are not monitored under Fault Tolerance or HA, select **Disabled**.
11. Click **OK**.
12. Optional: **If you are recovering the virtual machine after a failure and the virtual machine is not monitored under Fault Tolerance:** Perform the following actions:
    - **a** In the **Settings** window, click **VM/Host Groups**.
    - **b** Select the group for the VMS host where the virtual machine resides. Click **Edit**.
    - **c** Click **Add**.
    - **d** Select the check box next to the virtual machine. Click **OK**.

      For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
    - **e** Click **OK**.

    The restart priority setting for the newly deployed virtual machine is configured.

5.2
Conventional IVD M Core PDG Database Synchronization

You need to synchronize the PDG database with the network management database to perform other configuration and to enable data services on the PDG. The Database Synchronization Interface allows you to synchronize the PDG database with the network management database and download the database to the PDR. For the procedures, see “PM Data Sync State” in the *Unified Network Configurator User Guide*.

IMPORTANT: After the PDG database is synchronized, you have to perform a force initialization. For details, see “Distributing Full Configuration (Force Initialize Configuration)” in the *Provisioning Manager User Guide*.

5.3
High Availability Configuration

To enable the High Availability for Conventional IV&D (HA Data) feature for the PDG, perform the installation and configuration procedures in the *ASTRO 25 vCenter Setup and Operations Guide*. To learn more about the HA Data feature, see the *Conventional Data Services Feature Guide*.

5.4
Dynamic System Resilience Configuration

If your system supports Dynamic System Resilience (DSR), perform the procedures in this section. To learn more about the DSR feature, see the *Dynamic System Resilience Feature Guide*.

IMPORTANT: The DSR configuration procedures described in this section are only applicable if your system supports the DSR feature. For more information, contact your system administrator.

5.4.1
Setting Heartbeat Key on the Trunked PDG

The primary core Packet Data Router (PDR) and backup core PDR exchange authenticated heartbeats. The heartbeat message contains the number of sites connected to the Radio Network Router (RNG) and the operational health of the PDR itself.

Prerequisites: Ensure that PDR is running. If the PDR service is not running, perform the Starting the Trunked PDR on page 168 procedure before starting this procedure.

When and where to use: Perform this procedure on both the primary and the backup PDR and enter the same key on both.

Procedure:

1 Log on to the PDG and invoke the Main Menu (see Logging On to the Trunked PDG and Invoking the Main Menu on page 161).

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations** and press ENTER.

5 In the **PDR Specific Management and Operations** menu, type the number associated with **Heartbeat Key Setting** and press ENTER.

6 In the **Set Heartbeat Key** menu, perform one of the following actions:

IMPORTANT: Before performing this step, verify that the backup PDG is in the User Requested Standby (URS) state. Otherwise, the HA link goes down, and the peer (backup) PDG goes active. See Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

If…	Then…
If you want to set an ASCII-based key,	perform the following actions: **a** Type `1` and press ENTER. **b** Type the 16-character ASCII key. **c** Retype the same 16-character ASCII key. A message appears, informing that the operation has been successful, and you return to the **PDR Specific Management and Operations** menu.
If you want to set a Hexadecimal based key,	**a** Type `2` and press ENTER. **b** Type the 32-character Hexadecimal Key. **c** Retype the same 32-character Hexadecimal Key. A message appears, informing that the operation has been successful, and you return to the **PDR Specific Management and Operations** menu.
If you want to exit,	type `q` and press ENTER.

5.4.2 Verifying the HA Link Status on the PDR

Prerequisites: Ensure that the PDR is running. If the PDR service is not running, then perform Starting the Trunked PDR on page 168 before starting this procedure.

When and where to use:
After you set Heartbeat Key on both the active and the backup PDR, perform the following procedure to verify the HA Link status on both active and backup PDR.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **Local Configuration** interface, select **Redundancy Configuration** and press ENTER.
6. In the **Redundancy Configuration** menu, select **View Redundancy Configuration** and press ENTER.

   In the **View Redundancy Configuration** menu, the HA link status can be **Link Up** or **Link Down**. In a normally operated Dynamic System Resilience (DSR) system, the HA link status is **Link Up**.

7 To exit the **View Redundancy Configuration** menu, type `q`, and then type `y`.

8 To exit the **Main Menu**, type `q` and press Enter.

5.5
Trunked PDG Redundancy Configuration

In a Dynamic System Resilience (DSR) configuration, the Packet Data Gateway (PDG) is redundant in the backup core. In case of the primary PDG failure, an automatic switchover takes place and the backup PDG becomes active and minimizes loss of data services. In a non-DSR configuration, no backup core exists with a redundant PDG.

A PDG can be in one of the following three states:

- Active
- Standby
- User Requested Standby

Depending on your system configuration, set the PDG to active or standby state:

Table 8: PDG States in DSR and Non-DSR Systems

DSR System	Non-DSR System
Set the primary PDG to the active state. Set the backup PDG to the standby state.	Always keep the PDG in the active state.

Active State

In the active state, the PDR is capable of establishing a data session with a GGSN and RNG. Upon establishing a data session with a PDR, the RNG can accept connection requests from RF sites and a remote PDR in other zones. Upon establishing a data session with the PDR, the GGSN forwards outbound data for the radios that are currently context activated. To set the PDG to the active state, perform Setting the Trunked PDG to the Active State (DSR) on page 162.

Standby State

In the standby state, the PDR is capable of an automatic switchover. While a PDR is in a standby state, it suspends establishing a data session to the local RNG, remote RNG in other zones and GGSN. Without a connection to a PDR, the RNG does not accept link-up requests from RF sites or remote PDR in other zones. The GGSN does not forward any data to a PDR without a data session established. The PDR monitors heartbeat messages from the active PDR. If the PDR misses consecutive heartbeats or is informed that the other PDR can no longer remain active, it becomes active. To set the PDG to the standby state, perform Setting the Trunked PDG to the Standby State (DSR) on page 163.

User Requested Standby State

In the User Requested Standby state, the PDR disables the automatic switchover capability and remains in a User Requested Standby state until you change the state to standby or active. To set the PDG to the user requested standby state, perform Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

5.6

Migrating the PDG Configuration from a Previous Release (K Core)

Prerequisites:
Shut down the Packet Data Router (PDR) application before performing this procedure to ensure that all runtime information is saved in the database.

When and where to use:
Use the following procedure as part of the upgrade process to restore a PDR database backup file created on a previous release PDG to the current release PDG.

This procedure applies to K cores only.

Procedure:

1 Perform the following actions:
   - a Power off the current release PDG virtual machine.
   - b Right-click the current release PDG virtual machine.
   - c Select **Edit Setting**
   - d Click **Add**
   - e Select **Hard Disk** and click **Next**.
   - f Select **Use an existing virtual disk** and click **Next**.
   - g Click **Browse** and double-click **datastore1**.
   - h Double-click the name of the previous release PDG virtual machine.
   - i Select the ***<vm_name>_<x>*.vdmk** file with the highest number ***<x>*** and click **OK**.
   - j Click **Next**.
   - k Click **Finish**.
   - l Click **OK**.

2 Perform the following actions:
   - a Power on the current release PDG virtual machine.
   - b Log on to the PDG using the credentials for a user account that belongs to the Install Administrator or Platform Administrator group.
   - c At the login prompt, type `su -`. Press ENTER.
   - d At the password prompt, type the root password. Press ENTER.
   - e At the root prompt, type `fdisk -l` and press ENTER.
   - f Find the following device: **Disk /dev/yyy>1**.
   - g Enter: `mount /dev/yyy>1 /tmp`
   - h To verify, enter: `df -h` and look for the following line:

     ```
     /dev/yyy>1 2.0G xxx xxx xx /tmp
     ```

3 Enter: `cp /tmp/pdr_backup_`***`<date>`***`_`***`<time>`***`.zip /opt/Motorola/migration`

   The file is copied to the **/opt/Motorola/migration** directory.

4 Verify whether the file was copied. Enter: `ll / opt/Motorola/migration`

   The following file appears: `pdr_backup_`***`<date>`***`_`***`<time>`***`.zip`

5. Enter: `umount /tmp`
6. At the prompt, enter: `admin_menu`
7. From the main PDG administration menu, select **Application Administration** and press ENTER.
8. From the **Application Administration** menu, select **Application Specific Management and Operations** and press ENTER.
9. From the **Application Specific Management and Operations** menu, select **PDR Specific Management and Operations** and press ENTER.
10. From the **PDR Specific Management and Operations** menu, select **Migrate PDR** and press ENTER.
11. If the PDR is running, stop the PDR. At the prompt, enter: `y`
12. Select a backup file to use for restoration/migration and press ENTER.
13. Confirm that you want to remove the existing database. Enter: `y`

    PDG migration is complete.

14. From the menu, select **Display PDR Status** and press ENTER.

    A message appears, informing that the PDR is running.

15. To exit the main PDG administration menu, enter: `q`

    The user’s command prompt appears.

16. Enter: `/opt/Motorola/pdr/bin/update_pdg`
17. Enter the MotoAdmin Auth password.
18. Enter the MotoAdmin Priv password.
19. Enter the MotoMaster Auth password.
20. Enter the MotoMaster Priv password.
21. If communication issues with UEM or UNC occur, reset the SNMP credentials on the UEM or UNC to match the PDG credentials. See the *SNMPv3 Feature Guide*.

Chapter 6

PDG Local Configuration for Trunked IVD and HPD

This chapter details the local configuration procedures related to the Trunked IV&D and HPD Packet Data Gateway (PDG).

6.1 Trunked PDG Local Configuration Interface

The Packet Data Gateway (PDG) local configuration parameters are accessed from the Local Configuration Interface. It is a menu-driven interface with various selections for viewing/updating configuration parameters, running statistics, initiating activities, and viewing mobile device information. The Local Configuration Interface consists of the main menu from which all the configuration options are available.

PDGs reside as virtual machines on an ESXi platform which has its own installation and configuration process. For detailed information, see the *Virtual Management Server Software User Guide*.

6.1.1 Accessing the Trunked PDG Local Configuration Interface

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. Type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

   The **Local Configuration** interface appears.

6.1.2 Trunked PDG Local Configuration Interface Menu Items

The following table provides a brief explanation for each of the main menu selections on the PDG Local Configuration Interface.

Table 9: Trunked PDG Local Configuration Interface Menu Items

Menu Item	Description
View Mobile Device Information	Displays the current information for a particular Radio ID, including the ICMP flag setting, IP address, registration state, zone location, APN, and timer information.

Table continued…

Menu Item	Description
Create Device Summary Report	Generates summary reports for all the mobile devices provisioned in the PDR. The report includes the IP address, registration state, and last inbound/outbound message times for each mobile device. Several other fields of information are also reported. **NOTICE:** An inbound message is the one that goes from MSU to Host. The outbound message is the one that goes from Host to MSU.
PDG Configuration	Allows you to view and modify PDG configuration settings, including LAP-D timers and LAP-D frame parameters. It can also be used to view mobility query information, database synchronization status, the PDR software version, and system-wide outbound queue limits. Some parameters are read-only.
Redundancy Configuration	Displays various redundancy states in Dynamic System Resilience (DSR) configuration. Allows you to view and modify these redundancy states.
View Gateway Router Configuration	Displays configuration details of the gateway router.
View System Parameters	Displays various timers and other system parameters associated with the PDG.
View Zone Information	Displays zone information, such as the NTP source and the multicast IP addresses for Home Location Register (HLR) / Visitor Location Register (VLR) distribution.
View Zone Configuration Information	Displays details for the Zone configuration.
View Home Zone Mapping Information	Displays read-only home zone mapping information.
View Unconfirmed Outbound Message Filter	Displays read-only Unconfirmed Outbound Message Filter information.
Statistics Management	Includes information about inbound/outbound IP traffic, ICMP messages, InterZone roaming, mobile device activity, registration events, and link statistics. Provides access to various statistics for the following items: • Mobile Device Statistics • PDR Statistics • RNG Statistics • PDR-RNG Link Statistics • PDR-ZC Link Statistics • PDR-GGSN Link Statistics
RNG Configuration	Allows you to view and modify RNG parameters, such as the IP address, port numbers, software version, link states, and so on. Some parameters are read-only.
InterZone RNG Configuration	Displays details for the InterZone RNG configuration.

Table continued…

Menu Item	Description
Local RNG-Site Link Status	Displays the status of the link between the RNG and remote sites.
Diagnostic Tests	Performs a diagnostic test between the PDG and the zone controller.

6.1.3
Trunked PDG Local Configuration Command Keys

The Local Configuration Interface uses various keystrokes to navigate through the screens and manipulate the settings. The available keystrokes are always displayed at the bottom of each screen.

Table 10: Trunked PDG Local Configuration Command Keys

Keys	Functional Description
Up or Down Arrow	Use the Up or Down Arrow key to highlight a menu item, or page through multiple page screens.
Right Arrow	Use the Right Arrow key to follow a menu item link.
Left Arrow	Use the Left Arrow key to return to the previous link or menu item.
H or ?	Use the H key to obtain helpful information on how to use the browser.
O	Use the O key to change the browser options at runtime.
P	Use the P key to print a Local Configuration Interface screen.
G	Use the G key to open a document at the specified URL.
M	Use the M key to return to the main screen.
Q	Use the Q key to exit the Local Configuration Interface.
/	Use the / key to find a word or phrase within a current document.
Del	Use the Del key to display a browser history list.

6.1.4
Exiting the Local Configuration Interface

Procedure:

After making any additions, changes, or viewed data, press `q` to exit the Local Configuration Interface.

The **Local Configuration Interface** closes and returns to the `admin_menu` prompt.

6.2
Displaying Mobile Device Information on the Trunked PDG

The View Mobile Device Information Interface allows you to view the detailed information contained in the PDG database for any mobile device.

Prerequisites: To view the device information, you must know the Radio ID of the device. If the device does not exist in the database, a window appears, stating that the specified radio ID is not provisioned.

When and where to use:

Use this procedure to display information for a specified mobile device.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** menu, select **View Mobile Device Information** from the menu using the arrow keys and press ENTER.

6 In the **View Mobile Device Information** menu, type the Radio ID number in the Radio ID field.

7 Select **SUBMIT** using the arrow keys and press ENTER.

The information for the specified device appears.

8 To return to the **Local Configuration Interface**, select **Back to Start Page** using the arrow keys and press ENTER.

6.2.1 View Mobile Device Information Field Descriptions

The following table lists the names and descriptions of the fields on the View Mobile Device Information Interface.

Table 11: View Mobile Device Information Field Descriptions

Field	Description
Radio ID	The logical link identifier that uniquely identifies a mobile subscriber unit (MSU). Valid range: 0 - 16777215
Broadcast Flag	Set of bits (flag) to show the current broadcast status
Zone ID	The logical identifier for the zone currently being visited by the MSU
Ready Timer	The maximum time the MSU stays in the ready status after the latest data transmission. When this timer expires, the MSU returns to the standby status.
Last Registered Standby Timer	The displayed value is being currently used by MSU, and reflects the value at the last registration. The value is different from the Standby Timer value as specified in System Parameters. The values are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
Registration Time	Time stamp of the last registration state change
Registration State	MSU state: REGISTERED, DEREGISTERED.
ICMP Flag	Internet Control Message Protocol (ICMP). A flag to indicate whether the outbound ICMP received by PDR are always sent to MSU. If the flag is DISABLED, the ICMP is silently dropped.

Table continued…

Field	Description
Source Address Checking	Enabled or Disabled. Checks the IP sourced address in the Inbound message to see if it is the same as the one assigned during Packet Data registration.
SNDCP Version	Version of SNDCP
Provisioned IP Address	The configured IP address of the mobile subscriber unit
NSAPI	Network Layer Access Point Identity. Unique identifier of the mobile context.
IP Address in Use	IP address assigned during context activation and currently in use.
APN - Network ID	Network ID portion of the Access Point Name (APN)
VPLMN Allowed	Visited Public Land Mobile Network (VPLMN). Indicates whether this mobile is allowed to connect to its home network through a GGSN belonging to the visiting network.
RFC2507 Non-TCP Header Compression flag	Indicates whether the header compression is ENABLED or DISABLED.
RFC2507 Max No. of Non-TCP Header Compression Contexts	Indicates the maximum number of Non-TCP header compressions contexts per mobile used by system devices to allocate system and memory resources.
RFC2507 Max Time Between Full headers	Indicates the maximum time between full headers.
RFC2507 Max No. of Compressed Headers Between Full Headers	Indicates the maximum number of compressed headers between full headers.
RFC2507 Max Header Size to Compress	Indicates the threshold header size in bytes after which the system does not use compressed headers.

6.3

Generating a Device Summary Report on the Trunked PDG

The Device Summary Report lists all provisioned mobile devices in the system sorted by Radio ID. Both registered and deregistered mobiles are included. The reports are created in either a text format or the CSV format which is used with Microsoft Excel. See Table 12: Device Summary Report Fields (.txt file) on page 100 for the information in the text-formatted report, and Table 13: Device Summary Report Fields (.csv file) on page 100 for the information in the csv-formatted report.

The following procedure describes how to generate a device summary report.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** menu, use the arrow keys to select **Create Device Summary Report** and press ENTER.

6 In the **Create Device Summary Report** window, in the **File Name** field, type a file name or use the default file name. Use the arrow keys to highlight **SUBMIT** and press ENTER.

An interface appears, allowing you to select a `.txt` or a `.csv` (comma-separated value) format for the report file.

7 Use the arrow keys to highlight the desired report format and press ENTER.

The text version of the report appears in the browser.

8 Press SPACEBAR to view additional pages. This occurs if there are more devices in the database than can be shown on one page.

9 To return to the **Local Configuration Interface**, use the arrow keys to highlight **Back to The main Menu** and press ENTER.

6.3.1 Device Summary Report Fields (.txt file)

Table 12: Device Summary Report Fields (.txt file)

Field	Description
Radio ID	Also called Short Subscriber Identity (SSI). Unique logical link identifier for the MSU. Valid range: 0 - 16777215.
IP Address	The IP address the MSU is currently using.
Reg State	MSU states are: REGISTERED, DEREGISTERED.
Last IB Time	Time stamp indicating when the last inbound message was received.
Last OB Time	Time stamp indicating when the last outbound message was sent.

6.3.2 Device Summary Report Fields (.csv file)

Table 13: Device Summary Report Fields (.csv file)

Field	Description
Radio ID	Short Subscriber Identity. Unique logical link identifier for the MSU. Valid range: 0 - 16777215.
Broadcast Flag	Set of bits (flag) to show the current broadcast status.
Zone_ID	Logical identifier for the zone currently being visited by the MSU.
IP_Addr_In_use	The IP address of the MSU.
Ready_Timer	The maximum time MSU stays in the ready status after the latest data transmission. When this timer expires, the MSU returns to the standby status.
Last_Reg_Standby_timer	The value displayed is currently used by MSU, and reflects the value at last registration. It is also different from the Standby Timer value as specified in System Parameters.

Table continued…

Field	Description
	The values are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
Reg_time	The time stamp of the last registration state change
Reg_state	The state of the MSU: REGISTERED, DEREGISTERED.
Hlr_state	The HLR State is either "IDLE" or "DELETE_PENDING". "DELETE_PENDING" = the network manager has requested that the mobile be deleted, but associated Packet Data Contexts at the GGSN and RNG have not yet been cleaned up. "IDLE" = the mobile is NOT in the process of being deleted.
ICMP_flag	Flag indicating whether the outbound ICMP received by PDR is always sent to MSU. If the flag is "DISABLED", the ICMP is silently dropped.
ggsn_ip_addr	The GGSN IP address.
Ingress_Filter	Enabled or Disabled. Enabled = the system only allows datagrams originating from the MSU to use the assigned IP address as the source address. If the source address does not equal the assigned address, the datagram is discarded. Disabled = the system allows the MSU to initiate datagrams with any source address.
SNDCP_ver	The version of SNDCP.
NSAPI	Network Layer Access Point Identity. Uniquely identifies mobile context.
Context_State	State of the context or session.
Provision_Ip_addr	Displays the configured IP address of the MSU.
APN_Network_id	Access Point Name. Specifies the customer network that the MSU accesses.
VPLMN_Allowed	Indicates whether the MSU is allowed to be a part of VPLMN.
Queued_Msg_Receive_Count	The total number of messages currently queued for delivery to the MSU.
Queued_Msg_Byte_Count	The total number of bytes queued for delivery to the MSU.
Outbound_Messages	The number of outbound messages.
Outbound_Bytes	The number of outbound bytes.
Outbound_NAKs	The number of Negative Acknowledgement (NAK) messages.
Outbound_Message_Timeout_Count	Total number of outbound messages that are timed out.
Inbound_Messages	The number of inbound messages.
Inbound_Bytes	The number of inbound bytes.
Inbound_Failure_Count	Total number of failures received from RNG.
Stats_Start_Time	Time stamp indicating when the Mobile Device Statistics collection started (or when the last reset was done).

Table continued…

Field	Description
Last_IB_Time	Time stamp indicating when the last inbound message was received.
Last_OB_Time	Time stamp indicating when the last outbound message was sent.
Last_NAK_Time	Time stamp indicating the last outbound NAK message.
Last_NAK_Process_Status	The last outbound NAK status.
Last_NAK_Resp_Code	The last NAK response code.
Cause_For_Last_Deact	The reason why the MSU was last context deactivated. This can be one of the following values: 0 - None 1 - Error Indication from GGSN 2 - Standby Timeout 3 - Layer 2 Deregistration 4 - Mobile Initiated Deactivation 5 - Infrastructure Routing Error 6 - Failure during roaming 7 - Provisioning Change 8 - No record found in Zone Controller 9 - "Mobile not Registered" returned from Zone Controller
RFC2507 Non-TCP Header Compression Flag	Indicates whether the header compression is ENABLED or DISABLED.
RFC2507 Max No. of Non-TCP Header Compression Contexts	Indicates the maximum number of Non-TCP header compressions contexts per mobile used by system devices to allocate system and memory resources.
RFC2507 Max Time Between Full Headers	Indicates the maximum time between full headers.
RFC2507 Max No. of Compressed Headers Between Full Headers	Indicates the maximum number of compressed headers between full headers.
RFC2507 Max Header Size to Compress	Indicates the threshold header size in bytes after which the system does not use compressed headers.

6.4 Transferring the Device Summary Report of the Trunked PDG

Prerequisites: Obtain the password for the root account.

Procedure:

1. Device Summary Report files are generated in the `/opt/Motorola/pdr/reports` directory. Before transferring the reports from the PDG, log on to the PDG using a non-root account and change to the root account.
2. Type `su -` and press ENTER.
3. At the password prompt, type the root password. Press ENTER.
4. Copy the files with their native ownership to the user home directory and change permissions using the following two commands:

   ```
   cp -p /opt/Motorola/pdr/reports/dev_summ* /home/<user_home_directory>/
   chmod 644 /home/<user_home_directory>/dev_summ*
   ```
5. Type `exit` and press ENTER.

   You are now logged in with the non-root account.
6. Copy the reports using WinSCP (or other secure transfer protocol client) from the PDR using a non-root interactive login account.

   The reports are in `/home/<user_home_directory>`

6.5

Viewing the Trunked PDG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the PDG **Local Configuration Interface**, use the arrow keys to select **PDG Configuration** and press ENTER.
6. In the **PDG Configuration** menu, use the arrow keys to select **View PDG Configuration** and press ENTER.

   The PDG parameters appear.

6.5.1

View Trunked PDG Configuration Fields

The fields on the View PDG Configuration interface are described in the following table.

Table 14: View Trunked PDG Configuration Fields

Field	Description
Default Log File Directory	The default value is `/home/pdr/log`. Not used in the current system release.

Table continued…

Field	Description
System-Wide OB Queue Limits	The maximum number of bytes that is queued for outbound delivery.
Mobility Query Timeout	The time a mobility client (PDR or RNG) waits for a given query response from the zone controller before a time-out.
Maximum outstanding Queries	The Maximum number of outstanding queries allowed to the mobility server (zone controller) at one time.
PDR Instance ID	Logical identifier of the local PDR.
PDR SW Version	Software versions for the PDR.
PDG Instance ID	Logical identifier of the PDG.
LAPD Timers	Timers for framing, sequence control, error detection, and recovery of multiple logical data links.
LAP-D T200 Reply Timeout	The LAP-D ACK timer. It indicates the time-out on a response to the transmission of information (I) frame in milliseconds (RANGE 1000 -50000).
LAP-D T203 Keep alive timer	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between RNG and Base Site are torn down.
LAP-D N200 Max Re-transmission	The maximum number of retransmissions of a frame (range 1-3).
LAP-D N201 Max number of octets in information filed	The maximum number of data bytes in Information (I) frames. Default is 260.
LAP-D K Window size	The maximum number of outstanding Information (I) frames (Range 1-16).
PDG CA bit	Context activation bit
LOS Site count	Number of sites that the local RNG is connected to.
HA Link Timer	The amount of time that the PDR waits before considering the HA link down, when it stops getting heartbeat message from the associated PDR. Value in seconds.
HA Keep alive timer	The amount of time between sending Heart Beat message to the associated PDR for a health check. Value in milliseconds.
HA Destination port	Port number of the associated PDR on which the heartbeat messages are sent.
CA Holdoff timer	The time a subscriber waits before sending CA message, when it receives the CA status message from PDR. Value in minutes.
Gateway Link ICMP response time-out	Timestamp of the last time the link to the primary gateway router was down.
Gateway Link ICMP failures	Number of failures of Gateway Link ICMP
Gateway Link ICMP successes	Number of successes of Gateway Link ICMP
GTP Context Purge Timer	Response timer for GPRS Tunneling Protocol Context Purge
Voyage Host IP Address	(For HPD PDG only) Voyager Application IP address
Non DSR Context Reactivation Flag	(For Trunked IV&D PDG only) Indicates whether subscribers are triggered to reregister when a failure causes the PDG to lose all contexts for a zone. If the parameter is set to ENABLED,

Field	Description
	subscribers in both DSR and non-DSR systems will receive a context reactivation message from the PDG and reregister. If the parameter is set to DISABLED, only the subscribers in DSR systems will be notified to renew contexts.

6.6
Modifying the Trunked PDG Configuration

When and where to use:
Use this procedure to modify the PDG configuration.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the PDG **Local Configuration Interface**, select the **PDG Configuration** using the arrow keys and press ENTER.
6. In the **PDG Configuration** interface, select **Modify PDG Configuration** using the arrow keys and press ENTER.
7. In the **Modify PDG Configuration** interface, use the arrow keys to move to the desired field and make the changes.
8. When you have made all the changes, use the arrow keys to select **SUBMIT** and press ENTER.

   If the modifications were saved successfully, you return to the Modify PDG Configuration screen. If the modifications failed, the screen displays the invalid parameter and the reason for the failure.

6.6.1
Modify Trunked PDG Configuration Fields

Table 15: Modify Trunked PDG Configuration Fields

Field	Description
Default Log File Directory	The default value is `/home/pdr/log`. This is not used in the current system release.
LAP-D T200 Reply Timeout (in msec)	The LAP-D ACK timer. It indicates the timeout on a response to the transmission of information (I) frame in milliseconds (RANGE 1000-50000).
LAP-D T203 Keep alive timer (in msec)	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between RNG and Base Site are torn down.

Table continued…

Field	Description
LAP-D N200 Max Re-transmission	The maximum number of retransmissions of a frame (range 1-3)
LAP-D N201 Max number of octets in the information field	The maximum number of data bytes in Information (I) frames. Default is 260.
LAP-D K Window size	The maximum number of outstanding Information (I) frames (Range 1-16)
CA Holdoff timer	(For HPD PDG only) The time a subscriber waits before sending Context Activation/Renew message, when it receives the CA status message. Value in minutes.
Voyage Host IP Address	(For HPD PDG only) Voyager Application IP address.
Non DSR Context Reactivation Flag	(For Trunked IV&D PDG only) Indicates whether subscribers are triggered to reregister when a failure causes the PDG to lose all contexts for a zone. If the parameter is set to ENABLED, subscribers in both DSR and non-DSR systems will receive a context reactivation message from the PDG and reregister. If the parameter is set to DISABLED, only the subscribers in DSR systems will be notified to renew contexts. The setting only takes effect after a PDG reboot.

6.7
Viewing the System Parameters on the Trunked PDG

The Local Configuration Interface allows you to view the system parameters. You cannot change these values.

When and where to use:
Use this procedure to access the View System Parameters Interface.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations**, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **View System Parameters** using the arrow keys and press ENTER.

The **View System Parameters** screen displays the system parameters.

6.7.1 View System Parameter Field Definitions

Table 16: View System Parameter Field Definitions

Field	Description
GGSN List ID	GGSN Identifier.
GGSN IP address	IP address of peer GGSN.
GGSN Zone ID	Zone ID in which the GGSN resides physically.
GGSN GTP Connection status	GGSN GPRS Tunneling Protocol Connection status.
Delta Ready Timer	(For Trunked IV&D PDG only) Indicates minimum difference allowed in the Ready timer running in RNG and MSU.
Standby Timer	The time an MSU can retain its context following data service activity. Contexts are deleted at expiration of this timer, and the MSU returns to an Idle State. The value stored in the system parameters database and the value stored in the mobile device database may be different. For example, the system parameter is modified. When the MSU registers again, this value is updated in the mobile device database. The values of standby timer are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
SNDCP Queue Dwell Time	Duration a message can remain in the PDR outbound message queue.
Page Wait Timer	(For Trunked IV&D PDG only) If MSU is in the standby state and data arrives at RNG, this timer starts. Timer stops upon receipt of a Packet Date Page Access indicating that the MSU is on a data channel.
New User Timer	It monitors the time the RNG is waiting for New User action to be performed by the PDR. When the timer expires, the RNG deletes the MSU record and discards any related data.
Mobility Timer	This timer is used in the PDR during mobility change and context activation.
MIP Timer	This timer is used in the PDR when a message is sent to the RNG. When the MIP timer expires, it removes the message from the queue and generates an ICMP message.
LLC Retry Timer	Logical Link Control (LLC). The number of seconds the RNG waits before retrying the message to the mobile.
LLC Max Attempts	The number of times the RNG sends the same message to the MSU before giving up.
GTP T3 Timeout	The time interval between the retry attempts to send the signaling request message to the GGSN.
GTP N3 Attempts	The maximum number of attempts made to send the signaling request message to the GGSN.

Table continued…

Field	Description
APN - Operator ID	Is part of APN. This field is modified remotely only.
System ID	Indicates the identity of the system.
WACN ID	Wide Area Communication Network identifier.
RFC2507 Non-TCP Header Compression Flag	(For Trunked IV&D PDG only) Indicates whether the header compression is enabled or not.
RFC2507 Max No. of Non-TCP Header Compression Contexts per Mobile	(For Trunked IV&D PDG only) Indicates the maximum number of Non-TCP header compressions contexts per mobile used by system devices to allocate system and memory resources.
RFC2507 Max Time Between Full Headers	(For Trunked IV&D PDG only) Indicates the maximum time between full headers. Compressed non-TCP headers may not be sent more than this time after sending the last full header.
RFC2507 Max No. of Compressed Headers between Full Headers	(For Trunked IV&D PDG only) Indicates the maximum number of compressed headers between full headers.
RFC2507 Max Header Size to Compress	(For Trunked IV&D PDG only) Indicates the threshold header size in bytes after which the system does not use compressed headers. (Headers larger than this size are not compressed.)
Broadcast Data Capability	Indicates whether the broadcast data feature is ENABLED or DISABLED.
Broadcast Page Wait Timer	(For Trunked IV&D PDG only) Determines how long the RNG waits for the sites to allocate a PDCH for Broadcast and for the subscribers to move to the newly allocated channel. Its value is in seconds.
Broadcast Data Ack Timer	Determines how long the RNG waits after sending the last segment of the Broadcast Data message before sending an ACK to the PDR to indicate it has finished the transmission. Its value is in seconds.
Broadcast Multicast IP Address	The IP address of the multicast group that the RNG uses to send Broadcast Data messages.

6.8

Viewing Zone Information on the Trunked PDG

The Local Configuration Interface allows you to view the zone information. These values cannot be changed.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **View Zone Information** using the arrow keys.

The **Zone Information Field** interface displays the zone-specific fields.

6.8.1 View Zone Information Field Definitions

Table 17: View Zone Information Field Definitions

Field	Description
Home Zone ID	The Home Zone ID Number.
Core Type	Indicates whether it is a Primary or Backup core. **NOTICE:** In non-DSR systems, the core type is always Primary.
Primary Core Gateway1	ID of gateway Router #1 for the Primary Core.
Primary Core Gateway2	ID of gateway Router #2 for the Primary Core.
Backup Core Gateway1	(For DSR systems only) ID of gateway Router #1 for the Backup Core.
Backup Core Gateway2	(For DSR systems only) ID of gateway Router #2 for the Backup Core.
HLR Mobility Client MCIP	The multicast group that the PDR joins for response to multicast queries.
VLR Mobility Client MCIP	The multicast group that the RNG joins for mobility pushes and responses to mobility queries.
Mobility Server MCIP	The multicast IP group that the zone controller joins to receive Home Location Register (HLR) and Visitor Location Register (VLR) mobility requests from mobility clients.
Broadcast data MCIP	The IP address of the multicast group that the RNG uses to send Broadcast Data messages.
Primary broadcast data MCIP	Primary Multicast IP Address for broadcast messages
Secondary broadcast data MCIP	Secondary Multicast IP Address for broadcast messages
Peer PDR HA IP Address	(For DSR systems only) IP address of the peer PDR
NTP Active Flag	Flag indicating whether the Network Time Protocol (NTP) is in use or not. The value is ENABLE or DISABLE.
NTP Primary Source	The IP address of primary source for the network time protocol
NTP Secondary Source	The IP address of secondary source for the network time protocol

6.9 Viewing Zone Configuration Information on the Trunked PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **View Zone Configuration Information** and press ENTER.

   If the zones are configured, a list of Zone IDs appears.
6. Select the zone you want to view the configuration information for.

6.9.1 View Zone Configuration Information Field Definitions

Table 18: View Zone Configuration Information Field Definitions

Field	Description
Zone ID	Zone Number
Zone type	Primary or Backup
DSR Data Capability	Defines whether the zone is DSR-data capable.
DSR Voice Mobility Capability	Defines whether the zone is DSR-voice capable.

6.10 Viewing Home Zone Mapping Information on the Trunked PDG

The Local Configuration interface allows you to view the home zone mapping information. You cannot change these values.

When and where to use: Use this procedure to view Home Zone Mapping information.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, use the arrow keys to select **View Home Zone Mapping Information** using the arrow keys and press ENTER.

NOTICE: If there are more Home Zone IDs and Radio ID ranges than can be shown on one page, there are more pages. These pages are shown by pressing SPACEBAR.

The **Home Zone Mapping Information** interface displays the zone-specific fields.

6.10.1 View Home Zone Mapping Field Definitions

Table 19: View Home Zone Mapping Field Definitions

Field	Description
Home Map ID	An index in the home zone map table.
Home Zone ID	Displays the Home Zone ID number.
Radio ID range	The range of Radio IDs. There are a maximum of 256 ranges of Radio ID. The range is displayed in the format of Radio ID LO - Radio ID HI.

6.11 Viewing Unconfirmed Outbound Message Filter on the Trunked PDG

The Local Configuration interface provides the ability to view the unconfirmed outbound message filter fields. You cannot change these values.

This procedure is **not** applicable to the HPD PDG.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, use the arrow keys to select **View Unconfirmed Outbound Message Filter** and press ENTER.

   The **View Unconfirmed Outbound Message Filter** screen appears.

6. Press the SPACEBAR.

   The next page of the **View Unconfirmed Outbound Message Filter** screen appears.

6.11.1 View Unconfirmed Outbound Message Filter Field Definitions

Table 20: View Unconfirmed Outbound Message Filter Field Definitions

Field	Description
APN – Network ID	Displays a list of available Access Point Name Network IDs that can be used by the radio user. The APN identifies the home network of the radio user.
APN – Operator ID	Displays an alias that represents the APN (Access Point Name) Operator for this data system. **NOTICE:** Motorola Solutions recommends that the APN Operator ID consists of three labels separated by "." of which the last one should be "GPRS".
GGSN IP Address	Displays the IP address of the GGSN used in this data system.
Source IP Address	Source IP address of the outbound IP datagram from a CEN. **NOTICE:** Up to three entries are possible for each APN Network ID.
Destination Port	Destination port number of the outbound IP datagram from the CEN. **NOTICE:** Up to three entries are possible for each APN Network ID.

6.12 Statistics Management on the Trunked PDG

The Statistics Management Interface allows you to view or to reset statistics. The statistics are organized as follows:

- Mobility-related statistics are included in PDR Statistics.
- IP bearer statistics are included in Mobile Device Statistics and PDR Statistics.
- Context activation statistics are included in Mobile Device Statistics.
- GTP statistics are included in PDR Statistics.

All counters displayed in the statistics screen are positive integer values.

6.12.1 Viewing Mobile Device Statistics on the Trunked PDG

When and where to use: Use this procedure to view the mobile device statistics.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press Enter.

4 In the **Application Specific Management and Operations**, type the number associated with **PDG Local Configuration** and press Enter.

5 In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press Enter.

6 In the **Statistics Management** interface, select **View Statistics** using the arrow keys and press Enter.

7 In the **View Statistics** interface, select **Mobile Device Statistics** using the arrow keys and press Enter.

8 In the **View Mobile Device Statistics** interface, perform the following actions:

a In the **Radio ID** field, type the Radio ID number.

b Select **SUBMIT** using the arrow keys and press Enter.

The interface displays statistics for the specified device.

6.12.1.1 Mobile Device Statistics Fields

Table 21: Mobile Device Statistics Fields

Field	Description
Radio ID	The MSU for which statistics are being displayed.
Queued Msg. receive count	The total number of messages currently queued for delivery to the MSU.
Queued Msg. byte count	The total number of bytes queued for delivery to the MSU.
Outbound messages	Total number of messages sent to the RNG.
Outbound bytes	Total number of bytes in outbound messages.
Outbound NAKs	Total number of negative acknowledgments (NAKs) for outbound messages.
Outbound message timeout count	Total number of outbound messages that are timed out.
Inbound messages	Total number of messages received from the RNG.
Inbound bytes	Total number of bytes in inbound messages.
Inbound failure count	Total number of failures received from the RNG.
Last IB timestamp	Time stamp indicating when the last inbound message was received.
Last OB timestamp	Time indicating when the last outbound message was sent.
Last OB NAK timestamp	Time stamp indicating the last outbound NAK message.
Last OB NAK process status	The last outbound NAK status.
Last outbound NAK response code	The last NAK response code.
Cause for Last Deactivation Reason	The reason why the MSU was last deactivated.
Statistics start timestamp	Time stamp indicating when the Mobile Device Statistics collection started (or when the last reset was done).

