System Release 7.17
ASTRO ® 25
INTEGRATED VOICE AND DATA

Conventional Data Services

NOVEMBER 2016

MN003252A01-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.

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 particular system, or may be dependent upon the characteristics of a particular 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
MN003252A01-A	Original release of the *Conventional Data Services* manual	November 2016

This page intentionally left blank.

Contents

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

About Conventional Data Services

This manual provides descriptive and procedural information about the ASTRO® 25 Conventional with Integrated Data feature. Included in this manual is the description of the feature, including its components, how it works, and how data messages are processed. Additional information is provided for procedures on configuration, operation, and troubleshooting.

This manual is intended to be used by technicians and system operators as a resource for understanding, installing, and configuring the ASTRO® 25 Conventional with Integrated Data feature.

What Is Covered In This Manual?

This manual is organized into the following chapters:

- Conventional Data Services Description on page 23 provides a high-level description of the ASTRO® 25 Conventional with Integrated Data feature and the function it serves on your system.
- Conventional Data Services Theory of Operation on page 39 explains how the ASTRO® 25 Conventional with Integrated Data feature works in the context of your system.
- Conventional Data Services Configuration on page 61 explains configuration procedures pertaining to the ASTRO® 25 Conventional with Integrated Data feature.
- Conventional Data Services Operations and Optimization on page 65 covers operations and optimization tasks performed once the ASTRO® 25 Conventional with Integrated Data feature is installed and configured on your system.
- Conventional Data Services Troubleshooting on page 69 describes maintenance and troubleshooting tasks for the ASTRO® 25 Conventional with Integrated Data feature.

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:

Document Title	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 on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	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.
CAI Data Encryption Module User Guide	Describes data encryption services provided by the CAI Data Encryption Module (CDEM) for ASTRO® 25 Conventional IV&D appli-

Table continued…

Document Title	Purpose
	cations. The CDEM is an optional component of the Conventional IV&D feature. It is 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, upgrade, troubleshooting, and FRU/FRE replacement.
Packet Data Gateways	Covers the installation, configuration, and management of the Conventional IV&D Packet Data Gateway (PDG) and its components, namely the Packet Data Router (PDR), and the Radio Network Gateway (RNG).
Secure Communications Feature Guide	Describes the secure communications features found in ASTRO® 25 systems, intended for technicians and system operators. The manual should be used in conjunction with the ASTRO® 25 system documentation and the "Key Management Facility" manual.
KVL 3000 and KVL 3000 Plus Key Variable Loader User's Guide	Provides information for the KVL 3000 and the KVL 3000 Plus Key Variable Loaders.
KVL 4000 Key Variable Loader ASTRO 25 User Guide	Provides instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others, in ASTRO® 25 operating mode.
S6000 and S2500 Routers	Provides information relating to the installation, configuration, and management of the S6000 and S2500 routers as used in various network locations.
GGM 8000 System Gateway	Provides information relating to the installation, configuration, and management of the GGM 8000 Gateway as used in various network locations.
Provisioning Manager	Provides a description of the Provisioning Manager server application. Includes information to tailor this application for system use and contains information to provision your ASTRO® 25 radio communication system with various system-level, user-level, and device-level configuration parameters required for proper system operation. This manual also includes reference and troubleshooting information to ensure efficient and effective use of this application.
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.
Unified Network Configurator	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: Voyence Control and Unified Network Configurator Wizards (UNCW).

Table continued…

Document Title	Purpose
CSS Getting Started Guide	Provides setup instructions for the Configuration/Service Software (CSS) application used to configure, service, and maintainvarious devices in ASTRO® 25 systems.
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in an ASTRO® 25 system. Includes common procedures for virtual machines/virtual appliances on the virtual server host.
Conventional Operations	Provides information regarding conventional channel resource operating characteristics in standalone systems or ASTRO® 25 radio communication systems with K Series, L Series, or M Series.

This page intentionally left blank.

Chapter 1

Conventional Data Services Description

This chapter provides a high-level description of the ASTRO® 25 Conventional with Integrated Data feature and how it works on your system.

NOTICE: The ASTRO® 25 Conventional with Integrated Data feature is also referred to as "ASTRO® 25 Conventional IV&D" in this manual.