6.12.2 Viewing the PDR Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** menu, select **View Statistics** using the arrow keys and press ENTER.
7. In the **View Statistics** menu, select **PDR Statistics** using the arrow keys and press ENTER.

   The **PDR Statistics** screen appears.

6.12.2.1 PDR Statistics Fields

Table 22: PDR Statistics Fields

Field	Description
IB ICMP Messages	Total number of inbound ICMP messages due to failed delivery of outbound messages.
OB ICMP Messages	Total number of outbound ICMP messages due to undelivered outbound messages.
ICMP discarded messages	Total number of discarded outbound ICMP messages.
IB IP Messages	Total number of inbound IP messages.
IB IP Bytes	Total number of bytes in inbound IP messages.
OB IP Messages	Total number of outbound IP messages.
OB IP Bytes	Total number of bytes in outbound IP messages.
IP discarded messages	Total number of discarded inbound and outbound IP messages by the PDR.
ICMP generated	Total number of ICMP messages generated by the PDR.
Number of Broadcast Outbound Packets	Total number of broadcast messages received by the PDR.
Number of Broadcast Outbound Bytes Received	Total number of bytes received in broadcast messages.
Number of Broadcast Outbound Messages Discard Count	Number of broadcast messages received by the PDR that were not delivered, and were ICMPed.

Table continued…

Field	Description
Number of Broadcast Outbound Messages Dropped Count	Number of broadcast messages received by the PDR that were not delivered, but were not ICMPed. This scenario happens under overload condition.
Total Registration Request	Total number of registration requests received by the PDR.
Total number of InterZone roams	Total number of InterZone roaming requests in the system, for active users.
Total number of ADD-USER-REQUEST messages rejected	Total number of ADDUSER requests that were rejected by the RNG.
Total number of InterZone roaming indications for deregistered mobiles	Total number of InterZone roaming indications for MSU which are deregistered (and rejected by the PDR).
Total echo requests sent	Total number of echo request messages sent to GGSN.
Total echo responses received	Total number of echo response messages received from GGSN.
Time stamp of last echo request	Time stamp of last echo request sent to GGSN.
Time stamp of last echo response	Time stamp of last echo response received from GGSN.
Total number of error indications received from GGSN	Total number of error messages received from GGSN.
RFC2507 Total number of Non-TCP Header Compression errors	Total number of errors encountered during Non-TCP/IP header decompression.
RFC2507 Total number of received messages with compressed headers	Total number of messages received with non-TCP compressed headers.
RFC2507 Total number of sent messages with compressed headers	Total number of messages sent with non-TCP compressed headers.
PDR statistics start time	Time stamp indicating when the PDR Statistics collection started (or when last reset was done).

6.12.3

Viewing the RNG Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** menu, select **View Statistics** using the arrow keys and press ENTER.

7 In the **View Statistics** menu, select **RNG Statistics** using the arrow keys and press ENTER.

The **RNG Statistics** screen appears.

6.12.3.1
RNG Statistics Fields

Table 23: RNG Statistics Fields

Field	Description
Number of Add User Requests	The number of Add_User_Request (0x51) messages received from all PDRs.
Number of delete User Requests	The number of Delete_User_Request (0x52) messages received from all PDRs.
Number of slots requested	The number of segments requested.
Number of slots granted	The number of segments granted.
Number of Channel cancel requests	The number of cancel requests sent to the PDR.
Number of valid New User Responses	The number of valid New_User_response (0x58) messages received from the PDR.
Number of valid Facility Request Messages	The number of valid Facility_Req (0x59) messages received from the PDR.
Number of Valid Initialization Request	The number of valid Initialization_Request (0x50) messages received from the PDR.
Number of Invalid Initialization Request	The number of invalid Initialization_Request (0x50) messages received from the PDR.
Number of Valid Configuration Request	The number of valid Config_Request (0x56) messages received from the PDR.
Number of Invalid Configuration Request	The number of invalid Config_Request (0x56) messages received from the PDR.
Number of Reset RNG Messages	The number of Reset_RNG (0x54) messages received from the PDR.
Number of OB Data Requests received	The number of OB_Data_Request (0x29) messages received from the PDR.
Number of OB Data Responses – ACK	The number of OB_Data_Response (0xA9) messages sent to the PDR with “status” field set to ACK (0x00).
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) messages sent to the PDR with “status” field set to NACK (0x01).
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Invalid Message with “status” field set to NACK (0x01) and “response code” field set to “Invalid Message (0x81)”.
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Infrastructure Routing Error with “status” field set to NACK (0x01) and “response code” field set to “Infrastructure routing error (0x89)”.

Table continued…

Field	Description
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Message Not Sent with “status” field set to NACK (0x01) and “response code” field set to Message Not Sent (0x83)”.
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Subscriber Not in this Zone with “status” field set to NACK (0x01) and “response code” field set to “Mobile Subscriber Not in the Zone/Not found (0x88)”.
Number of IB Data Indication sent	The number of IB_Data_Indication (0xAC) messages sent to the PDR.
Number of Valid Start Flow Requests	The number of valid Start_Flow_Request (0x01) messages received from the PDR.
Number of Invalid Start Flow Requests	The number of invalid Start_Flow_Request (0x01) messages received from the PDR.
Number of Valid Loop Back Messages	The number of valid Loop_Message (0x22) messages received from the PDR.
Number of Invalid Loop Back Messages	The number of invalid Loop_Message (0x22) messages received from the PDR.
Number of Invalid Init CID Requests	The number of invalid Init_CID_Request (0x72) messages received from the PDR.
Number of Valid Init CID Requests	The number of valid Init_CID_Request (0x72) messages received from the PDR.

6.12.4
Viewing the PDR-RNG Link Statistics

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **Application Administration** and press Enter.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press Enter.

5 In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys. Press Enter.

6 In the **Statistics Management** menu, select **View Statistics** using the arrow keys. Press Enter

7 In the **View Statistics** menu, select **PDR-RNG Link Statistics** using the arrow keys. Press Enter.

The PDR-RNG Link Statistics screen appears.

6.12.4.1
PDR-RNG Link Statistics Fields

Table 24: PDR-RNG Link Statistics Fields

Field	Description
RNG Name	Name of the RNG.
Total Connections	Total number of established connections to the RNG.
Total Failed Connections	Total number of failed establishments to the RNG.
Total IB FLM Messages	Total number of inbound messages received.
Total IB FLM Unknown Messages	Total number of inbound messages not containing a valid message content.
Total OB FLM Messages	Total number of outbound messages.
Total OB FLM Unknown Messages	Total number of outbound messages not containing a valid message type.
Total IB Discarded Messages	Total number of messages that contained an invalid message length prefix.
Host Loopback Request Count	Total number of loop back messages sent to the RNG.
Host Loopback Response Count	Total number of loop back messages received from the RNG.
PDR-RNG Link Statistics Time stamp	Time stamp indicating when the PDR-RNG Link Statistics collection started (or when the last reset was done).
Active RNG	Status of RNG which is currently active under Dynamic System Resilience (DSR) configuration.
InterZone link state	Link state between the peer devices in different zones under Dynamic System Resilience (DSR) configuration.
InterZone TCP connect state	TCP status between the peer devices in different zones under Dynamic System Resilience (DSR) configuration.
InterZone control link state	Control link status between the peer devices in different zones under Dynamic System Resilience (DSR) configuration.

6.12.5
Viewing the PDR-ZC Link Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.

6. In the **Statistics Management** menu, select **View Statistics** using the arrow keys and press ENTER.
7. In the **View Statistics** menu, select **PDR-ZC Link Statistics** using the arrow keys and press ENTER.

   The **PDR-ZC Link Statistics** screen appears.

6.12.5.1 PDR-ZC Link Statistics Fields

Table 25: PDR-ZC Link Statistics Fields

Field	Description
Number of failed HLR queries, since the last successful query (including retries)	The total number of failed HLR queries since the last successful query was sent. The count includes retries done for failed queries.
Total number of HLR queries	Total number of queries that were attempted.
Total number of HLR query responses	Total number of responses received for queries.
Total number of dropped HLR queries	Total number of queries that failed in the second try.
PDR-ZC Link Statistics start time	Time stamp indicating when the PDR-ZC Link Statistics collection started (or when the last reset was done).

6.12.6 Resetting the Statistics on the Trunked PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** menu, select **Reset Statistics** using the arrow keys and press ENTER.
7. On the **Reset Statistics** screen, press ENTER to select or deselect the statistics you want to reset.
8. Select **SUBMIT** using the arrow keys and press ENTER.

   The statistics are reset.

6.13
Viewing the RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **RNG Configuration** using the arrow keys and press ENTER.
6. In the **RNG Configuration** menu, select **View RNG Configuration** using the arrow keys. Press ENTER.
7. In the **View RNG Configuration** screen, if there is more than one RNG in the system, press ENTER to access the **Option List**.
8. Select the desired RNG using the arrow keys and press ENTER.
9. Select **SUBMIT** using the arrow keys and press ENTER.

   The **View RNG Configuration** screen displays the configuration parameters for the selected RNG.

6.13.1
View RNG Configuration Fields

Table 26: View RNG Configuration Fields

Field	Description
	Table continued…
RNG Name	The name of the RNG.
RNG Instance ID	The number of the RNG.
RNG PDG Instance ID	The logical identifier of the RNGs PDG.
RNG IP Address	The IP address of the RNG.
Zone ID	The zone in which the RNG resides.
Co-resident Flag	A flag indicating if the RNG is co-resident.
RNG Statistics Update Interval	The interval between updates of statistics from the RNG.
Data Port	Port number used for data messages.
Control Port	Port number used for control messages.
Keep Alive Interval	The amount of time (seconds) between automatically sending keep-alive messages. A value of zero disables sending keep-alive messages.

Field	Description
Keep Alive Count	The number of missed keep-alive responses the PDR allows before bringing down the link with the RNG.
RNG SW Version	The current software version for the RNG.
Control Link State	The status of the control link. The possible values are: STARTING, STARTED, STOPPED
RNG Link TCP Connect State	The status of the TCP layer connect state of the PDR-RNG link. The possible values are: STARTING, STARTED, STOPPED
RNG Link Established State	The Status of the PDR-RNG link: UP, DOWN

6.14 Modifying the RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **RNG Configuration** using the arrow keys and press ENTER.
6. In the **RNG Configuration** menu, select **Modify RNG Configuration** using the arrow keys. Press ENTER.
7. In the **Modify RNG Configuration** screen, if there is more than one RNG in the system, press ENTER to access the **Option List**. Use the arrow keys to select the desired RNG and press ENTER.
8. Select **SUBMIT** using the arrow keys and press ENTER.

   NOTICE: If you have selected a non co-resident RNG to modify, you can only modify the Keep Alive Interval and Keep Alive Count values.

   The **Modify RNG Configuration** screen displays the configuration parameters for the selected RNG.
9. Using the arrow keys, move to the desired fields and make the changes.
10. Using the arrow keys, select **SUBMIT** and press ENTER.

    If the modifications were saved successfully, you return to the Modify RNG Configuration screen. If the modifications failed, the screen displays the invalid parameter and the reason for the failure.

6.14.1
Modify RNG Configuration Fields

Table 27: Modify RNG Configuration Fields

Field	Description
RNG Name	The Name used to identify the RNG. This field cannot be modified.
Keep Alive Interval	Specifies the amount of time between automatically sending a keep alive message. The possible values are: 1 sec, 2 sec, 3 sec, 4 sec, 5 sec, 10 sec, 15 sec, 20 sec, 30 sec, 45 sec, 50 sec. Default value is 5 sec.
Keep Alive count	The number of keep alive timeouts the PDR allows before assuming a CID is down. The valid range is 2 - 10. Default value is 2.
RNG Statistics Update Interval	Specifies the interval between updates of statistics from the RNG. This field is applicable to the local RNG only. The valid range is 0 - 255 (0 = disabled). Default value is 30 sec.

6.15
Viewing the InterZone RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, use the arrow keys to select **InterZone RNG Configuration**. Press ENTER.
6. In the **InterZone RNG Configuration** menu, if there is more than one zone in the system, press ENTER to access the **Option List**.
7. Use the arrow keys to select **Zone**. Press ENTER.
8. Use the arrow keys to select **SUBMIT**. Press ENTER.

   The **View InterZone RNG Configuration** screen displays the configuration parameters for all configured remote RNGs in the selected zone.

6.15.1
View InterZone RNG Configuration Field Descriptions

Table 28: View InterZone RNG Configuration Field Descriptions

Field	Description
Primary RNG Name	Name of the RNG

Table continued…

Field	Description
Primary RNG Instance ID	The number of the RNG
Primary RNG PDG Instance ID	The logical identifier of the RNGs PDG
Primary RNG IP Address	The IP address of the RNG
Primary RNG Keep Alive Interval	The amount of time (seconds) between automatically sending keep-alive messages. A value of zero disables sending keep-alive messages.
Primary RNG Keep Alive Count	The number of missed keep-alive responses the PDR allows before bringing down the link with the RNG
Data Port	Port number used for data messages
Control Port	Port number used for control messages
Active RNG	Status of RNG which is currently active under the Dynamic System Resilience (DSR) configuration
InterZone Link State	Link state between the peer devices in different zones under the Dynamic System Resilience (DSR) configuration
InterZone TCP Connect State	The status of the TCP layer connect state between the peer devices in different zones under the Dynamic System Resilience (DSR) configuration
InterZone Control Link State	Control link status between the peer devices in different zones under the Dynamic System Resilience (DSR) configuration

6.16 Modifying the InterZone RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** menu, use the arrow keys to select **InterZone RNG Configuration**. Press ENTER.
6. In the **InterZone RNG Configuration** menu, select **Modify InterZone RNG Configuration**. Press ENTER.
7. If there is more than one zone in the system, press ENTER to access the **Option List**.
8. Use the arrow keys to select **Zone**. Press ENTER.
9. Use the arrow keys to select **SUBMIT**. Press ENTER.

   The **Modify InterZone RNG Configuration** screen displays the configuration parameters for all the remote RNGs in the selected zone.

6.16.1 Modify InterZone RNG Configuration Field Descriptions

Table 29: Modify InterZone RNG Configuration Field Descriptions

Field	Description
Zone ID	Zone identifier
Primary RNG name	Name of the RNG
Primary RNG Keep Alive Interval	The amount of time (seconds) between automatically sending keep-alive messages. A value of zero disables sending keep-alive messages.
Primary RNG Keep Alive Count	The number of missed keep-alive responses the PDR allows before bringing down the link with the RNG

6.17 Viewing the Status of the Local RNG-Site Link

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, use the arrow keys to select **Local RNG-Site Link Status** and press **Enter**.

   The **Local RNG-Site Link Status** screen displays the status fields.

6.17.1 Local RNG-Site Link Status Fields

Table 30: Local RNG-Site Link Status Fields

Field	Description
Site ID	Site ID
Link Status	The values are: Disconnected, Connected.

6.18 Viewing the Gateway Router Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, use the arrow keys to select **View Gateway Router Configuration** and press ENTER.

6 On the **View Gateway Router Configuration** screen, if there is more than one gateway in the system, press ENTER to access the **Option List**.

7 Use the arrow keys to select the desired gateway and press ENTER.

8 Use the arrow keys to select **SUBMIT** and press ENTER.

The **View Gateway Router Configuration** screen displays the configuration parameters for the selected gateway.

6.18.1 Gateway Router Configuration Fields

Table 31: Gateway Router Configuration Fields

Field	Description
Gateway Router ID	Gateway router identity
Gateway link status	Link status with the peer router
Gateway Router IP address	IP address of the gateway router
Gateway Router last link drop Timestamp	Timestamp of the last time the link to the primary gateway router was down
Gateway Router last link recover Timestamp	Timestamp of the last time the link to the primary gateway router was recovered

6.19 SNMPv3 Credentials Maintenance

The following SNMPv3 configurations can be configured on the Packet Data Gateway (PDG):

- Configuring USM User Security for the PDG
- Modifying User Passphrases for the PDG
- Modifying User Security Levels for the PDG

For more information on changing SNMPv3 credentials, see “Configuring the PDG for SNMPv3” in the *SNMPv3 Feature Guide*.

6.20 SSH Configuration on the Trunked PDG

SSH configuration should be backed up for later recovery in case of any failure. For more information on configuring and restoring SSH Configuration on the PDG, see the *Securing Protocols with SSH Feature Guide*.

6.21 Minimum Configuration Requirements for the RNG and System

The following sections provide the configuration parameters for configuring the RNG and the system.

The following table describes the key parameters that must be set up in the Modify RNG interface.

Table 32: RNG Configuration Parameters

Field	Comment
RNG name	RNG Name is set by Network Management.
Keep Alive Interval	This must be set to 5 (default).
Keep Alive Count	This must be set to 2 (default).
RNG Statistics Update Interval	This must be set to 30 (default).

The following table provides the key system parameters that must be set up in the Modify PDG configuration screen.

Table 33: PDG Configuration Fields

Field	Comment
Default Log File Directory	This must be set to `/home/pdr/log` (default).
LAP-D T200 Reply timeout	The acknowledgment (ACK) timer indicates the timeout on a response to the transmission of information (I) frame in milliseconds (RANGE 1000-50000).
LAP-D T203 Keep alive timer	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between the RNG and Base Site are torn down.
LAP-D N200 Max Retransmissions	The maximum number of retransmissions of a frame (range 1-3)
LAP-D N201 Max number of octets in the information field	The maximum number of data bytes in Information (I) frames. Default is 260.
LAP-D K Window Size	The maximum number of outstanding Information (I) frames (Range 1-16)

6.22 PDR Configuration

The PDR provides two configuration features:

- Remote Configuration – Used by the Network Manager to configure the PDR
- Local Configuration – PDR local configuration interface

The PDG configuration interface is used to configure the PDR and to verify that the PDG database is synchronized. For more information, see Trunked PDG Database Synchronization on page 69.

6.23 Changing the Welcome Banner on a Linux-Based Device

See “Changing the Welcome Banner on a Linux-Based Device” in the *Unix Supplemental Configuration Setup Guide*.

This page intentionally left blank.

Chapter 7

PDG Local Configuration for Conventional IVD M Core and K Core

This chapter details the local configuration procedures related to the Conventional IV&D M core and K core Packet Data Gateway (PDG).

7.1 Conventional PDG Local Configuration Interface

The Packet Data Gateway (PDG) local configuration parameters are accessed from the Local Configuration interface. It is a menu-driven interface with various selections for viewing/updating configuration parameters, running statistics, initiating activities, and viewing mobile device information. The Local Configuration interface consists of a main menu from which all the configuration options are available.

NOTICE: The Conventional IV&D K core PDG uses the Command Line Interface commands to configure the parameters that for M core are configured in the UNC. For details, see Conventional IVD K Core PDG Configuration on page 261.

PDGs reside as virtual machines on an ESXi platform which has its own installation and configuration process. For detailed information, see the *Virtual Management Server Software User Guide*.

7.1.1 Accessing the Conventional PDG Local Configuration Interface

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

   The **Local Configuration** interface appears.

7.1.2

Conventional PDG Local Configuration Interface Menu Items

The following table provides a brief explanation for each of the main menu selections on the PDG Local Configuration Interface.

Table 34: Conventional PDG Local Configuration Interface Menu Items

Menu Item	Description
View Mobile Device Information	Displays the current information for a particular Radio ID, including the ICMP flag setting, IP address, registration state, zone location, APN, and various timer information.
Create Device Summary Report	Generates summary reports for all the mobile devices provisioned in the PDR. The report includes the IP address, registration state, and last inbound/outbound message times for each mobile device. Several other fields of information are also reported. **NOTICE:** An inbound message is the one that goes from MSU to Host. The outbound message is the one that goes from Host to MSU.
PDG Configuration	Allows you to view and modify PDG configuration settings, including LAP-D timers and LAP-D frame parameters. This can also be used to view mobility query information, database synchronization status, the PDR software version, and system-wide outbound queue limits. Some parameters are read-only.
View Gateway Router Configuration	Displays configuration details of the gateway router.
View System Parameters	Displays various timers and other system parameters associated with the PDG.
View Zone Information	Displays zone information, such as the NTP source and the multicast IP addresses.
View Home Zone Mapping Information	Displays read-only home zone mapping information.
View Unconfirmed Outbound Message Filter	Displays read-only Unconfirmed Outbound Message Filter information.
View Channels Per Site Information	Displays read-only Channels information.
View Key Management Facility Information	Displays read-only KMF information.
View CAI Data Encryption Module Information	Displays read-only CDEM information.
Statistics Management	Includes information about inbound/outbound IP traffic, ICMP messages, mobile device activity, registration events, and link statistics. Provides access to various statistics for the following items: • Mobile Device Statistics • PDR Statistics • RNG Statistics

Table continued…

Menu Item	Description
	• PDR-RNG Link Statistics • PDR-GGSN Link Statistics
RNG Configuration	Allows you to view and modify RNG parameters, such as the IP address, port numbers, software version, link states, and so on. Some parameters are read-only.
Local RNG-Site Link Status	Displays the status of the link between the RNG and remote sites.

7.1.3
Conventional PDG Local Configuration Command Keys

The Local Configuration Interface uses various keystrokes to navigate through the screens and manipulate the settings. The available keystrokes are always displayed at the bottom of each screen.

Table 35: Conventional PDG Local Configuration Command Keys

Keys	Functional Description
Up or Down Arrow	Use the Up or Down Arrow key to highlight a menu item, or page through multiple page screens.
Right Arrow	Use the Right Arrow key to follow a menu item link.
Left Arrow	Use the Left Arrow key to return to the previous link or menu item.
H or ?	Use the H key to obtain helpful information on how to use the browser.
O	Use the O key to change the browser options at runtime.
P	Use the P key to print a Local Configuration Interface screen.
G	Use the G key to open a document at the specified URL.
M	Use the M key to return to the main screen.
Q	Use the Q key to exit the Local Configuration Interface.
/	Use the / key to find a word or phrase within a current document.
Del	Use the Del key to display a browser history list.

7.1.4
Exiting the Local Configuration Interface

Procedure:

After making any additions, changes, or viewed data, press `q` to exit the Local Configuration Interface.

The **Local Configuration Interface** closes and returns to the `admin_menu` prompt.

7.2 Displaying Mobile Device Information on the Conventional PDG

The View Mobile Device Information Interface allows you to view the detailed information contained in the PDG database for any mobile device.

Prerequisites: To view the device information, you must know the Radio ID of the device. If the device does not exist in the database, a window appears, stating that the specified radio ID is not provisioned.

When and where to use:
Use this procedure to display information for a specified mobile device.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** menu, select **View Mobile Device Information** from the menu using the arrow keys and press ENTER.
6. In the **View Mobile Device Information** menu, type the Radio ID number in the Radio ID field.
7. Select **SUBMIT** using the arrow keys and press ENTER.

   The information for the specified device appears.
8. To return to the **Local Configuration Interface**, select **Back to Start Page** using the arrow keys and press ENTER.

7.2.1 View Mobile Device Information Field Descriptions

The following table lists the names and descriptions of the fields on the View Mobile Device Information Interface.

Table 36: View Mobile Device Information Field Descriptions

Field	Description
Radio ID	The logical link identifier that uniquely identifies a mobile subscriber unit (MSU). Valid range: 0 - 16777215
Broadcast Flag	Set of bits (flag) to show the current broadcast status
Zone ID	The logical identifier for the zone currently being visited by the MSU
Last Registered Standby Timer	The displayed value is being currently used by MSU, and reflects the value at the last registration. The value is different from the Standby Timer value as specified in System Parameters. The values are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
Registration Time	Time stamp of the last registration state change

Table continued…

Field	Description
Registration State	MSU state: REGISTERED, DEREGISTERED.
ICMP Flag	Internet Control Message Protocol (ICMP). A flag to indicate whether the outbound ICMP received by the PDR is always sent to MSU. If the flag is DISABLED, the ICMP is silently dropped.
Source Address Checking	Enabled or Disabled. Checks the IP sourced address in the Inbound message to see if it is the same as the one assigned during Packet Data registration.
SNDCP Version	Version of SNDCP
Provisioned IP Address	The configured IP address of the mobile subscriber unit
NSAPI	Network Layer Access Point Identity. Unique identifier of the mobile context.
IP Address in Use	IP address assigned during context activation and currently in use
APN - Network ID	Network ID portion of the Access Point Name (APN)
Actual Site Id	The site on which the subscriber is currently operating (for manually registered subscribers, this may be different than the provisioned site ID).
Actual Channel Ids	The channel on which the subscriber is currently operating (for manually registered subscribers, this may be different than the provisioned channel).
Actual Scan Mode	The current scan mode of the subscriber (for manually registered and data-triggered subscribers, this may be different than the provisioned site ID).
Inbound Data Encryption Mode	Indicates whether the data received from the subscriber is being encrypted. When encryption mode is “clear”, PDG discards inbound encrypted data; when it is “secure”, PDG discards inbound clear data.
Outbound Data Encryption Mode	Indicates whether the data being sent to the subscriber is being encrypted.
CKR Index	Indicates the Traffic Common Key Index used for outbound data encryption.
KMF ID	Indicates the ID of the Key Management Facility being used by the subscriber.

7.3
Generating a Device Summary Report on the Conventional PDG

The Device Summary Report lists all provisioned mobile devices in the system sorted by Radio ID. Both registered and deregistered mobiles are included. The reports are created in either a text format or the CSV format which is used with Microsoft Excel.

The following procedure describes how to generate a device summary report.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** menu, use the arrow keys to select **Create Device Summary Report** and press ENTER.

6 In the **Create Device Summary Report** window, in the **File Name** field, type a file name or use the default file name. Use the arrow keys to highlight **SUBMIT** and press ENTER.

   An interface appears, allowing you to select a `.txt` or a `.csv` (comma-separated value) format for the report file.

7 Use the arrow keys to highlight the desired report format and press ENTER.

   The text version of the report appears in the browser.

8 Press SPACEBAR to view additional pages. This occurs if there are more devices in the database than can be shown on one page.

9 To return to the **Local Configuration Interface**, use the arrow keys to highlight **Back to The main Menu** and press ENTER.

7.3.1 Device Summary Report Fields (.txt file)

See the following table for the information in the text-formatted report.

Table 37: Device Summary Report Fields (.txt file)

Field	Description
Radio ID	Also called Short Subscriber Identity (SSI). Unique logical link identifier for the MSU. Valid range: 0 - 16777215.
IP Address	The IP address the MSU is currently using.
Reg State	MSU states are: REGISTERED, DEREGISTERED.
Last IB Time	Time stamp indicating when the last inbound message was received.
Last OB Time	Time stamp indicating when the last outbound message was sent.

7.3.2 Device Summary Report Fields (.csv file)

Table 38: Device Summary Report Fields (.csv file)

Field	Description
Radio ID	Short Subscriber Identity. Unique logical link identifier for the MSU. Valid range: 0 - 16777215.
Broadcast Flag	Set of bits (flag) to show the current broadcast status.
Zone_ID	Logical identifier for the zone currently being visited by the MSU.
IP_Addr_In_use	The IP address of the MSU.

Table continued…

Field	Description
Last_Reg_Standby_timer	The value displayed is currently used by MSU, and reflects the value at last registration, it is also different from Standby Timer value as specified in System Parameters. The values are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
Reg_time	The time stamp of the last registration state change.
Reg_state	The state of the MSU: REGISTERED, DEREGISTERED.
Hlr_state	The HLR State is either "IDLE" or "DELETE_PENDING". "DELETE_PENDING" = the network manager has requested that the mobile be deleted, but associated Packet Data Contexts at the GGSN and RNG have not yet been cleaned up. "IDLE" = the mobile is NOT in the process of being deleted.
ICMP_flag	Flag indicating whether the outbound ICMP received by PDR is always sent to MSU. If the flag is "DISABLED", the ICMP is silently dropped.
ggsn_ip_addr	The GGSN IP address.
SNDCP_ver	The version of SNDCP.
NSAPI	Network Layer Access Point Identity. Uniquely identifies mobile context.
Context_State	State of the context or session.
Provision_Ip_addr	Displays the configured IP address of the MSU.
APN_Network_id	Access Point Name. Specifies the customer network that the MSU accesses.
Queued_Msg_Receive_Count	The total number of messages currently queued for delivery to the MSU.
Queued_Msg_Byte_Coun t	The total number of bytes queued for delivery to the MSU.
Outbound_Messages	The number of outbound messages. Reset when a “reset statistics” command is received.
Outbound_Bytes	The number of outbound bytes. Reset when a “reset statistics” command is received.
Outbound_NAKs	The number of Negative Acknowledgement (NAK) messages. Reset when a “reset statistics” command is received.
Outbound_Message_Timeout_Count	Total number of outbound messages that are timed out. Reset when a “reset statistics” command is received.
Inbound_Messages	The number of inbound messages. Reset when a “reset statistics” command is received.
Inbound_Bytes	The number of inbound bytes. Reset when a “reset statistics” command is received.
Inbound_Failure_Count	Total number of failures received from the RNG.

Table continued…

Field	Description
Stats_Start_Time	Time stamp indicating when the Mobile Device Statistics collection started (or when the last reset was done).
Last_IB_Time	Time stamp indicating when the last inbound message was received.
Last_OB_Time	Time stamp indicating when the last outbound message was sent.
Last_NAK_Time	Time stamp indicating the last outbound NAK message.
Last_NAK_Process_Status	The last outbound NAK status.
Last_NAK_Resp_Code	The last NAK response code.
Cause_For_Last_Deact	The reason why the MSU was last context deactivated. This can be one of the following values: 0 - None 1 - Error Indication from GGSN 2 - Standby Timeout 3 - Layer 2 Deregistration 4 - Mobile Initiated Deactivation 5 - Infrastructure Routing Error 6 - Failure during roaming 7 - Provisioning Change

7.4 Transferring the Device Summary Report of the Conventional PDG

Prerequisites: Obtain the password for the root account.

Procedure:

1. Device Summary Report files are generated in the `/opt/Motorola/pdr/reports` directory. Before transferring the reports from the PDG, log on to the PDG using a non-root account and change to the root account.
2. Type `su -` and press Enter.
3. At the password prompt, type the root password. Press Enter.
4. Copy the files with their native ownership to the user home directory and change permissions using the following two commands:

   ```
   cp -p /opt/Motorola/pdr/reports/dev_summ* /home/<user_home_directory>/
   ```

   ```
   chmod 644 /home/<user_home_directory>/dev_summ*
   ```
5. Type `exit` and press Enter.

   You are now logged in with the non-root account.
6. Copy the reports using WinSCP (or other secure transfer protocol client) from the PDR using a non-root interactive login account.

   The reports are in `/home/<user_home_directory>`

7.5 Viewing the Conventional PDG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the PDG **Local Configuration Interface**, use the arrow keys to select **PDG Configuration** and press ENTER.
6. In the **PDG Configuration** menu, use the arrow keys to select **View PDG Configuration** and press ENTER.

   The PDG parameters appear.

7.5.1 View Conventional PDG Configuration Fields

The fields on the View PDG Configuration interface are described in the following table.

Table 39: View Conventional PDG Configuration Fields

Field	Description
Default Log File Directory	The default value is `/home/pdr/log`. Not used in the current system release.
System-Wide OB Queue Limits	The maximum number of bytes that is queued for outbound delivery
PDR Instance ID	Logical identifier of the local PDR
PDR SW Version	Software versions for the PDR
PDG Instance ID	Logical identifier of the PDG
LAPD Timers	Timers for framing, sequence control, error detection, and recovery of multiple logical data links
LAP-D T200 Reply Timeout	The LAP-D ACK timer. It indicates the timeout on a response to the transmission of information (I) frame in milliseconds (RANGE 1000 -50000).
LAP-D T203 Keep alive timer	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between RNG and Base Site are torn down.
LAP-D N200 Max Re-transmission	The maximum number of retransmissions of a frame (range 1-3)
LAP-D N201 Max number of octets in information filed	The maximum number of data bytes in Information (I) frames. Default is 260.

Table continued…

Field	Description
LAP-D K Window size	The maximum number of outstanding Information (I) frames (Range 1-16)
LOS Site count	Number of sites that the local RNG is connected to.
Gateway Link ICMP response timeout	Timestamp of the last time the link to the primary gateway router was down
Gateway Link ICMP failures	No of failure of Gateway Link ICMP
Gateway Link ICMP successes	No of successes of Gateway Link ICMP
GTP Context Purge Timer	Response timer for GPRS Tunneling Protocol Context Purge

7.6 Modifying the Conventional PDG Configuration

When and where to use:
Use this procedure to modify the PDG configuration.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the PDG **Local Configuration Interface**, select the **PDG Configuration** using the arrow keys and press ENTER.
6. In the **PDG Configuration** interface, select **Modify PDG Configuration** using the arrow keys and press ENTER.
7. In the **Modify PDG Configuration** interface, use the arrow keys to move to the desired field and make the changes.
8. When you have made all the changes, use the arrow keys to select **SUBMIT** and press ENTER.

   If the modifications were saved successfully, you return to the Modify PDG Configuration screen. If the modifications failed, the screen displays the invalid parameter and the reason for the failure.

7.6.1 Modify Conventional PDG Configuration Fields

Table 40: Modify Conventional PDG Configuration Fields

Field	Description
Default Log File Directory	The default value is `/home/pdr/log`. This is not used in the current system release.

Table continued…

Field	Description
LAP-D T200 Reply Timeout (in msec)	The LAP-D ACK timer. It indicates the timeout on a response to the transmission of information (I) frame in milliseconds (RANGE 1000-50000).
LAP-D T203 Keep alive timer (in msec)	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between RNG and Base Site are torn down.
LAP-D N200 Max Retransmission	The maximum number of retransmissions of a frame (range 1-3)
LAP-D N201 Max number of octets in the information field	The maximum number of data bytes in Information (I) frames. Default is 260.
LAP-D K Window size	The maximum number of outstanding Information (I) frames (Range 1-16)

7.7 Viewing the System Parameters on the Conventional PDG

The Local Configuration Interface allows you to view the system parameters. You cannot change these values.

When and where to use:
Use this procedure to access the View System Parameters Interface.

The system parameter fields are described in Table 41: View System Parameter Field Definitions on page 139.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations**, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **View System Parameters** using the arrow keys and press ENTER.

   The **View System Parameters** screen displays the system parameters.

7.7.1 View System Parameter Field Definitions

Table 41: View System Parameter Field Definitions

Field	Description
GGSN List ID	GGSN Identifier.
GGSN IP address	IP address of peer GGSN.

Table continued…

Field	Description
GGSN Zone ID	Zone ID in which the GGSN resides physically.
GGSN GTP Connection status	GGSN GPRS Tunneling Protocol Connection status.
Standby Timer	The time an MSU can retain its context following data service activity. Contexts are deleted at expiration of this timer, and the MSU returns to an Idle State. The value stored in the system parameters database and the value stored in the mobile device database may be different. For example, the system parameter is modified. When the MSU registers again, this value is updated in the mobile device database. The values of standby timer are: 10 sec, 30 sec, 1 min, 5 min, 10 min, 30 min, 1 h, 2 h, 4 h, 8 h, 12 h, 24 h, 48 h.
New User Timer	Timeout of subscriber registration, for example, when no response is received from GGSN.
Unicast MIP Timer	This timer is used in the PDR when an outbound Unicast message is sent to the RNG. When the MIP timer expires, it removes the message from the queue and generates an ICMP message.
Broadcast MIP Timer	This timer is used in the PDR when a Broadcast message is sent to the RNG. When the MIP timer expires, it removes the message from the queue and generates an ICMP message.
LLC Retry Timer	Logical Link Control (LLC). The number of seconds the RNG waits before retrying the message to the mobile.
LLC Max Attempts	The number of times the RNG sends the same message to the MSU before giving up.
GTP T3 Timeout	Time interval between the retry attempts to send the signaling request message to the GGSN.
GTP N3 Attempts	The maximum number of attempts made to send the signaling request message to the GGSN.
APN - Operator ID	Is part of APN. This field is modified remotely only. APN consists of an Operator ID and a Network ID, which together identify the Customer Network a subscriber is able to exchange Conventional packet data with.
System ID	Indicates identity of the system.
WACN ID	Wide Area Communication Network identifier.
Broadcast Data Capability	Indicates whether the broadcast data feature is ENABLED or DISABLED.
Broadcast Multicast IP Address	The IP address of the multicast group that the RNG uses to send Broadcast Data messages.
Transmit Attempts Before Radio Finder	The maximum number of attempts to reach the radio before entering the Radio Finder mode.
Radio Finder Transmit Attempts	The number of broadcast attempts made to deliver an outbound datagram to a subscriber when in Radio Finder mode.
Host Status Interval	How often (in seconds) to notify the subscribers that Conventional Data Service is available.

Table continued…

Field	Description
Channel Requests Attempts	The maximum number of attempts the RNG makes to obtain access to a Conventional channel in order to deliver an outbound Unicast datagram. Multiple attempts may be needed, if the channel is busy.
Channel Wait Timer	The number of milliseconds between Channel Request attempts.
Scan Suspend Timer	The number of seconds the PDG expects a Conventional Unit to remain on the channel after sending an inbound datagram or acknowledgment.
OTEK Keep Alive Time Period	The frequency (in minutes) with which the PDG sends a keep alive message to the KMF to keep the OTEK connection active through the Radio Network Infrastructure Firewall.
OTAR Availability Indications	Informs the KMF that a Conventional Unit may be available for OTAR transactions.
CDEM TCP Port	Defines the TCP port used by the RNG to communicate with the CDEM.
Unicast Scan Preamble Duration	Defines the number of milliseconds the Unicast Scan Preamble is transmitted before the start of an outbound unicast data transaction.
Broadcast Scan Preamble Duration	Defines the number of milliseconds the Broadcast Scan Preamble is transmitted before the start of a broadcast data transaction.
Decryption Errors Enabled	Defines whether the PDG sends decryption errors to the KMF.
Maximum OTAR Registration Delay	Defines the maximum amount of time (in minutes) between OTAR Registration attempts for subscribers which are automatically registered (such as static/manual subscribers).
Inter Broadcast Data Delay	The number of seconds the PDG waits between group/broadcast datagram block transmissions.
Unicast SNDCP Queue Dwell Time	Defines how many seconds a unicast message is allowed to wait in the PDR outbound queue before it is discarded and an ICMP message is sent to the originating host.
Broadcast SNDCP Queue Dwell Time	Defines how many seconds a broadcast message is allowed to wait in a High Capacity Broadcast Data Agency queue before it is discarded and an ICMP message is sent to the originating host.
Broadcast Time Sensitive SNDCP Queue Dwell Time	The number of seconds a broadcast message is allowed to wait in a Time Sensitive Broadcast Data Agency queue before it is discarded and an ICMP message is sent back to the originating host.
Broadcast Block Size	Defines the maximum number of PDUs which are sent in a broadcast block. This does not apply to Time Sensitive Broadcast Data Agencies.