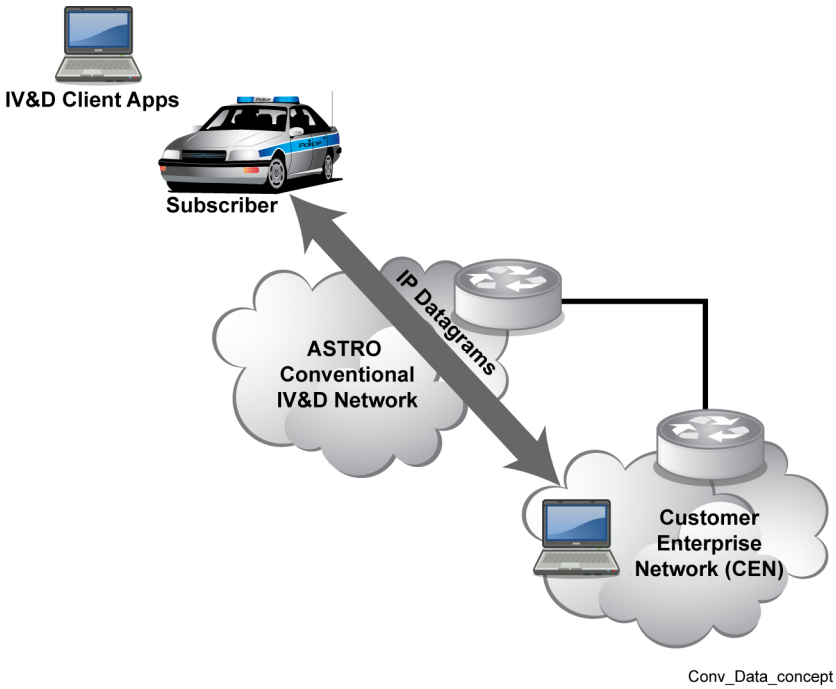
1.1 ASTRO 25 Conventional with Integrated Data Overview

ASTRO® 25 Conventional with Integrated Data is an optional feature that can be added to an ASTRO® 25 Conventional system, allowing applications running on a subscriber unit (SU) or an attached mobile computer to exchange data with applications residing in networks outside the ASTRO® 25 system. This enables a remote user to access various communications applications including OTAR, location-based services, text message service, and database inquiry.

The service passes data packets (IP datagrams) between Simple CAI Encapsulation Protocol (SCEP) conventional SUs and Customer Enterprise Network (CEN) host servers, providing the appearance that an SU is located on the same LAN as a host computer even though the CEN is physically separate from the ASTRO® 25 network. An IP datagram is a single data packet consisting of an IP header, a transport header (typically UDP), and payload data (information passed to the Transport Layer from the application).

Datagrams are transported through the ASTRO® 25 system by the various physical communication links and their associated protocols. Secure data encryption and decryption services are an option for the ASTRO® 25 Conventional with Integrated Data feature.

Figure 1: Datagram Transport in the ASTRO 25 Conventional with Integrated Data Feature



IMPORTANT: ASTRO® 25 Conventional with Integrated Data is supported in systems with trunked IV&D and High Performance Data (HPD), but conventional, trunking, and HPD each require separate devices such as a different PDG and site equipment.

1.1.1
Application Support

Conventional packet data messaging enables a number of useful applications, such as:

- OTAR for over-the-air key management of secure delivery services
- Location applications for tracking the movement of an SU
- POP25 for over-the-air programming of SU capabilities
- Information queries, text message service and other services

Both internal SU applications (for example, OTAR, POP25) and mobile computer-based applications are supported. Applications running on a host in the CEN can initiate outbound IP datagram traffic to an SU or attached mobile computer. Conversely, applications running in an SU or attached mobile computer can initiate inbound IP datagram traffic to a host in the CEN.

NOTICE: Motorola Solutions Conventional SUs are currently not able to at the same time route IP datagrams to/from on-board applications and applications running on a mobile computer or attached data device. (This constraint does not apply to running OTAR as an on-board application since OTAR is not an IP application from the perspective of the SU).

1.1.2
Data Traffic Examples

The following sections provide examples of data traffic handled by the ASTRO® 25 Conventional with Integrated Data feature.

1.1.2.1
Inbound Datagram Example

A vehicle location application is an example where only inbound data packets are sent to a host. The client (through GNSS equipment) notifies the host computer of the vehicle's location. All packets are inbound from the client application/SU to the host computer. The inbound datagrams are typically small; only 80-100 bytes each.

Although the application messages are inbound in this example, traffic on the outbound channel can still be significant. Since inbound datagrams are usually sent using confirmed delivery, outbound acknowledgments are sent. Also, if Data Scan or Vote Scan is used by the SU the acknowledgment is often preceded by a preamble sequence, adding to outbound traffic.