7.8 Viewing Zone Information on the Conventional PDG

The Local Configuration Interface allows you to view the zone information. These values cannot be changed.

When and where to use:

The Local Configuration Interface allows you to view the zone information. These values cannot be changed.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **View Zone Information** using the arrow keys.

The **Zone Information Field** interface displays the zone-specific fields.

7.8.1
View Zone Information Field Definitions

Table 42: View Zone Information Field Definitions

Field	Description
Home Zone ID	The Home Zone ID Number.
Core Type	The core type is always Primary.
Primary Core Gateway1	ID of gateway Router #1 for the Primary Core.
Primary Core Gateway2	ID of gateway Router #2 for the Primary Core.
Broadcast data MCIP	The IP address of the multicast group that the RNG uses to send Broadcast Data messages.
Primary broadcast data MCIP	Primary Multicast IP Address for broadcast messages.
Secondary broadcast data MCIP	Secondary Multicast IP Address for broadcast messages.
NTP Active Flag	Flag indicating whether the Network Time Protocol (NTP) is in use or not. The value is ENABLE or DISABLE.
NTP Primary Source	The IP address of the primary source for the network time protocol.
NTP Secondary Source	The IP address of the secondary source for the network time protocol.

7.9
Viewing Zone Configuration Information on the Conventional PDG

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **View Zone Configuration Information** and press ENTER.

If the zones are configured, a list of Zone IDs appears.

6 Select the zone you want to view the configuration information for.

7.9.1 View Zone Configuration Information Field Definitions

Table 43: View Zone Configuration Information Field Definitions

Field	Description
Zone ID	Zone Number
Zone type	Primary or Backup
DSR Data Capability	Defines whether the zone is DSR-data capable.
DSR Voice Mobility Capability	Defines whether the zone is DSR-voice capable.

7.10 Viewing Home Zone Mapping Information on the Conventional PDG

The Local Configuration interface allows you to view the home zone mapping information. You cannot change these values.

When and where to use: Use this procedure to view Home Zone Mapping information.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, use the arrow keys to select **View Home Zone Mapping Information** using the arrow keys and press ENTER.

NOTICE: If there are more Home Zone IDs and Radio ID ranges than can be shown on one page, there are more pages. These pages are shown by pressing SPACEBAR.

The **Home Zone Mapping Information** interface displays the zone-specific fields.

7.10.1
View Home Zone Mapping Field Definitions

Table 44: View Home Zone Mapping Field Definitions

Field	Description
Home Map ID	An index in the home zone map table.
Home Zone ID	Displays the Home Zone ID number.
Radio ID range	The range of Radio IDs. There are a maximum of 256 ranges of Radio ID. The range is displayed in the format of Radio ID LO - Radio ID HI.

7.11
Viewing Unconfirmed Outbound Message Filter on the Conventional PDG

The Local Configuration interface provides the ability to view the unconfirmed outbound message filter fields. You cannot change these values.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, use the arrow keys to select **View Unconfirmed Outbound Message Filter** and press ENTER.

   The **View Unconfirmed Outbound Message Filter** screen appears.
6. Press the SPACEBAR.

   The next page of the **View Unconfirmed Outbound Message Filter** screen appears.

7.11.1
View Unconfirmed Outbound Message Filter Field Definitions

Table 45: View Unconfirmed Outbound Message Filter Field Definitions

Field	Description
APN – Network ID	Displays a list of available Access Point Name Network IDs that can be used by the radio user. The APN identifies the home network of the radio user.
APN – Operator ID	Displays an alias that represents the Access Point Name (APN) Operator for this data system. Motorola Solutions recommends that the APN Operator ID consists of three labels separated by "." of which the last one should be "GPRS".

Table continued…

Field	Description
GGSN IP Address	Displays the IP address of the GGSN used in this data system.
Source IP Address	Source IP address. Outbound Unicast IP datagrams with this Source Address and Destination Port combination are transmitted using unconfirmed delivery. Up to three entries are possible for each APN Network ID.
Destination Port	Destination Port number. Outbound Unicast IP datagrams with this Source Address and Destination Port combination are transmitted using unconfirmed delivery. Up to three entries are possible for each APN Network ID.

7.12 Statistics Management on the Conventional PDG

The Statistics Management Interface allows you to view or to reset statistics. The statistics are organized as follows:

- IP bearer statistics are included in Mobile Device Statistics and PDR Statistics.
- Context activation statistics are included in Mobile Device Statistics.
- GTP statistics are included in PDR Statistics.

All counters displayed in the statistics screen are positive integer values, or zero.

7.12.1 Viewing Mobile Device Statistics on the Conventional PDG

When and where to use: Use this procedure to view the mobile device statistics.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations**, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** interface, select **View Statistics** using the arrow keys and press ENTER.
7. In the **View Statistics** interface, select **Mobile Device Statistics** using the arrow keys and press ENTER.
8. In the **View Mobile Device Statistics** interface, perform the following actions:
   a. In the **Radio ID** field, type the Radio ID number.
   b. Select **SUBMIT** using the arrow keys and press ENTER.

   The interface displays statistics for the specified device.

7.12.2 Mobile Device Statistics Fields

Table 46: Mobile Device Statistics Fields

Field	Description
Radio ID	The MSU for which statistics are being displayed.
Queued Msg. receive count	The total number of messages currently queued for delivery to the MSU.
Queued Msg. byte count	The total number of bytes queued for delivery to the MSU.
Outbound messages	Total number of messages sent from the RNG.
Outbound bytes	Total number of bytes in outbound messages.
Outbound NAKs	Total number of negative acknowledgments (NAKs) for outbound messages.
Outbound message timeout count	Total number of outbound messages that are timed out.
Inbound messages	Total number of messages received from the MSU.
Inbound bytes	Total number of bytes in inbound messages.
Inbound failure count	Total number of failures received from the RNG.
Last IB timestamp	Time stamp indicating when the last inbound message was received.
Last OB timestamp	Time indicating when the last outbound message was sent.
Last OB NAK timestamp	Time stamp indicating the last outbound NAK message.
Last OB NAK process status	The last outbound NAK status.
Last outbound NAK response code	The last NAK response code.
Cause for Last Deactivation Reason	The reason why the MSU was last deactivated.
Statistics start timestamp	Time stamp indicating when the Mobile Device Statistics collection started (or when the last reset was done).

7.12.3 Viewing the PDR Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.

6 In the **Statistics Management** menu, select **View Statistics** using the arrow keys and press ENTER.

7 In the **View Statistics** menu, select **PDR Statistics** using the arrow keys and press ENTER.

The **PDR Statistics** screen appears.

7.12.4 PDR Statistics Fields

Table 47: PDR Statistics Fields

Field	Description
IB ICMP Messages	Total number of ICMP messages sent to mobile applications due to failed inbound datagram delivery.
OB ICMP Messages	Total number of ICMP messages sent to host applications due to failed outbound datagram delivery.
ICMP discarded messages	Total number of discarded outbound ICMP messages.
IB IP Messages	Total number of inbound IP messages.
IB IP Bytes	Total number of bytes in inbound IP messages.
OB IP Messages	Total number of outbound IP messages.
OB IP Bytes	Total number of bytes in outbound IP messages.
IP discarded messages	Total number of discarded inbound and outbound IP messages by the PDR.
ICMP generated	Total number of ICMP messages generated by the PDR.
Number of Broadcast Outbound Packets	Total number of broadcast messages received by the PDR.
Number of Broadcast Outbound Bytes Received	Total number of bytes received in broadcast messages.
Number of Broadcast Outbound Messages Discard Count	Number of broadcast messages received by the PDR that were not delivered, and were ICMPed.
Number of Broadcast Outbound Messages Dropped Count	Number of broadcast messages received by the PDR that were not delivered, but were not ICMPed. This scenario happens under overload condition.
Total Registration Request	Total number of registration requests received by the PDR.
Total number of ADD-USER-REQUEST messages rejected	Total number of ADD-USER requests that were rejected by the RNG.
Total echo requests sent	Total number of echo request messages sent to GGSN.
Total echo responses received	Total number of echo response messages received from GGSN.
Time stamp of last echo request	Time stamp of last echo request sent to GGSN.
Time stamp of last echo response	Time stamp of last echo response received from GGSN.

Table continued…

Field	Description
Total number of error indications received from GGSN	Total number of error messages received from GGSN.
PDR statistics start time	Time stamp indicating when the PDR Statistics collection started (or when last reset was done).

7.12.5

Viewing the RNG Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** menu, select **View Statistics** using the arrow keys and press ENTER.
7. In the **View Statistics** menu, select **RNG Statistics** using the arrow keys and press ENTER.

   The **RNG Statistics** screen appears.

7.12.6

RNG Statistics Fields

Table 48: RNG Statistics Fields

Field	Description
Number of Add User Requests	The number of Add_User_Request (0x51) messages received from all PDRs.
Number of delete User Requests	The number of Delete_User_Request (0x52) messages received from all PDRs.
Number of valid New User Responses	The number of valid New_User_response (0x58) messages received from the PDR.
Number of valid Facility Request Messages	The number of valid Facility_Req (0x59) messages received from the PDR.
Number of Valid Initialization Requests	The number of valid Initialization_Request (0x50) messages received from the PDR.
Number of Invalid Initialization Request	The number of invalid Initialization_Request (0x50) messages received from the PDR.

Table continued…

Field	Description
Number of Valid Configuration Requests	The number of valid Config_Request (0x56) messages received from the PDR.
Number of Invalid Configuration Request	The number of invalid Config_Request (0x56) messages received from the PDR.
Number of Reset RNG Messages	The number of Reset_RNG (0x54) messages received from the PDR.
Number of OB Data Requests received	The number of OB_Data_Request (0x29) messages received from the PDR.
Number of OB Data Responses – ACK	The number of OB_Data_Response (0xA9) messages sent to the PDR with “status” field set to ACK (0x00).
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) messages sent to the PDR with “status” field set to NACK (0x01).
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Invalid Message with “status” field set to NACK (0x01) and response code” field set to “Invalid Message (0x81)”.
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Infrastructure Routing Error with “status” field set to NACK (0x01) and “response code” field set to “Infrastructure routing error (0x89)”.
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Message Not Sent with “status” field set to NACK (0x01) and “response code” field set to “Message Not Sent (0x83)”.
Number of OB Data Responses – NACK	The number of OB_Data_Response (0xA9) message sent to the PDR Subscriber Not in this Zone with “status” field set to NACK (0x01) and “response code” field set to “Mobile Subscriber Not in the Zone/Not found (0x88)”.
Number of IB Data Indication sent	The number of IB_Data_Indication (0xAC) messages sent to the PDR.
Number of Valid Start Flow Requests	The number of valid Start_Flow_Request (0x01) messages received from the PDR.
Number of Invalid Start Flow Requests	The number of invalid Start_Flow_Request (0x01) messages received from the PDR.
Number of Valid Loop Back Messages	The number of valid Loop_Message (0x22) messages received from the PDR.
Number of Invalid Loop Back Messages	The number of invalid Loop_Message (0x22) messages received from the PDR.
Number of Invalid Init CID Requests	The number of invalid Init_CID_Request (0x72) messages received from the PDR.
Number of Valid Init CID Requests	The number of valid Init_CID_Request (0x72) messages received from the PDR.

7.12.7 Viewing the PDR-RNG Link Statistics

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys. Press ENTER.

6 In the **Statistics Management** menu, select **View Statistics** using the arrow keys. Press ENTER

7 In the **View Statistics** menu, select **PDR-RNG Link Statistics** using the arrow keys. Press ENTER.

The PDR-RNG Link Statistics screen appears.

7.12.8 PDR-RNG Link Statistics Fields

Table 49: PDR-RNG Link Statistics Fields

Field	Description
RNG Name	Name of the RNG.
Total Connections	Total number of established connections to the RNG.
Total Failed Connections	Total number of failed establishments to the RNG.
Total IB FLM Messages	Total number of inbound messages received.
Total IB FLM Unknown Messages	Total number of inbound messages not containing a valid message content.
Total OB FLM Messages	Total number of outbound messages.
Total OB FLM Unknown Messages	Total number of outbound messages not containing a valid message type.
Total IB Discarded Messages	Total number of messages that contained an invalid message length prefix.
Host Loopback Request Count	Total number of loop back messages sent to the RNG.
Host Loopback Response Count	Total number of loop back messages received from the RNG.
PDR-RNG Link Statistics Time stamp	Time stamp indicating when the PDR-RNG Link Statistics collection started (or when last reset was done).

7.12.9 Resetting the Statistics on the Conventional PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **Statistics Management** using the arrow keys and press ENTER.
6. In the **Statistics Management** menu, select **Reset Statistics** using the arrow keys and press ENTER.
7. On the **Reset Statistics** screen, press ENTER to select or deselect the statistics you want to reset.
8. Select **SUBMIT** using the arrow keys and press ENTER.

   The statistics are reset.

7.13 Viewing the RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **RNG Configuration** using the arrow keys and press ENTER.
6. In the **RNG Configuration** menu, select **View RNG Configuration** using the arrow keys. Press ENTER.
7. In the **View RNG Configuration** screen, if there is more than one RNG in the system, press ENTER to access the **Option List**.
8. Select the desired RNG using the arrow keys and press ENTER.
9. Select **SUBMIT** using the arrow keys and press ENTER.

   The **View RNG Configuration** screen displays the configuration parameters for the selected RNG.

7.13.1 View RNG Configuration Fields

Table 50: View RNG Configuration Fields

Field	Description
RNG Name	The name of the RNG.
RNG Instance ID	The number of the RNG.
RNG PDG Instance ID	The logical identifier of the RNGs PDG.
RNG IP Address	The IP address of the RNG.
Zone ID	The zone in which the RNG resides.
Co-resident Flag	A flag indicating if the RNG is co-resident.
RNG Statistics Update Interval	The interval between updates of statistics from the RNG.
Data Port	Port number used for data messages.
Control Port	Port number used for control messages.
Keep Alive Interval	The amount of time (seconds) between automatically sending keep-alive messages. A value of zero disables sending keep-alive messages.
Keep Alive Count	The number of missed keep-alive responses the PDR allows before bringing down the link with RNG.
RNG SW Version	The current software version for the RNG.
Control Link State	The status of the control link. The possible values are: STARTING, STARTED, STOPPED.
RNG Link TCP Connect State	The status of the TCP layer connect state of the PDR-RNG link. The possible values are: STARTING, STARTED, STOPPED.
RNG Link Established State	The Status of the PDR-RNG link: UP, DOWN.

7.14 Modifying the RNG Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press Enter.
5. In the **PDG Local Configuration** interface, select **RNG Configuration** using the arrow keys and press Enter.
6. In the **RNG Configuration** menu, select **Modify RNG Configuration** using the arrow keys. Press Enter.

7 In the **Modify RNG Configuration** screen, if there is more than one RNG in the system, press ENTER to access the **Option List**. Use the arrow keys to select the desired RNG and press ENTER.

8 Select **SUBMIT** using the arrow keys and press ENTER.

NOTICE: If you have selected a non co-resident RNG to modify, you can only modify the Keep Alive Interval and Keep Alive Count values.

The **Modify RNG Configuration** screen displays the configuration parameters for the selected RNG.

9 Using the arrow keys, move to the desired fields and make the changes.

10 Using the arrow keys, select **SUBMIT** and press ENTER.

If the modifications were saved successfully, you return to the Modify RNG Configuration screen. If the modifications failed, the screen displays the invalid parameter and the reason for the failure.

7.14.1 Modify RNG Configuration Fields

Table 51: Modify RNG Configuration Fields

Field	Description
RNG Name	The Name used to identify the RNG. This field cannot be modified.
Keep Alive Interval	Specifies the amount of time between automatically sending a keep alive message. The possible values are: 1 sec, 2 sec, 3 sec, 4 sec, 5 sec, 10 sec, 15 sec, 20 sec, 30 sec, 45 sec, 50 sec. Default value is 5 sec.
Keep Alive count	The number of keep alive timeouts the PDR allows before assuming a CID is down. The valid range is 2 - 10. Default value is 2.
RNG Statistics Update Interval	Specifies the interval between updates of statistics from the RNG. This field is applicable for local RNG only. The valid range is 0 - 255 (0 = disabled). Default value is 30 sec.

7.15 Viewing the Status of the Local RNG-Site Link

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, use the arrow keys to select **Local RNG-Site Link Status** and press **Enter**.

The **Local RNG-Site Link Status** screen displays the status fields.

7.15.1 Local RNG-Site Link Status Fields

Table 52: Local RNG-Site Link Status Fields

Field	Description
Site ID	Site ID
Link Status	The values are: Disconnected, Connected.

7.16 Viewing the Gateway Router Configuration

Procedure:

1 Log on to the PDG and invoke the **Main Menu**. See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, use the arrow keys to select **View Gateway Router Configuration** and press ENTER.

6 On the **View Gateway Router Configuration** screen, if there is more than one gateway in the system, press ENTER to access the **Option List**.

7 Use the arrow keys to select the desired gateway and press ENTER.

8 Use the arrow keys to select **SUBMIT** and press ENTER.

The **View Gateway Router Configuration** screen displays the configuration parameters for the selected gateway.

7.16.1 Gateway Router Configuration Fields

Table 53: Gateway Router Configuration Fields

Field	Description
Gateway Router ID	Gateway router identity
Gateway link status	Link status with the peer router
Gateway Router IP address	IP address of the gateway router
Gateway Router last link drop Timestamp	Timestamp of the last time the link to the primary gateway router was down

Table continued…

Field	Description
Gateway Router last link recover Timestamp	Timestamp of the last time the link to the primary gateway router was recovered

7.17 Viewing the KMF Configuration on the Conventional PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.
5. In the **PDG Local Configuration** interface, select **View Key Management Facility Information**. Press ENTER.

   A list of KMFs appears. If no KMF is installed and configured, a message informs you that no KMFs have been found.
6. In the **View Key Management Facility Information** menu, perform the following actions:
   - If there is more than one KMF, use the arrow keys to select an appropriate KMF and select **SUBMIT**. Press ENTER
   - If there is only one KMF, select **SUBMIT**. Press ENTER.

   The KMF configuration information appears.

7.17.1 View Key Management Facility Information Fields

Table 54: View Key Management Facility Information Fields

Field	Description
RNG-KMF OTEK Link Status	Defines whether the RNG-KMF link is up or down.
OTEK Service Port Number	Defines the port number of the KMF to be used in OTEK Communication.
OTAR Service Port Number	Defines the port number of the KMF to be used in OTAR Communication.
Network KMF IP Address	Defines the KMF RNI IP address. This address is used for OTEK.
CEN KMF IP Address	Defines the KMF CEN IP address. This address is used for OTAR.
KMF Domain Name	Defines the FQDN of the KMF.
KMF RSI	Defines the Radio Set Identifier of the KMF (Hexadecimal).

7.18 Viewing the CDEM Configuration on the Conventional PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration** and press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press Enter.
5. In the **PDG Local Configuration** interface, select **View CAI Data Encryption Module Information**. Press Enter.

   If no CDEM is installed and configured in the system, a message appears informing that no CDEMs have been found.
6. In the **View CAI Data Encryption Module Information** interface, select **SUBMIT**. Press Enter.

   The CDEM configuration information appears.

7.18.1 View CAI Data Encryption Module Configuration Fields

Table 55: View CAI Data Encryption Module Configuration Fields

Field	Description
RNG-CDEM Link Status	Defines whether the RNG-CDEM link is up or down.
CDEM IP Address	Defines the network IP address of the CDEM.
KMF Id	Defines the ID of the KMF associated with this CDEM (0 if OTEK is disabled).
OTEK Transmit Security Level	Defines the OTEK security level (Secure or Basic) when sending KMM messages to the KMF.
OTEK Receive Security Level	Defines the OTEK security level (secure or basic) when receiving KMM messages from the KMF.
OTEK Inactivity Time Period	Defines the frequency with which the PDG sends a registration message to the KMF in the absence of other OTEK activity. The units are defined in hours.

7.19 Viewing the Channels Per Sites Information on the Conventional PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration** and press ENTER.

5 In the **PDG Local Configuration** interface, select **View Channels Per Site Information**. Press ENTER.

If the sites are configured, the **View Channels Per Sites Information** interface appears.

6 Use arrow keys to select the site that you want to view the information for. Select **SUBMIT**. Press ENTER.

The read-only site information appears.

7.19.1
View Channels Information Fields

Table 56: View Channels Information Fields

Field	Description
Site ID	Site number
Number of channels	Number of channels in the site
Channel ID	Channel identifier within the site
Data Conventional Channel Mode	Channel mode of the digital conventional channel
Vote Scan Flag	This parameter is used when sending outbound data to the channel. If the channel is configured for Vote Scan, a preamble is transmitted before the start of every data transaction to a scan enabled subscriber. If the channel is not configured for Vote Scan, a preamble is transmitted when Scan Suspend Timer has expired for a scan enabled subscriber. If the channel is not configured for Vote Scan, a scan-enabled subscriber is considered as using Data (Conventional) Scan. The RNG uses the Scan Suspend Timer to determine when a Data Scan subscriber is locked on a data channel. A preamble is transmitted before an outbound datagram or acknowledgment when a Data Scan subscriber is not locked on a data channel. A preamble is not transmitted when a Data Scan subscriber is locked on a data channel. **NOTICE:** The RNGs Scan Suspend Timer must be set to the same value as the CPS-configured data hang time in the subscriber unit in order for the preamble to be sent correctly to Data Scan subscribers.

7.20
SNMPv3 Credentials Maintenance

The following SNMPv3 configuration can be configured on the Packet Data Gateway (PDG):

- Configuring USM User Security for the PDG

- Modifying User Passphrases for the PDG
- Modifying User Security Levels for the PDG

For more information on changing SNMPv3 credentials, see “Configuring the PDG for SNMPv3” in the *SNMPv3 Feature Guide*.

7.21 SSH Configuration on the Conventional PDG

SSH configuration should be backed up for later recovery in case of any failure. For more information on configuring and restoring SSH Configuration on the PDG, see the *Securing Protocols with SSH Feature Guide*.

7.22 Minimum Configuration Requirements for the RNG and the System

The following tables provide the configuration parameters for configuring the RNG and the system.

The following table describes the key parameters that must be set up in the Modify RNG interface.

Table 57: RNG Configuration Parameters

Field	Comment
RNG name	RNG Name is set by Network Management
Keep Alive Interval	This must be set to 5 (default)
Keep Alive Count	This must be set to 2 (default)
RNG Statistics Update Interval	This must be set to 30 (default)

The following table provides the key system parameters that must be set up in the Modify PDG configuration screen.

Table 58: Conventional PDG Configuration Fields

Field	Comment
Default Log File Directory	This must be set to `/home/pdr/log` (default)
LAP-D T200 Reply timeout	The acknowledgment (ACK) timer indicates the timeout on a response to the transmission of information (I) frame in milliseconds (RANGE 1000 -50000).
LAP-D T203 Keep alive timer	Maximum time allowed without frames being exchanged, in milliseconds (range 1000-50000). When the timer expires, the links between the RNG and Base Site are torn down.
LAP-D N200 Max Retransmissions	The maximum number of retransmissions of a frame (range 1-3)
LAP-D N201 Max number of octets in the information field	The maximum number of data bytes in Information (I) frames. Default is 260
LAP-D K Window Size	The maximum number of outstanding Information (I) frames (Range 1-16)

7.23 PDR Configuration

PDR provides two configuration features:

- Remote Configuration – Used by the Network Manager to configure the PDR
- Local Configuration – PDR local configuration interface

The PDG configuration interface is used to configure the PDR and to verify that the PDG database is synchronized. For more information, see Conventional IVD M Core PDG Database Synchronization on page 90.

7.24 Changing the Conventional PDG Welcome Banner

See “Changing the Welcome Banner on a Linux-Based Device” in the *Unix Supplemental Configuration Setup Guide*.

This page intentionally left blank.

Chapter 8

Trunked IVD and HPD PDG Operation

This chapter details the tasks that you perform once the Trunked IV&D and HPD Packet Data Gateway is installed and operational on your system.

8.1 Starting the Trunked PDG Hardware

Procedure:

1. Verify that the power On/Off button on the PDG hardware is off.
2. Press and hold the power On/Off button on the front panel of the PDG until the LED lights up green.

   The PDG hardware starts booting.

8.2 Logging On to the Trunked PDG and Invoking the Main Menu

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see Appendix B in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the Packet Data Gateway (PDG) in one of the following ways:

If…	Then…
The PDG you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	Log on using your Active Directory account credentials. For instructions about using PuTTY for SSH sessions, see the *Securing Protocols with SSH Feature Guide*.
The PDG you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	Use a vSphere client connection to access the server and log on with the root account. For more information, see the *Virtual Management Server Software User Guide*.

2. To invoke the **Main Menu**, enter the following command: `admin_menu`

8.3 Checking the Trunked PDG Redundancy State (DSR)

This section is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) systems.

Procedure:

1. Connect to the PDG ESXi-based server through the VMware vSphere Client and open the console of the PDG virtual machine.

2 Access the PDG Local Configuration interface.

See Accessing the Trunked PDG Local Configuration Interface on page 95.

3 Select **Redundancy Configuration**. Press Enter.

4 In the **Redundancy Configuration** menu, select **View Redundancy Configuration**. Press Enter.

The **View Redundancy Configuration** window appears, displaying the PDG state. The initial default state is user requested standby.

5 To exit the **View Redundancy Configuration** window, type `q` and then type `y`.

8.3.1
Trunked PDG States in DSR Systems

Table 59: Trunked PDG States in a Dynamic System Resilience (DSR) Configuration

PDG State	Description
Active Operable	PDG is active and running.
Active In-Operable	PDG is active but not in the operable condition.
Standby Operable	PDG is in the standby and operable condition.
Standby In-Operable	PDG is in standby but not in the operable condition.
User Requested Standby (URS) Operable	PDG is in the user requested standby and operable condition.
User Requested Standby (URS) In-Operable	PDG is in user requested standby but not in the operable condition.
Active Semi-Operable	PDG is active and operable but it has no link to the CDEM.
Standby Semi-Operable	PDG is in standby and operable but it has no link to the CDEM.
User Requested Standby (URS) Semi-Operable	PDG is in user requested standby and operable but it has no link to the CDEM.

8.4
Setting the Trunked PDG to the Active State (DSR)

This procedure is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) feature.

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Trunked PDR on page 168.

Procedure:

1 Log on to the PDG as the root user.

2 Enter: `admin_menu`

3 In the **Main Menu**, select **Application Administration**. Press Enter.

4 In the **Application Administration** menu, select **Application Specific Management and Operations**. Press Enter.

5. In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press ENTER.
6. In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press ENTER.
7. In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

   The menu displays the PDG status. The initial default state is user requested standby.

8. In the **Modify Redundancy Configuration** menu, perform the following actions:
   a. Select **Active** by using the arrow keys. Press ENTER.
   b. Select **Submit** by using the arrow keys. Press ENTER.

   A message appears, warning that this action enables automatic switchover and may enable the PDG for data service.

9. Select **Yes** to proceed. Press ENTER.

   A message confirms that the PDG redundancy state is active.

10. To exit the **PDG Local Configuration** menu, type `q` and then type `y`.

    The **Application Specific Management and Operations** menu appears.

11. To exit the **Main Menu**, type `q`. Press ENTER.

    The command prompt appears.

8.5 Setting the Trunked PDG to the Standby State (DSR)

This procedure is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) feature.

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Trunked PDR on page 168.

Procedure:

1. Log on to the PDG as the root user.
2. Enter: `admin_menu`
3. In the **Main Menu**, select **Application Administration**. Press ENTER.
4. In the **Application Administration** menu, select **Application Specific Management and Operations**. Press ENTER.
5. In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press ENTER.
6. In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press ENTER.
7. In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

   The menu display the PDG status. The initial default state is user requested standby.

8. In the **Modify Redundancy Configuration** menu, perform the following actions:
   a. Select **Standby** by using arrow keys. Press ENTER.
   b. Select **Submit** by using arrow keys. Press ENTER.

NOTICE: If there is no other active PDG, putting the backup PDG to standby automatically makes it go active. If there is another active PDG, the backup PDG remains in standby state.

A message confirms that the PDG redundancy state is standby.

9 To exit the **PDG Local Configuration** menu, type `q` and then type `y`.

The **Application Specific Management and Operations** menu appears.

10 To exit the **Main Menu**, type `q`. Press ENTER.

The user's command prompt appears.

8.6 Checking the Fault Tolerance Status of a High Availability PDG with UEM

If your system supports the High Availability for IV&D and HPD (HA Data) feature, perform this procedure to check the status of a Packet Data Gateway (PDG) in the Fault Tolerance application by using Unified Event Manager (UEM).

Prerequisites:
Ensure that VMware vCenter is discovered in UEM.

Procedure:

1 From the navigation tree in UEM, select **Network Database** and find the PDG Fault Tolerant Virtual Machine on the list of managed resources.

In the **Type** column, the PDG is displayed as Fault Tolerant Virtual Machine. The **Managed Resources** column shows the name of the PDG virtual machine assigned during installation.

2 Select the PDG Fault Tolerant Virtual Machine.

3 From the top menu, select **View** → **Alarms**.

4 In the **Alarms** window, search for an alarm for the **Fault Tolerant Service**.

NOTICE:
If no alarm for the Fault Tolerant Service is displayed, it means that Fault Tolerance is enabled for the PDG and is not reporting any issues.

UEM reports the state of the Fault Tolerant Service for each redundant PDG group separately.

The status of the Fault Tolerant Service for the PDG virtual machine is displayed in the **Message** column.

8.7 Performing a Manual Switchover between High Availability PDGs

If your system supports the High Availability for Trunked IV&D (including Enhanced Data) and HPD (HA Data) feature, use this procedure to control which Packet Data Gateway (PDG) is active by initiating a switchover from the primary to the secondary PDG. This operation is available to the user, but not performed in a regular scenario.

Prerequisites: Ensure that VMware vCenter is discovered in Unified Event Manager (UEM).

Procedure:

1 From the **Navigation View** pane in UEM, select **Network Database** and find the PDG Fault Tolerant Virtual Machine on the list of managed resources.

   NOTICE: In the Type column, the PDG is displayed as Fault Tolerant Virtual Machine. The Managed Resources column shows the name of the PDG virtual machine.

2 Right-click the PDG Fault Tolerant Virtual Machine and select **Issue Command**.

   The **Command** window appears.

3 Select **Switchover** and click **Apply**.

   A switchover is performed. The secondary PDG becomes active, and the previously active PDG becomes redundant.

8.8 Accessing the PDR Specific Management and Operations Menu

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.

   The **PDR Specific Management and Operations** menu appears.

8.9 Accessing the RNG Specific Management and Operations Menu

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

   The **RNG Specific Management and Operations** menu appears.

8.10 Verifying the Trunked PDR and RNG Status

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Manage Application Status**. Press ENTER.

4 In the **Manage Application Status** menu, type the number associated with **Display Application Status**. Press ENTER.

The status of the PDR and RNG is displayed.

8.11 Verifying the RNG Status

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **Display RNG Status**. Press ENTER.

The RNG application status is displayed.

8.12 Shutting Down the Trunked PDG

Perform this procedure to disable the Trunked Packet Data Gateway (PDG) applications, shut down the Linux OS of the PDG, and power off the PDG hardware in an orderly manner to avoid any potential data loss.

⚠ **CAUTION:**
Executing this procedure results in a loss of data messaging.

NEVER shut down the Packet Data Router (PDR) and Radio Network Gateway (RNG) applications by just pressing the power switch or disconnecting the power cord.

To disable the PDG applications and shut down the Linux OS of the PDG, perform the following procedure.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Manage Application Status**. Press ENTER.

4 In the **Manage Application Status** menu, type the number associated with **Disable Application**. Press ENTER.

The RNG and PDR shut down.

5 Type `b` and press ENTER twice to return to the **Main Menu**.

6 In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.

7 In the **OS Administration** menu, type the number associated with **Shutdown**. Press ENTER.

The Linux OS of the PDG shuts down and the PDG VM powers off.

8 To shut down the PDG hardware, shut down the VMware ESXi-based server.

See "Shutting Down the ESXi Server" in the *Virtual Management Server Software User Guide*.

8.13 Rebooting the Trunked PDG

Perform this procedure to reboot the Packet Data Gateway (PDG) due to an update or a configuration change.

CAUTION: Executing this procedure results in a loss of data messaging.

IMPORTANT:
If the redundancy state of the PDG is active and the redundancy state of the peer PDG is standby, rebooting the PDG causes the peer PDG to become active. To avoid an undesired switchover, ensure that the redundancy state of the peer PDG is set to User Requested Standby (URS) before restarting or stopping the PDG. When the PDG is restarted and in the active state, set the peer PDG back to the standby state.

To set the peer PDG to the User Requested Standby (URS) state, see Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

To view the redundancy state of the PDG, see Checking the Trunked PDG Redundancy State (DSR) on page 161.

NOTICE:
You do not have to stop the Packet Data Router (PDR) application manually as it is a part of this procedure.

The Radio Network Gateway (RNG) is reset during this procedure.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **Software Administration**. Press ENTER.

3 In the **Software Administration** menu, type the number associated with **Server Reboot**. Press ENTER.

NOTICE: If the Virtual PDG is properly configured as described in the software installation manual, the Linux OS and the PDR application are automatically reloaded without further user intervention.

The Linux OS shuts down, and the PDR shuts down if it is running. The Linux OS pauses momentarily and restarts.

8.14 Starting and Stopping the Trunked PDR and RNG

After you performed Creating a Default Trunked PDG Database on page 216, the PDR and RNG are up and running. However, if you want to manually start and stop the PDR and/or the RNG, perform the following procedures:

- Starting the Trunked PDR on page 168

- Stopping the Trunked PDR on page 168
- Starting the Trunked RNG on page 169
- Stopping the Trunked RNG on page 170

8.15

Starting the Trunked PDR

The Packet Data Route (PDR) is automatically started when the power to the system hardware is turned on as part of the system initialization routine. If there is a problem during the system startup and the PDR is not started, perform the following procedure, to manually start the PDR once the problem is resolved.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.
5. In the **PDR Application Specific Management and Operations** menu, type the number associated with **Start PDR**. Press ENTER.

   The PDR application is started.

8.16

Stopping the Trunked PDR

The procedure for stopping the Packet Data Router (PDR) ensures that the runtime information is saved to the Packet Data Gateway (PDG) database before terminating the system activity. Perform this procedure only if you intend to upgrade or reinstall the PDR software, restore the PDR database, or other maintenance activities that do not include powering off the Packet Data Gateway (PDG).

Do not shut down the PDG if only the RNG software is updated.

To shut down the system in preparation for powering off the PDG hardware, see Shutting Down the Trunked PDG on page 166.

⚠ **CAUTION:**
Executing this procedure results in a loss of data messaging.

Never shut down the PDR and RNG applications by just flipping off the power switch or by disconnecting the power cord. If the power to the PDG hardware is to be turned off, the Operating System (OS) must be shut down as described in Shutting Down the Trunked PDG on page 166.

IMPORTANT:
If the redundancy state of the PDG is active and the redundancy state of the peer PDG is standby, rebooting the PDG causes the peer PDG to become active. To avoid an undesired switchover, ensure that the redundancy state of the peer PDG is set to User Requested Standby (URS) before restarting or stopping the PDG. When the PDG is restarted and in the active state, set the peer PDG back to the standby state.

To set the peer PDG to the User Requested Standby (URS) state, see Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

To view the redundancy state of the PDG, see Checking the Trunked PDG Redundancy State (DSR) on page 161.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press Enter.

5 In the **PDR Specific Management and Operations** menu, select **Stop PDR**. Press Enter.

NOTICE: If the process times out, a notification message appears and all PDR processes terminate.

The PDR is stopped.

6 To check that the PDR is stopped, in the **PDR Specific Management and Operations** menu, select **Display PDR Status**. Press Enter.

The PDR status is displayed.

7 To exit from the **Main Menu**, type **q**. Press Enter.

The user’s command prompt appears.

8.17
Starting the Trunked RNG

The Radio Network Gateway (RNG) is automatically started when the power to the system hardware is turned on as part of the system initialization routine. If there is a problem during the system startup and the RNG is not started, perform the following procedure to manually start the RNG once the problem is resolved.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.

5 In the **RNG Specific Management and Operations** menu, select **Start RNG**. Press Enter.

The RNG is started.

8.18 Stopping the Trunked RNG

The procedure for stopping the Radio Network Gateway (RNG) ensures that the runtime information is saved to the RNG database before terminating the system activity. Execute this procedure only if you are intending to upgrade or reinstall the RNG or Packet Data Router (PDR) software, or perform other maintenance activities that do not include powering off the Packet Data Gateway (PDG).

CAUTION:
Executing this procedure results in a loss of data messaging.

Never shut down the RNG application by just pressing the power button or disconnecting the power cord. If you want to turn off the power to the PDG hardware, shut down the Operating System (OS) as described in Shutting Down the Trunked PDG Hardware on page 170.

IMPORTANT:
If the redundancy state of the PDG is active and the redundancy state of the peer PDG is standby, rebooting the PDG causes the peer PDG to become active. To avoid an undesired switchover, ensure that the redundancy state of the peer PDG is set to User Requested Standby (URS) before restarting or stopping the PDG. When the PDG is restarted and in the active state, set the peer PDG back to the standby state.

To set the peer PDG to the User Requested Standby (URS) state, see Setting the Trunked PDG to the User Requested Standby (URS) State on page 208.

To view the redundancy state of the PDG, see Checking the Trunked PDG Redundancy State (DSR) on page 161.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **Stop RNG**. Press Enter.

The RNG is shut down.

8.19 Shutting Down the Trunked PDG Hardware

Prerequisites:
Before turning off the power to the Packet Data Gateways (PDG) hardware, shut down the Linux Operating System (OS) in an orderly manner avoid potential data loss. This procedure describes how to shut down the Linux OS in an orderly manner to avoid any potential data loss.

CAUTION:
Executing this procedure results in a loss of data messaging.

Never shut down the Packet Data Router (PDR) and Radio Network Gateway (RNG) applications by just pressing the power button or disconnecting the power cord. If you want to turn off the power to the PDG hardware, shut down the OS as described in Shutting Down the Trunked PDG on page 166.

NOTICE: You do not have to stop the RNG and PDR applications manually as it is a part of this procedure.

Procedure:

1. Log on to the PDG as `root`.

   The `[root@pdr /root]#` prompt appears.

2. At the prompt, type `halt`. Press ENTER.

   A message confirms that the system is halted.

8.20

Changing Passwords on the Trunked PDG

When changing passwords, follow the rules listed in Domain User Names and Domain User/Root Account Passwords Data Value Requirements and Criteria for the Trunked PDG on page 57.

Procedure:

1. Log on to the PDG as the user that you wish to change the password for.
2. At the prompt, type `passwd`. Press ENTER.
3. Type the new password. Press ENTER.
4. Retype the new password. Press ENTER.