1.1.2.2
Inbound and Outbound Datagram Example – Database Query

A database query/response is a typical example of bi-directional datagram exchange. In this example, a short inbound datagram is required for inquiry of license plate number "XXX YYY". Two outbound datagrams are sent to acknowledge the request and to send the requested database record. Typically, total data transferred is less than 512 bytes.

1.1.2.3
Large Inbound Packets – Image Transfer

Transferring an image such as a fingerprint requires a multi-kilobyte-sized file to be transferred. In this case, the application breaks the file into a number of messages to facilitate the transfer. Then the mobile computer sending the file must fragment each message into 512 byte datagrams (IP fragmentation) to meet the over-the-air interface specification.

1.1.2.4
Over-The-Air Rekeying

The number of key management messages (KMMs) in an OTAR transaction ranges from a single inbound or outbound KMM (such as an Inhibit or Hello KMM) to multiple inbound and outbound KMMs (such as a Full Update transaction containing Rekey, Changeover, and Change RSI KMMs). Multiple Rekey KMMs may be required for a Full Update, depending on the number of CKRs and secure algorithms in the device and the frequency of key updates and keyset changeovers. The Conventional OTAR service supports both individual and group updates – an OTAR traffic profile must consider the number and size of both types of updates. Group updates can be significantly more efficient than individual updates when multiple OTAR SUs are on a Conventional channel at the same time.

1.1.3
Unicast and Group/Broadcast Messaging Service Support

Both Unicast and Group/Broadcast messaging services are provided. The Unicast service allows IPv4 datagrams to be sent in a point-to-point fashion between a Conventional SU (or attached mobile computer) and a CEN host. The Group/Broadcast service allows IPv4 messages to be sent in a point to multipoint fashion to all Conventional SUs who are members of the addressed Group within a zone. Group/Broadcast data is sent using a "best effort" method and its delivery is not guaranteed.

1.2
Supported ASTRO 25 Architectures

ASTRO® 25 Conventional with Integrated Data is supported by a various ASTRO® 25 system architectures.

Table 1: ASTRO 25 Conventional with Integrated Data Feature – Supporting Architectures

ASTRO 25 System Architecture	Centralized Conventional Architecture	Distributed Conventional Architecture
K core	No	Yes
M1/M2 core	Yes	Yes
M3 core	Yes	Yes
L core	No	No

ASTRO® 25 Conventional with Integrated Data is supported on the K System and consists of a Conventional Master Site – Non-Redundant (K1 core) or Redundant (K2 core) and various Conventional Hub Sites and Conventional Base Radio Sites in an interconnected Distributed Conventional Architecture.

M-Series zone cores are part of the ASTRO® 25 Trunking and Conventional system architectures which employ Master Site locations with zone core equipment in a single-zone (M1/M2 core) or Multizone-capable (M3 core) architecture. These systems support conventional data services for conventional remote sites of the Centralized Conventional Architecture or Distributed Conventional Architecture (interconnected conventional remote site architecture).

1.2.1
PDG – High Availability Conventional IVD – System Architecture

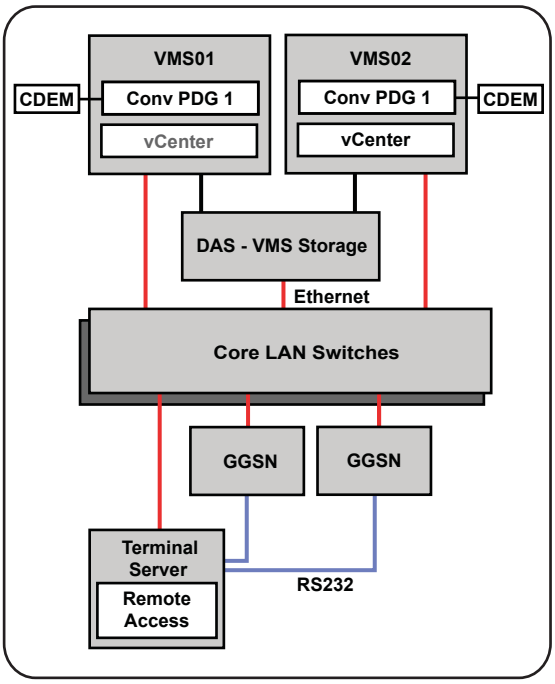
The High Availability for Conventional IV&D (HA Data) feature provides a high availability data solution within a single zone core by establishing two Packet Data Gateways (PDGs) on separate virtual servers, two GGSN routers, and redundant CNI path devices at a zone core to support conventional data 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.