8.21

Managing AAA Client Configuration

See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide* to join the PDG to the Active Directory domain and verify the domain membership status.

8.22

Managing Syslog Client Configuration

See “Enabling/Disabling Centralized Event Logging on Linux Devices” in the *Centralized Event Logging Feature Guide*.

8.23

Displaying the NTP Client Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161

2. In the **Main Menu**, type the number associated with **Services Administration**. Press ENTER.

3 In the **Services Administration** menu, type the number associated with **Manage NTP Client Configuration**. Press ENTER.

4 In the **Manage NTP Client Configuration** menu, type the number associated with **Display NTP Client Configuration**. Press ENTER.

If the NTP client is not configured, a message informs you that there are no remote NTP time sources. If the NTP client is configured, you can see the Hosted NTP aliases and IP addresses of the remote NTP time sources.

8.24
Configuring the NTP Client

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161

2 In the **Main Menu**, type the number associated with **Services Administration**. Press ENTER.

3 In the **Services Administration** menu, type the number associated with **Manage NTP Client Configuration**. Press ENTER.

4 In the **Manage NTP Client Configuration** menu, type the number associated with **Configure NTP Client**. Press ENTER.

5 In the **Enter NTP Client Configuration** menu, perform one of the following actions:

If…	Then…
If you want to add the NTP Server IP to the PDG NTP client configuration,	perform the following actions: a Select **Add NTP Server IP Address**. **Result:** You are prompted to enter the IP address of an external NTP time source. b Type the valid IP of the NTP server according to the system IP plan. The synchronization with the new NTP source is started. If the process is successful, the IP is added as an external NTP time source.
If you want to remove the NTP Server IP from the PDG NTP client configuration,	Select **Remove NTP Server IP Address**. The synchronization with the NTP server which is left in the list of the NTP sources is started, and the message about removing the selected NTP time source appears.

8.25
RNG Diagnostics

The Radio Network Gateway (RNG) is capable of storing the average number of data packets transmitted and received on each of its links to the base sites per hour.

Averages are computed for each data type and separately for five data packet length ranges. Averages are updated every 15 minutes since the last reset or start procedure.

The RNG provides statistics for the following data types:

- Confirmed inbound

- Confirmed outbound
- Unconfirmed inbound
- Unconfirmed outbound
- Enhanced data

The RNG provides statistics for the following data packet length ranges:

- Less than 64 bytes
- 64 to 127 bytes
- 128 to 255 bytes
- 256 to 511 bytes
- 512 to 1023 bytes
- More than 1024 bytes

The information collected by using this function can be used by engineering application tools for traffic analysis and coverage prediction.

8.25.1

Starting RNG Enhanced Logging

Perform this procedure to start collecting and storing Radio Network Gateway (RNG) diagnostics information. The log file includes information on the cumulative moving average number of data messages calculated every 15 minutes for messages received up to the time of calculation per site and per each user data size. The system collects and stores information on both Classic Data and Enhanced Data.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, select **Application Administration**.
3. In the **Application Administration** menu, select **Application Specific Management and Operations**.
4. In the **Application Specific Management and Operations** menu, select **RNG Specific Management and Operations**.
5. The **RNG Specific Management and Operations** menu, select **Start RNG Enhanced Logging**.

   The system starts collecting and storing RNG diagnostics information in a log file.

8.25.2

Stopping RNG Enhanced Logging

Perform this procedure to stop collecting and storing Radio Network Gateway (RNG) diagnostics information.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, select **Application Administration**.

3 In the **Application Administration** menu, select **Application Specific Management and Operations**.

4 In the **Application Specific Management and Operations** menu, select **RNG Specific Management and Operations**.

5 The **RNG Specific Management and Operations** menu, select **Stop RNG Enhanced Logging**.

The system stops collecting and storing RNG diagnostics information in a log file.

8.25.3 Resetting RNG Enhanced Logging Statistics

Perform this procedure to reset the Radio Network Gateway (RNG) diagnostics information stored in a log file.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, select **Application Administration**.

3 In the **Application Administration** menu, select **Application Specific Management and Operations**.

4 In the **Application Specific Management and Operations** menu, select **RNG Specific Management and Operations**.

5 The **RNG Specific Management and Operations** menu, select **Reset Enhanced Logging Stats**.

The system resets the RNG diagnostics information stored in a log file.

8.25.4 Exporting RNG Enhanced Logging Statistics

Perform this procedure to export the Radio Network Gateway (RNG) diagnostics information in a `.csv` file. The log file includes the information on the cumulative moving average number of data messages calculated every 15 minutes for messages received up to the time of calculation per site and per each user data size. The system collects and stores information on both Classic Data and Enhanced Data.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, select **Application Administration**.

3 In the **Application Administration** menu, select **Application Specific Management and Operations**.

4 In the **Application Specific Management and Operations** menu, select **RNG Specific Management and Operations**.

5 The **RNG Specific Management and Operations** menu, select **Export Enhanced Logging Stats**.

The system exports the RNG diagnostics information in a `.csv` file in the `/var/tmp` directory.

Chapter 9

Conventional IVD M Core and Conventional IVD K Core PDG Operation

This chapter details the tasks that you perform once the Conventional IV&D M core and K core Packet Data Gateway (PDG is installed and operational on your system.

9.1 Starting the Conventional PDG Hardware

Procedure:

1. Verify that the power On/Off button on the PDG hardware is Off.
2. Press and hold the power On/Off button on the front panel of the PDG until the button LED lights up green.

   The PDG hardware starts booting.

9.2 Logging On to the Conventional PDG and Invoking the Main Menu

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see Appendix B in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the Packet Data Gateway (PDG) in one of the following ways:

If…	Then…
The PDG you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	Log on using your Active Directory account credentials. For instructions about using PuTTY for SSH sessions, see the *Securing Protocols with SSH Feature Guide*.
The PDG you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	Use a vSphere client connection to access the server and log on with the root account. For more information, see the *Virtual Management Server Software User Guide*.

2. To invoke the Main Menu, enter the following command: `admin_menu`.

9.3 Checking the Conventional PDG Redundancy State (DSR)

This section is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) systems.

Procedure:

1. Connect to the PDG ESXi-based server through the VMware vSphere Client and open the console of the PDG virtual machine.
2. Access the PDG Local Configuration interface.

   See Accessing the Conventional PDG Local Configuration Interface on page 129.
3. Select **Redundancy Configuration**. Press ENTER.
4. In the **Redundancy Configuration** menu, select **View Redundancy Configuration**. Press ENTER.

   The **View Redundancy Configuration** window appears, displaying the PDG state. The initial default state is user requested standby.
5. To exit the **View Redundancy Configuration** window, type `q` and then type `y`.

9.4 Setting the Conventional PDG to the Active State (DSR)

This procedure is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) feature.

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Trunked PDR on page 168.

Procedure:

1. Log on to the PDG as the root user.
2. Enter: `admin_menu`
3. In the **Main Menu**, select **Application Administration**. Press ENTER.
4. In the **Application Administration** menu, select **Application Specific Management and Operations**. Press ENTER.
5. In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press ENTER.
6. In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press ENTER.
7. In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

   The menu displays the PDG status. The initial default state is user requested standby.
8. In the **Modify Redundancy Configuration** menu, perform the following actions:
   a. Select **Active** by using the arrow keys. Press ENTER.
   b. Select **Submit** by using the arrow keys. Press ENTER.

   A message appears, warning that this action enables automatic switchover and may enable the PDG for data service.
9. Select **Yes** to proceed. Press ENTER.

   A message confirms that the PDG redundancy state is active.

10 To exit the **PDG Local Configuration** menu, type `q` and then type `y`.

The **Application Specific Management and Operations** menu appears.

11 To exit the **Main Menu**, type `q`. Press ENTER.

The command prompt appears.

9.5 Setting the Conventional PDG to the Standby State (DSR)

This procedure is only applicable to Packet Data Gateways (PDGs) in systems employing the Dynamic System Resilience (DSR) feature.

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Trunked PDR on page 168.

Procedure:

1 Log on to the PDG as the root user.

2 Enter: `admin_menu`

3 In the **Main Menu**, select **Application Administration**. Press ENTER.

4 In the **Application Administration** menu, select **Application Specific Management and Operations**. Press ENTER.

5 In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press ENTER.

6 In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press ENTER.

7 In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

The menu display the PDG status. The initial default state is user requested standby.

8 In the **Modify Redundancy Configuration** menu, perform the following actions:

a Select **Standby** by using arrow keys. Press ENTER.

b Select **Submit** by using arrow keys. Press ENTER.

NOTICE: If there is no other active PDG, putting the backup PDG to standby automatically makes it go active. If there is another active PDG, the backup PDG remains in standby state.

A message confirms that the PDG redundancy state is standby.

9 To exit the **PDG Local Configuration** menu, type `q` and then type `y`.

The **Application Specific Management and Operations** menu appears.

10 To exit the **Main Menu**, type `q`. Press ENTER.

The user’s command prompt appears.

9.6 Checking the Fault Tolerance Status of a High Availability PDG with UEM

If your system supports the High Availability for Conventional (HA Data) feature, perform this procedure to check the status of a Packet Data Gateway (PDG) in the Fault Tolerance application by using Unified Event Manager (UEM).

Prerequisites:
Ensure that VMware vCenter is discovered in UEM.

Procedure:

1. From the navigation tree in UEM, select **Network Database** and find the PDG Fault Tolerant Virtual Machine on the list of managed resources.

   In the **Type** column, the PDG is displayed as Fault Tolerant Virtual Machine. The **Managed Resources** column shows the name of the PDG virtual machine assigned during installation.

2. Select the PDG Fault Tolerant Virtual Machine.
3. From the top menu, select **View** → **Alarms**.
4. In the **Alarms** window, search for an alarm for the **Fault Tolerant Service**.

   NOTICE:
   If no alarm for the Fault Tolerant Service is displayed, it means that Fault Tolerance is enabled for the PDG and is not reporting any issues.

   UEM reports the state of the Fault Tolerant Service for each redundant PDG group separately.

   The status of the Fault Tolerant Service for the PDG virtual machine is displayed in the **Message** column.

9.7 Performing a Manual Switchover between High Availability PDGs

Prerequisites: Ensure that VMware vCenter is discovered in Unified Event Manager (UEM).

When and where to use: If your system supports the High Availability for Conventional IV&D (HA Data) feature, use this procedure to control which Packet Data Gateway (PDG) is active by initiating a switchover from the primary to the secondary PDG. This operation is available to the user, but not performed in a regular scenario.

Procedure:

1. From the **Navigation View** pane in UEM, select **Network Database** and find the PDG Fault Tolerant Virtual Machine on the list of managed resources.

   NOTICE: In the Type column, the PDG is displayed as Fault Tolerant Virtual Machine. The Managed Resources column shows the name of the PDG virtual machine.

2. Right-click the PDG Fault Tolerant Virtual Machine and select **Issue Command**.

   The **Command** window appears.

3. Select **Switchover**. Click **Apply**.

   A switchover is performed. The secondary PDG becomes active, and the previously active PDG becomes redundant.

9.8 Accessing the PDR Specific Management and Operations Menu

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175).
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.

   The **PDR Specific Management and Operations** menu appears.

9.9 Accessing the RNG Specific Management and Operations Menu

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175).
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

   The **RNG Specific Management and Operations** menu appears.

9.10 Verifying the Conventional PDR and RNG Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Manage Application Status**. Press ENTER.
4. In the **Manage Application Status** menu, type the number associated with **Display Application Status**. Press ENTER.

   The status of the PDR and RNG is displayed.

9.11 Verifying the Conventional RNG Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2. Type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **Display RNG Status**. Press Enter.

   The RNG application status is displayed.

9.12
Shutting Down the Conventional PDG

Perform this procedure to disable the Trunked Packet Data Gateway (PDG) applications, shut down the Linux OS of the PDG, and power off the PDG hardware in an orderly manner to avoid any potential data loss.

CAUTION:
Executing this procedure results in a loss of data messaging.

NEVER shut down the Packet Data Router (PDR) and Radio Network Gateway (RNG) applications by just pressing the power switch or disconnecting the power cord.

To disable the PDG applications and shut down the Linux OS of the PDG, perform the following procedure.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration** menu, type the number associated with **Manage Application Status**. Press Enter.
4. In the **Manage Application Status** menu, type the number associated with **Disable Application**. Press Enter.

   The RNG and PDR shut down.
5. Type `b` and press Enter twice to return to the **Main Menu**.
6. In the **Main Menu**, type the number associated with **OS Administration**. Press Enter.
7. In the **OS Administration** menu, type the number associated with **Shutdown**. Press Enter.

   The Linux OS of the PDG shuts down and the PDG VM powers off.
8. To shut down the PDG hardware, shut down the VMware ESXi-based server.

   See “Shutting Down the ESXi Server” in the *Virtual Management Server Software User Guide*.

9.13
Rebooting the Conventional PDG

Perform this procedure to reboot the Packet Data Gateway (PDG) due to an update or a configuration change.

CAUTION: Executing this procedure results in a loss of data messaging.

NOTICE:
You do not have to stop the Packet Data Router (PDR) application manually as it is a part of this procedure.

The Radio Network Gateway (RNG) is reset during this procedure.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Software Administration**. Press ENTER.
3. In the **Software Administration** menu, type the number associated with **Server Reboot**. Press ENTER.

   NOTICE: If the PDG virtual machine is properly configured as described in the software installation manual, the Linux OS and the PDR application are automatically reloaded without further user intervention.

   The Linux OS shuts down, and the PDR shuts down if it is running. The Linux OS pauses momentarily and restarts.

9.14
Starting and Stopping the Conventional PDR and RNG

After you performed Creating a Default Conventional PDG Database on page 239, the PDR and RNG are up and running. However, if you want to manually start and stop the PDR and/or the RNG, perform the following procedures:

- Starting the Conventional PDR on page 181
- Stopping the Conventional PDR on page 182
- Starting the Conventional RNG on page 182
- Stopping the Conventional RNG on page 183

9.15
Starting the Conventional PDR

The Packet Data Router (PDR) is automatically started when the power to the system hardware is turned on as part of the system initialization routine. If there is a problem during the system startup and the PDR is not started, perform the following procedure, to manually start the PDR once the problem is resolved.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.

5. In the **PDR Application Specific Management and Operations** menu, type the number associated with **Start PDR**. Press ENTER.

   The PDR application is started.

9.16
Stopping the Conventional PDR

The procedure for stopping the Packet Data Router (PDR) ensures that the runtime information is saved to the PDG database before terminating the system activity. Perform this procedure only if you intend to upgrade or reinstall the PDR software, restore the PDR database, or perform other maintenance activities that do not include powering off the PDG.

Do not shut down the PDG if only the RNG software is updated.

To shut down the system in preparation for powering off the PDG hardware, see Shutting Down the Conventional PDG on page 180.

CAUTION:
Executing this procedure results in a loss of data messaging.

Never shut down the PDR and RNG applications by just flipping off the power switch or by disconnecting the power cord. If the power to the PDG hardware is to be turned off, the Operating System (OS) must be shut down as described in Shutting Down the Conventional PDG on page 180.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.
5. In the **PDR Specific Management and Operations** menu, select **Stop PDR**. Press ENTER.

   The PDR is stopped.

9.17
Starting the Conventional RNG

The Radio Network Gateway (RNG) is automatically started when the power to the system hardware is turned on, as part of the system initialization routine. If there is a problem during the system startup and the RNG is not started, perform the following procedure to manually start the RNG once the problem is resolved.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. Type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **Start RNG**. Press ENTER.

   The RNG is started.

9.18
Stopping the Conventional RNG

The procedure for stopping the Radio Network Gateway (RNG) ensures that the runtime information is saved to the RNG database before terminating the system activity. Execute this procedure only if you intend to upgrade/reinstall the RNG or PDR software, or perform other maintenance activities that do not include powering off the PDG.

⚠ **CAUTION:**
Executing this procedure results in a loss of data messaging.

Never shut down the RNG application by just pressing the power button or disconnecting the power cord. If you want to turn off the power to the PDG hardware, shut down the Operating System (OS), as described in Shutting Down the Conventional PDG Hardware on page 183.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 Type the number associated with **Application Administration**. Press ENTER.

3 In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **Stop RNG**. Press ENTER.

   The RNG is stopped.

9.19
Shutting Down the Conventional PDG Hardware

Prerequisites:
Before turning off the power to the Packet Data Gateways (PDG) hardware, shut down the Linux Operating System (OS) in an orderly manner. This procedure describes how to shut down the Linux OS in an orderly manner to avoid any potential data loss.

⚠ **CAUTION:**
Executing this procedure results in a loss of data messaging.

Never shut down the Packet Data Router (PDR) and Radio Network Gateway (RNG) applications by just pressing the power button or disconnecting the power cord. If you want to turn off the power to the PDG hardware, shut down the OS as described in Shutting Down the Conventional PDG on page 180.

NOTICE: You do not have to stop the RNG and PDR applications manually as it is a part of this procedure.

Procedure:

1. Log on to the PDG as `root`.

   The `[root@pdr /root]#` appears.

2. At the prompt, type `halt`. Press ENTER.

   A message confirms that the system is halted.

9.20
Changing Passwords on the Conventional PDG

When changing passwords, follow the rules that are listed in Domain User Names and Domain User/Root Account Passwords Data Value Requirements and Criteria for the Conventional PDG on page 75.

Procedure:

1. Log on to the PDG as the user that you want to change the password for.
2. At the prompt, type `passwd`. Press ENTER.
3. Type the new password. ENTER.
4. Retype the new password. ENTER

9.21
Backing Up a Conventional IVD PDG in a K Core

Perform this process to back up a Conventional IV&D Packet Data Gateway (PDG) in a K core for disaster recovery purposes.

Process:

1. Create a PDR database backup file in the PDG Backup Archive Directory.

   See Creating a Conventional IVD PDG Backup File (K Core) on page 184.

2. Transfer a PDR database backup file to another computer.

   See Transferring a Conventional IVD PDG Backup File to Another PC (K Core) on page 185.

9.21.1
Creating a Conventional IVD PDG Backup File (K Core)

The following backup procedure creates a copy of the current Conventional IV&D Packet Data Gateway (PDG) database and archives the copy in the PDG Backup Archive Directory.

Backing up the PDG database minimizes the risk of losing valuable data caused by the disk failure or an operator error. Backing up also reduces the amount of time it takes to recover the system after one of these failures.

Perform the backup procedure when someone changes the PDG configuration, especially if losing these changes would adversely affect the operation of the packet data services.

A backup taken manually on a Conventional IV&D PDG in a K core can be restored on the PDG.

NOTICE: You can perform the backup procedure while the PDR application is running and actively providing packet data services. You can also perform the backup procedure while the PDR application is stopped.

Procedure:

1. Log on to the PDG using the credentials for a user account that belongs to the Install Administrator or Platform Administrator group.
2. At the prompt, type `admin_menu`. Press ENTER.
3. From the main PDG administration menu, select **Application Administration**. Press ENTER.
4. From the **Application Administration** menu, select **Application Specific Management and Operations**. Press ENTER.
5. From the **Application Specific Management and Operations** menu, select **PDR Specific Management and Operations**. Press ENTER.
6. From the **PDR Specific Management and Operations** menu, select **Backup PDR**. Press ENTER.

   The PDR database backup is initiated. The files in the PDR database directory are copied to a file in the `/opt/Motorola/backup` directory in a compressed format. Do **not** interrupt this operation.

7. At the prompt, type the following command `ls /opt/Motorola/backup`. Press ENTER.

   The following file appears: **pdrdb_*<date>*_*<time>*.zip**. Verify whether the file is created in the directory.

8. At the prompt, type `q` and press ENTER to exit the administration menu.
9. At the command prompt, type `exit` and press ENTER to log out of the PDG.

Postrequisites: Transfer the backup file to another computer as a means of safe archival in case of the PDG disk failure or accidental deletion due to an operator error. See Transferring a Conventional IVD PDG Backup File to Another PC (K Core) on page 185.

9.21.2

Transferring a Conventional IVD PDG Backup File to Another PC (K Core)

Perform the following procedure to transfer a Conventional IV&D Packet Data Gateway (PDG) backup file stored on a PDG to another computer. This procedure applies to K cores only.

Procedure:

1. Perform the following steps to open the Command Prompt window from any Windows-based computer, for example, NM client, CSMS:
   a. Log on to the Windows-based machine with Admin permissions.
   b. From the **Start** menu, select **Run**.
   c. In the **Run** dialog box, in the **Open** field, type `cmd` and click **OK**.
2. Change to the directory to which you want to transfer the PDR database backup file. At the prompt, type `cd` ***<pathname>*** and press ENTER.
3. Perform one of the following sets of actions, depending on your system security configuration:

If…	Then…
If the system is secure (IA),	perform the following actions: **a** At the prompt, type the following command and press Enter: `psftp <user_name>@<hostname>.zone<X>` where: ***<hostname>*** is convpdr01 for a Conventional PDR. ***<X>*** is the zone number. ***<user_name>*** is the name of a user on the PDG. **b** At the prompt, type the user's password and press Enter.
If the system is non-secure,	perform the following actions: **a** At the prompt, type the following command and press Enter: `ftp <hostname>.zone<X>` where: ***<hostname>*** is convpdr01 for a Conventional PDR. ***<X>*** is the zone number. **b** At the login prompt, type the user name and press Enter. **c** At the prompt, type the user's password and press Enter.

4. Switch to the selected directory. Type `cd /opt/Motorola/backup` and press Enter.
5. Display a list of files in the selected directory. Type `ls` and press Enter.

   The latest backup file appears in the following format: `pdrdb_`***`<date>`***`_`***`<time>`***`.zip`
6. Transfer the file to the location indicated in step 4. Type `get pdrdb_`***`<date>`***`_`***`<time>`***`.zip` and press Enter.
7. Type `bye` and press Enter.
8. Verify that the file appears in the location specified in step 4:

   a Type `dir` and press Enter.

   b Verify that the file has the correct name and size.

Postrequisites: Once you have copied the backup file to another computer, Motorola recommends deleting the backup file from the `/tmp` directory of the PDR. Otherwise, the accumulation of backups could result in the PDR running out of disk space.

9.22
Transferring a Backup File to a Conventional IVD PDG (K Core)

When and where to use:
Use this procedure to transfer a backup file saved on another computer to a Conventional IV&D Packet Data Gateway (PDG). This procedure applies to K cores only.

Procedure:

1. Open the Command Prompt window from a Windows-based computer, for example, NM client, CSMS:

   a Log on to the Windows-based machine with Admin permissions.

   b. From the **Start** menu, open the **Run** dialog box.
   c. In the **Run** dialog box, in the **Open** field, type `cmd` and click **OK**.

2. Change to the directory where the PDR database backup file is located by entering: `cd` ***`<pathname>`***
3. If the `psftp.exe` file does not exist in the location specified in step 2, copy the file to this location.
4. Perform one of the following sets of actions, depending on your system security configuration:

If…	Then…
If the system is secure (IA),	perform the following actions: **a** At the prompt, enter: `psftp` ***`<user_name>`***`@`***`<hostname>`***`.zone`***`<X>`*** where: ***`<hostname>`*** is convpdr01 for a Conventional PDR. ***`<X>`*** is the zone number. ***`<user_name>`*** is the name of a user on the PDG. **b** At the prompt, enter the user's password.
If the system is non-secure,	perform the following actions: **a** At the prompt, enter: `ftp` ***`<hostname>`***`.zone`***`<X>`*** where: ***`<hostname>`*** is convpdr01 for a Conventional PDR. ***`<X>`*** is the zone number. **b** At the login prompt, enter the user name. **c** At the prompt, enter the user's password.

5. Switch to the selected directory by entering: `cd /opt/Motorola/backup`
6. Transfer the file by entering: `put pdrdb_`***`<date>`***`_`***`<time>`***`.zip`
7. Verify that the file appears in the `/opt/Motorola/backup` directory by entering: `ls`

   The `pdrdb_`***`<date>`***`_`***`<time>`***`.zip` file appears in the list.

8. Enter: `bye`

   The file transfer session with the PDR is terminated.

9.23 Managing AAA Client Configuration

This section is **not** applicable to the Conventional IV&D K core Packet Data Gateway (PDG).

See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide* to join the PDG to the Active Directory domain and verify the domain membership status.

9.24 Managing Syslog Client Configuration

The Centralized Event Logging feature is **not** supported on the Conventional IV&D K core Packet Data Gateway (PDG).

See “Enabling/Disabling Centralized Event Logging on Linux Devices” in the *Centralized Event Logging Feature Guide*.

9.25 Displaying the NTP Client Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Services Administration**. Press ENTER.
3. In the **Services Administration** menu, type the number associated with **Manage NTP Client Configuration**. Press ENTER.
4. In the **Manage NTP Client Configuration** menu, type the number associated with **Display NTP Client Configuration**. Press ENTER.

   If the NTP client is not configured, a message informs you that there are no NTP time sources. If the NTP client is configured, you can see the Hosted NTP aliases and IP addresses of the remote NTP time sources.

9.26 Configuring the NTP Client

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Services Administration**. Press ENTER.
3. In the **Services Administration** menu, type the number associated with **Manage NTP Client Configuration**. Press ENTER.
4. In the **Manage NTP Client Configuration** menu, type the number associated with **Configure NTP Client**. Press ENTER.
5. In the **Enter NTP Client Configuration** menu, perform one of the following actions:

If…	Then…
If you want to add the NTP Server IP to the PDG NTP client configuration,	perform the following actions: a Select **Add NTP Server IP Address**. **Result:** You are prompted to enter the IP address of an external NTP time source. b Type the valid IP of the NTP server according to the system IP plan.

If…	Then…
	Result: The synchronization with the new NTP source is started. If the process is successful, the IP is added as an external NTP time source.
If you want to remove the NTP Server IP from the PDG NTP client configuration,	Select **Remove NTP Server IP Address**. **Result:** The synchronization with the NTP server which is left in the list of the NTP sources is started, and the message about removing the selected NTP time source appears.

9.27

RNG Specific Management and Operations

The RNG Specific Management and Operations menu provides the following functions:

- Displaying the RNG status and configuration
- Displaying the RNG link status
- Displaying the configured channel status
- Displaying the configured CDEM status
- Displaying the configured KMF status
- Displaying the RNG statistics
- Resetting the RNG statistics

9.27.1

Displaying the RNG Status and Configuration

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Status and Configuration**. Press Enter.
6. In the **RNG Status and Configuration**, type the number associated with **Display RNG Status/Configuration**. Press Enter.

   The information about the RNG software version, uptime, and mode is displayed.

9.27.2

Displaying the RNG Link Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2. In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Status and Configuration**. Press Enter.
6. In the **RNG Status and Configuration** menu, type the number associated with **Display RNG Link Status**. Press Enter.

   The status of the following RNG links is displayed:

   - RNG-PDR
   - RNG-CDEM
   - RNG-KMF
   - RNG-Sites

   Example:

   ```
   RNG LINK STATUS
   Serving PDR - 1 : Control UP, Data UP
   CDEM - : UP
   KMF - : UP
   Broadcast - Preferred : ACTIVE
   Broadcast - Backup : STANDBY
   Gateway Router - Preferred : UP
   Gateway Router - Backup : UP
   CCGW - 2001 : UP
   ```

9.27.3
Displaying the Configured Channel Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Status and Configuration**. Press Enter.
6. In the **RNG Status and Configuration** menu, type the number associated with **Display Configured Channel Status**. Press Enter.

   The information about the configured channel is displayed, including the site ID, Packet Data Channel ID, channel status, and OB queue size.

9.27.4 Displaying the Configured CDEM Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Status and Configuration**. Press ENTER.
6. In the **RNG Status and Configuration** menu, type the number associated with **Display Configured CDEM Status**. Press ENTER.

   The information about the CDEM configured for the RNG is displayed.

9.27.5 Displaying the Configured KMF Status

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.
5. In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Status and Configuration**. Press ENTER.
6. In the **RNG Status and Configuration** menu, type the number associated with **Display Configured KMF Status**. Press ENTER.

   The OTAR KMF table appears.

9.27.6 Displaying the RNG Statistics

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press ENTER.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Statistics**. Press Enter.

The **RNG Statistics** menu allows you to display the following statistics:

RNG System Statistics
Displays the system-wide statistics of the RNG.

Per Site Statistics
Displays the statistics collected by the RNG for a specified site link.

Per Mobile Subscriber Unit (MSU) Statistics
Displays the statistics collected by the RNG for a specified subscriber.

Per CDEM Statistics
Displays the statistics for the CDEM.

RNG-Gateway Router Statistics
Displays the statistics collected by the RNG for the gateway routers.

9.27.7
Resetting the RNG Statistics

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.

5 In the **RNG Specific Management and Operations** menu, type the number associated with **RNG Statistics**. Press Enter.

6 In the **RNG Statistics** menu, type the number associated with **Reset RNG Statistics**. Press Enter.

A message confirms that the statistics are reset.

9.27.8
Requesting the CDEM to Send the Registration KMM to the KMF

Prerequisites: Configure the CDEM.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2 In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.

3 In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations** menu, type the number associated with **RNG Specific Management and Operations**. Press Enter.

5. In the **RNG Specific Management and Operations** menu, type the number associated with **Request CDEM to Send Registration KMM to KMF**. Press ENTER.

   A message confirms that a KMM registration request message is requested and sent to the KMF.

9.28 PDR Specific Management and Operations

The PDR Specific Management and Operations menu provides the following functions:

- Showing the CDEM IP address
- Updating the CDEM IP address
- Setting the default CDEM IP address

9.28.1 Showing the CDEM IP Address in the PDR

After the deployment of the Conventional IV&D PDG, the CDEM IP is configured with a default value. The PDG network interface NIC3, which provides communication with CDEM, is also configured with a default value.

NOTICE: It is **not** recommended to change the CDEM IP from the default value.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.
5. In the **PDR Specific Management and Operations**, type the number associated with **Show CDEM IP**. Press ENTER.

   The CDEM IP address appears.

9.28.2 Updating the CDEM IP Address in the PDR

NOTICE: It is **not** recommended to change the CDEM IP from the default value.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.

5. In the **PDR Specific Management and Operations**, type the number associated with **Update CDEM IP**. Press ENTER.
6. At the prompt, type the CDEM IP address. Press ENTER.
7. At the prompt, restart the PDR application for the changes to take effect:
   a. Stop the PDR.
   b. Start the PDR.

9.28.3
Setting the Default CDEM IP Address in the PDR

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration**, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations**. Press ENTER.
5. In the **PDR Specific Management and Operations** menu, type the number associated with **Set Default CDEM IP**. Press ENTER.
6. At the prompt, restart the PDR application for the changes to take effect:
   a. Stop the PDR.

      See Stopping the Conventional PDR on page 182.
   b. Start the PDR.

      See Starting the Conventional PDR on page 181.

Chapter 10

Packet Data Gateway Maintenance

There are no serviceable parts in the Packet Data Gateway (PDG) that require maintenance or calibration. Exterior cleaning to maintain clean ventilation ports is highly recommended. It is also advisable to do periodic interior cleaning by using a low-suction vacuum cleaner.

This page intentionally left blank.

Chapter 11

Trunked IVD and HPD PDG Troubleshooting

This chapter provides fault management and troubleshooting information related to the Trunked Integrated Voice and Data (IV&D) and High Performance Data (HPD) Packet Data Gateway (PDG).

11.1 Troubleshooting Tools

Review the following sections for information on the various tools available for troubleshooting the Packet Data Gateway (PDG).

11.1.1 Troubleshooting the Trunked PDG with the Unified Event Manager (UEM)

The Packet Data Gateway (PDG) sends event notifications to the Unified Event Manager (UEM) network fault management application. For a list of PDG alarms, traps, and other information on using the UEM for troubleshooting this device, see the *Unified Event Manager Online Help*.

11.1.2 Checking the CPU Utilization on the Trunked PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.
3. In the **OS Administration** menu, type the number associated with **Display Platform Recourses Usage Information**. Press ENTER.

   The CPU and memory usage information is displayed.

11.1.3 Trunked PDG Subsystem Troubleshooting Commands

The following table lists general commands that you can run while logged on to the PDG to check different aspects of the system status or view system logs.

Table 60: Trunked PDG Subsystem Troubleshooting Commands

Command	Description
`/usr/bin/free`	Displays memory usage.
`/bin/df`	Displays disk usage.
`/sbin/ifconfig -a`	Displays the network interface configuration.

Table continued…

Command	Description
`/etc/rc.d/init.d/motorola_pdr status`	Checks the PDR running status.
`/bin/netstat -r`	Displays network routing information.
`/bin/netstat -a`	Displays all the connections and states of the connections on the PDG.
`/opt/Motorola/pdr/bin/versionstamp`	Checks the PDR software version.
`cat /etc/motorola-gems-redhat-linux-os-release`	Checks the Kickstart OS version.
`cat /etc/redhat-release`	Checks the PDR OS version.
`/opt/Motorola/pdr/bin/create_device_rpt`	Creates the PDR mobile device summary report. The default output file is `device_report.txt` and `device_report.csv`.
`/bin/ifconfig`	Displays the network interface configuration.
`/bin/netstat`	Displays the network connections.
`/bin/ps eLf or grep w rng`	Displays all the RNG processes and threads along with their priorities.
`/bin/uptime`	Displays the current time and how long the device is running.
`memory`	Gathers information about different memory buffers used in the RNG.

11.1.4 Accessing the PDR Diagnostic Tests Interface

The following procedure describes how to run diagnostic tests for the query path between the zone controller and the Packet Data Router (PDR). Using the Local Configuration Interface, initiate a query request to the zone controller and wait for a response. The response received appears on the interface.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDG Local Configuration**. Press Enter.
5. In the **PDG Local Configuration** interface, select **Diagnostic Tests**. Press Enter.
6. To start the diagnostic test, select **PDR to ZC Diagnostics**. Press Enter.

11.1.4.1 Diagnostic Tests Fields

Table 61: Diagnostic Tests Fields

Field	Description
Status	The status of the diagnostic tests. The available values are: • In Progress • Finished
Result	The result of the diagnostic tests. The available values are: • Success • Interface Not Configured • Queue Full • No Reply

11.1.5 Trunked PDG System Logs

For information on the log management, see the *Centralized Event Logging Feature Guide*.

11.2 Troubleshooting Problems on the Trunked PDG

If you experience any problems with the Trunked IV&D or HPD Packet Data Gateway (PDG), check the possible causes and perform the recommended actions in the order that they are listed.

If you need assistance, contact the Motorola Solution Support Center. See Motorola Solution Support Center Contact Information on page 245.

11.2.1 Trunked PDG Database Corrupts as a Result of Power Cut

When there is a sudden power outage or the Packet Data Gateway (PDG) is switched off abruptly due to loss of power supply, the PDG database can lose its configuration or get corrupted. In such a situation, the PDG sends a special trap message to the Radio Network Management Subsystem, informing the system about the corruption of the PDG configuration. After receiving a PDG configuration corruption alert in the Unified Event Manager (UEM) application, create a default PDG database to resolve this problem. See Creating a Default Trunked PDG Database on page 216.

⚠ **CAUTION:** Having to re-establish the PDG with the default database upon a power failure is rare and only necessary when you receive a PDG configuration corruption alert in the UEM. To restore the PDG, it should be provisioned with full configuration from the Network Manager.

11.2.2 Power LED Fails to Illuminate

If the power LED fails to illuminate, the typical causes include a defective power supply or a problem with the power connection. Check the AC cable connection, verify that the power switch is in the ON position, and check for a possible power supply failure. If required, replace any defective power supplies. For replacement instructions, see Removing and Installing the Power Supply on page 243.

11.2.3 Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network

If the PDR/RNG cannot ping other devices on the network, the following items are the most likely causes:

- The gateway router is down.
- The PDG NIC is running at the wrong speed.
- The PDG port on the LAN switch is disabled.
- The PDG NIC is disabled.
- The PDG NIC is faulty.
- The PDR and RNG port on the LAN switch is configured to the wrong speed or Duplex Mode (100 FD is the appropriate speed).

Procedure:

1. Check the cable connection between the PDG and the LAN switch:
   - **a** Verify that the network cable is correctly plugged into the PDR/RNG and to the appropriate port on the LAN switch.
   - **b** Verify that there are no obvious breaks or sharp bends in the network cable.
   - **c** Verify that the link LED on the LAN switch is on.
   - **d** Replace the cable if necessary.
2. Log on to the PDG as `root`. If you are unable to log on to the PDG, see Troubleshooting when the Trunked PDG Does Not Boot on page 203.
3. Enter `ifconfig` and look for the following lines of output.

   The values displayed can be different on your system.

   ```
   eth0 Link encap:Ethernet HWaddr 00:1A:4B:A9:0F:54
   inet addr: Bcast: Mask:
   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
   RX packets:480557 errors:1 dropped:0 overruns:0 frame:1
   TX packets:537195 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1000
   RX bytes:35882061 (34.2 MiB) TX bytes:40499477 (38.6 MiB)
   Interrupt:185 Memory:f8000000-f8011100
   eth1 Link encap:Ethernet HWaddr 00:1A:4B:A9:0F:50
   inet addr: Bcast: Mask:
   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
   RX packets:32261048 errors:3961 dropped:0 overruns:0 frame:3961
   TX packets:32195685 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1000
   RX bytes:2130755316 (1.9 GiB) TX bytes:2123104124 (1.9 GiB)
   Interrupt:193 Memory:fa000000-fa011100
   ```

   If the eth0 listing for the PDR is not shown, the network interface is not connected.
4. To connect the network interface, perform the following actions:
   - **a** As the root user, enter: `service networks restart`

     The PDR uses the eth0 interface.
   - **b** Wait for a few seconds before attempting any network traffic.

5 If the symptoms persist, enter: `ifconfig` and verify that the IP address and netmask displayed in the eth0 listing are correct.

6 If the IP address and netmask are incorrect, reconfigure the network interface:

   a Enter: `admin_menu`

   b Enter the number associated with **OS Administration**.

   c Enter the number associated with **Manage Platform Configuration**.

   d Enter the number associated with **Configure Network Parameters**.

   The following output appears:

```
Host Information ...
Hostname [def: wdselab-a-80-2-12]:
Domain name [def: comm.mot.com ] [- to delete]:
DNS Configuration ...
First DNS nameserver [def: [- to delete]:
Second DNS nameserver [def: ] [- to delete]:
Third DNS nameserver [def: ] [- to delete]:
Fourth DNS nameserver [def: ] [- to delete]:
Default Gateway ...
Default Gateway [def: ] [- to delete]:
Network device eth0 ...
ipaddr [def: ] [- to delete]:
netmask [def: ]:
Network device eth1 ...
ipaddr [def: ] [- to delete]:
netmask [def: ]:
Type y to restart networking with new values:
```

   e Verify that the IP address and netmask are correct. If they are incorrect, enter the correct values.

   f Verify that the default gateway IP address is correct for the zone that the PDR is located in. If it is incorrect, enter the correct default gateway IP address.

   g If all the fields are correct, do not do anything. Press Enter every time.

   h Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

   The following message appears:

```
.../etc/resolv.conf SUCCESSFULLY updated ...
...Syslog SUCCESSFULLY updated....
```

   i Wait for the prompt to return and try to ping another device in the system.

   IMPORTANT:
   The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.

   If any network parameters were modified, reboot the PDR. See Rebooting the Trunked PDG on page 167.

   Set up SNMPv3 AuthPriv and credentials according to the “Configuring USM User Security for the PDG” procedure in the *SNMPv3 Feature Guide*.

7 If the symptoms persist, enter: `netstat -r` and look for the following lines of output.

   The values displayed can be different on your system.

```
Kernel IP routing table
Destination GatewayGenmaskFlagsMetricRef UseIface
.Z.  .*255.255.255.255UH000eth0
.Z. .*255.255.0.0U000eth0
...*255.0.0.0U000lo
default.Z..0.0.0.0UG000eth0
```

where Z represents the zone ID of the PDR.

8 If the default line is not shown or does not list the zone gateway IP address, reconfigure the routing:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

c Enter the number associated with **Manage Platform Configuration**.

d Enter the number associated with **Configure Network Parameters**.

e Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is incorrect, enter the correct default gateway IP address.

f Press ENTER to activate the changes.

g Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

IMPORTANT:
If the default gateway was changed, reboot the PDG.

The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.

If the eth1 listing is not shown for the RNG, the network interface is not connected.

9 To connect the network interface, perform the following actions:

a Enter: `ifdown eth0; ifup eth0`

RNG uses the eth1 interface.

b Wait for a few seconds before attempting any network traffic.

10 If the symptoms persist, enter: `ifconfig` and verify that the IP address and netmask displayed in the eth1 listing are correct.

11 If the IP address and netmask are incorrect, reconfigure the network interface:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

c Enter the number associated with **Manage Platform Configuration**.

d Enter the number associated with **Configure Network Parameters**.

e Verify that the IP address and netmask are correct. If they are incorrect, enter the correct values.

f Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is incorrect, enter the correct the default gateway IP address.

g If all the fields are correct, do not do anything. Press ENTER every time.

h Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

i Wait for the prompt to return and try to ping another device in the system.

IMPORTANT:
If any network parameters were modified, reboot the PDG.

The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.

12 If the symptoms persist, enter: `netstat -r` and look for the following lines of output.

The values displayed can be different on your system.

```
Kernel IP routing table
Destination GatewayGenmaskFlagsMetricRef UseIface
.Z.  .*255.255.255.255UH000eth0
.Z. .*255.255.0.0U000eth0
...*255.0.0.0U000lo
default.Z..0.0.0.0UG000eth0
```

where Z represents the zone ID of the RNG.

13 If the default line is not shown or does not list the zone gateway IP address, reconfigure the routing:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

c Enter the number associated with **Manage Platform Configuration**.

d Enter the number associated with **Configure Network Parameters**.

e Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is incorrect, enter the correct the default gateway IP address.

f Press Enter to activate the changes.

g Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

11.2.4
Troubleshooting when the Trunked PDG Does Not Boot

If the Packet Data Gateway (PDG) hardware does not boot, perform the following procedure.

NOTICE: The GRUB Bootloader can get stuck at the OS selection screen due to an unexpected input. Press Enter to continue the boot process.

Procedure:

1 At the PDG console prompt, press Enter a few times.

2 Depending on the result, perform one of the following actions:

If…	Then…
If a prompt does not appear,	perform the following actions: a Verify the console port connection. b Verify that the chassis is powered.
If a normal login prompt appears but the root login is not accepted,	perform the following actions: a Verify that you are using the correct root login password. b Verify that the Caps Lock key is not selected.

3 If you are unable to correct the problem, contact the Motorola Solution Support Center.

See Motorola Solution Support Center Contact Information on page 245.

11.2.5 Troubleshooting when UEM Is Not Receiving PDR Alarms

If the Unified Event Manager (UEM) application is not receiving Packet Data Router (PDR) alarms, the following items are the most likely causes:

- No alarm conditions are occurring.
- The manager is not registered.
- The manager registration table is full.
- The PDR is not running.
- The network connectivity between the PDR and the UEM has failed.

Process:

1. Ensure that the device is otherwise operational, has connectivity to the network, and the network is operational.
2. In UEM, verify that the device is discovered by using the subnet discovery.

   For more information, see the *Unified Event Manager User Guide*.
3. If the secure SNMPv3 operation is enabled, ensure that the credentials are set up correctly on the device.

   For more information, see the *SNMPv3 Feature Guide*.
4. If the manager registration table is full and there are unwanted managers in the registration table, delete the PDG managed object from the unwanted manager.

   For more information on removing unwanted UEM entries, see the *Unified Event Manager Online Help*.

11.2.6 Troubleshooting when the Trunked PDR Does Not Appear on the UEM Topology Map

If the Packet Data Router (PDR) does not appear on the Unified Event Manager (UEM) topology map, the following items are the most likely causes:

- The network outage prevents the device from sending alarms to the UEM.
- The device may not be discovered in the UEM.

Process:

1. Ensure that the device is otherwise operational, has connectivity to the network, and the network is operational.
2. In the UEM, verify that the device is discovered, using the subnet discovery.

   For more information, see the *Unified Event Manager User Guide*.
3. If the secure SNMPv3 operation is enabled, make sure that the credentials are set up correctly on the device.

   For more information, see the *SNMPv3 Feature Guide*.

11.2.7 PDR Configuration Data Out-of-Sync

Use the VoyenceControl application to determine if the Provisioning Manager data for the Packet Data Router (PDR) is synchronized. If the configuration data is out-of-sync, use VoyenceControl to re-synchronize the data. For more information, see “PM Data Sync State” in the *Unified Network Configurator User Guide*.

NOTICE: The names EMC Smarts Network Configuration Manager and VoyenceControl are used interchangeably for this product.

11.2.8
Troubleshooting when the PDR-ZC Link in Down State

If the Packet Data Router (PDR) to zone controller (ZC) link is in the down state, the following items are the most likely causes:

- The zone controller is overloaded.
- The network is down.
- No Home Location Register (HLR) mobility transactions have occurred since the last failure. The link does not transition up until there is a successful transaction. Under normal conditions, there may be no HLR mobility transactions.

Procedure:

1. Initiate the PDR to ZC diagnostics from the PDG Local Configuration interface by selecting **Diagnostic Tests → PDR to ZC diagnostics**.
2. If the PDR to ZC diagnostics was not successful, check the connectivity between the PDR and the zone controller by running the ping command.

11.2.9
Trunked PDG Clock Problems

The Packet Data Router (PDR) synchronizes its clock with the Network Time Protocol (NTP) server at the master site. The PDR periodically polls the NTP server. The PDR then receives an NTP packet and updates its internal clock. If the PDR clock seems to be drifting from the NTP server clock, it can be related to one of the following causes:

- A power outage has occurred.
- The PDR is reset without a proper shutdown.
- A network disconnection between the PDR and the NTP server has occurred for a significant amount of time.

For more information, see the *Network Time Protocol Server Feature Guide*.

11.2.10
Troubleshooting DVD-ROM Drive Problems

For server hardware troubleshooting information, see the *Virtual Management Server Hardware User Guide*.

11.2.11
Troubleshooting when the PDR Application Does Not Start (start_pdr Command Failed)

If the Packet Data Router (PDR) application does not start (the start_pdr command fails), the following items are the most likely causes:

- The PDR database is not initialized.
- The PDR database is corrupted due to a power outage or other hardware problem.

- The PDR disk space is full.

Procedure:

1. Log on to the PDG as `root`.
2. Verify the PDR status through the **admin_menu**.

   See Verifying the Trunked PDR and RNG Status on page 165.
3. Perform one of the following actions:

If…	Then…
If the PDR is running,	go to step 6.
If the PDR is not running,	go to step 4.
4. Verify if the database is initialized:
   - **a** Enter: `cd /opt/Motorola/pdr/bin`
   - **b** Enter: `ls oms_db`
   - **c** Enter: `ls dbfiles`

   If in response to either command, a message appears informing that there is no such file or directory, this means that the database was not initialized during the PDR installation. Initialize the PDR database through the **admin_menu**.
5. Start the PDR application through the **admin_menu** again. If the database has already been initialized, but the start of the PDR still fails, go to step 6.
6. Verify that enough disk space is available:
   - **a** From the **admin_menu**, select **Display Platform Resource Usage Information** to check if the disk space is a problem.
   - **b** If the disk space for `/opt` is greater than 90%, enter `ls /opt/Motorola/pdr/bin/cor*` to check for the existence of the core files. If any entries exist, contact the Motorola Solution Support Center.

     See Motorola Solution Support Center Contact Information on page 245.
   - **c** If no core files exist, copy some database backups (SFTP) from the PDR and delete those database backups until the used disk space for this partition is between 85% and 90%.
   - **d** After cleaning up the disk, start the PDR through the **admin_menu**. If the start PDR still fails, go to step 7.
7. A corrupted database may cause various symptoms. Run the following commands to back up the current database and create another database:
   - **a** Log on as a member of the **instadm** or **bkupadm** group.
   - **b** Produce the backup PDR database through the **admin_menu**.
   - **c** Log out and log on as root.
   - **d** Enter: `rm -r oms_db`
   - **e** Enter: `rm -r dbfiles`
   - **f** Initiate the PDR database through the **admin_menu** and start the PDR application.
   - **g** If the PDR does not start, the problem is not a corrupted database. Restore the PDR database through the **admin_menu**. When restoring the PDR database, select the backup file with the current date.

8. If the PDR can start, the problem was a corrupted database. If the corrupted database is not related to a power hit, send the backup file made in this procedure to the Motorola Solution Support Center for analysis.
9. Reboot the PDG server through the **admin_menu**.
10. If the PDR does not start, contact Motorola for assistance.

11.2.12 RNG Site Link in Unknown State

If the Radio Network Gateway (RNG) site link state shows up as unknown in the Packet Data Router (PDR) Local Configuration user interface, it is because the PDR Local RNG link is down. The RNG reports the RNG site link state to the PDR to display in to the Local Configuration and also report it to the Unified Event Manager (UEM) application. If the PDR link to the Local RNG is down, the PDR does not know the actual state of the site links. Check if the RNG is running. If the RNG is not running, start the RNG by using the `start_rng` command.

11.2.13 Other Trunked PDG Failure Conditions

The following table lists other Packet Data Gateway (PDG) failure conditions, and provides their causes and remedies.

Table 62: Other Trunked PDG Failure Scenarios

Failure Condition	Cause	Remedy
Data is not delivered to the subscriber unit or to the CEN.	Potential failure on the communication path	Check the local link between the RNG and the PDR in the Local Configuration view.
	Serving PDR failure	Check the UEM for the state of the PDR. Check the PDR state in the Local Configuration view.
The PDG fails to register a subscriber unit.	The resolution of the GGSN IP failed.	Check the provisioned GGSN information and the DNS server configuration. From the Local Configuration Interface, check if the PDR is in the active operable redundancy state. See Trunked PDG Local Configuration Interface on page 95
The PDR notifies the UEM about a Critical Malfunction state. The PDR state is shown as inoperable in the Local Configuration interface.	Communication Failure: PDR health check failed.	Check connection between the PDR and the RNG, the PDR and the GGSN, and the PDR and gateway routers. Check if the resolution of IP addresses through the DNS lookup failed.

Table continued…

Failure Condition	Cause	Remedy
The PDR notifies the UEM about a Critical Malfunction state. The PDR state is shown as inoperable in the Local Configuration interface.	No Configuration: PDG Configuration failure - the PDR failed to start up with the previously running configuration.	Recreate the PDR database. Reprovision the PDR with full configuration.
The PDR notifies the UEM about a Minor Malfunction.	Communication Failure: The PDR lost connection with one of the gateway routers.	Check connection between the PDR and the gateway routers.
The PDR notifies the UEM about an RNG overloaded state.	RNG message capacity exceeded: Excessive message traffic through the RNG.	Reduce data traffic.
The PDR notifies the UEM that the RNG-ZC link is down.	The RNG-ZC communication failed: A number of failed mobility queries sent by the RNG to the Zone Controller exceeded the predetermined threshold. This could be due to an excessive load on the Zone Controller, as well as network failures.	Check the connectivity between the RNG and the Zone Controller. Check whether the DNS lookup has failed for at least one VLR mobility group.
The PDR notifies the UEM that the PDR-gateway router link is down.	Communication Failure: The PDR has not received any ICMP echo responses from the gateway router.	Check the connectivity between the PDR and the gateway router. Check if the IP address of the gateway router was resolved correctly.
The PDR notifies the UEM about an overload condition.	Data traffic is too heavy.	Reduce data traffic.

11.2.14 Setting the Trunked PDG to the User Requested Standby (URS) State

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Trunked PDR on page 168 before starting this procedure.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 Select **Application Administration**. Press Enter.

3 In the **Application Administration** menu, select **Application Specific Management and Operations**. Press Enter.

4 In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press Enter.

5 In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press Enter.

6 In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

   The PDG can be in the active state if it is in a primary core or in the standby state if it is in a backup core.

7 In the **Modify Redundancy Configuration** menu, perform the following actions:

   a Select **User Requested Standby** by using the arrow keys. Press ENTER.

   b Select **Submit** by using the arrow keys. Press ENTER.

   A message appears, warning that this action can disable the PDG.

8 Select **Yes** to proceed. Press ENTER.

   A message confirms that the PDG redundancy state is user requested standby. The PDG restarts and the **Application Management and Operations** menu appears.

9 To exit the **Main Menu**, type `q`. Press ENTER.

   The command prompt appears.

11.3 Troubleshooting the SNMPv3 Configuration

For the SNMPv3 configuration related to the PDG, see SNMPv3 Credentials Maintenance on page 125.

For information on troubleshooting problems with the SNMPv3 operation, see the *SNMPv3 Feature Guide*.

11.3.1 Troubleshooting SNMPv3 Configuration Loss after a PDG Power Failure or Hard Reset

The SNMPv3 Common Agent can lose the content of the configuration file as a result of a Packet Data Gateways (PDG) virtual machine power failure or hard reset.

When and where to use:
Use this process to troubleshoot the loss of SNMPv3 configuration related to the PDG in the following cases:

- If Unified Event Manager (UEM) displays the “CommFailure” alarm for a PDG that experienced a power failure or a recent hard reset.
- If an application cannot communicate over SNMPv3 to or from a PDG that experienced a power failure or a recent hard reset.
- If you cannot select the **Configure SNMPv3 Agent/Manager** option from the **Manage SNMP Passphrases** menu in the main PDG administration menu despite using the correct MotoAdmin credentials.

Process:

1 Reset the MotoAdmin credentials to be able to change other users’ credentials. See “Recovering MotoAdmin Passphrases” in the *SNMPv3 Feature Guide*.

2 Configure the rest of SNMPv3 users on the affected PDG. See “Configuring USM User Security for the PDG” in the *SNMPv3 Feature Guide*. Make sure to fix all SNMPv3 paths to/from the PDG based on the “SNMPv3 Communication Matrix” in the *SNMPv3 Feature Guide*.

NOTICE: This has to be done on the PDG and all servers which communicate with it over SNMPv3.

3 Verify that the updated communication paths are operational.

11.4 Troubleshooting the Packet Data Service

Issues with the packet data service on the Packet Data Gateway (PDG) include:

- Mobile data users cannot register
- Packet data service is not available to subscribers in the zone
- Subscriber is not receiving all messages from the PDR
- Subscriber does not receive ICMP messages from the host
- Mobile data users are being deregistered by the PDR

11.4.1 Mobile Data Users Cannot Register

If mobile data users cannot register, the following items are the most likely causes:

- Subscriber is not provisioned in the PDG by the Network Manager for packet data service.
- The link to the GGSN is down.
- The link to the site is down.
- The subscriber is not mapped to the appropriate home zone or the database is not synchronized.
- The dynamic IP address was requested, but there is a problem with the DHCP server.
- The T3 timeout parameter is too short.
- The APN configured for the mobile does not match any of the APNs configured for the GGSN.

Table 63: Mobile Data Users Cannot Register

Possible Cause	Recommended Actions
Subscriber is not provisioned for packet data service.	In the Provisioning Manager, verify that the radio user is configured for packet data service. Configure and enable packet data services for the radio user if necessary.
The link to the GGSN is down.	1 Check the link status between the PDR and GGSN through the network fault management application. 2 Ping the GGSN to confirm that it is accessible.
Link to the site is down.	1 Navigate to the PDG local configuration interface. See Accessing the Trunked PDG Local Configuration Interface on page 95. 2 In the main menu, select **Local RNG-Site Link Status**. 3 If the status of all the sites is down, check for general network problems. 4 If some of the sites are down, check for problems at those particular sites. Verify the base station configuration: IP address and site

Table continued…

Possible Cause	Recommended Actions
	ID. Ping the base station from the RNG, and ping the RNG from the base station. **5** Restart the RNG. **6** If the problem persists, contact Motorola Solutions for assistance.
The subscriber is not mapped to the appropriate home zone or the database is not synchronized.	**1** In the Provisioning Manager, check the home zone mapping and verify that the subscriber is mapped to the appropriate zone. **2** Navigate to the PDG local configuration interface. See Accessing the Trunked PDG Local Configuration Interface on page 95. **3** In the main menu, select **View Mobile Device Information**. **4** Enter the radio ID for the subscriber. If the View Device Detail Screen does not appear, then check the data sync state. See Trunked PDG Database Synchronization on page 69. **5** If the database cannot be synchronized, check the status of the Network Management servers.
The dynamic IP address was requested, but there is a problem with the DHCP server.	**1** Check the network fault management application alarms for the PDR object. The PDR sends a trap indicating the reason whenever it rejects a packet data registration (as long as the same trap is not sent within the previous 10 minutes). **2** Alarm 5065, `GGSN Returned No Resources Available`, indicates a problem with the DHCP server or the link between the GGSN and DHCP server.
The T3 timeout parameter is too short.	If alarm 5075, `No Response for GGSN`, is frequently received from the PDR in the network fault management application, and the link to the GGSN is known to be up during this period, verify in the Provisioning Manager that the product of GTP T3 Timeout and GTP N3 Attempts is at least 16 seconds long.
The APN configured for the mobile does not match any of the APNs configured for the GGSN.	Alarm 5066, `Service Not Support`, indicates a problem with the APN network configuration. In the Provisioning Manager, check the APN assigned to the radio user. Verify that the APN is programmed into the GGSN.

11.4.2 Packet Data Service Not Available to Subscribers in the Zone

If packet data service is not available to subscribers in the zone, those particular subscribers can configure or synchronize the database.

Table 64: Packet Data Service Not Available to Subscribers in the Zone

Possible Cause	Recommended Actions
Verify that a specific subscriber is available in the database and the database is synchronized.	Verify the mobile database: **1** Navigate to the PDG local configuration interface, select **View Mobile Device Information**, and enter the radio ID for the subscriber.

Possible Cause	Recommended Actions
	See Accessing the Trunked PDG Local Configuration Interface on page 95. **2** If the **View Device Detail** screen does not appear, check the data sync state. See Trunked PDG Database Synchronization on page 69. **3** If the database cannot be synchronized, check the status of the Network Management servers.

11.4.3

Subscriber Is Not Receiving All Messages From the PDR

If a subscriber is not receiving all its messages, the following items are the most likely causes:

- The outbound traffic load is too high.
- The subscriber is operating in a fringe coverage area or intermittent voice services are taking precedence over data.

Table 65: Subscriber Is Not Receiving All Messages

Possible Cause	Recommended Actions
The outbound traffic load is too high.	Check for outbound queue overflows: **1** Log on to the PDG and navigate to the PDG Local Configuration interface. See Accessing the Trunked PDG Local Configuration Interface on page 95. **2** Enter: `grep 5150 /var/log/messages` Each instance includes the text `ERROR Enumeration: 5150` and lists the ID of the radio for which the message was destined. If numerous outbound queue overflows are reported, the application is sending data too quickly. The PDR only buffers a limited number of bytes of data for each mobile subscriber. **NOTICE:** For the HPD PDG, the value is 15360. For the Trunked IV&D PDG, the value is 8192. Any additional messages that arrive when the buffer is full are discarded. If the application uses TCP, the TCP receive buffer at the mobile terminals should be set at 15360 or less for the HPD PDG, and 8192 or less for the Trunked IV&D PDG.
The subscriber is operating in a fringe coverage area or intermittent voice services are taking precedence over data.	Check for NAK events in the PDG local configuration interface: **1** Log on to the PDG and navigate to the PDG Local Configuration Interface. See Accessing the Trunked PDG Local Configuration Interface on page 95.

Possible Cause	Recommended Actions
	2 Select **Statistics Management** → **View Statistics** → **Mobile Device Statistics**. **3** Enter the Radio ID for the subscriber. **4** Check the **Outbound NAK Count** field. This field shows the number of times outbound messages to the subscriber are not successfully delivered since the last time the statistics were reset. This could be due to the subscriber being in fringe coverage or due to voice transactions taking precedence over data.

11.4.4
Subscriber Does Not Receive ICMP Messages From the Host

If a subscriber does not receive ICMP messages from the infrastructure, the ICMP Enabled setting for the radio user may need to be set.

Table 66: Subscriber Does Not Receive ICMP Messages From the Host

Possible Cause	Recommended Actions
ICMP messages are disabled from the host.	In the Provisioning Manager, open the appropriate radio user record and select the **Data Services** tab. Change the **ICMP Enabled** field to **Yes**.

11.4.5
Mobile Data Users Are Being Deregistered by the PDR

If mobile data users are being deregistered by the Packet Data Router (PDR), the following items are the most likely causes:

- The link to the GGSN is down.
- Mobile user provisioning data has changed (such as the IP address).

Table 67: Mobile Data Users Are Being Deregistered by the PDR

Possible Cause	Recommended Actions
Link to GGSN is down.	**1** Check the status of the PDR-GGSN link in the network fault management application. **2** Check that the GGSN is provisioned in the PDR by checking the Local Configuration view.
Mobile user provisioning data has changed (such as the IP address).	**1** Navigate to the PDG Local Configuration Interface. See Accessing the Trunked PDG Local Configuration Interface on page 95. **2** Select **Statistics Management** → **View StatisticsMobile Device Statistics**. **3** Enter the radio ID for the affected mobile data user. **4** In the **Mobile Device Statistics** menu, check the **Reason for Last Deactivation**.

11.5 Dynamic System Resilience (DSR) Specific Troubleshooting

This section contains failure scenarios and troubleshooting procedures specific to the Dynamic System Resilience (DSR) feature. For information on typical failure scenarios and recovery sequences for the data subsystem, see the “Dynamic System Resilience Troubleshooting” chapter in the *Dynamic System Resilience Feature Guide*.

DSR-related troubleshooting described in this section is required only if your system supports DSR. For more information, contact your system administrator.

11.5.1 HA Link Is Down

If the HA link is down, perform the following troubleshooting steps:

- Ping the peer Packet Data Router (PDR). See Pinging a Peer Device on page 214.

  If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.
- Try setting the same key on both Packet Data Gateways (PDGs). See Setting Heartbeat Key on the Trunked PDG on page 70.

11.5.2 InterZone RNG Link Is Down

If the InterZone RNG link is down, perform the following troubleshooting steps:

- Ping the peer Radio Network Gateway (RNG). See Pinging a Peer Device on page 214.

  If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.
- Check if the Packet Data Gateway (PDG) is in the active state. See Trunked PDG Redundancy Configuration on page 71.

11.5.3 Pinging a Peer Device

Use the Ping command to test if a peer device such as the Packet Data Router (PDR) or Radio Network Gateway (RNG) in the backup core is reachable.

Prerequisites: Obtain the required IP address, account logins, and passwords from your system administrator.

Procedure:

1. Log on to the PDG as a member of the **instadm** or **platadm** group.
2. Type `ping` ***<IP address>***. Press Enter.

   Ping is successful if you receive the following output:

   ```
   64 bytes from  <PDR IP address>: icmp_seq=1 ttl=64 time=0.218 ms
   64 bytes from  <PDR IP address>: icmp_seq=2 ttl=64 time=0.493 ms
   64 bytes from  <PDR IP address>: icmp_seq=3 ttl=64 time=0.307 ms
   64 bytes from  <PDR IP address>: icmp_seq=4 ttl=64 time=0.525 ms
   ```

   Ping is unsuccessful if you receive the following output:

   ```
   From  <PDR IP address> icmp_seq=1 Destination Host Unreachable
   From  <PDR IP address> icmp_seq=2 Destination Host Unreachable
   ```

```
From  <PDR IP address> icmp_seq=3 Destination Host Unreachable
From  <PDR IP address> icmp_seq=5 Destination Host Unreachable
```

NOTICE: If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.

3 Press Ctrl + C to exit the ping command interface.

11.5.4

Component Failures in Dynamic System Resilience (DSR) Enabled Systems

If there is a component failure that involves the RNG, PDR or GGSN, the subscribers which are home to the zone must initiate a Context Activation request. The failure forces a switchover to the backup data subsystem, which does not have context records. Context activation is not shared between the two cores.

To alert the subscribers, the newly active PDR sends a Context Activation Status message to the local RNG. The RNG forwards the message to sites as the Site Controller (SC) to RNG links are established. The message targets subscribers, which are home to this zone and are currently registered in the zone. Those subscribers begin to perform context activation.

For the DSR-related configuration, see Dynamic System Resilience Configuration on page 69. For the DSR troubleshooting, see the “Dynamic System Resilience Troubleshooting” chapter in the *Dynamic System Resilience Feature Guide*.

11.6

Trunked PDG OS Administration

This section contains procedures performed using the **OS Administration** menu.

11.6.1

Configuring Time Parameters

CAUTION: This procedure can be used only for the initial configuration of the time parameters. The time on the running Packet Data Gateway (PDG) is synchronized with the Zone NTP Server.

Procedure:

1 Log on to the PDG and invoke the **Main Menu**.

See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.

2 In the **Main Menu**, type the number associated with **OS Administration**. Press Enter.

3 In the **OS Administration** menu, type the number associated with **Manage Platform Configuration**. Press Enter.

4 In the **Manage Platform Configuration** menu, type the number associated with **Configure Time Parameters**. Press Enter

The **Time Parameters** menu appears. In this menu, you can configure the following time parameters on the PDG:

- Time of the day
- Date
- Time Zone

11.6.2 Configuring Network Parameters

See “Viewing and Configuring Network Parameters on the Juniper Firewall Manager” in the *Unix Supplemental Configuration Setup Guide*.

11.6.3 Displaying Platform Configuration Information

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.
3. In the **OS Administration** menu, type the number associated with **Display Platform Configuration Information**. Press ENTER.

   The following information is displayed:

   - Version of operating system
   - Kernel release version
   - Host name
   - Domain name
   - MAC addresses for all network interfaces
   - Uptime information
   - IP addresses of all network interfaces

11.6.4 Displaying Platform Resource Usage Information

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.
3. In the **OS Administration** menu, type the number associated with **Display Platform Resource Usage Information**. Press ENTER.

   The following information is displayed:

   - Memory Usage
   - Disk Usage
   - CPU Usage

11.7 Creating a Default Trunked PDG Database

The Packet Data Gateway (PDG) virtual appliance is built with the initiated database. After the deployment of this appliance and the PDG initial configuration, the database is rebuilt according to the

PDG initial configuration parameters. If the database is corrupt and recovery from a backup database is unavailable or unsuccessful, perform this procedure to recreate a default database.

Prerequisites:
If the system is already installed and the Packet Data Router (PDR) software is running, stop the PDR. See Stopping the Trunked PDR on page 168.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Trunked PDG and Invoking the Main Menu on page 161.
2. In the **Main Menu**, type the number associated with **Application Administration**. Press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operation**. Press ENTER.
5. In the **PDR Specific Management and Operation** menu, type the number associated with **Initialize Database**. Press ENTER.
6. Perform one of the following actions:

If…	Then…
If the PDR database is initialized for the first time on the device and the database creation process is completed,	go to step 7.
If the PDR database has already been initialized on this device and a message appears informing that the database already exists and asking you if you want to remove the database,	perform one of the following actions: • To quit the database creation process, type `n`. The PDR database is retained. • To recreate the database, type `y`. The PDR database is recreated.

7. From the **PDR Specific Management and Operations** menu, select **Start PDR**.

   To start the RNG application, see Starting the Trunked RNG on page 169.
8. To enable the PDG with inbound and outbound capabilities, set the PDG to the active state.

   See Changing the Trunked PDG State to Active in Non-DSR Systems on page 68.

11.8
Recreating the Default Trunked PDG Database

To recreate the default PDG database, see step 6 in Creating a Default Trunked PDG Database on page 216.

This page intentionally left blank.

Chapter 12

Conventional IVD M Core and K Core PDG Troubleshooting

This chapter provides fault management and troubleshooting information related to the Conventional IV&D M core and K core Packet Data Gateway (PDG).

12.1 Troubleshooting Tools

Review the following sections for information on the various tools available for troubleshooting the Packet Data Gateway (PDG).

12.1.1 Conventional PDG Troubleshooting with the Unified Event Manager (UEM)

The Packet Data Gateway (PDG) sends event notifications to the Unified Event Manager (UEM) network fault management application. For a list of PDG alarms, traps, and other information on using the UEM for troubleshooting this device, see the *Unified Event Manager Online Help*.

12.1.2 Checking CPU Utilization on the Conventional PDG

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.
3. In the **OS Administration** menu, type the number associated with **Display Platform Recourses Usage Information**. Press ENTER.

   The CPU and memory usage information is displayed.

12.1.3 Conventional PDG Subsystem Troubleshooting Commands

The following table lists the general commands that you can run while logged on to the Packet Data Gateway (PDG) to check different aspects of the system status or view system logs.

Table 68: Conventional PDG Subsystem Troubleshooting Commands

Command	Description
`/usr/bin/free`	Displays memory usage.
`/bin/df`	Displays disk usage.
`/sbin/ifconfig -a`	Displays the network interface configuration.

Table continued…

Command	Description
`/etc/rc.d/init.d/motorola_pdr status`	Checks the PDR running status.
`/bin/netstat -r`	Displays network routing information.
`/bin/netstat -a`	Displays all the connections and states of the connections on the PDG.
`/opt/Motorola/pdr/bin/versionstamp`	Checks the PDR software version.
`cat /etc/motorola-gems-redhat-linux-os-release`	Checks the Kickstart OS version.
`cat /etc/redhat-release`	Checks the PDR OS version.
`/opt/Motorola/pdr/bin/create_device_rpt`	Creates the PDR mobile device summary report. The default output file is `device_report.txt` and `device_report.csv`.
`/bin/ifconfig`	Displays the network interface configuration.
`/bin/netstat`	Displays the network connections.
`/bin/ps eLf or grep w rng`	Displays all the RNG processes and threads along with their priorities.
`/bin/uptime`	Displays the current time and how long the device is running.
`memory`	Gathers information about different memory buffers used in the RNG.

12.1.4 Conventional PDG System Logs

For information on log management, see the *Centralized Event Logging Feature Guide*.

NOTICE: The Centralized Event Logging feature is supported on all Packet Data Gateways (PDGs) with the exception of the Conventional IV&D PDG in a K core. However, local log information for Linux-based devices in the *Centralized Event Logging Feature Guide* is applicable to all PDGs.

12.2 Troubleshooting Problems on the Conventional PDG

If you experience any problems with the Conventional IV&D Packet Data Gateway (PDG), check the possible causes and perform the recommended actions in the order they are listed. If you need assistance, contact the Motorola Solution Support Center. See Motorola Solution Support Center Contact Information on page 245.

12.2.1 Conventional PDG Database Corrupts as a Result of Power Cut

When there is a sudden power outage or the Packet Data Gateway (PDG) is switched off abruptly due to loss of power supply, the PDG database can lose its configuration or get corrupted. In such a situation, the PDG sends a special trap message to the Radio Network Management Subsystem, informing the system about the corruption of the PDG configuration. After receiving the PDG configuration corruption alert in the Unified Event Manager (UEM) application, create a default PDG database to resolve this problem. See Creating a Default Conventional PDG Database on page 239.

For the Conventional IV&D K core PDG, the configuration corruption alert is logged in Syslog.

CAUTION: Having to re-establish the PDG with the default database upon a power failure is rare and only necessary when you receive a PDG configuration corruption alert in UEM. To restore the PDG, it should be provisioned with full configuration from the Network Manager.

12.2.2

Power LED Fails to Illuminate

If the power LED fails to illuminate, the typical causes include a defective power supply or a problem with the power connection. Check the AC cable connection, verify that the power switch is in the ON position, and check for a possible power supply failure. If required, replace any defective power supplies. For replacement instructions, see Removing and Installing the Power Supply on page 243.

12.2.3

Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network

If the PDR/RNG cannot ping other devices on the network, the following items are the most likely causes:

- The gateway router is down.
- The PDG NIC is running at the wrong speed.
- The PDG port on the LAN switch is disabled.
- The PDG NIC is disabled.
- The PDG NIC is faulty.
- The PDR and RNG port on the LAN switch is configured to the wrong speed or Duplex Mode (100 FD is the appropriate speed).

Procedure:

1. Check the cable connection between the PDG and the LAN switch:
   - **a** Verify that the network cable is correctly plugged into the PDR/RNG and to the appropriate port on the LAN switch.
   - **b** Verify that there are no obvious breaks or sharp bends in the network cable.
   - **c** Verify that the link LED on the LAN switch is on.
   - **d** Replace the cable if necessary.
2. Log on to the PDG as `root`. If unable to log on to the PDG, see Troubleshooting when the Conventional PDG Does Not Boot on page 224.
3. Enter `ifconfig` and look for the following lines of output.

   The values displayed can be different on your system.

```
eth0 Link encap:Ethernet HWaddr 00:1A:4B:A9:0F:54
inet addr: Bcast: Mask:
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:480557 errors:1 dropped:0 overruns:0 frame:1
TX packets:537195 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:35882061 (34.2 MiB) TX bytes:40499477 (38.6 MiB)
Interrupt:185 Memory:f8000000-f8011100
eth1 Link encap:Ethernet HWaddr 00:1A:4B:A9:0F:50
```

```
inet addr: Bcast: Mask:
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:32261048 errors:3961 dropped:0 overruns:0 frame:3961
TX packets:32195685 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2130755316 (1.9 GiB) TX bytes:2123104124 (1.9 GiB)
Interrupt:193 Memory:fa000000-fa011100
```

If the eth0 listing for the PDR is not shown, the network interface is not connected.

4 To connect the network interface, perform the following actions:

a As the root user, enter: `service networks restart`

The PDR uses the eth0 interface.

b Wait for a few seconds before attempting any network traffic.

5 If the symptoms persist, enter: `ifconfig` and verify that the IP address and netmask displayed in the eth0 listing are correct.

6 If the IP address and netmask are incorrect, reconfigure the network interface:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

c Enter the number associated with **Manage Platform Configuration**.

d Enter the number associated with **Configure Network Parameters**.

The following output appears:

```
Host Information ...
Hostname [def: wdselab-a-80-2-12]:
Domain name [def: comm.mot.com ] [- to delete]:
DNS Configuration ...
First DNS nameserver [def: [- to delete]:
Second DNS nameserver [def: ] [- to delete]:
Third DNS nameserver [def: ] [- to delete]:
Fourth DNS nameserver [def: ] [- to delete]:
Default Gateway ...
Default Gateway [def: ] [- to delete]:
Network device eth0 ...
ipaddr [def: ] [- to delete]:
netmask [def: ]:
Network device eth1 ...
ipaddr [def: ] [- to delete]:
netmask [def: ]:
Type y to restart networking with new values:
```

e Verify that the IP address and netmask are correct. If they are incorrect, enter the correct values.

f Verify that the default gateway IP address is correct for the zone that the PDR is located in. If it is incorrect, enter the correct default gateway IP address.

g If all the fields are correct, do not do anything. Press Enter every time.

h Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

The following message appears:

```
.../etc/resolv.conf SUCCESSFULLY updated ...
...Syslog SUCCESSFULLY updated....
```

i Wait for the prompt to return and try to ping another device in the system.

> **IMPORTANT:**
> The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.
>
> If any network parameters were modified, reboot the PDR. See Rebooting the Conventional PDG on page 180.
>
> Set up SNMPv3 AuthPriv and credentials according to the “Configuring USM User Security for the PDG” procedure in the *SNMPv3 Feature Guide*.

7 If the symptoms persist, enter: `netstat -r` and look for the following lines of output.

The values displayed can be different on your system.

```
Kernel IP routing table
Destination GatewayGenmaskFlagsMetricRef UseIface
.Z.  .*255.255.255.255UH000eth0
.Z. .*255.255.0.0U000eth0
...*255.0.0.0U000lo
default.Z..0.0.0.0UG000eth0
```

where Z represents the zone ID of the PDR.

8 If the default line is not shown or does not list the zone gateway IP address, reconfigure the routing:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

c Enter the number associated with **Manage Platform Configuration**.

d Enter the number associated with **Configure Network Parameters**.

e Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is incorrect, enter the correct default gateway IP address.

f Press ENTER to activate the changes.

g Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

> **IMPORTANT:**
> If the default gateway was changed, reboot the PDG.
>
> The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.

If the eth1 listing is not shown for the RNG, the network interface is not connected.

9 To connect the network interface, perform the following actions:

a Enter: `ifdown eth0; ifup eth0`

RNG uses the eth1 interface.

b Wait for a few seconds before attempting any network traffic.

10 If the symptoms persist, enter: `ifconfig` and verify that the IP address and netmask displayed in the eth1 listing are correct.

11 If the IP address and netmask are incorrect, reconfigure the network interface:

a Enter: `admin_menu`

b Enter the number associated with **OS Administration**.

- **c** Enter the number associated with **Manage Platform Configuration**.
- **d** Enter the number associated with **Configure Network Parameters**.
- **e** Verify that the IP address and netmask are correct. If they are incorrect, enter the correct values.
- **f** Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is not, correct the default gateway IP address.
- **g** If all the fields are correct, do not do anything. Press ENTER every time.
- **h** Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`
- **i** Wait for the prompt to return and try to ping another device in the system.

  IMPORTANT:
  If any network parameters were modified, reboot the PDG.

  The **Configure Network Parameters** option and the `/opt/Motorola/pdr/bin/update_os_conf_files.sh` command cannot be used to change the location of the PDG from one domain to another.

12 If the symptoms persist, enter: `netstat -r` and look for the following lines of output.

The values displayed can be different on your system.

```
Kernel IP routing table
Destination GatewayGenmaskFlagsMetricRef UseIface
.Z.  .*255.255.255.255UH000eth0
.Z. .*255.255.0.0U000eth0
...*255.0.0.0U000lo
default.Z..0.0.0.0UG000eth0
```

where Z represents the zone ID of the RNG.