1.2.1.1
PDG – High Availability Conventional IVD – System Architecture, Non-DSR

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



1.2.1.2
PDG – High Availability Conventional IVD – System Architecture, DSR

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.

1.2.2
PDG – High Availability Conventional IVD – Description

The High Availability for Conventional IV&D feature introduces redundant components into the conventional data subsystem to provide maximum data service reliability in case of hardware failure.

High Availability for Conventional IV&D is available for:

- ASTRO® 25 IV&D systems
- K2, M2, and M3 zone cores

Components needed for HA Data include:

- VMware vCenter application with Fault Tolerance
- Direct Attached Storage (DAS)
- Redundant Packet Data Gateway (PDG) Virtual Machines
- Redundant (GPRS Gateway Support Node) GGSN routers
- Redundant Customer Network Interface (CNI) path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers)

High Availability for Conventional IV&D provides:

- Improved system resilience to component failure
- Automatic or user-initiated switchover from a failed device to a redundant peer device
- Real-time synchronization of the redundant PDG and GGSN databases for seamless recovery of data services upon switchover

1.2.3
PDG Redundancy

Redundancy for the Packet Data Gateway (PDG) is provided by enabling Fault Tolerance for a PDG. Fault Tolerance is a VMware feature that creates a secondary PDG virtual machine on another server and keeps the secondary PDG VM in sync with the primary device. If the server hosting the primary PDG fails, Fault Tolerance provides automatic switchover to the secondary PDG, which immediately takes over the role of the primary device.

You can use the Unified Event Manager (UEM) application to check if a PDG is protected with Fault Tolerance (that is, both the primary and the secondary virtual machines are functional) and if the application is reporting any alarms for the redundant PDG pair.

For information on how to set up VMware vCenter in the system and enable Fault Tolerance for a Trunked IV&D PDG, see the *ASTRO 25 vCenter Application Setup and Operations Guide*.

1.2.4
ASTRO 25 K Core Configuration Functionalities

In the ASTRO® 25 K core configurations, a complete central fault and configuration manager (Network Manager) is not supported, including: Provisioning Manager, Unified Event Manager (UEM), United Network Configurator (UNC), and Zone Database Server (ZDS).

Table 2: Data Functionality Comparison: M Core and K Core Systems for ASTRO 25 Conventional IV&D

Function	M1/M2/M3 core	K core
Fault and configuration management	Network Manager (UEM, UNC, Provisioning Manager, and ZDS)	• Configuration Manager provisions the CSCs, PDG, console operations, and Site Gateway (Conventional Channel Interface) • Pdgconf Command Line Interface (CLI) to configure sites, channels, and GGSN in the PDG • PDG local configuration tool to initially set PDG active and configure optional parameters
Firewall management	RNI-DMZ/Firewall	Firewall; no RNI-DMZ

1.3
ASTRO 25 Conventional with Integrated Data Components

The ASTRO® 25 Conventional with Integrated Data feature relies on the following components:

- For M core systems: Network Management Subsystem (NM)
  - Unified Event Manager (UEM)

  - Provisioning Manager
  - Unified Network Configurator (UNC)
- For K core systems: Configuration Manager

For M core and K core systems:

- Border Gateway
- RNI-DMZ Firewall (no RNI-DMZ in K core systems)
- Gateway GPRS Support Node (GGSN)
- Conventional IV&D or Conventional (K core) Packet Data Gateway (PDG)
  - Packet Data Router (PDR)
  - Radio Network Gateway (RNG)
- CAI Data Encryption Module (CDEM) (optional)
- Site Gateway (Conventional Channel Interface)
- Conventional Channel (Base Radio)
- Data-Capable SU
- Key Management Facility (KMF) (optional)
- Key Variable Loader (KVL) (optional)

Figure 3: ASTRO 25 Conventional with Integrated Data Architecture for M Core Systems