13 If the default line is not shown or does not list the zone gateway IP address, reconfigure the routing:

- **a** Enter: `admin_menu`
- **b** Enter the number associated with **OS Administration**.
- **c** Enter the number associated with **Manage Platform Configuration**.
- **d** Enter the number associated with **Configure Network Parameters**.
- **e** Verify that the default gateway IP address is correct for the zone the PDR is located in. If it is incorrect, enter the correct the default gateway IP address.
- **f** Press ENTER to activate the changes.
- **g** Enter: `/opt/Motorola/pdr/bin/update_os_conf_files.sh`

12.2.4
Troubleshooting when the Conventional PDG Does Not Boot

If the Packet Data Gateway (PDG) hardware does not boot, perform the following procedure.

NOTICE: The GRUB Bootloader can get stuck at the OS selection screen due to an unexpected input. Press ENTER to continue the boot process.

Procedure:

1. At the PDG console prompt, press ENTER a few times.
2. Depending on the result, perform one of the following actions:

If…	Then…
If a prompt does not appear,	perform the following actions: **a** Verify the console port connection. **b** Verify that the chassis is powered.
If a normal login prompt appears but the root login is not accepted,	perform the following actions: **a** Verify that you are using the correct root login password. **b** Verify that the CAPS LOCK key is not selected.

3. If you are unable to correct the problem, contact the Motorola Solution Support Center.

   See Motorola Solution Support Center Contact Information on page 245.

12.2.5
Troubleshooting when the UEM Is Not Receiving PDR Alarms

If the Unified Event Manager (UEM) application is not receiving Packet Data Router (PDR) alarms, the following items are the most likely causes:

- No alarm conditions are occurring.
- The manager is not registered.
- The manager registration table is full.
- The PDR is not running.
- The network connectivity between the PDR and the UEM has failed.

When and where to use:
This procedure is only applicable to the Conventional IV&D M core PDG.

Process:

1. Ensure that the device is otherwise operational, has connectivity to the network, and the network is operational.
2. In UEM, verify that the device is discovered by using the subnet discovery.

   For more information, see the *Unified Event Manager User Guide*.
3. If the secure SNMPv3 operation is enabled, ensure that the credentials are set up correctly on the device.

   For more information, see the *SNMPv3 Feature Guide*.
4. If the manager registration table is full and there are unwanted managers in the registration table, delete the PDG managed object from the unwanted manager.

   For more information on removing unwanted UEM entries, see the *Unified Event Manager Online Help*.

12.2.6
Troubleshooting when the PDR Does Not Appear on the UEM Topology Map

If the Packet Data Router (PDR) does not appear on the Unified Event Manager (UEM) topology map, the following items are the most likely causes:

- The network outage prevents the device from sending alarms to the UEM.

- The device may not be discovered in the UEM.

When and where to use:
This procedure is only applicable to the Conventional IV&D M core PDG.

Process:

1. Ensure that the device is otherwise operational, has connectivity to the network, and the network is operational.
2. In the UEM, verify that the device is discovered, using the subnet discovery.

   For more information, see the *Unified Event Manager User Guide*.
3. If the secure SNMPv3 operation is enabled, make sure that the credentials are set up correctly on the device.

   For more information, see the *SNMPv3 Feature Guide*.

12.2.7 PDR Configuration Data Out-of-Sync

Use the VoyenceControl application to determine whether the Provisioning Manager data for the Packet Data Router (PDR) is synchronized. If the configuration data is out-of-sync, use VoyenceControl to re-synchronize the data. For more information, see “PM Data Sync State” in the *Unified Network Configurator User Guide*.

NOTICE:
This section is **not** applicable to the Conventional IV&D K core PDG.

The names EMC Smarts Network Configuration Manager and VoyenceControl are used interchangeably for this product.

12.2.8 Conventional PDG Clock Problems

The Packet Data Router (PDR) synchronizes its clock with the Network Time Protocol (NTP) server at the master site. The PDR periodically polls the NTP server. The PDR then receives an NTP packet and updates its internal clock. If the PDR clock seems to be drifting from the NTP server clock, it can be related to one of the following causes:

- A power outage has occurred.
- The PDR is reset without a proper shutdown.
- A network disconnection between the PDR and the NTP server has occurred for a significant amount of time.

For more information, see the *Network Time Protocol Server Feature Guide*.

12.2.9 Troubleshooting DVD-ROM Drive Problems

For server hardware troubleshooting information, see the *Virtual Management Server Hardware User Guide*.

12.2.10 Troubleshooting when the PDR Application Does Not Start (start_pdr Command Failed)

If the Packet Data Router (PDR) application does not start (the start_pdr command fails), the following items are the most likely causes:

- The PDR database is not initialized.
- The PDR database is corrupted due to a power outage or other hardware problem.
- The PDR disk space is full.

Procedure:

1. Log on to the PDG as `root`.
2. Verify the PDR status through the **admin_menu**.

   See Verifying the Conventional PDR and RNG Status on page 179.
3. Perform one of the following actions:

If…	Then…
If the PDR is running,	go to step 6.
If the PDR is not running,	go to step 4.

4. Verify if the database is initialized:
   - **a** Enter: `cd /opt/Motorola/pdr/bin`
   - **b** Enter: `ls oms_db`
   - **c** Enter: `ls dbfiles`

   If in response to either command, a message appears informing that there is no such file or directory, this means that the database was not initialized during the PDR installation. Initialize the PDR database through the **admin_menu**.
5. Start the PDR application through the admin_menu again. If the database has already been initialized, but the start of the PDR still fails, go to step 6.
6. Verify that enough disk space is available:
   - **a** From the **admin_menu**, select **Display Platform Resource Usage Information** to check if the disk space is a problem.
   - **b** If the disk space for `/opt` is greater than 90%, enter `ls /opt/Motorola/pdr/bin/cor*` to check for the existence of the core files. If any entries exist, contact the Motorola Solution Support Center.

     See Motorola Solution Support Center Contact Information on page 245.
   - **c** If no core files exist, copy some database backups (SFTP) from the PDR and then delete those database backups until the used disk space for this partition is between 85% and 90%.
   - **d** After cleaning up the disk, start the PDR through the **admin_menu**. If the start PDR still fails, go to step 7.
7. A corrupted database may cause various symptoms. Run the following commands to back up the current database and create another database:
   - **a** Log on as a member of the **instadm** or **bkupadm** group.
   - **b** Produce the backup PDR database through the **admin_menu**.
   - **c** Log out and log on as root.
   - **d** Enter: `rm -r oms_db`
   - **e** Enter: `rm -r dbfiles`
   - **f** Initiate the PDR database through the **admin_menu** and start the PDR application.

- **g** If the PDR does not start, the problem is not a corrupted database. Restore the PDR database through the **admin_menu**. When restoring the PDR database, select the backup file with the current date.

8. If the PDR can start, the problem was a corrupted database. If the corrupted database is not related to a power hit, send the backup file made in this procedure to the Motorola Solution Support Center for analysis.
9. Reboot the PDG server through the **admin_menu**.
10. If the PDR does not start, contact Motorola for assistance.

12.2.11 RNG Site Link in Unknown State

If the Radio Network Gateway (RNG) site link state shows up as unknown in the Packet Data Router (PDR) Local Configuration user interface, it is because the PDR Local RNG link is down. The RNG reports the RNG site link state to the PDR to display in to the Local Configuration and also report it to the Unified Event Manager (UEM) application. If the PDR link to the Local RNG is down, the PDR does not know the actual state of the site links. Check if the RNG is running. If the RNG is not running, start the RNG by using `start_rng` command.

12.2.12 Other Conventional PDG Failure Conditions

The following table lists other Packet Data Gateway (PDG) failure conditions, and provides their causes and remedies.

Table 69: Other Conventional PDG Failure Scenarios

Failure Condition	Cause	Remedy
Data is not delivered to the subscriber unit or to the CEN.	Potential failure on the communication path	Check the local link between the RNG and the PDR in the Local Configuration view.
	Serving PDR failure	• M core PDG: Check the UEM for the state of the PDR. K core: Check the alarms and events logged in Syslog.or the UEM. • Check the PDR state in the Local Configuration view.
The PDG fails to register a subscriber unit.	The resolution of the GGSN IP failed.	• Check the provisioned GGSN information and the DNS server configuration. This step is **not** applicable to the Conventional IV&D K core PDG. • In the Local Configuration view, check if the PDR is in the active operable redundancy state. See Accessing the Conventional PDG Local Configuration Interface on page 129.

Table continued…

Failure Condition	Cause	Remedy
M core: The PDR notifies the UEM about a Critical Malfunction state. K core: This notification is logged in Syslog. The PDR state is shown as inoperable in the Local Configuration interface.	Communication Failure: PDR health check failed.	• Check the connection between the PDR and the RNG, the PDR and the GGSN, and the PDR and gateway routers. • Check whether the resolution of IP addresses through the DNS lookup failed.
	This cause and remedy are not applicable to the Conventional IV&D K core PDG.	
M core: The PDR notifies the UEM about a Critical Malfunction state. K core: This notification is logged in Syslog. The PDR state is shown as inoperable in the Local Configuration interface.	No Configuration: PDG Configuration failure - the PDR failed to start up with the previously running configuration.	Recreate the PDR database. Re-provision the PDR with full configuration.
M core: The PDR notifies the UEM about a Minor Malfunction. K core: This notification is logged in Syslog.	Communication Failure: The PDR lost connection with one of the gateway routers.	Check connection between the PDR and the gateway routers.
M core: The PDR notifies the UEM about an RNG overloaded state. K core: This notification is logged in Syslog.	RNG message capacity exceeded: Excessive message traffic through the RNG.	Reduce data traffic.
M core: The PDR notifies the UEM that the CDEM is unreachable. K core: This notification is logged in Syslog.	Communication Failure	Check connection between the PDR and the RNG, and between the RNG and the CDEM.
M core: The PDR notifies the UEM about a CDEM Minor Malfunction state. K core: This notification is logged in Syslog.	• Duplicate Key ID or Algorithm ID is present in the CDEM. • CDEM battery is low.	• Check the CDEM key database. • Check the CDEM battery level.
M core: The PDR notifies the UEM about a CDEM Major Malfunction state.	Lack of keys in the CDEM	Check the CDEM key database.

Table continued…

Failure Condition	Cause	Remedy
K core: This notification is logged in Syslog.		
M core: The PDR notifies the UEM that the RNG-CDEM link is down. K core: This notification is logged in Syslog. The link status is also shown in the Local Configuration interface.	RNG-CDEM communication failed.	• Check connectivity between the RNG and the CDEM. • Check if the KMF IP address was resolved correctly.
M core: The PDR notifies the UEM that the PDG-KMF link is down. K core: This notification is logged in Syslog.	PDG-KMF communication failed.	Check connectivity between the PDG and the KMF.
M core: The PDR notifies the UEM that the PDR-gateway router link is down. K core: Not applicable.	Communication Failure: The PDR has not received any ICMP echo responses from the gateway router.	• Check the connectivity between the PDR and the gateway router. • Check if the gateway router IP address was resolved correctly.
M core: The PDG notifies the UEM that it fails to encrypt/ decrypt outbound/inbound traffic. K core: This notification is logged in Syslog.	Various causes	• Check the CDEM key database. • Check the PDG communication with the CDEM and the KMF. • Check whether the encryption mode of the mobile device is correct. • Review any other PDG notifications about link failures or state changes.
M core: The PDR notifies the UEM about an overload condition. K core: This notification is logged in Syslog.	Data traffic is too heavy.	Reduce data traffic.

12.2.13

Setting the Conventional PDG to the User Requested Standby (URS) State

Prerequisites: Ensure that the Packet Data Router (PDR) is running. If the PDR service is not running, start the PDR. See Starting the Conventional PDR on page 181.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2. Select **Application Administration**. Press ENTER.

3. In the **Application Administration** menu, select **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations**, select **PDG Local Configuration**. Press ENTER.
5. In the **PDG Local Configuration** menu, select **Redundancy Configuration**. Press ENTER.
6. In the **Redundancy Configuration** menu, select **Modify Redundancy Configuration**. Press ENTER.

   The PDG can be in the active state if it is in a primary core or in the standby state if it is in a backup core.
7. In the **Modify Redundancy Configuration** menu, perform the following actions:
   a. Select **User Requested Standby** by using the arrow keys. Press ENTER.
   b. Select **Submit** by using the arrow keys. Press ENTER.

   A message appears, warning that this action can disable the PDG.
8. Select **Yes** to proceed. Press ENTER.

   A message confirms that the PDG redundancy state is user requested standby. The PDG restarts and the **Application Management and Operations** menu appears.
9. To exit the **Main Menu**, type `q`. Press ENTER.

   The command prompt appears.

12.3 Troubleshooting the SNMPv3

For the SNMPv3 configuration related to the PDG, see SNMPv3 Credentials Maintenance on page 157.

For information on troubleshooting problems with the SNMPv3 operation, see the *SNMPv3 Feature Guide*.

12.3.1 Troubleshooting SNMPv3 Configuration Loss after a PDG Power Failure or Hard Reset

The SNMPv3 Common Agent can lose the content of the configuration file as a result of a Packet Data Gateways (PDG) virtual machine power failure or hard reset.

When and where to use:
Use this process to troubleshoot the loss of SNMPv3 configuration related to the PDG in the following cases:

- If Unified Event Manager (UEM) displays the “CommFailure” alarm for a PDG that experienced a power failure or a recent hard reset.
- If an application cannot communicate over SNMPv3 to or from a PDG that experienced a power failure or a recent hard reset.

- If you cannot select the **Configure SNMPv3 Agent/Manager** option from the **Manage SNMP Passphrases** menu in the main PDG administration menu despite using the correct MotoAdmin credentials.

Process:

1. Reset the MotoAdmin credentials to be able to change other users' credentials. See "Recovering MotoAdmin Passphrases" in the *SNMPv3 Feature Guide*.
2. Configure the rest of SNMPv3 users on the affected PDG. See "Configuring USM User Security for the PDG" in the *SNMPv3 Feature Guide*. Make sure to fix all SNMPv3 paths to/from the PDG based on the "SNMPv3 Communication Matrix" in the *SNMPv3 Feature Guide*.

   NOTICE: This has to be done on the PDG and all servers which communicate with it over SNMPv3.
3. Verify that the updated communication paths are operational.

12.4 Troubleshooting the Packet Data Service

Issues with the packet data service on the Packet Data Gateway (PDG) include:

- Mobile data users cannot register
- Packet data service is not available to subscribers in the zone
- Subscriber is not receiving all messages from the PDR
- Subscriber does not receive ICMP messages from the host
- Mobile data users are being deregistered by the PDR

12.4.1 Mobile Data Users Cannot Register

If mobile data users cannot register, the following items are the most likely causes:

- Subscriber is not provisioned in the PDG by the Network Manager for packet data service.
- The link to the GGSN is down.
- The link to the site is down.
- The subscriber is not mapped to the appropriate home zone or the database is not synchronized.
- The dynamic IP address was requested, but there is a problem with the DHCP server.
- The T3 timeout parameter is too short.
- The APN configured for the mobile does not match any of the APNs configured for the GGSN.

Table 70: Mobile Data Users Cannot Register

Possible Cause	Recommended Actions
Subscriber is not provisioned for packet data service.	In the Provisioning Manager, verify that the radio user is configured for packet data service. Configure and enable packet data services for the radio user if necessary. This action is **not** applicable to the Conventional IV&D K core PDG.
The link to the GGSN is down.	1 Check the link status between the PDR and GGSN through the network fault management application.

Table continued…

Possible Cause	Recommended Actions
	2 Ping the GGSN to confirm that it is accessible.
Link to the site is down.	**1** Navigate to the PDG local configuration interface. See Accessing the Conventional PDG Local Configuration Interface on page 129. **2** In the main menu, select **Local RNG-Site Link Status**. **3** If the status of all the sites is down, check for general network problems. **4** If some of the sites are down, check for problems at those particular sites. Verify the Site Gateway (Conventional Channel Interface) configuration (IP address and site ID). Ping the base station from the RNG, and ping the RNG from the base station. **5** Restart the RNG. **6** If the problem persists, contact Motorola Solutions for assistance.
The subscriber is not mapped to the appropriate home zone or the database is not synchronized.	**1** In the Provisioning Manager, check the home zone mapping and verify that the subscriber is mapped to the appropriate zone. This step is **not** applicable to the Conventional IV&D K core PDG. **2** Navigate to the PDG local configuration interface. See Accessing the Conventional PDG Local Configuration Interface on page 129. **3** In the main menu, select **View Mobile Device Information**. **4** Enter the radio ID for the subscriber. If the View Device Detail Screen does not appear, then check the data sync state. Conventional IVD M Core PDG Database Synchronization on page 90. This step is **not** applicable to the Conventional IV&D K core PDG. **5** If the database cannot be synchronized, check the status of the Network Management servers.
The dynamic IP address was requested, but there is a problem with the DHCP server.	**1** Check the network fault management application alarms for the PDR object. The PDR sends a trap indicating the reason whenever it rejects a packet data registration (as long as the same trap is not sent within the previous 10 minutes). **2** Alarm 5065, `GGSN Returned No Resources Available`, indicates a problem with the DHCP server or the link between the GGSN and DHCP server.
The T3 timeout parameter is too short.	If alarm 5075, `No Response for GGSN`, is frequently received from the PDR in the network fault management application, and the link to the GGSN is known to be up during this period, verify in the Provisioning Manager that the product of GTP T3 Timeout and GTP N3 Attempts is at least 16 seconds long. This action is **not** applicable to the Conventional IV&D K core PDG.
The APN configured for the mobile does not	Alarm 5066, `Service Not Support`, indicates a problem with the APN network configuration. In the Provisioning Manager, check the

Possible Cause	Recommended Actions
match any of the APNs configured for the GGSN.	APN assigned to the radio user. Verify that the APN is programmed into the GGSN. This action is **not** applicable to the Conventional IV&D K core PDG.

12.4.2
Packet Data Service Not Available to Subscribers in the Zone

If packet data service is not available to subscribers in the zone, those particular subscribers may configure or synchronize the database.

Table 71: Packet Data Service Not Available to Subscribers in the Zone

Possible Cause	Recommended Actions
Verify that a specific subscriber is available in the database and the database is synchronized.	Verify the mobile database: **1** Navigate to the PDG local configuration interface, select **View Mobile Device Information**, and enter the radio ID for the subscriber. See Accessing the Conventional PDG Local Configuration Interface on page 129. **2** If the **View Device Detail** screen does not appear, check the data sync state. See Conventional IVD M Core PDG Database Synchronization on page 90. **NOTICE:** This is **not** applicable to the Conventional IV&D K core PDG. **3** If the database cannot be synchronized, check the status of the Network Management servers.

12.4.3
Subscriber Is Not Receiving All Messages From the PDR

If a subscriber is not receiving all its messages, the following items are the most likely causes:

- The outbound traffic load is too high.
- The subscriber is operating in a fringe coverage area or intermittent voice services are taking precedence over data.

Table 72: Subscriber Is Not Receiving All Messages

Possible Cause	Recommended Actions
The outbound traffic load is too high.	Check for outbound queue overflows: **1** Navigate to the PDG local configuration interface. See Accessing the Conventional PDG Local Configuration Interface on page 129. **2** Enter: `grep 5150 /var/log/messages`

Table continued…

Possible Cause	Recommended Actions
	Each instance includes the following text and lists the ID of the radio for which the message was destined. `ERROR Enumeration: 5150` If numerous outbound queue overflows are reported, the application is sending data too quickly. Any additional messages that arrive when the buffer is full are discarded.
The subscriber is operating in a fringe coverage area or intermittent voice services are taking precedence over data.	Check for NAK events in the PDG local configuration interface: **1** Navigate to the PDG local configuration interface. See Accessing the Conventional PDG Local Configuration Interface on page 129. **2** Select **Statistics Management** → **View Statistics** → **Mobile Device Statistics**. **3** Enter the Radio ID for the subscriber. **4** Check the **Outbound NAK Count** field. This field shows the number of times outbound messages to the subscriber are not successfully delivered since the last time the statistics were reset. This could be due to the subscriber being in fringe coverage or due to voice transactions taking precedence over data.

12.4.4
Subscriber Does Not Receive ICMP Messages From the Host

If a subscriber does not receive ICMP messages from the infrastructure, the ICMP Enabled setting for the radio user may need to be set.

Table 73: Subscriber Does Not Receive ICMP Messages From the Host

Possible Cause	Recommended Actions
ICMP messages are disabled from the host	In the Provisioning Manager, open the appropriate radio user record and select the **Data Services** tab. Change the **ICMP Enabled** field to **Yes**. **NOTICE:** This is **not** applicable to the Conventional IV&D K core PDG.

12.4.5
Mobile Data Users Are Being Deregistered by the PDR

If mobile data users are being deregistered by the PDR, the following items are the most likely causes:

- The link to the GGSN is down.

- Mobile user provisioning data has changed (such as the IP address).

Table 74: Mobile Data Users Are Being Deregistered by the PDR

Possible Cause	Recommended Actions
Link to GGSN is down.	• Check the status of the PDR-GGSN link in the network fault management application. • Check that the GGSN is provisioned in the PDR, by checking the Local Configuration view.
Mobile user provisioning data has changed (such as the IP address).	**1** Navigate to the PDG local configuration interface. See Accessing the Conventional PDG Local Configuration Interface on page 129. **2** Select **Statistics Management** → **View StatisticsMobile Device Statistics**. **3** Enter the radio ID for the affected mobile data user. **4** In the **Mobile Device Statistics** menu, check the **Reason for Last Deactivation**.

12.5 Dynamic System Resilience (DSR) Specific Troubleshooting

This section contains failure scenarios and troubleshooting procedures specific to the Dynamic System Resilience (DSR) feature. For information on typical failure scenarios and recovery sequences for the data subsystem, see the “Dynamic System Resilience Troubleshooting” chapter in the *Dynamic System Resilience Feature Guide*.

DSR-related troubleshooting described in this section is required only if your system supports DSR. For more information, contact your system administrator.

12.5.1 HA Link Is Down

If the HA link is down, perform the following troubleshooting steps:

- Ping the peer Packet Data Router (PDR). See Pinging a Peer Device on page 214.

  If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.
- Try setting the same key on both Packet Data Gateways (PDGs). See Setting Heartbeat Key on the Trunked PDG on page 70.

12.5.2 InterZone RNG Link Is Down

If the InterZone RNG link is down, perform the following troubleshooting steps:

- Ping the peer Radio Network Gateway (RNG). See Pinging a Peer Device on page 214.

  If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.
- Check if the Packet Data Gateway (PDG) is in the active state. See Trunked PDG Redundancy Configuration on page 71.

12.5.3
Pinging a Peer Device

Use the Ping command to test if a peer device such as the Packet Data Router (PDR) or Radio Network Gateway (RNG) in the backup core is reachable.

Prerequisites: Obtain the required IP address, account logins, and passwords from your system administrator.

Procedure:

1. Log on to the PDG as a member of the **instadm** or **platadm** group.
2. Type `ping` ***<IP address>***. Press Enter.

   Ping is successful if you receive the following output:

   ```
   64 bytes from  <PDR IP address>: icmp_seq=1 ttl=64 time=0.218 ms
   64 bytes from  <PDR IP address>: icmp_seq=2 ttl=64 time=0.493 ms
   64 bytes from  <PDR IP address>: icmp_seq=3 ttl=64 time=0.307 ms
   64 bytes from  <PDR IP address>: icmp_seq=4 ttl=64 time=0.525 ms
   ```

   Ping is unsuccessful if you receive the following output:

   ```
   From  <PDR IP address> icmp_seq=1 Destination Host Unreachable
   From  <PDR IP address> icmp_seq=2 Destination Host Unreachable
   From  <PDR IP address> icmp_seq=3 Destination Host Unreachable
   From  <PDR IP address> icmp_seq=5 Destination Host Unreachable
   ```

   NOTICE: If the Ping command is not successful, see Troubleshooting when the PDR/RNG Cannot Ping Other Devices on the Network on page 200.

3. Press Ctrl + C to exit the ping command interface.

12.5.4
Component Failures in Dynamic System Resilience (DSR) Enabled Systems

If there is a component failure that involves the RNG, PDR or GGSN, the subscribers which are home to the zone must initiate a Context Activation request. The failure forces a switchover to the backup data subsystem, which does not have context records. Context activation is not shared between the two cores.

To alert the subscribers, the newly active PDR sends a Context Activation Status message to the local RNG. The RNG forwards the message to sites as the Site Controller (SC) to RNG links are established. The message targets subscribers, which are home to this zone and are currently registered in the zone. Those subscribers begin to perform context activation.

For the DSR-related configuration, see Dynamic System Resilience Configuration on page 69. For the DSR troubleshooting, see the “Dynamic System Resilience Troubleshooting” chapter in the *Dynamic System Resilience Feature Guide*.

12.6
Conventional PDG OS Administration

This section contains procedures performed using the **OS Administration** menu.

12.6.1 Configuring Time Parameters

CAUTION: This procedure can be used only for the initial configuration of the time parameters. The time on the running Packet Data Gateway (PDG) is synchronized with the Zone NTP Server.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press Enter.
3. In the **OS Administration** menu, type the number associated with **Manage Platform Configuration**. Press Enter.
4. In the **Manage Platform Configuration** menu, type the number associated with **Configure Time Parameters**. Press Enter

   The **Time Parameters** menu appears. In this menu, you can configure the following time parameters on the PDG:

   - Time of the day
   - Date
   - Time Zone

12.6.2 Configuring Network Parameters

See “Viewing and Configuring Network Parameters on the Juniper Firewall Manager” in the *Unix Supplemental Configuration Setup Guide*.

12.6.3 Displaying Platform Configuration Information

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.
2. In the **Main Menu**, type the number associated with **OS Administration**. Press Enter.
3. In the **OS Administration** menu, type the number associated with **Display Platform Configuration Information**. Press Enter.

   The following information is displayed:

   - Version of operating system
   - Kernel release version
   - Host name
   - Domain name
   - MAC addresses for all network interfaces
   - Uptime information
   - IP addresses of all network interfaces

12.6.4 Displaying the Platform Resource Usage Information

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2. In the **Main Menu**, type the number associated with **OS Administration**. Press ENTER.
3. In the **OS Administration** menu, type the number associated with **Display Platform Resource Usage Information**. Press ENTER.

   The following information is displayed:

   - Memory Usage
   - Disk Usage
   - CPU Usage

12.7 Creating a Default Conventional PDG Database

The Packet Data Gateway (PDG) virtual appliance is built with the initiated database. After the deployment of this appliance and the PDG initial configuration, the database is rebuilt according to the PDG initial configuration parameters. If the database is corrupt and recovery from a backup database is unavailable or unsuccessful, perform this procedure to recreate a default database.

Prerequisites:
If the system is already installed and the Packet Data Router (PDR) software is running, stop the PDR. See Stopping the Conventional PDR on page 182.

Procedure:

1. Log on to the PDG and invoke the **Main Menu**.

   See Logging On to the Conventional PDG and Invoking the Main Menu on page 175.

2. In the **Main Menu**, type the number associated with **Application Administration** and press ENTER.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations**. Press ENTER.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operation**. Press ENTER.
5. In the **PDR Specific Management and Operation** menu, type the number associated with **Initialize Database**. Press ENTER.
6. Perform one of the following actions:

If…	Then…
If the PDR database is initialized for the first time on the device and the database creation process is completed,	go to step 7.
If the PDR database has already been initialized on this device and a message appears informing that the database already exists	perform one of the following actions: • To quit the database creation process, type `n`.

If…	Then…
and asking you if you want to remove the database,	**Step result**: The PDR database is retained. - To recreate the database, type `y`. **Step result**: The PDR database is recreated.

7 From the **PDR Specific Management and Operations** menu, select **Start PDR**.

To start the RNG application, see Starting the Conventional RNG on page 182.

8 To enable the PDG with inbound and outbound capabilities, set the PDG in the active state.

See Changing the Conventional PDG State to Active on page 87.

12.8 Recreating the Default Conventional PDG Database

To recreate the default PDG database, see step 6 in Creating a Default Conventional PDG Database on page 239.

Chapter 13

Packet Data Gateway FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the Packet Data Gateway (PDG).

13.1 Packet Data Gateway Physical Description

For the physical description of the HP DL380 server hosting the Packet Data Gateway (PDG), see the *Virtual Management Server Hardware User Guide*.

13.2 Required Tools and Equipment

Take the following items to the replacement site when replacing any equipment in the Packet Data Gateway (PDG):

- Electrostatic discharge (ESD) strap (Motorola Solutions part number 4280385A59 or equivalent)
- Phillips, slotted, and Torx (T-25 and T-30) screwdrivers

13.3 Packet Data Gateway FRUs/FREs

The following table lists each field replaceable unit (FRU) available for the PDG along with its part number and the appropriate procedure for replacing the item. Use the part number for the item when ordering. You must order and receive the parts before performing any procedures.

Table 75: Packet Data Gateway – Field Replaceable Units/Field Replaceable Entities

Motorola Solutions Kit Number	Description	Vendor Part Number
DLN6744A	300 GB SAS Hard Disk Drive. See Hard Disk Drive on page 242.	Synnex 2291511
DLN6742A	460 Watt Power Supply. See Removing and Installing the Power Supply on page 243.	Synnex 2378786
DLN6745A	DVD-RW SATA Drive	Synnex 2407809
DLN6747A	Fan Module. See Removing and Installing the Fan Module on page 244. (Order through Motorola Solutions North America Parts Organization).	HP 532149-001
DLN6746A	2 GB PC3-10600R Memory (Order through Motorola Solutions North America Parts Organization)	Synnex 2408125
DDN1073A	HP DL380 Gen8 Virtual Server without Software	Synnex 2667050
DLN6974A	HP DL380 Gen9 Virtual Server without Software	NA

13.4 Hard Disk Drive

To assess the status of a hard drive, observe and understand the hot-plug hard drive status LEDs. For a detailed explanation of hard drive status LEDs, see the appropriate *HP Server Setup and Installation Guide*.

Contact the System Support Center for advice on service support. For phone numbers, see Motorola Solution Support Center Contact Information on page 245.

13.4.1 Hard Disk Drive Locations

Table 76: Hard Disk Drive Locations

Location	Description
1	Hot-plug U320 SCSI hard drive, SCSI ID 0
2	Hot-plug U320 SCSI hard drive, SCSI ID 1
3	Hot-plug U320 SCSI hard drive, SCSI ID 2
4	Hot-plug U320 SCSI hard drive, SCSI ID 3

13.4.2 Removing the Hard Disk Drive from the Server

⚠ **WARNING:** The PDG contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the PDG and remove the power cabling before servicing this equipment.

⚠ **CAUTION:** Do not operate the server without a hard drive or a hard drive blank installed. Failure to install a hard drive or a hard drive blank can lead to improper cooling and may damage the system.

Prerequisites:
Switch off the PDG while replacing the components. This causes any data traffic between the external data network and the system infrastructure to be suspended until the PDG is brought back into service.

Before removing a hard drive, read “Hot-plug Hard Drive Replacement Guidelines” in the *HP Servers Troubleshooting Guide*.

Take the following items to the replacement site:

- Electrostatic discharge (ESD) strap (Motorola part number 4280385A59 or equivalent)
- Phillips, slotted, and Torx (T-25 and T-30) screwdrivers

Procedure:

1. Determine the status of the hard drive from the hard drive LEDs.
2. Back up all the server data on the hard drive.
3. Press the button on the hard drive to release the drive latch.
4. Open the drive latch on the hard drive.
5. Pull the hard drive to remove it from the server.

Postrequisites: After servicing the equipment, always verify that the equipment is operational before leaving the site.

13.4.3 Installing the Hard Disk Drive into the Server

WARNING: The PDG contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the PDG and remove the power cabling before servicing this equipment.

CAUTION: Do not operate the server without a hard drive or a hard drive blank installed. Failure to install a hard drive or a hard drive blank can lead to improper cooling and may damage the system.

Prerequisites:
Switch off the PDG while replacing the components. This causes any data traffic between the external data network and the system infrastructure to be suspended until the PDG is brought back into service.

Before replacing a hard drive, read “Hot-plug Hard Drive Replacement Guidelines” in the *HP Servers Troubleshooting Guide*.

Take the following items to the replacement site:

- Electrostatic discharge (ESD) strap (Motorola part number 4280385A59 or equivalent)
- Phillips, slotted, and Torx (T-25 and T-30) screwdrivers

Procedure:

1. Slide the hard drive into the open bay until the latch mechanism engages the server.
2. Close the drive latch handle to lock the hard drive in the server.

Postrequisites: After servicing the equipment, always verify that the equipment is operational before leaving the site.

13.5 Removing and Installing the Power Supply

WARNING: The PDG contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the PDG and remove the power cabling before servicing this equipment.

CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with a component.

Prerequisites:
Switch off the PDG while replacing the components. This causes any data traffic between the external data network and the system infrastructure to be suspended until the PDG is brought back into service.

Take the following items to the replacement site:

- Electrostatic discharge (ESD) strap (Motorola part number 4280385A59 or equivalent)
- Phillips, slotted, and Torx (T-25 and T-30) screwdrivers

When and where to use: The procedure assumes that the server is configured with two power supplies.

Procedure:

1. If a conventional cable management solution is in place, unfasten the cable management solution to access the power supply bays.
2. Disconnect the power cord.
3. Remove the power supply from the hot-plug power supply bay by pressing the power supply release lever, and then pulling the power supply from the server.

4 To replace the component, reverse the removal procedure.

Postrequisites: After servicing the equipment, always verify that the equipment is operational before leaving the site.

13.6 Removing and Installing the Fan Module

WARNING: The Packet Data Gateway (PDG) contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the PDG and remove the power cabling before servicing this equipment.

CAUTION: Do not operate the server for long periods without the access panel. Operating the server without the access panel results in improper airflow and improper cooling that can lead to thermal damage.

Prerequisites:
Switch off the PDG while replacing the components. This causes any data traffic between the external data network and the system infrastructure to be suspended until the PDG is brought back into service.

Take the following items to the replacement site:

- Electrostatic discharge (ESD) strap (Motorola part number 4280385A59 or equivalent)
- Phillips, slotted, and Torx (T-25 and T-30) screwdrivers

Procedure:

1 Power down the server.

2 Perform the following actions:

   a Disconnect cables from the rear of the server.

   b Unfasten two M6 screws which secure the rear of the server to the slide rails.

   c Unfasten two M5 screws which secure the front of the server to the slide rails.

   d Remove the server from the rack and place on a workbench.

3 Remove the access panel.

4 **WARNING:**
   To reduce the risk of personal injury or equipment damage, follow these guidelines:

   - Ensure that the rack is adequately stabilized before extending a component from the rack.
   - Be careful when pressing the server rail-release latches and sliding the server into the rack. The sliding rails could pinch your fingers.

   Press the latches and lift to release the triple fan module from the server.

5 Remove the component from the server.

6 To replace the component, reverse the removal procedure.

   IMPORTANT: When replacing the component, ensure that the power converter module is properly seated in the server.

Postrequisites: After servicing the equipment, verify that the equipment is operational before leaving the site.

13.7 Motorola Solution Support Center Contact Information

The Motorola Solution Support Center (SSC) provides technical support, Return Material Authorization (RMA) numbers for FRUs and FREs, and confirmations for troubleshooting results. Call the Solution Support Center for information about returning faulty equipment or ordering advance exchanges.

North America: 1-800-221-7144

International: 001-302-444-9800

This page intentionally left blank.

Chapter 14

Packet Data Gateway Reference

This chapter contains supplemental reference information relating to Packet Data Gateway (PDG).

14.1 LED Indicators

For information about the LEDs found on the Packet Data Gateway (PDG), see the *Virtual Management Server Hardware User Guide*.

This page intentionally left blank.

Chapter 15

Packet Data Gateway Disaster Recovery

This chapter provides references and information enabling you to recover the Packet Data Gateway (PDG), including the Packet Data Router (PDR) and the Radio Network Gateway (RNG), before restoring data communications in an ASTRO® 25 system in the event of a failure.

NOTICE: Backup of the PDG database and SSH configuration is performed as part of the installation process. Review the entire recovery process and each supporting procedure before recovering the PDG.

15.1 Recovery Sequence for the Packet Data Gateway in DSR Systems

In systems employing the Dynamic System Resilience (DSR) feature, recovery consists in recovering the Packet Data Gateways (PDGs) in the primary and secondary zone cores.

15.1.1 Recovering the Primary Packet Data Gateway in DSR Systems

In a system with Dynamic System Resilience (DSR), if the primary Packet Data Gateway (PDG) goes out of service, the backup PDG automatically takes over.

When and where to use:
Perform this procedure to recover the primary PDG.

Process:

1. This step can be skipped, if only the VM needs to be recovered. Recover the ESXi-based Virtual Management Server (VMS). See the “Virtual Management Server Disaster Recovery” chapter in the *Virtual Management Server Software User Guide*.
2. This step can be skipped, if only the VM needs to be recovered. Depending on your system configuration and the failure scenario, perform one of the following actions:
   - If your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server, add the PDG VM to the inventory. Perform the “Adding a Virtual Machine to the Inventory for Expansions” procedure in the *Virtual Management Server Software User Guide*.
   - If the PDG VM is on a dedicated VMS Host Server, or if your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server and the DAS is the device being replaced or the PDG VM itself needs to be reinstalled, recover the PDG VM. Go to step 4.
3. If a system has vCenter, then remove the failed network management server container from the vCenter application inventory. See “Removing Virtual Machines from the vCenter Inventory” in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
4. Satisfy all the appropriate requirements and review all the appropriate installation considerations before deploying the PDG virtual appliance. See Trunked PDG Software Installation –

Requirements and Considerations on page 56 and Conventional PDG Software Installation – Requirements and Considerations on page 74

5. Deploy the PDG virtual appliance to the virtual server. Perform the appropriate procedure for your system configuration:
   - To deploy the Trunked PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 57.
   - To deploy the Trunked PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Trunked PDG as a VM on a Dedicated VMS Host Server (DL380) on page 60.
   - To install the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380), see Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75
   - To install the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380), see Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380) on page 78
6. If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88
7. Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61.
8. Apply the supplemental configuration. See Applying Supplemental Configuration to Virtual Machines on page 63.
9. If required by your organizational policies, disable password aging on the PDG. See “Disabling Password Aging for the Root Account” in the *Unix Supplemental Configuration Setup Guide*.
10. Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.
11. Configure the PDG. See Configuring the Trunked PDG after Installation on page 66 and Configuring the Conventional PDG after Installation on page 84.
12. If applicable, perform Linux OS patching on the PDG. Installation procedures for the MOTOPATCH are available at: https://sites.google.com/a/motorolasolutions.com/susmotopatch/

    If you cannot open the link, this means that MOTOPATCH for RHEL v7 is not available yet. Skip this step.
13. If required by your organization’s policies, configure the PDG for SNMPv3 and SSH. For more information, see the *SNMPv3 Feature Guide* and *Securing Protocols with SSH Feature Guide*.

    Ask your system administrator which procedures and/or commands you should use, depending on your organization’s policies.
14. Join the PDG to an Active Directory domain. See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide*.
15. Apply the platform patch to the PDG. See Applying the Platform Patch on page 67.
16. Register the PDG as a BAR client. See “Registering and Enabling Linux BAR Clients” in the *Backup and Restore Services Feature Guide*.
17. Initiate restore of the backup data from the BAR server to the deployed virtual PDG. See “Executing a BAR Client Data Restore” in the *Backup and Restore Services Feature Guide*.
18. Restore operation at the PDG. See Restoring the PDG on page 257.

    The backup data includes:

- Database backup
- SSH configuration backup
- SNMPv3 credentials backup
- HA keys
- For Conventional: CDEM IP Address

19 Synchronize the PDG databases from Unified Network Configurator (UNC). PDG databases are automatically synchronized by the Network Manager. To synchronize databases manually, see the “Publishing Infrastructure Data to the PM” procedure in the *Unified Network Configurator User Guide*.

20 If vCenter is installed and configured:

a Perform the "Enabling Legacy Fault Tolerance Mode" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide*.

b Perform the "Enabling Fault Tolerance on a Virtual Machine" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide*.

21 Set the PDG to the active or standby state.

- To set the PDG to the active state, see Setting the Trunked PDG to the Active State (DSR) on page 162.
- To set the PDG to the standby state, see Setting the Trunked PDG to the Standby State (DSR) on page 163.
- To set the Conventional PDG to the active state, see Setting the Conventional PDG to the Active State (DSR) on page 176
- To set the Conventional PDG to the standby state, see Setting the Conventional PDG to the Standby State (DSR) on page 177

15.1.2
Recovering the Backup Packet Data Gateway in DSR Systems

In a system with Dynamic System Resilience (DSR), if the backup Packet Data Gateway (PDG) goes out of service, it does not cause interruptions to the data service when the Primary PDG is in the active state.

When and where to use:
Perform this procedure to recover the backup PDG for normal DSR functionality of the ASTRO® 25 data subsystem.

Process:

1 This step can be skipped, if only the VM needs to be recovered. Recover the ESXi-based Virtual Management Server (VMS). See the “Virtual Management Server Disaster Recovery” chapter in the *Virtual Management Server Software* manual.

2 This step can be skipped, if only the VM needs to be recovered. Depending on your system configuration and the failure scenario, perform one of the following actions:

- If your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), add the PDG VM to the inventory. Perform the “Adding a Virtual Machine to the Inventory for Expansions” procedure in the *Virtual Management Server Software* manual.
- If the PDG VM is on a dedicated VMS Host Server (DL380), or if your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server and the DAS is the device being replaced or the PDG VM itself needs to be reinstalled, recover the PDG VM. Go to step 4.

3 If a system has vCenter, then remove the failed network management server container from the vCenter application inventory. See “Removing Virtual Machines from the vCenter Inventory” in the *ASTRO 25 vCenter Application Setup and Operations Guide*.

4 Satisfy all the appropriate requirements and review all the appropriate installation considerations before deploying the PDG virtual appliance. See Trunked PDG Software Installation – Requirements and Considerations on page 56 and Conventional IVD M Core and K Core PDG Installation on page 73.

5 Deploy the PDG virtual appliance to the virtual server. Perform the appropriate procedure for your system configuration:

- To deploy the Trunked PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 57.
- To deploy the Trunked PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Trunked PDG as a VM on a Dedicated VMS Host Server (DL380) on page 60.
- To install the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380), see Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75
- To install the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380), see Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380) on page 78

6 If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88

7 Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61

8 Apply the supplemental configuration. See Applying Supplemental Configuration to Virtual Machines on page 63.

9 If required by your organizational policies, disable password aging on the PDG. See “Disabling Password Aging for the Root Account” in the *Unix Supplemental Configuration Setup Guide*.

10 Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.

11 Configure the PDG. See Configuring the Trunked PDG after Installation on page 66 and Configuring the Conventional PDG after Installation on page 84.

12 Join the PDG to an Active Directory domain. See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide*.

13 Apply the platform patch to the PDG. See Applying the Platform Patch on page 67.

14 Register the PDG as a BAR client. See “Registering and Enabling Linux BAR Clients” in the *Backup and Restore Services Feature Guide*.

15 Initiate restore of the backup data from the BAR server to the deployed virtual PDG. See “Executing a BAR Client Data Restore” in the *Backup and Restore Services Feature Guide*.

16 Restore operation at the PDG. See Restoring the PDG on page 257.

The backup data includes:

- Database backup
- SSH configuration backup
- SNMPv3 credentials backup

- HA keys
- For Conventional: CDEM IP Address

17 Synchronize the PDG databases from Unified Network Configurator (UNC). PDG databases are automatically synchronized by the Network Manager. If you want to synchronize databases manually, see the “Publishing Infrastructure Data to the PM” procedure in the *Unified Network Configurator User Guide*.

18 If vCenter is installed and configured:

a Perform the "Enabling Legacy Fault Tolerance Mode" procedure from the *ASTRO25 vCenter Application Setup and Operations Guide*.

b Perform the "Enabling Fault Tolerance on a Virtual Machine" procedure from the *ASTRO25 vCenter Application Setup and Operations Guide*.

19 Put the PDG in the standby state.

- To set the Trunked PDG to the standby state, see Setting the Trunked PDG to the Standby State (DSR) on page 163.
- To set the Conventional PDG to the standby state, see Setting the Conventional PDG to the Standby State (DSR) on page 177.

15.2
Recovery Sequence for the Packet Data Gateway in Non-DSR Systems

The Dynamic System Resilience (DSR) feature is optional for the Trunked IV&D and HPD PDG. To recover the PDG in a system without DSR, perform the procedure that is appropriate for your PDG type.

15.2.1
Recovering the Trunked IVD and/or HPD PDG in Non-DSR Systems

When and where to use:
Perform this procedure to recover the Trunked IV&D and/or HPD Packet Data Gateways (PDG) in a system without Dynamic System Resilience (DSR).

Process:

1 This step can be skipped, if only the VM needs to be recovered. Recover the ESXi-based Virtual Management Server (VMS). See the “Virtual Management Server Disaster Recovery” chapter in the *Virtual Management Server Software User Guide*.

2 This step can be skipped, if only the VM needs to be recovered. Depending on your system configuration and the failure scenario, perform one of the following steps:

- If your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), add the PDG VM to the inventory. Perform the “Adding a Virtual Machine to the Inventory for Expansions” procedure in the *Virtual Management Server Software User Guide*.
- If the PDG VM is on a dedicated VMS Host Server (DL380), or if your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server and the DAS is the device being replaced or the PDG VM itself needs to be reinstalled, recover the PDG VM. Go to step 4.

3 If a system has vCenter, then remove the failed network management server container from the vCenter application inventory. See “Removing Virtual Machines from the vCenter Inventory” in the *ASTRO 25 vCenter Application Setup and Operations Guide* manual.

4 Satisfy all the appropriate requirements and review all the appropriate installation considerations before deploying the PDG virtual appliance. See Trunked PDG Software Installation – Requirements and Considerations on page 56 in the *Packet Data Gateways Feature Guide*.

5 Deploy the PDG virtual appliance to the virtual server. Perform the appropriate procedure for your system configuration:

   - To deploy the Trunked PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Trunked PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 57 in the *Packet Data Gateways Feature Guide*.
   - To deploy the Trunked PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Trunked PDG as a VM on a Dedicated VMS Host Server (DL380) on page 60 in the *Packet Data Gateways Feature Guide*.

6 If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88

7 Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61

8 Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.

9 Configure the PDG. See Configuring the Trunked PDG after Installation on page 66 in the *Packet Data Gateways Feature Guide*.

10 Join the PDG to an Active Directory domain. See “Joining a Linux-Based Device to the Domain” in the *Authentication Services Feature Guide*.

11 Apply the platform patch to the PDG. See Applying the Platform Patch on page 67.

12 Register the PDG as a BAR client See “Registering and Enabling Linux BAR Clients” in the *Backup and Restore Services Feature Guide*.

13 Initiate restore of the backup data from the BAR server to the deployed virtual PDG. See “Executing a BAR Client Data Restore” in the *Backup and Restore Services Feature Guide*.

14 Restore operation at the PDG. See Restoring the PDG on page 257 in the *Packet Data Gateways Feature Guide*.

   The backup data includes:

   - Database backup
   - SSH configuration backup
   - SNMPv3 credentials backup

15 Synchronize the PDG databases from Unified Network Configurator (UNC). PDG databases are automatically synchronized by the Network Manager. To synchronize databases manually, see the Publishing Infrastructure Data to the PM” in the *Unified Network Configurator User Guide*.

16 If vCenter is installed and configured:

   a Perform the "Enabling Legacy Fault Tolerance Mode" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide* manual.

   b Perform the "Enabling Fault Tolerance on a Virtual Machine" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide* manual.

17 Set the PDG to the active state. See Changing the Trunked PDG State to Active in Non-DSR Systems on page 68 in the *Packet Data Gateways Feature Guide*.

15.2.2 Recovering the Conventional IVD M Core PDG

Process:

1. This step can be skipped, if only the VM needs to be recovered. Recover the ESXi-based Virtual Management Server (VMS). See the "Virtual Management Server Disaster Recovery" chapter in the *Virtual Management Server Software User Guide*.
2. This step can be skipped, if only the VM needs to be recovered. Depending on your system configuration and the failure scenario, perform one of the following actions:
   - If your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), add the PDG VM to the inventory. Perform the "Adding a Virtual Machine to the Inventory for Expansions" procedure in the *Virtual Management Server Software User Guide*.
   - If the PDG VM is on a dedicated VMS Host Server (DL380), or if your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server and the DAS is the device being replaced or the PDG VM itself needs to be reinstalled, recover the PDG VM. Go to step 4.
3. If a system has vCenter, then remove the failed network management server container from the vCenter application inventory. See "Removing Virtual Machines from the vCenter Inventory" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
4. Satisfy all the appropriate requirements and review all the appropriate installation considerations before deploying the PDG virtual appliance. See Conventional PDG Software Installation – Requirements and Considerations on page 74 in the *Packet Data Gateways Feature Guide*.
5. Deploy the PDG virtual appliance to the virtual server. Perform the appropriate procedure for your system configuration:
   - To deploy the Conventional PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75 in the *Packet Data Gateways Feature Guide*.
   - To deploy the Conventional PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380) on page 78 in the *Packet Data Gateways Feature Guide*.
6. If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88
7. Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61
8. Configure the time zone on the PDG. See "Configuring the Time Zone on Linux Servers" in the *Unix Supplemental Configuration Setup Guide*.
9. Configure the PDG. See Configuring the Conventional PDG after Installation on page 84 in the *Packet Data Gateways Feature Guide*.
10. Join the PDG to an Active Directory domain. See "Joining a Linux-Based Device to the Domain" in the *Authentication Services Feature Guide*.
11. Apply the platform patch to the PDG. See Applying the Platform Patch on page 86.
12. Register the PDG as a BAR client. See "Registering and Enabling Linux BAR Clients" in the *Backup and Restore Services Feature Guide*.
13. Initiate restore of the backup data from the BAR server deployed virtual PDG. See "Executing a BAR Client Data Restore" in the *Backup and Restore Services Feature Guide*.

14 Restore operation at the PDG. See Restoring the PDG on page 257 in the *Packet Data Gateways Feature Guide*.

The backup data includes:

- Database backup
- SSH configuration backup
- SNMPv3 credentials backup
- CDEM IP address

15 Synchronize the PDG databases. For the Conventional IV&D M core PDG, the PDG databases are automatically synchronized by the Network Manager. If you want to synchronize databases manually, see the “Publishing Infrastructure Data to the PM” procedure in the *Unified Network Configurator User Guide*.

16 If vCenter is installed and configured:

a Perform the "Enabling Legacy Fault Tolerance Mode" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide*.

b Perform the "Enabling Fault Tolerance on a Virtual Machine" procedure from the *ASTRO 25 vCenter Application Setup and Operations Guide*.

17 Set the PDG to the active state. See Changing the Conventional PDG State to Active on page 87 in the *Packet Data Gateways Feature Guide*.

15.2.3

Recovering the Conventional IVD K Core PDG

Process:

1 Recover the ESXi-based Virtual Management Server (VMS). See the “Virtual Management Server Disaster Recovery” chapter in the *Virtual Management Server Software User Guide*.

2 Depending on your system configuration and the failure scenario, perform one of the following actions:

- If your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), add the PDG VM to the inventory. Perform the “Adding a Virtual Machine to the Inventory for Expansions” procedure in the *Virtual Management Server Software User Guide*.
- If the PDG VM is on a dedicated VMS Host Server (DL380), or if your system employs the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server and the DAS is the device being replaced or the PDG VM itself needs to be reinstalled, recover the PDG VM. Go to step 3.

3 Satisfy all the appropriate requirements and review all the appropriate installation considerations before deploying the PDG virtual appliance. See Conventional PDG Software Installation – Requirements and Considerations on page 74 in the *Packet Data Gateways Feature Guide*.

4 Deploy the PDG virtual appliance to the virtual server. Perform the appropriate procedure for your system configuration:

- To deploy the Conventional PDG in a system employing the Common Server Architecture (CSA) where the PDG VM is incorporated with other VMs on a VMS Host Server (DL380), perform Installing the Conventional PDG as a VM Incorporated with Other VMs on a VMS Host Server (DL380) on page 75 in the *Packet Data Gateways Feature Guide*.
- To deploy the Conventional PDG in a system where the PDG VM is on a dedicated VMS Host Server (DL380), perform Installing the Conventional PDG as a VM on a Dedicated VMS Host Server (DL380) on page 78 in the *Packet Data Gateways Feature Guide*.

5 If vCenter is already installed in the system, follow Configuring the vCenter for the Newly Deployed VM on page 88

6 Set the correct start up/shut down order. See Setting the Virtual Machine Startup and Shutdown Order on page 61

7 Configure the time zone on the PDG. See “Configuring the Time Zone on Linux Servers” in the *Unix Supplemental Configuration Setup Guide*.

8 Configure the PDG. See Configuring the Conventional PDG after Installation on page 84 in the *Packet Data Gateways Feature Guide*.

9 Apply the platform patch to the PDG. See Applying the Platform Patch on page 86.

10 Transfer the PDR database backup file that was created before the failure to the newly deployed PDG virtual machine. See Transferring a Backup File to a Conventional IVD PDG (K Core) on page 186 in the *Packet Data Gateways Feature Guide*.

The file is transferred from another computer as described in the backup section.

11 Stop the PDR application software. See Stopping the Conventional PDR on page 182 in the *Packet Data Gateways Feature Guide*.

12 Restore the PDG database. See Restoring the PDG on page 257 in the *Packet Data Gateways Feature Guide*.

The backup data includes:

- Database backup
- SSH configuration backup
- SNMPv3 credentials backup
- CDEM IP address
- NTP IP address
- User accounts (user folders and passwords)

13 Start the PDR application. See Starting the Conventional PDR on page 181 in the *Packet Data Gateways Feature Guide*.

14 Synchronize the PDG databases. To provision the Conventional IV&D K core PDG with the necessary configuration and to push the full mobile device configuration using the Configuration Manager – Conventional application, see Conventional IVD K Core PDG Configuration on page 261 in the *Packet Data Gateways Feature Guide*

For the Conventional IV& K core PDG, the database is not synchronized using the Unified Network Configurator (UNC). It is configured using the Command Line Interface and the Configuration Manager – Conventional application.

15 Set the PDG to the active state. See Changing the Conventional PDG State to Active on page 87 in the *Packet Data Gateways Feature Guide*.

16 After the system is successfully installed, make sure to back up the PDG database on a regular basis. See Backing Up a Conventional IVD PDG in a K Core on page 184 in the *Packet Data Gateways Feature Guide*.

15.3

Restoring the PDG

Perform this procedure for disaster recovery purposes to restore a Packet Data Router (PDR) database backup file that was created on the current release Packet Data Gateway (PDG) automatically by the Backup and Restore (BAR) server (in L and M cores) or manually (in a K core).

NOTICE: The following points describe the PDR behavior before, during, and after the restore operation:

- PDR backs up the current configuration and database before the restore operation starts. If the restore operation fails, the PDR can revert back to the previous working configuration and database.
- If the PDR is not running when you select the restore option, the PDR is started to back up the current configuration and database, and stopped before the restore operation.
- During the restore operation, the PDR is stopped. If the PDR is running before the restore operation, it is automatically started after the operation. If the PDR is not running before the restore operation, it remains stopped after the operation.

Procedure:

1. Log on to the PDG using the credentials for a user account that belongs to the Install Administrator or Platform Administrator group.

   The user's command prompt appears.

2. Perform the following actions to switch the user to root:

   a. At the login prompt type `su -` and press Enter.

   b. At the password prompt, type the root password and press Enter.

3. At the prompt, type `ls /opt/Motorola/backup/` and press Enter.

   If your system has a BAR server (L or M core), the following file appears: `pdr_backup_bar_client.zip`. If your system does not have a BAR server (K core), the following file appears: `pdr_backup_`***`<date>`***`_`***`<time>`***`.zip`.

4. Type `admin_menu` and press Enter.

5. From the main PDG administration menu, select **Backup and Restore Administration** and press Enter.

6. From the **Backup and Restore Administration** menu, select **Post Restore Operations** and press Enter.

7. From the **Post Restore Operations** menu, select **Restore All Critical Data** and press Enter.

   If your system has a BAR server (L or M core), the restore operation starts. When the restore operation is completed, a confirmation message appears.

8. **Systems without a BAR server (K cores)**: Select a backup file that you want to restore.

   The restore operation starts. When the restore operation is completed, a confirmation message appears.

9. To exit from the main PDG administration menu, type `q` and press Enter.

   The user's command prompt appears.

10. To log out of the PDG, type `exit` and press Enter.

15.4 Restoring the PDG Database in the L and M Core

Prerequisites: Copy the archived PDR database backup file from a storage computer to the PDG Backup Archive Directory or restore the database to the PDG from the Backup and Restore (BAR) server.

IMPORTANT: Stop the PDR application so it is not actively providing Packet Data Services **before** you perform the restore procedure. If the PDR is active at the time of execution of the procedure, the procedure notifies you of the active status, and asks whether you want to stop the PDR. If you approve, the procedure stops the PDR and continues with the restoration activities. To verify the status of the PDR application, see Verifying the Trunked PDR and RNG Status on page 165. To stop the PDR application, see Stopping the Trunked PDR on page 168.

When and where to use:
The following procedure restores a previously saved copy of the PDR database from the PDG Backup Archive Directory.

CAUTION: Executing this procedure results in a temporary loss of data messaging.

NOTICE: For the recovery process for the PDG, see Packet Data Gateway Disaster Recovery on page 249 in the *Packet Data Gateways Feature Guide*.

Procedure:

1. Log on to the PDG and invoke the Main Menu. See Logging On to the Trunked PDG and Invoking the Main Menu on page 161 in the *Packet Data Gateways Feature Guide*.
2. Type the number associated with **Application Administration** and press Enter.
3. In the **Application Administration** menu, type the number associated with **Application Specific Management and Operations** and press Enter.
4. In the **Application Specific Management and Operations** menu, type the number associated with **PDR Specific Management and Operations** and press Enter.
5. In the **PDR Specific Management and Operations** menu, type the number associated with **Restore Database** and press Enter.

   The PDR Backup File list appears.
6. Type the number of the backup file to restore and press Enter.

   When the backup is restored, the following message appears:

   ```
   <Current Date and Time>
   PDR database restore of pdrdb_<date>_<time>.zip completed ....
   ```
7. To start the PDR, perform Starting the Trunked PDR on page 168 in the *Packet Data Gateways Feature Guide*.

This page intentionally left blank.

Appendix A

Conventional IVD K Core PDG Configuration

For the Conventional IV&D K core PDG, the database is not synchronized using Unified Network Configurator (UNC). You need to configure it using the Command Line Interface and the Configuration Manager – Conventional application.

To provision the Conventional IV&D K core PDG with the necessary configuration and to push the full mobile device configuration using the Configuration Manager – Conventional application.

NOTICE: The term “Express” may be used in software or firmware to configure the Conventional IV&D K core PDG in an ASTRO® 25 Conventional with Integrated Data system.

Configure the Conventional IV&D K core PDG as follows:

- PDG system configuration – using the pdgconf Command Line Interface (CLI).
- Mobile device configuration – using the Configuration Manager – Conventional application.

A.1 Conventional IV&D K Core PDG Configuration with the pdgconf Command Line Interface (CLI)

After you have installed the Conventional IV&D K core PDG (see Deploying the Conventional PDG Virtual Appliance on page 73), you need to provision the PDG with the system configuration.

The basic configuration includes the following PDG scalar and tables:

- **pdgZone**
- **pdrGGSNListTable**
- **pdgUnCnfMsgFilterTable**
- **pdrGGSNMapTable**
- **pdrConventionalSitesTable**
- **pdrConventionalChannelsTable**

If you want to use encrypted inbound and outbound data call, set also the following tables:

- **pdrConventionalKeyManagementFacilityTable**
- **pdrConventionalCAIDataEncryptionModuleTable**

Use the CLI to set the PDG system values into the PDG according to the system architecture. For details on how to use the CLI, see Conventional IVD K Core PDG Configuration – Command Reference on page 265.

A.1.1 Conventional IV&D K Core PDG Configuration with the pdgconf Command Line Interface (CLI) – Example

The following is an example of the PDG configuration using the CLI.

NOTICE: This example reflects a system with one GGSN and one site with two channels. The pdgZone needs to be modified to fit the correct values. Since the pdgZone is created by default, you do not need to create it first. In this example, the KMF and CDEM are also set. See Conventional IVD K Core PDG Configuration – Command Reference on page 265 for specific values to select.

Set the CLI flag to 1 (this is a necessary pre-action before starting the configuration):

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrExpressConventionalCLISyncDB -
id 0 pdrExpressConventionalCLISyncDBSyncFlag=1"
```

Create the GGSN-List and Map tables:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNListTable -id 1.1"
  ```

  NOTICE: The **-id 1.1** means that you create a **pdrGGSNListTable** entry with **pdrGGSNListId** equal to **1**, and **pdrGGSNListZoneId** equal to **1**. The **pdrGGSNListTable** is a double key table (table with two keys **pdrGGSNListId** and **pdrGGSNListZoneId**), so the first **1** represents the first key, and the second **1** represents the second one, respectively.

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNMapTable -id 1
  pdrGGSNApn=cen17pdg.default-op.gprs pdrGGSNId=1 pdrGGSNZoneId=1"
  ```

  NOTICE: The **-id 1** means that you create a **pdrGGSNMapTable** entry with **pdrGGSNIndex** equal to **1**. The **pdrGGSNMapTable** is a one key table (table with one key **pdrGGSNIndex**), so **1** represents the **pdrGGSNIndex**. The pdrGGSNApn value depends on the TNCT configuration.

Modify the pdgZone:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrStandbyTimer=3600"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrAPNOperatorId=default-op.gprs"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrSNDCPQueueDwellTime=25"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrGtpT3Timeout=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrGtpN3Attempts=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0 pdrLLCTimer=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrLLCMaxAttempts=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrMccSystemId=1"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0 pdrMncWacn=1"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrBcastDataCapable=2"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrTxBeforeRadioFinderAttempts=3"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrTxRadioFinderAttempts=3"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrHostStatusInterval=600"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrChannelRequestAttempts=6"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrChannelWaitTimer=4000"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrScanSuspendTimer=3"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrUnicastScanPreambleDuration=1000"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrKeepAliveTimeOTEKPeriod=29"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrOTARAvailabiltyIndicationsEnabled=2"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrCDEMTCPPort=49166"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrBcastScanPreambleDuration=10"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrDecryptionErrorsEnabled=2"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrMaximumOTARRegistrationDelay=480"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrInterBcastDataDelay=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrBcastSNDCPQueueDwellTime=120"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrBcastBlockSize=15"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
  pdrBcastTimeSensSNDCPQueueDwellTime=5"
  ```

NOTICE: To modify the **pdgZone**, always use **-id 0**. This is because the **pdgZone** is a scalar and not a table, and has no key.

Create the KMF and CDEM tables:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc
  pdrConventionalKeyManagementFacilityTable -id 10
  pdrOTEKServicePortNumber=64420 pdrOTARServicePortNumber=64410
  pdrCENKMFIPAddress=0A0B0C0D
  pdrKMFFullyQualifiedDomainName=KMF01.cen1.zone1 pdrKMFRSI=1"
  ```

  NOTICE: The **–id 10** means that you create a KMF entry with **pdrKMFId** equal to **10** (**pdrKMFId** is the key for this table).

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc
  pdrConventionalCAIDataEncryptionModuleTable -id 1 pdrOTEKKMFId=10
  pdrOTEKTransmitSecurityLevel=1 pdrOTEKReceiveSecurityLevel=1
  pdrOTEKInactivityTimePeriod=1"
  ```

  NOTICE: The **–id 1** means that you create a **CDEM** entry with **pdrCDEMId** equal to **1** (**pdrCDEMId** is the key for this table).

IMPORTANT: The CDEM must be associated with the KMF. In this example, the **pdrOTEKKMFId=10** represents this association.

Create the Site and Channel tables:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id
  2003"
  ```

  NOTICE: The **–id 2003** means that you create an entry with **pdrConventionalSitesSiteId** equal to **2003**.

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -
  id 2003.1 pdrConventionalChannelsDataConventionalChannelMode=1
  pdrConventionalChannelsVoteScanEnable=1"
  ```

  NOTICE: The **–id 2003.1** means that you create a Channel with **pdrConventionalChannelsChannelId** equal to 1, and this channel is associated with site 2003. The **pdrConventionalChannelsTable** is a double key table (table with two keys **pdrConventionalChannelsSiteId** and **pdrConventionalChannelsChannelId**), so the first **2003** represents the first key and the second **1** represents the second one.

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -
  id 2003.2 pdrConventionalChannelsDataConventionalChannelMode=1
  pdrConventionalChannelsVoteScanEnable=2"
  ```

Set the CLI flag to 0 (this is a necessary post-action after finishing the configuration):

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrExpressConventionalCLISyncDB -
id 0 pdrExpressConventionalCLISyncDBSyncFlag=0"
```

A.2

Conventional IV&D K Core PDG Configuration with the Configuration Manager – Conventional Application

Once you have provisioned the Conventional IV&D K core PDG with the system configuration, you need to provision the PDG with the mobile device information, using the Configuration Manager – Conventional application. For information on how to use the Configuration Manager, see the *Configuration Manager for Conventional Systems User Guide*.

For information on how to display mobile device information, see the following sections:

- Displaying Mobile Device Information on the Conventional PDG on page 132
- Generating a Device Summary Report on the Conventional PDG on page 133

Appendix B

Conventional IVD K Core PDG Configuration – Command Reference

NOTICE: The term “Express” may be used in software or firmware to configure the Conventional IV&D K core PDG in an ASTRO® 25 Conventional with Integrated Data system.

Log on to the PDG as a root or pdg_mgr user and provision the Conventional IV&D K core PDG by using commands described in this Appendix.

The basic commands are:

- `pdgconf settime` – for changing the session timeout (by default, the session timeout is 60 minutes)
- `pdgconf show` – for viewing the configuration (all the attributes or the selected ones)
- `pdgconf create` – for creating a new table or an entity in the table
- `pdgconf modify` – for modifying the configured or default non-mandatory parameters
- `pdgconf delete` – for deleting the configured parameters
- `pdgconf retry` – for retrying the already provisioned configuration
- `pdgconf abort` – for aborting the configuration provisioning at any time

NOTICE: There are no mandatory attributes for the `pdgconf modify` command.

The Conventional IV&D K core PDG provisioning commands should be used to initialize the PDR configuration, as well as for partial configuration, which can be required for changing some system parameters.

For the initial Conventional IV&D K core PDG configuration, make sure the parameters configured in the CLI for Conventional sites, Conventional channels, KMF, and GGSN are consistent with the PDG parameters. Verify if a KMF and/or a CDEM exist in the system. If the KMF exists, then one entry in **pdrConventionalKeyManagementFacilityTable** should be configured. If the CDEM exists, then one entry in the **pdrConventionalCAIDataEncryptionModuleTable** should be configured with pdrOTEKKMFId = 0 (if no KMF exists in the system), or with the KMF ID from the KMF table.

All the other tables always exist and should be provisioned:

- **pdrGGSNListTable**, **pdrGGSNMapTable** for each GGSN
- **pdrConventionalSitesTable** for Conventional Sites
- **pdrConventionalChannelsTable** for Conventional Channels
- **pdgUnCnfMsgSrcIP** may be provisioned for GGSN
- **pdgZone** parameters different from defaults should be set

IMPORTANT:

- Before provisioning the configuration, set the pdrExpressConventionalCLISyncDB flag to 1. Use the following command:

  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc
  pdrExpressConventionalCLISyncDB -id 0
  pdrExpressConventionalCLISyncDBSyncFlag=1"
  ```

- After provisioning the configuration, set the pdrExpressConventionalCLISyncDB flag to 0. Use the following command:

  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc
  pdrExpressConventionalCLISyncDB -id 0
  pdrExpressConventionalCLISyncDBSyncFlag=0"
  ```

For the partial Conventional IV&D K Core PDG configuration, only the entries/tables which are to be updated should be provisioned. For example, the KMF and/or CDEM entry may be added or deleted, a Conventional Channel or Site may be added, deleted, or modified, or the pdgZone parameters may change.

The following PDR scripts should not be run simultaneously with the `pdgconf` command:

- `backup_pdrdb`
- `create_pdrdb`
- `recover_pdrdb`
- `restart_pdg`
- `restore_pdrdb`
- `start_pdg`
- `start_pdr`
- `stop_pdg`
- `stop_pdr`
- `pdgconf`
- `update_ntp_info`

IMPORTANT:
If you run the `pdgconf` command while any of the scripts is running, the `PDR_OPERATION_BUSY` message is returned.

The PDR must be running for the configuration to be provisioned. If you run the `pdgconf` command when the PDR is not running, the `PDR_NOT_RUNNING` message is returned.

B.1

pdgconf Command Line Interface Overview

Pdgconf Command Line Interface (CLI) is a command line-based application. The application engine consists of two parts: pdgconf PDG script and MotoManagement CLI. Only one PDG user can provision the configuration through the pdgconf CLI at a time.

The following objects should be provisioned through CLI:

- **pdgZone**
- **pdrExpressConventionalCLISyncDB**
- **pdrGGSNListTable**
- **pdrGGSNMapTable**

- **pdgUnCnfMsgFilterTable**
- **pdrConventionalKeyManagementFacilityTable**
- **pdrConventionalCAIDataEncryptionModuleTable**
- **pdrConventionalSitesTable**
- **pdrConventionalChannelsTable**

The following scalar objects are show-only:

- **pdgGGSNList**
- **pdgGGSNMap**
- **pdgUnCnfMsgFilter**
- **pdgConventionalKeyManagementFacility**
- **pdgConventionalCAIDataEncryptionModule**
- **pdgConventionalSites**
- **pdgConventionalChannels**

B.2 System and Zone Parameters Configuration

pdgZone is a group of scalar variables that includes System and Zone parameters. Only one pdgZone object instance always exists.

B.2.1 System and Zone Parameters Configuration – Viewing

To view the System and Zone Parameters configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] –moc pdgZone [-id 0 [ATTR-LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`ATTR-LIST`: attribute 1, attribute 2...

Default: all attributes are returned

The following attributes can be used in the `pdgconf show` command:

- **pdrStandbyTimer**
- **pdrZoneId**
- **pdrAPNOperatorId**
- **pdrNtpPrimary**
- **pdrNtpSecondary**
- **pdrSNDCPQueueDwellTime**
- **pdrGtpT3Timeout**
- **pdrGtpN3Attempts**
- **pdrLLCTimer**
- **pdrLLCMaxAttempts**

- **pdrPDRInstance**
- **pdrMccSystemId**
- **pdrMncWacn**
- **pdrPDGInstance**
- **pdrBcastDataCapable**
- **pdrGW1IPaddress**
- **pdrGW2IPaddress**
- **pdrPriBcastDataMulticastIpAddress**
- **pdrSecBcastDataMulticastIpAddress**
- **pdrTxBeforeRadioFinderAttempts**
- **pdrTxRadioFinderAttempts**
- **pdrHostStatusInterval**
- **pdrChannelRequestAttempts**
- **pdrChannelWaitTimer**
- **pdrScanSuspendTimer**
- **pdrUnicastScanPreambleDuration**
- **pdrKeepAliveTimeOTEKPeriod**
- **pdrOTARAvailabiltyIndicationsEnabled**
- **pdrCDEMTCPPort**
- **pdrBcastScanPreambleDuration**
- **pdrDecryptionErrorsEnabled**
- **pdrMaximumOTARRegistrationDelay**
- **pdrInterBcastDataDelay**
- **pdrBcastSNDCPQueueDwellTime**
- **pdrBcastTimeSensSNDCPQueueDwellTime**
- **pdrBcastBlockSize**

Examples of usage:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgZone"
```

To view the running pdrZoneId only:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgZone -id 0 pdrZoneId"
```

To view the entire pdgZone object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc pdgZone"
```

B.2.2
System and Zone Parameters Configuration – Modification

To modify the System and Zone Parameters configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0 ATTR-VALUE-LIST"
```

where:

`ATTR-VALUE-LIST:` attribute 1 = value 1, attribute 2 = value 2…, where attribute X is one of the moc non-MOI attributes from the following table.

Table 77: pdgZone Writable Attributes

Object Name	Description	Type	Format	Range/Values	Default
pdrStandby-Timer	Monitors the time an MSU can retain its context following the data service activity. Value in seconds.	INTE-GER	Decimal integer	3600, 7200, 14400, 28800, 43200, 86400, 172800, 259200	43200
pdrAPNOper-atorId	Access Point Name - Operator ID portion. Maximum length = 133 octets	OCTET STRIN G	Literal string, no “”	The string must end with “.gprs”. Maximum length = 133 octets (includes a terminating NULL character)	.gprs
pdrSNDCPQ ueueDwell-Time	How long a message is allowed to wait in the PDR outbound queue before it is discarded. Value in seconds.	INTE-GER	Decimal integer	15...120	25
pdrGtpT3Tim eout	Time interval between retries when delivering a signaling PDU to the GGSN. Value in seconds.	INTE-GER	Decimal integer	1...30	4
pdrGtpN3At-tempts	The maximum number of attempts when delivering a signaling PDU to the GGSN.	INTE-GER	Decimal integer	1...7	4
pdrLLCTimer	The number of seconds the RNG waits before retrying the message to the MSU. Value in seconds.	INTE-GER	Decimal integer	1...10	4
pdrLLCMax-Attempts	The number of times the RNG sends the same message to the MSU before giving up.	INTE-GER	Decimal integer	1-7	4
pdrMccSyste-mId	Defines identity of the system (mobile country code portion of tunnel ID)	INTE-GER	Decimal integer	1...4094	1
pdrMncWacn	Wide area communication network identifier (mobile network	INTE-GER	Decimal integer	1...1048574	1

Table continued…

Object Name	Description	Type	Format	Range/Values	Default
	code portion of tunnel ID).				
pdrBcastDataCapable	Indicates whether the broadcast data feature is enabled or disabled.1 - enable2 - disable	nmaEnable-Disable	Decimal integer	1...2	1
pdrTxBeforeRadioFinderAttempts	This field represents the maximum number of attempts to reach the radio before entering radio finder.	INTEGER	Decimal integer	1...6	3
pdrTxRadioFinderAttempts	This field is the maximum number of attempts to reach the radio while in the radio finder.	INTEGER	Decimal integer	2...6	3
pdrHostStatusInterval	How often, in seconds, the Host Status message is broadcast on ASTRO® 25 systems. Zero indicates never.	INTEGER	Decimal integer	0...600	0
pdrChannelRequestAttempts	This parameter defines the maximum number of times a channel can be requested in order to initiate an outbound data transaction. This value is used when the Conventional PDG needs to retry transmission of outbound data.	INTEGER	Decimal integer	1...22	15
pdrChannelWaitTimer	Defines the frequency with which the PDG requests a channel. This attribute can be incremented/decremented in 100 msec increments.	INTEGER	Decimal integer	1000...5000	1000
pdrScanSuspendTimer	It defines the amount of time the Conventional PDG expects a Conventional Unit to remain on the channel during an active data	INTEGER	Decimal integer	0...255	3

Table continued…

Object Name	Description	Type	Format	Range/Values	Default
	transaction. When the subscriber sends a confirmed data packet or an acknowledgement to the FNE, this timer is restarted.				
pdrUnicastScanPreambleDuration	It defines the amount of time the Unicast Scan Preamble is transmitted before the start of an outbound data transaction. This value is used when transmitting a data preamble to a Conventional Unit configured for scan operation. This attribute can be changed in 100 msec increments.	INTEGER	Decimal integer	0...10000	0
pdrKeepAliveTimeOTEKPeriod	It defines the frequency with which the PDG sends a keep alive message to the KMF to keep the RNI FW OTEK mappings active. Dependent on the RNI FW used.	INTEGER	Decimal integer	1...29	29
pdrOTARAvailabiltyIndicationsEnabled	It is used to inform the KMF that a Conventional Unit may be available for OTAR transactions.1 - enable2 - disable	nmaEnable-Disable	Decimal integer	1...2	2
pdrCDEMTCPPort	It defines the port number used to communicate to the CDEM.	INTEGER	Decimal integer	49166… 65535	49166
pdrBcastScanPreambleDuration	It defines the amount of time the Broadcast Scan Preamble is transmitted before the start of an outbound data transaction. This value is used when transmitting a data preamble to a Broadcast Conventional Unit configured for	INTEGER	Decimal integer	0...10000	0

Table continued…

Object Name	Description	Type	Format	Range/Values	Default
	scan operation. This attribute can be changed in 100 msec increments.				
pdrDecryptionErrorsEnabled	It defines if the PDR sends Decryption errors to the UEM (Unable to decrypt the message flag)1 - enable2 - disable	nmaEnable-Disable	Decimal integer	1...2	2
pdrMaximumOTARRegistrationDelay	Defines the maximum amount of time (in minutes) that Conventional PDG spaces the OTAR Registrations for Conventional Units that are designated as fixed location units.	INTEGER	Decimal integer	15, 30, 60, 120, 480, 1440, 4320, 10080	480
pdrInterBcastDataDelay	It determines how long the PDG waits between transmitting broadcast data to an agency. The parameter is in sec units.	INTEGER	Decimal integer	1...4	2
pdrBcastSND CPQueueDwellTime	It defines how long a broadcast message is allowed to wait in the PDR outbound queue (for high capacity agency) before it is discarded. Value in minutes.	INTEGER	Decimal integer	1...360	120
pdrBcastTimeSensSNDCPQue ueDwellTime	It defines how long a broadcast message is allowed to wait in the Conventional PDR outbound queue (for time sensitive agency) before it is discarded. Value is in seconds.	INTEGER	Decimal integer	1...120	5
pdrBcastBlockSize	It defines the maximum number of PDUs which is sent in a broadcast block. This does not apply to time sensitive Broadcast Data Agencies.	INTEGER	Decimal integer	1...15	15

Examples of usage:

To provision the pdrStandbyTimer attribute only:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
pdrStandbyTimer=86400"
```

To provision the pdrStandbyTimer and pdrBcastDataCapable attributes:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0
pdrStandbyTimer=86400 pdrBcastDataCapable=1"
```

B.3 Conventional IV&D K Core PDG SyncCLIDB Configuration

The pdrExpressConventionalCLISyncDB is a group of one scalar variable, which defines whether provisioning of some tables through the local MotoAgent CLI is in progress or not. A single instance of the pdrExpressConventionalCLISyncDB object always exists.