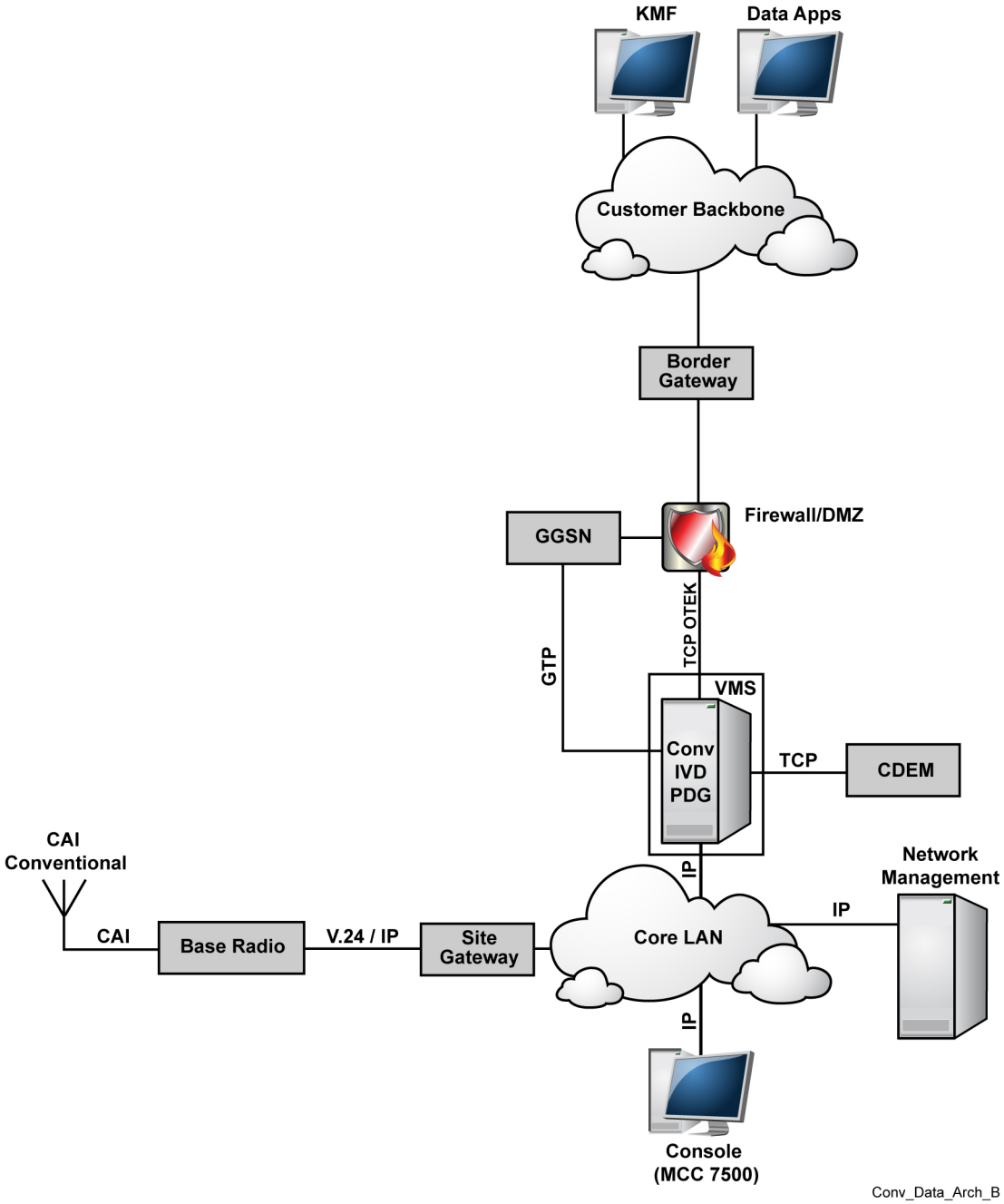
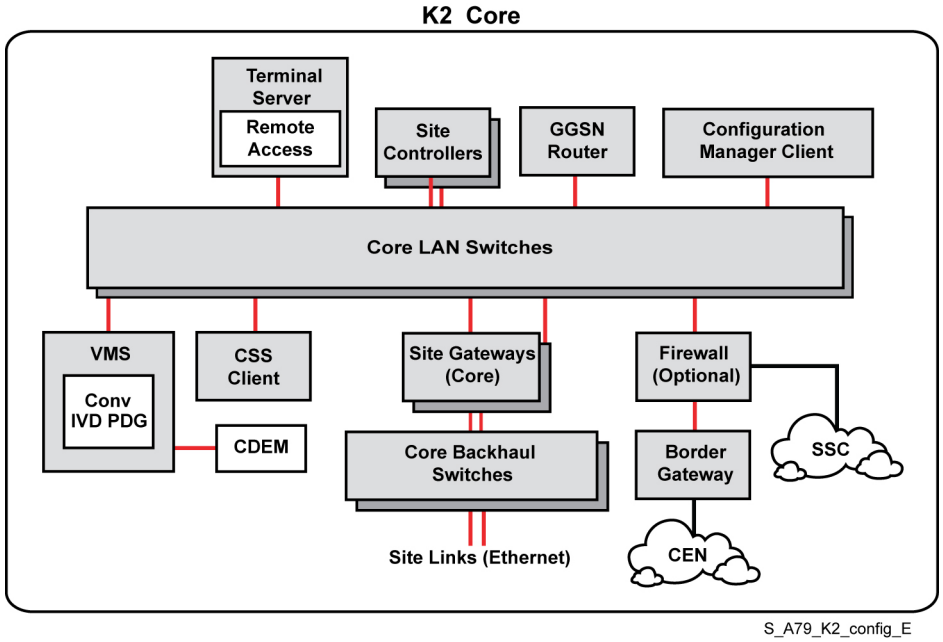