B.3.1 Conventional IV&D K Core PDG SyncCLIDB Configuration – Viewing

To view the Conventional IV&D K core PDG SyncCLIDB configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc
pdrExpressConventionalCLISyncDB [-id 0
[pdrExpressConventionalCLISyncDBSyncFlag]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

Examples of usage:

To view the entire running pdrExpressConventionalCLISyncDB object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrExpressConventionalCLISyncDB"
```

To view the entire pdgZone object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrExpressConventionalCLISyncDB"
```

B.3.2 Conventional IV&D K Core PDG SyncCLIDB Configuration – Modification

To modify the Conventional IV&D K core PDG SyncCLIDB configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrExpressConventionalCLISyncDB -
id 0 pdrExpressConventionalCLISyncDBSyncFlag=(0|1)"
```

where:

0 means syncCompleted; 1 means syncInProgress

Examples of usage:

After the CLI configuration provisioning is complete, enter:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrExpressConventionalCLISyncDB -
id 0 pdrExpressConventionalCLISyncDBSyncFlag=0"
```

B.4

GGSN List Configuration

You can use the `pdgconf show`, `pdgconf create`, and `pdgconf delete` commands.

B.4.1

GGSN List Configuration – Viewing

To view the GGSN List configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc pdrGGSNListTable [MOI
[GGSNListIpAddress]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry indexes, delimited by '.' in the following order: pdrGGSNListZoneId.pdrGGSNListId)

MOC readable attributes:

The `pdgconf show` command may show all or several of the following managed object class readable attributes:

- **pdrGGSNListId (MOI attribute)**
- **pdrGGSNListIpAddress**
- **pdrGGSNListZoneId (MOI attribute)**

Examples of usage:

To view the entire running pdrGGSNListTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrGGSNListTable"
```

To view the running pdrGGSNListIpAddress only, where pdrGGSNListId = 1 and pdrGGSNListZoneId = 3:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrGGSNListTable -id 3.1
pdrGGSNListIpAddress"
```

To view the entire pdrGGSNListTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrGGSNListTable"
```

To view the number of entries of the pdrGGSNListTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgGGSNList -id 0
pdgGGSNListNumOfEntries"
```

B.4.2

GGSN List Configuration – Creation

To create the GGSN List configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNListTable -id X.Y"
```

where:

X is the value of pdrGGSNListZoneId and Y is the value of pdrGGSNListId.

See the following table for the description of the attributes:

Table 78: pdrGGSNListTable Writable Attributes

Object Name	Description	Type	Format	Range/ Values	Default
pdrGGSNListId	GGSN identifier. Zero value is invalid. (MOI attribute – second index)	INTEGER	decimal integer	1...1	1
pdrGGSNListZoneId	Zone ID in which the GGSN resides physically (MOI attribute – first index)	INTEGER	decimal integer	1...7	none - this attribute is mandatory for the `pdgconf create` command

Examples of usage:

To initially provision the GGSN with configuration from Zone 3, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNListTable -id 3.1"
```

B.4.3

GGSN List Configuration – Deletion

To delete the GGSN List configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrGGSNListTable -id X.Y"
```

where:

X is the value of pdrGGSNListZoneId and Y is the value of pdrGGSNListId.

See Table 78: pdrGGSNListTable Writable Attributes on page 275 for the description of the attributes.

Examples of usage:

To change the GGSN the PDG is working with from Zone 3 to Zone 2, use the following commands:

- `/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrGGSNListTable -id 3.1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNListTable -id 2.1"`

B.5

GGSN Map Configuration

You can use the `pdgconf show`, `pdgconf create`, `pdgconf modify`, and `pdgconf delete` commands.

B.5.1

GGSN Map Configuration – Viewing

To view the GGSN Map configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc pdrGGSNMapTable [MOI
[ATTR-LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry index - pdrGGSNIndex)

`ATTR-LIST`: attribute 1, attribute 2…

Default: all attributes are returned

The MOI (table index - pdrGGSNIndex) attribute is not supported in the ATTR-LIST.

MOC readable attributes:

The `pdgconf show` command may show all or several of the following managed object class readable attributes:

- **pdrGGSNIndex (MOI attribute)**
- **pdrGGSNApn**
- **pdrGGSNId**
- **pdrGGSNZoneId**

Examples of usage:

To view the entire running pdrGGSNMapTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrGGSNMapTable"
```

To view the running pdrGGSNApn only, where pdrGGSNIndex =2:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrGGSNMapTable -id 2 pdrGGSNApn"
```

To view the entire pdrGGSNMapTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc pdrGGSNMapTable"
```

To view the number of entries of the pdrGGSNMapTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgGGSNMap -id 0
pdgGGSNMapNumOfEntries"
```

B.5.2
GGSN Map Configuration – Creation

To create the GGSN Map configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNMapTable MOI ATTR-VALUE-
LIST"
```

where:

`MOI`: -id (table entry index – the value of pdrGGSNIndex attribute)

`ATTR-VALUE-LIST`: attribute 1 = value …

NOTICE: The MOI (table index - pdrGGSNIndex) attribute is not supported in the ATTR-VALUE-LIST.

See the following table for the description of all the writable attributes:

Table 79: pdrGGSNMapTable Writable Attributes

Object Name	Description	Type	Format	Range/ Values	Default
pdrGGSNIndex	The GGSN table index. Its value uniquely identifies a combination of pdrGGSNApn and	INTEGER	Decimal integer	1...10	none - this attribute is mandatory for the `pdgconf`

Table continued…

Object Name	Description	Type	Format	Range/ Values	Default
	pdrGGSNId and pdrGGSNZoneId (MOI attribute).				`create` command
pdrGGSNApn	The Access Point Name for the GGSN. Comprised of two components: NetworkId and OperatorId.	OCTET STRING	Literal string, no “”.		none - this attribute is mandatory for the `pdgconf create` command
pdrGGSNId	ID of the GGSN for which the APN corresponds to.	INTEGER	Decimal integer	1	none - this attribute is mandatory for the `pdgconf create` command
pdrGGSNZoneId	Zone ID of the GGSN to which the APN corresponds to.	INTEGER	Decimal integer	1...7	none - this attribute is mandatory for the `pdgconf create` command

NOTICE: All the writable non-MOI attributes which do not have defaults should be included in ATTR-VALUE-LIST in the `pdgconf create` command.

B.5.3
GGSN Map Configuration – Modification

To modify the GGSN Map configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrGGSNMapTable MOI ATTR-VALUE-
LIST"
```

where:

`MOI`: -id (table entry index – the value of pdrGGSNIndex attribute)

`ATTR-VALUE-LIST`: attribute 1 = value …

NOTICE: The MOI (table index - pdrGGSNIndex) attribute is not supported in the ATTR-VALUE-LIST.

See Table 79: pdrGGSNMapTable Writable Attributes on page 276 for the description of all the writable attributes.

NOTICE: The `pdgconf modify` command is not applicable to the MOI attribute (table index – pdrGGSNIndex).

B.5.4
GGSN Map Configuration – Deletion

To delete the GGSN Map configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrGGSNMapTable -id X"
```

where:

X is the value of the pdrGGSNIndex. See Table 79: pdrGGSNMapTable Writable Attributes on page 276 for the description of the pdrGGSNIndex.

Examples of usage for the`pdgconf create`, `pdgcong modify`, and `pdgconf delete`**commands:**

To initially provision the GGSN with index 2, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNMapTable -id 2 pdrGGSNApn
=APN.gprs pdrGGSNId =1 pdrGGSNZoneId=3"
```

To change the GGSN the PDG is working with from Zone 3 to Zone 2 (and change the index from 2 to 4), use the following commands:

- `/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrGGSNMapTable -id 2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNMapTable -id 4 pdrGGSNApn =newAPN.gprs pdrGGSNId =1 pdrGGSNZoneId=2"`

To change the APN PDG, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrGGSNMapTable -id 4 pdrGGSNApn
=otherAPN.gprs"
```

B.6 Unconfirmed Outbound Message Filter Table Configuration

Follow the initial provisioning and modifying configuration rule: if an entry of pdrGGSNMapTable should be deleted, then the corresponding pdgUnCnfMsgFilterTable entries (with pdgUnCnfMsgGGSNIndex = pdrGGSNIndex) should be also deleted.

B.6.1 Unconfirmed Outbound Message Filter Table Configuration – Viewing

To view the Unconfirmed Outbound message filter table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc pdgUnCnfMsgFilterTable
[MOI [ATTR- LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry indexes, delimited by '.' - pdgUnCnfMsgGGSNIndex.pdgUnCnfMsgFilterIndex)

`ATTR-LIST`: attribute 1, attribute 2…

Default: all attributes are returned

NOTICE: The MOI (table indexes – pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex) attributes are not supported in the ATTR-LIST.

MOC readable attributes:

The `pdgconf show` command may show all or several of the following pdgUnCnfMsgFilterTable MOC readable attributes:

- **pdgUnCnfMsgSrcIP**
- **pdgUnCnfMsgDstPort**
- **pdgUnCnfMsgGGSNIndex (MOI attribute)**

- **pdgUnCnfMsgFilterIndex (MOI attribute)**
- **pdgUnCnfMsgFilterNumOfEntries (pdgUnCnfMsgFilter MOC readable attribute)**

Examples of usage:

To view the entire running pdgUnCnfMsgFilterTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgUnCnfMsgFilterTable"
```

To view the running pdgUnCnfMsgSrcIP only, where pdgUnCnfMsgGGSNIndex = 2 and pdgUnCnfMsgFilterIndex = 1:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgUnCnfMsgFilterTable -id 2.1
pdgUnCnfMsgSrcIP"
```

To view the entire pdgUnCnfMsgFilterTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdgUnCnfMsgFilterTable"
```

To view the number of entries of the pdgUnCnfMsgFilterTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgUnCnfMsgFilter -id 0
pdgUnCnfMsgFilterNumOfEntries"
```

B.6.2

Unconfirmed Outbound Message Filter Table Configuration – Creation

To create the Unconfirmed Outbound message filter table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdgUnCnfMsgFilterTable MOI ATTR-
VALUE-LIST"
```

where:

`MOI`: -id (table entry indexes, delimited by '.' - pdgUnCnfMsgGGSNIndex.pdgUnCnfMsgFilterIndex)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table indexes – pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex) attributes are not supported in the ATTR-VALUE-LIST.

See the following table for the description of all writable attributes:

Table 80: pdgUnCnfMsgFilterTable Writable Attributes

Object Name	Description	Type	Format	Range/ Values	Default
pdgUnCnfMsgSrcIP	Source IP address of the outbound IP datagram from a CEN	NmaIpAddr	XXXXXXXX, where X is a hexadecimal symbol in uppercase	XXXXXXXX, where each two XX are two HEX characters representing one Octet (0-255). 0=X=9 or A=X=F	00000000
pdgUnCnfMsgDstPort	Destination Port number of the out-	INTEGER	Decimal integer	1...65535	none - this attribute is

Table continued…

Object Name	Description	Type	Format	Range/ Values	Default
	bound IP datagram from a CEN.				mandatory for the `pdgconf create` command
pdgUnCnfMsg GGSNIndex	The GGSN map index. Its value uniquely identifies a combination of pdrGGSNApn and pdrGGSNId and pdrGGSNZoneId	INTEGER	Decimal integer		none - this attribute is mandatory for the `pdgconf create` command
pdgUnCnfMsg GGSNIndex	The GGSN map index. Its value uniquely identifies a combination of pdrGGSNApn and pdrGGSNId and pdrGGSNZoneId	INTEGER	Decimal integer		none - this attribute is mandatory for the `pdgconf create` command

NOTICE: All the writable non-MOI attributes which do not have defaults should be included in ATTR-VALUE-LIST in the `pdgconf create` command.

B.6.3

Unconfirmed Outbound Message Filter Table Configuration – Modification

To modify the Unconfirmed Outbound message filter table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify –moc pdgUnCnfMsgFilterTable MOI ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry indexes, delimited by '.' - pdgUnCnfMsgGGSNIndex.pdgUnCnfMsgFilterIndex)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table indexes – pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex) attributes are not supported in the ATTR-VALUE-LIST.

See Table 80: pdgUnCnfMsgFilterTable Writable Attributes on page 279 for the description of all writable attributes.

NOTICE: The `pdgconf modify` command is not applicable to MOI attributes (table indexes – pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex).

B.6.4

Unconfirmed Outbound Message Filter Table Configuration – Deletion

To delete the Unconfirmed Outbound message filter table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete –moc pdgUnCnfMsgFilterTable –id X.Y"
```

where:

X and Y are the values of pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex.

NOTICE: The MOI (table indexes – pdgUnCnfMsgGGSNIndex and pdgUnCnfMsgFilterIndex) attributes are not supported in the ATTR-VALUE-LIST.

See Table 80: pdgUnCnfMsgFilterTable Writable Attributes on page 279 for the description of all writable attributes.

Examples of usage for the`pdgconf create`, `pdgconf modify`, and `pdgconf delete`**commands:**

To initially provision the filter for the GGSN with index 2 and pdgUnCnfMsgFilterIndex =1:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdgUnCnfMsgFilterTable -id 2.1
pdgUnCnfMsgSrcIP=38413841 pdgUnCnfMsgDstPort =3456"
```

To change the GGSN the PDG is working with from index 2 to index 4 and define the same filter, use the following commands:

- `/opt/Motorola/pdr/bin/pdgconf "delete -moc pdgUnCnfMsgFilterTable -id 2.1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdgUnCnfMsgFilterTable -id 4.1 pdgUnCnfMsgSrcIP=38413841 pdgUnCnfMsgDstPort=3456"`

To change the pdgUnCnfMsgDstPort:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdgUnCnfMsgFilterTable -id 4.1
pdgUnCnfMsgDstPort=5634"
```

B.7

Conventional Key Management Facility Configuration

Follow the initial provisioning and modifying configuration rules:

- If an entry of pdrConventionalKeyManagementFacilityTable should be deleted and no other entry is created instead, then the corresponding pdrConventionalCAIDataEncryptionModuleTable entries (with pdrOTEKKMFId = pdrKMFId) should be also deleted.
- If an entry of pdrConventionalKeyManagementFacilityTable with a pdrKMFId should be deleted and the other pdrConventionalKeyManagementFacilityTable entry with a new pdrKMFId is created instead, then pdrConventionalCAIDataEncryptionModuleTable entries (with pdrOTEKKMFId = pdrKMFId) should be deleted or modified so that pdrOTEKKMFId is equal to the new pdrKMFId.

B.7.1

Conventional Key Management Facility Configuration – Viewing

To view the Conventional Key Management Facility configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc
pdrConventionalKeyManagementFacilityTable [MOI [ATTR-LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry index - pdrKMFId)

`ATTR-LIST`: attribute 1, attribute 2…

NOTICE: The MOI (table index - pdrKMFId) attribute is not supported in the ATTR-LIST.

MOC readable attributes:

The `pdgconf show` command may show all or several of the following managed object class readable attributes:

- **pdrKMFId (MOI attribute)**
- **pdrOTEKServicePortNumber**
- **pdrOTARServicePortNumber**
- **pdrKMFIPAddress**
- **pdrKMFFullyQualifiedDomainName**
- **pdrKMFRSI**
- **pdrCENKMFIPAddress**

Examples of usage:

To view the entire running pdrConventionalKeyManagementFacilityTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdrConventionalKeyManagementFacilityTable"
```

To view the running pdrOTEKServicePortNumber only, where pdrKMFId =2:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdrConventionalKeyManagementFacilityTable -id 2 pdrOTEKServicePortNumber"
```

To view the entire pdrConventionalKeyManagementFacilityTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrConventionalKeyManagementFacilityTable"
```

To view the number of entries of the pdrConventionalKeyManagementFacilityTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdgConventionalKeyManagementFacility -id 0
pdrConventionalKeyManagementFacilityNumOfEntries"
```

B.7.2 Conventional Key Management Facility Configuration – Creation

To create the Conventional Key Management Facility configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc
pdrConventionalKeyManagementFacilityTable MOI ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry index – the value of pdrKMFId attribute)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table index - pdrKMFId) attribute is not supported in the ATTR-VALUE-LIST.

See the following table for the description of all the writable attributes:

Table 81: pdrConventionalKeyManagementFacilityTable Writable Attributes

Object Name	Description	Type	Format	Range/Values	Default
pdrKMFId	This parameter defines the ID of the KMF (MOI attribute)	INTEGER	Decimal integer	1...20	none
pdrOTEKServicePortNumber	KMF TCP Port to which the PDG sends OTEK messages.	INTEGER	Decimal integer	50152… 65535 CM and firewall always use a value of 64416.	none - this attribute is mandatory for the `pdgconf create` command
pdrOTARServicePortNumber	Fully Qualified Domain Name of the KMF used for DNS lookup/local resolution of the KMF IP address	INTEGER	Decimal integer	49152...65535	none - this attribute is mandatory for the `pdgconf create` command
pdrKMFFullyQualifiedDomainName	Fully Qualified Domain Name of the KMF used for DNS lookup/local resolution of the KMF IP address	OCTET STRING	Literal string, no “”	1 to 63 ASCII chars	none - this attribute is mandatory for the `pdgconf create` command
pdrKMFRSI	Defines the Radio Set Identifier of the KMF. Defined in hexadecimal.	INTEGER	hexadecimal integer	1...9999999	none - this attribute is mandatory for the `pdgconf create` command
pdrCENKMFIPAddress	Defines the CEN IP address of the KMF. This is the actual IP address of the KMF in a CEN. It is used when sending subscriber data to the KMF device (for OTAR)	NmaIpAddr	XXXXXXXX where X is a hexadecimal symbol	XXXXXXXX, where each two XX are two HEX characters representing one Octet (0-255). 0=X=9 or A=X=F	none - this attribute is mandatory for the `pdgconf create` command

NOTICE: All the writable non-MOI attributes which do not have defaults should be included in ATTR-VALUE-LIST in the `pdgconf create` command.

B.7.3 Conventional Key Management Facility Configuration – Modification

To modify the Conventional Key Management Facility configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc
pdrConventionalKeyManagementFacilityTable MOI ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry index – the value of pdrKMFId attribute)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table index - pdrKMFId) attribute is not supported in the ATTR-VALUE-LIST.

See Table 81: pdrConventionalKeyManagementFacilityTable Writable Attributes on page 283 for the description of all the writable attributes.

B.7.4

Conventional Key Management Facility Configuration – Deletion

To delete the Conventional Key Management Facility configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc
pdrConventionalKeyManagementFacilityTable -id X"
```

where:

X is the value of pdrKMFId. See Table 81: pdrConventionalKeyManagementFacilityTable Writable Attributes on page 283 for the description of pdrKMFId.

Examples of usage for the`pdgconf create`, `pdgconf modify`, and `pdgconf delete`**commands:**

NOTICE: CM and firewall always use a value of 64416 for ***<pdrOTEKServicePortNumber>***.

To initially provision the KMF with index 2:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc
pdrConventionalKeyManagementFacilityTable -id 2 pdrOTEKServicePortNumber
=3142 pdrOTARServicePortNumber=4444
pdrKMFFullyQualifiedDomainName=KMF02.cen2.zone5 pdrKMFRSI=3A4B
pdrCENKMFIPAddress=45A3F467"
```

To change the KMF the PDG is working with from 2 to 3, use the following commands:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc
  pdrConventionalKeyManagementFacilityTable -id 2"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc
  pdrConventionalKeyManagementFacilityTable -id 4 pdrOTEKServicePortNumber
  =3142 pdrOTARServicePortNumber=4444
  pdrKMFFullyQualifiedDomainName=KMF04.cen2.zone3 pdrKMFRSI=3A4C
  pdrCENKMFIPAddress=45A3F468"
  ```

To change the pdrOTARServicePortNumber:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc
pdrConventionalKeyManagementFacilityTable -id 4
pdrOTARServicePortNumber=4445"
```

B.8

Conventional CAI Data Encryption Module Table Configuration

Follow the initial provisioning and modifying configuration rules:

- If an entry of pdrConventionalKeyManagementFacilityTable should be deleted and no other entry is created instead, then the corresponding pdrConventionalCAIDataEncryptionModuleTable entries (with pdrOTEKKMFId = pdrKMFId) should be also deleted.
- If an entry of pdrConventionalKeyManagementFacilityTable with a pdrKMFId should be deleted and the other pdrConventionalKeyManagementFacilityTable entry with a new pdrKMFId is created instead, then pdrConventionalCAIDataEncryptionModuleTable entries (with pdrOTEKKMFId = pdrKMFId) should be deleted or modified so that pdrOTEKKMFId is equal to the new pdrKMFId.

B.8.1

Conventional CAI Data Encryption Module Table Configuration – Viewing

To view the Conventional CAI Data Encryption Module table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc
pdrConventionalCAIDataEncryptionModuleTable [MOI [ATTR-LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry index - pdrCDEMId)

`ATTR-LIST`: attribute 1, attribute 2…

Default: all attributes are returned

NOTICE: The MOI (table index - pdrCDEMId) attribute is not supported in the ATTR-LIST.

MOC readable attributes:

The `pdgconf show` command may show all or several of the following managed object class readable attributes:

- **pdrCDEMId (MOI attribute)**
- **pdrOTEKKMFId**
- **pdrOTEKTransmitSecurityLevel**
- **pdrOTEKReceiveSecurityLevel**
- **pdrOTEKInactivityTimePeriod**
- **pdrCDEMIP**

Examples of usage:

To view the entire running pdrConventionalCAIDataEncryptionModuleTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdrConventionalCAIDataEncryptionModuleTable"
```

To view the running pdrOTEKServicePortNumber only, where pdrCDEMId = 1:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdrConventionalCAIDataEncryptionModuleTable -id 1 pdrOTEKServicePortNumber"
```

To view the entire pdrConventionalCAIDataEncryptionModuleTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrConventionalCAIDataEncryptionModuleTable"
```

To view the number of entries of the pdrConventionalCAIDataEncryptionModuleTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc
pdgConventionalCAIDataEncryptionModule -id 0
pdgConventionalCAIDataEncryptionModuleNumOfEntries"
```

B.8.2 Conventional CAI Data Encryption Module Table Configuration – Creation

To create the Conventional CAI Data Encryption Module table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc
pdrConventionalCAIDataEncryptionModuleTable MOI ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry index – the value of the pdrCDEMId attribute)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table index - pdrCDEMId) attribute is not supported in the ATTR-VALUE-LIST.

See the following table for the description of all the writable attributes:

Table 82: pdrConventionalCAIDataEncryptionModuleTable Writable Attributes

Object Name	Description	Type	Format	Range/ Values	Default
pdrCDEMId	Defines the ID of the CDEM. (MOI attribute)	INTEGER	Decimal integer	1	none
pdrOTEKKMFId	The ID of the KMF which the CDEM communicates with for OTEK	INTEGER	Decimal integer	0...20	none - this attribute is mandatory for the `pdgconf create` command
pdrOTEKTransmitSecurityLevel	Sets the OTEK security rules for sending a KMM to the KMF.0 - Basic1 - Enhanced	INTEGER	Decimal integer	0...1	none - this attribute is mandatory for the `pdgconf create` command
pdrOTEKReceiveSecurityLevel	Sets the OTEK security rules for receiving a KMM from the KMF.0 - Basic1 - Enhanced	INTEGER	Decimal integer	0...1	none - this attribute is mandatory for the `pdgconf create` command
pdrOTEKInactivityTimePeriod	Defines the frequency with which the PDG sends a registration message to the KMF with no other OTEK activity. The units	INTEGER	Decimal integer	1...168	none - this attribute is mandatory for the `pdgconf create` command

Object Name	Description	Type	Format	Range/ Values	Default
	are defined in hours.				

NOTICE: All the writable non-MOI attributes which do not have defaults should be included in ATTR-VALUE-LIST in the `pdgconf create` command.

B.8.3

Conventional CAI Data Encryption Module Table Configuration – Modification

To modify the Conventional CAI Data Encryption Module table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc
pdrConventionalCAIDataEncryptionModuleTable MOI ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry index – the value of the pdrCDEMId attribute)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table index - pdrCDEMId) attribute is not supported in the ATTR-VALUE-LIST.

See Table 82: pdrConventionalCAIDataEncryptionModuleTable Writable Attributes on page 286 for the description of all the writable attributes.

NOTICE: The `pdgconf modify` command is not applicable to the MOI attribute (table index – pdrCDEMId).

B.8.4

Conventional CAI Data Encryption Module Table Configuration – Deletion

To delete the Conventional CAI Data Encryption Module table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc
pdrConventionalCAIDataEncryptionModuleTable -id X"
```

where:

X is the value of pdrCDEMId. See Table 82: pdrConventionalCAIDataEncryptionModuleTable Writable Attributes on page 286 for the description of the pdrCDEMId.

Examples of usage for the`pdgconf create`, `pdgconf modify`, and `pdgconf delete`**commands:**

To initially provision the CDEM working with KMF 2 with index 1:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc
pdgConventionalCAIDataEncryptionModule -id 1 pdrOTEKKMFId=2
pdrOTEKTransmitSecurityLevel=0 pdrOTEKReceiveSecurityLevel=0
pdrOTEKInactivityTimePeriod=24"
```

To change the CDEM to work with KMF 4, use the following commands:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc
  pdrConventionalCAIDataEncryptionModuleTable -id 1"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc
  pdrConventionalCAIDataEncryptionModuleTable -id 1 pdrOTEKKMFId=4
  pdrOTEKTransmitSecurityLevel=0 pdrOTEKReceiveSecurityLevel=0
  pdrOTEKInactivityTimePeriod=24"
  ```

To change the CDEM to work with KMF 4:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc
pdrConventionalCAIDataEncryptionModuleTable -id 1 pdrOTEKKMFId=4"
```

B.9

Conventional Sites Configuration

Follow the initial provisioning and modifying configuration rules: If an entry of pdrConventionalSitesTable should be deleted, then the corresponding pdrConventionalChannelsTable entries (with pdrConventionalChannelsSiteId = pdrConventionalSitesSiteId) should be also deleted.

B.9.1

Conventional Sites Configuration – Viewing

To view the Conventional Sites configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc
pdrConventionalSitesTable [MOI]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

`MOI`: -id (table entry index - pdrConventionalSitesSiteId)

MOC readable attributes:

The `pdgconf show` command may show the following managed object class readable attribute: **pdrConventionalSitesSiteId (MOI attribute)**

Examples of usage:

To view the entire running pdrConventionalSitesTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrConventionalSitesTable"
```

To view the pdrConventionalSitesTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrConventionalSitesTable"
```

To view the number of entries of the pdrConventionalSitesTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgConventionalSites -id 0
pdrConventionalSitesNumOfEntries"
```

B.9.2

Conventional Sites Configuration – Creation

To create the Conventional Sites configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id X"
```

where:

X is the value of pdrConventionalSitesSiteId.

See the following table for the attribute description:

Table 83: pdrConventionalSitesTable Writable Attribute

Object Name	Description	Type	Format	Range/ Values	Default
pdrConventionalSitesSiteId	unique site identifier within the site zone (MOI attribute)	INTEGER	decimal integer	2001...2255	none

B.9.3 Conventional Sites Configuration – Deletion

To delete the Conventional Sites configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalSitesTable -id X"
```

where:

X is the value of pdrConventionalSitesSiteId.

See Table 83: pdrConventionalSitesTable Writable Attribute on page 289 for the attribute description.

Examples of usage for the`pdgconf create` and `pdgconf delete`**commands:**

To initially provision one Conventional Site with the PDG:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id
2022"
```

To add another Conventional Site with the PDG:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id
2025"
```

To remove the first Conventional Site with the PDG:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalSitesTable -id
2022"
```

B.10 Conventional Channels Table Configuration

Follow the initial provisioning and modifying configuration rules: If an entry of pdrConventionalSitesTable should be deleted, then the corresponding pdrConventionalChannelsTable entries (with pdrConventionalChannelsSiteId = pdrConventionalSitesSiteId) should be also deleted.

B.10.1 Conventional Channels Table Configuration – Viewing

To view the Conventional Channels table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "show [CFG-STATE] -moc
pdrConventionalChannelsTable [MOI [ATTR-LIST]]"
```

where:

`CFG-STATE`: -state (Running | FactDefault)

Default: Running

MOI: -id (table entry indexes, delimited by '.' - pdrConventionalChannelsSiteId.pdgConventionalChannelsIndex)

Default: all attributes are returned

NOTICE: The MOI (table indexes – pdrConventionalChannelsSiteId and pdgConventionalChannelsIndex) attributes are not supported in the ATTR-LIST.

MOC readable attributes:

The `pdgconf show` command may show all or several of the following pdrConventionalChannelsTable managed object class readable attributes:

- **pdrConventionalChannelsDataConventionalChannelMode**
- **pdrConventionalChannelsVoteScanEnable**
- **pdrConventionalChannelsSiteId (MOI attribute)**
- **pdgConventionalChannelsIndex (MOI attribute)**

Examples of usage:

To view the entire running pdrConventionalChannelsTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrConventionalChannelsTable"
```

To view the running pdrConventionalChannelsDataConventionalChannelMode only, where pdrConventionalChannelsSiteId = 2022 and pdgConventionalChannelsIndex = 1:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdrConventionalChannelsTable -id
2022.1 pdrConventionalChannelsDataConventionalChannelMode"
```

To view the entire pdrConventionalChannelsTable object defaults:

```
/opt/Motorola/pdr/bin/pdgconf "show -state FactDefault -moc
pdrConventionalChannelsTable"
```

To view the number of entries of pdrConventionalChannelsTable object:

```
/opt/Motorola/pdr/bin/pdgconf "show -moc pdgConventionalChannels -id 0
pdgConventionalChannelsNumOfEntries"
```

B.10.2
Conventional Channels Table Configuration – Creation

To create the Conventional Channels table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable MOI
ATTR-VALUE-LIST"
```

where:

MOI: -id (table entry indexes, delimited by '.' - pdrConventionalChannelsSiteId.pdgConventionalChannelsIndex)

ATTR-VALUE-LIST: attribute 1 = value 1…

NOTICE: The MOI (table indexes – pdrConventionalChannelsSiteId and pdgConventionalChannelsIndex) attributes are not supported in the ATTR-VALUE-LIST.

See Table 84: pdrConventionalChannelsTable Writable Attributes on page 291 for the description of all the writable attributes.

NOTICE: All the writable non-MOI attributes which do not have defaults should be included in ATTR-VALUE-LIST in the `pdgconf create` command.

B.10.3
Conventional Channels Table Configuration – Modification

To modify the Conventional Channels table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrConventionalChannelsTable MOI
ATTR-VALUE-LIST"
```

where:

`MOI`: -id (table entry indexes, delimited by '.' - pdrConventionalChannelsSiteId.pdgConventionalChannelsIndex)

`ATTR-VALUE-LIST`: attribute 1 = value 1…

NOTICE: The MOI (table indexes – pdrConventionalChannelsSiteId and pdgConventionalChannelsIndex) attributes are not supported in the ATTR-VALUE-LIST.

SeeTable 84: pdrConventionalChannelsTable Writable Attributes on page 291 for the description of all the writable attributes.

NOTICE: The `pdgconf modify` is not applicable to MOI attributes (table indexes – pdrConventionalChannelsSiteId and pdgConventionalChannelsIndex).

B.10.4
Conventional Channels Table Configuration – Deletion

To delete the Conventional Channels table configuration, use the following command:

```
/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable -id
X.Y"
```

where:

X and Y are the values of pdrConventionalChannelsSiteId and pdgConventionalChannelsIndex.

See the following table for the description of the attributes:

Table 84: pdrConventionalChannelsTable Writable Attributes

Object Name	Description	Type	Format	Range/ Values	Default
pdrConventionalChannelsSiteId	Unique Site number within the site's home zone. (MOI attribute)	INTEGER	Decimal integer	2001...2055	none - this attribute is mandatory for the `pdgconf create` command
pdrConventionalChannelsChannelId	Conventional Channel numeric identifier within Conventional Site. (MOI attribute)	INTEGER	Decimal integer	1...30	none - this attribute is mandatory for the `pdgconf create` command
pdrConventionalChannelsDataConven-	Digital conventional channel mode. Possible modes are:	Normal ASTRO®	Decimal integer	1...3	none - this attribute is mandatory

Table continued…

Object Name	Description	Type	Format	Range/ Values	Default
tionalChannel-Mode	• Normal - Normal ASTRO® 25 Conventional channel • Sub-site Steered - This mode causes the Conventional PDG to steer outbound data to the correct subsite. • Control Station - This mode causes the Conventional PDG to pause outbound data transmissions while waiting for confirmed outbound data to be acknowledged from Control Station (half duplex)	25 (1), Sub-site Steered (2), Control Station (3)			for the `pdgconf create` command
pdrConventionalChannels-VoteScanEnable	This parameter is used when sending outbound data to the channel. If the channel is configured for Vote Scan, a preamble is transmitted before the start of every data transaction to a scan enabled subscriber. If the channel is not configured for Vote Scan, a preamble is transmitted when Scan Suspend Timer has expired.	nmaEnable-Disable	Decimal integer	1...2	none - this attribute is mandatory for the `pdgconf create` command

Examples of usage for the`pdgconf create`, `pdgconf modify`, and `pdgconf delete`**commands:**

To initially provision a conventional channel for the conventional site with index 2022 and pdgConventionalChannelsIndex = 1:

```
/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id
2022.1 pdrConventionalChannelsDataConventionalChannelMode=1
pdrConventionalChannelsVoteScanEnable=1"
```

To delete one of the conventional sites the PDG is working with, delete all the conventional channels within this site from the conventional channels table and delete the site entry from the conventional site table:

- `/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable –id 2021.1"`
- `/opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable –id 2021.2"`

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable –id 2021.3"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable –id 2021.5"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalChannelsTable –id 2021.11"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "delete -moc pdrConventionalSitesTable -id 2021"
  ```

To change the pdrConventionalChannelsVoteScanEnable:

```
/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrConventionalChannelsTable -id 2022.1 pdrConventionalChannelsVoteScanEnable=2"
```

B.11

Example of the Initial CLI Configuration Provisioning for the Conventional IVD K Core PDG

Use the following system parameters:

- **Zone ID = 4**
- **APN = “APN.gprs”**
- **GGSNIndex = 3**
- **CEN = 2**
- **KMF_ID = 5**
- **pdrBcastDataCapable = enable**
- **pdrOTEKTransmitSecurityLevel = Basic**
- **pdrOTEKReceiveSecurityLevel = Basic**
- **one Gateway router**

Enter the following commands:

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "modify -moc pdgZone -id 0 pdrAPNOperatorId=APN.gprs pdrBcastDataCapable=1"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNListTable -id 4.1"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrGGSNMapTable -id 3 pdrGGSNApn=APN.gprs pdrGGSNId=1 pdrGGSNZoneId=4"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdgUnCnfMsgFilterTable -id 3.2 pdgUnCnfMsgSrcIP=0A0B0C0D pdgUnCnfMsgDstPort=63000"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalKeyManagementFacilityTable -id 5 pdrOTEKServicePortNumber=64416 pdrOTARServicePortNumber=64414 pdrKMFFullyQualifiedDomainName=KMF05.cen2.zone4 pdrKMFRSI=10 pdrCENKMFIPAddress=45A3F467"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalCAIDataEncryptionModuleTable -id 1 pdrOTEKKMFId=5 pdrOTEKTransmitSecurityLevel=0 pdrOTEKReceiveSecurityLevel=0 pdrOTEKInactivityTimePeriod=24"
  ```

-
  ```
  /opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id 2021"
  ```

- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.1 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.2 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.3 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.4 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.5 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2021.6 pdrConventionalChannelsDataConventionalChannelMode=3 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalSitesTable -id 2022"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.1 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.2 pdrConventionalChannelsDataConventionalChannelMode=2 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.3 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.4 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=1"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.5 pdrConventionalChannelsDataConventionalChannelMode=1 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "create -moc pdrConventionalChannelsTable -id 2022.6 pdrConventionalChannelsDataConventionalChannelMode=3 pdrConventionalChannelsVoteScanEnable=2"`
- `/opt/Motorola/pdr/bin/pdgconf "modify -moc pdrExpressConventionalCLISyncDB -id 0 pdrExpressConventionalCLISyncDBSyncFlag=0"`

If the provisioning is completed successfully, the following message appears: `> CNEOMI_SUCCESS`

B.12 Error Codes and Error Messages for the CLI Failed Operations

Table 85: Error Codes and Messages for the CLI Failed Operations

`pdgconf` Error Code	Description
`MOC_NOT_PERMITTED`	Managed object class provisioning from the pdgconf CLI is prohibited.
`SYNTAX_ERROR`	CLI command syntax error
`COMMAND_NOT_PERMITTED`	CLI command is not supported by the pdgconf CLI.
`MULTI_USER_ACCESS_DENIED`	Multi-user access to the pdgconf CLI is prohibited.
`PDR_OPERATION_BUSY`	Running a PDR script simultaneously with the pdgconf is prohibited. The scripts are: • **Backup_pdrdb** • **Create_pdrdb** • **Recover_pdrdb** • **Restart_pdg** • **Restore_pdrdb** • **Start_pdg** • **Start_pdr** • **Stop_pdg** • **Stop_pdr** • **Pdgconf** • **Update_ntp_info**
`PDR_NOT_RUNNING`	Configuration cannot be provisioned if the PDR is not running.
`CONFIGURATION_NOT_FINISHED`	Retry command is not applicable to an incomplete configuration change: pdrExpressConventionalCLI-SyncDBSyncFlag is not set to syncCompleted.
`TIMER_DEFINITION_ERROR`	setTimeout command syntax or time range violation
`UCML_PROVISIONING_IN_PROGRESS`	Configuration Manager provisioning is in progress. Try CLI provisioning later.

This page intentionally left blank.