Figure 4: ASTRO 25 Conventional with Integrated Data Architecture for K Core Systems



1.3.1
Network Management (NM) Subsystem

NOTICE: The Network Management subsystem is used for M core systems only.

The Network Management subsystem is composed of different applications that provide a means for managing the system in accordance with the Fault, Configuration, Accounting, Performance, Security (FCAPS) network management model.

NOTICE: With the large quantity of configuration options, it is very important to document variations from default configuration values (and why the default was changed) as well to maintain version control on sets of configuration parameters. As parameter tuning occurs, parameter documentation must also be updated. This provides history for Motorola Solutions service support personnel to troubleshoot undesired system operation that might have been caused by misconfiguration. Lastly, it is necessary to validate the latest configuration parameter baseline documentation against the parameters actually configured into the system's Network Management Subsystems as well as in the configuration of each SU.

Three components of the NM subsystem are used to manage the ASTRO® 25 Conventional IV&D feature: Unified Event Manager (UEM), Provisioning Manager, and Unified Network Configurator (UNC).

1.3.1.1
Unified Event Manager (UEM)

UEM is an application that provides fault management services for the ASTRO® 25 radio systems. The main functions of UEM are:

- Device discovery
- Fault management
- Supervision
- Synchronization

1.3.1.2
Provisioning Manager

Provisioning Manager is the management application used to enter and maintain configuration information for the User Configuration Server (UCS). Provisioning Manager configures the Site Gateway (Conventional Channel Interface), System, SUs, Security, and ZoneWatch Configuration objects. Provisioning Manager is part of the Motorola Solutions Private Radio Network Management (PRNM) Suite.

1.3.1.3
Unified Network Configurator (UNC)

UNC is a configuration management application for the ASTRO® 25 system that manages the following data-related devices: PDG, GGSN, routers, switches, terminal servers, and base radios. The UNC provides two applications for network management: VoyenceControl and Unified Network Configurator Wizard. These applications are launched through a Web browser. Updates made in the Provisioning Manager application must be distributed to UNC before they are active in the system.

NOTICE: The names EMC Ionic Network Configuration Manager and VoyenceControl are used interchangeably for this product.

1.3.2
Configuration Manager

NOTICE: The Configuration Manager is used for K core systems only.

The Configuration Manager is an ASTRO® 25 software application that enables customers to configure the ASTRO® 25 Conventional with Integrated Data system. The Configuration Manager provides configuration for digital APCO P25 conventional voice, supplementary signaling, and integrated data service in the system. Supported data applications include OTAR, POP25, Outdoor Location, KMF, and text message service.

The Configuration Manager is used to configure the MCC 7500 Dispatch Consoles, MCC 7100 IP Dispatch Consoles, ASTRO® 25 Conventional Channel Gateways (CCGWs), AIS, subscriber information for the Packet Data Gateway (PDG), and alias information, channels table information, and the main/alt table for the GCP 8000 Site Controller.

The Configuration Manager ships standard with the K core systems and can cohabitate on an MCC 7500 or MCC 7100 operator position or on a dedicated PC. There should be only one Configuration Manager that is connected and running continuously and can only be used from the core.

1.3.3
Border Gateway

The Border Gateway provides the CEN with an access point into the ASTRO® Conventional infrastructure. In addition to routing datagrams between the ASTRO® 25 system and the CEN, the Border Gateway may be configured to route an inbound datagram (from one SU) to an outbound path (to a different SU, possibly in a different zone than the originating SU). The determination of whether to route an inbound datagram to the CEN or to an outbound path depends on the routing table definitions of the Border Gateway.

1.3.4
RNI-DMZ Firewall

NOTICE: For K core systems, only a firewall is used (no RNI-DMZ).

The RNI-DMZ Firewall inspects IP traffic to and from a CEN to ensure security of the ASTRO® 25 infrastructure equipment is not compromised. The firewall guards against known network-based security threats such as Denial of Service attacks, malicious intrusion, malware, Trojan Horses, worms and other viruses.

1.3.5
Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node (GGSN) is a special purpose router that provides various services in support of ASTRO® 25 Conventional IV&D operation, mainly tunneling of radio system datagrams into and out of the Customer Enterprise Network (CEN) using either an IP-in-IP tunnel or a Virtual Private Network (VPN).

All Conventional Packet Data traffic must be routed through a single GGSN. This GGSN may also be used to carry Trunking IV&D and/or High Performance Data (HPD) traffic. The GGSN interfaces between the Motorola Solutions radio network and the Border Gateway connecting to a CEN. The GGSN is used to tunnel datagrams from the CEN to the appropriate PDG, which ultimately passes the datagram on to a specified subscriber unit.

Two GGSN routers support the High Availability for Conventional IV&D (HA Data) feature.

1.3.6
Conventional IV&D or Conventional (K Core) Packet Data Gateway (PDG)

The Motorola Solutions Packet Data Gateway (PDG) links a user's data network to the conventional integrated data network. The PDG is a virtual machine that resides on a host virtual management server.

Each zone in the ASTRO® 25 Conventional IV&D system contains a Packet Data Gateway (PDG) made up of two separate functional elements – a Radio Network Gateway (RNG) and a Packet Data Router (PDR). PDG interfaces between the GGSN and the Motorola Solutions Radio Network. Conventional PDR in a zone can communicate with RNGs across all zones in the system.

Two Conventional PDGs support the High Availability for Conventional IV&D (HA Data) feature.

1.3.6.1
Packet Data Router (PDR)

The PDR is one of two functional elements in the Packet Data Gateway (PDG). The PDR manages all aspects of the IP protocol and provides a logical interface between the Gateway General Packet Radio Service (GPRS) Support Node (GGSN) and the RNG.

The Conventional PDR is responsible for managing Packet Data registrations and deregistrations, tracking SU location, interfacing with the Network Manager for configuration and fault management, and proxying configuration and fault management messaging for the Conventional RNG and CDEM.

1.3.6.2
Radio Network Gateway (RNG)

The Radio Network Gateway (RNG) provides a logical interface between the Radio Frequency (RF) resources and the PDR to support data calls to subscriber units.

The Conventional RNG in a zone provides a link (CAI) layer termination point for all the Conventional sites in that same zone.

If secure data encryption and decryption services are required, a CDEM is connected to the RNG via a dedicated Ethernet port. 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 via

OTEK, the RNG proxies the OTEK connection to the KMF on behalf of the CDEM. Inbound and Outbound message processing is described in Secure Delivery of Inbound and Outbound Datagrams on page 47.

1.3.7
CAI Data Encryption Module (CDEM)

The CDEM is an optional component that provides Conventional data encryption and decryption services for the ASTRO® 25 Conventional with Integrated Data feature. Conventional data supports CAI layer data encryption. The CDEM receives key management services from the KMF, and is a key management client. Key management is supported via KVL and OTEK.

To provide a high level of network security, the CDEM is connected to the RNG via a dedicated Ethernet port. No Layer 2 switch or other LAN access device is used to establish this connection. Only a single CDEM is connected to the RNG. The CDEM is deployed strictly as a client device to the RNG. The RNG sends datagrams to the CDEM for encryption/decryption and receives the results via the dedicated Ethernet link.

Two CDEM devices support encryption and decryption services for the High Availability for Conventional IV&D (HA Data) feature.

1.3.8
Site Gateway (Conventional Channel Interface)

The Site Gateway (Conventional Channel Interface) interfaces with the RNG component of the PDG. The Site Gateway (Conventional Channel Interface) is responsible for managing access to the conventional channel resource for conventional data.

NOTICE: See the *GGM 8000 System Gateway* manual for details regarding the GGM 8000 as a Conventional Channel Gateway (CCGW) interface device.

1.3.9
Conventional RF Site Equipment

Conventional site equipment is needed to transmit and receive Conventional datagrams over the air. See the supported Channel Topologies in Table 3: ASTRO 25 Conventional with Integrated Data Capabilities on page 36.

When configuring the conventional site equipment for Integrated Data, consideration should be given to the following:

- **Hang Time** – Data reliability is significantly decreased when hang time is not configured on a conventional channel. Conventional channels that provide packet data service should enable hang time on the channel.
  - GTR 8000 Base Radio configurations should enable the Infrastructure Data Drop Out Delay parameter and set the Infrastructure Data Drop Out Delay Timer parameter to the desired value.
  - GCM 8000 Comparator configurations should configure the Console Data Hang Time parameter to be a non-zero value.
  - ATAC 3000 Comparator configurations should configure the Digital Data Console Hangtime parameter to be a non-zero value.
  - QUANTAR® station configurations should configure the Drop Out Delay parameter to be a non-zero value.
- **Site Steering** – In simulcast configurations, packet data is site steered. As such, the Conventional Channel Data Mode parameter of the conventional channel needs to be set to `ASTRO25SubsiteSteered` in simulcast configurations.

1.3.9.1

Conventional Channel (Base Radio)

The Conventional site equipment implements one or more Conventional Channels. A Conventional Channel is the logical entity over which Conventional datagrams are exchanged between the site equipment and the SU. A Conventional Channel is comprised of the over-the-air transmit and receive frequencies as well as the wireless or wireline links connecting the channel's RF equipment to the Site Gateway (Conventional Channel Interface). A Conventional Channel may terminate in a single transmit/receive location or may be comprised of multiple terminating "subsites" (each of which is connected to the Site Gateway (Conventional Channel Interface) via a Comparator). Conventional channels that are intended to support Conventional Packet Data between SU's and the CEN need to be configured as Data Capable in the Network Manager. If a channel is used for repeated data between SU's, Data should be disabled in the Network Manager.

NOTICE: A Conventional Channel is always present (not allocated on demand) and is shared for both audio and Packet Data services in ASTRO® 25 Conventional IV&D. Therefore, audio calls preempt Packet Data calls. Also, packet size should be considered when using repeat data on conventional channels to minimize the risk of truncated audio. This is most important for Conventional Talkgroups.

A Repeater may be configured to route inbound datagrams to the infrastructure ("Radio-to-Infrastructure" mode) or to repeat them over the outbound channel ("Repeated Data" mode). Channels on a Repeater configured for "Repeated Data" mode should be configured as not Data Capable via the Network Manager.

NOTICE: QUANTAR® station support of Repeated Data is uncertified. Although the Repeated Data feature can be enabled in the QUANTAR® station, and may work in certain circumstances, there are exceptions where unexpected and undesirable data performance may result.

1.3.10

Data-Capable Conventional Subscriber Unit (SU)

The SU provides an interface between an attached mobile computer and the radio network. Some SUs are capable of running onboard IP-based applications directly. An SU that needs to have access to data service needs to have its Conventional Unit record configured as Data Capable in the Network Manager.

When an IP-aware SU detects a condition in an inbound message that makes the message undeliverable, the SU generates and sends Internet Control Message Protocol (ICMP) error notifications to the Mobile Computer (MC). The mobile computer can then notify the end-user application of the event. For more information about ICMP messages, see Internet Control Message Protocol (ICMP) Messaging on page 75.

1.3.11

Key Management Facility (KMF)

The Key Management Facility (KMF) is a Motorola Solutions-provided server residing within the CEN that manages the encryption keys used in an ASTRO® 25 system. The KMF has been modified in ASTRO® 25 release 7.12 to support the ASTRO® 25 Conventional IV&D transport service (known within the KMF as "IP Conventional") in addition to the already supported Trunking transport service and an ASTRO® 3.1 Conventional transport service. A single KMF may be used to control centralized key management operations for Trunking, Conventional, and ASTRO® 25 Conventional IV&D systems. Each ASTRO® 25 7.12 Conventional transport service may be associated with a Conventional Broadcast Data Agency IP address for use in delivering group OTAR datagrams to Conventional SUs. Up to 6 Trunking and (separately) 6 Conventional transport services are supported by a single KMF.

The KMF controls key management for both OTAR clients (for example, SU units) and OTEK clients (the CDEM in the case of ASTRO® 25 Conventional IV&D). The KMF supports a maximum of 64,000

OTAR clients across all key management Transport services. The Key Variable Loader (KVL) is used with the KMF to perform Store and Forward key management activities and to initialize key management client devices to enable the use of OTAR or OTEK.

1.3.12
Key Variable Loader (KVL)

The Key Variable Loader (KVL) is a handheld device that allows encryption key management and configuration for the CDEM and SUs, and can install software updates into the CDEM (the device ships with necessary hardware installed).

The following KVL models can be used in the ASTRO® 25 Conventional with Integrated Data feature:

KVL 3000
Supports DES-OFB algorithm, does not support AES algorithm or black (encrypted) keyloading.

KVL 3000 Plus
Supports all algorithms. Version R03.52.45 or later supports black (encrypted) keyloading.

KVL 4000
Supports all algorithms, supports black (encrypted) keyloading.

NOTICE: The CDEM supports a serial shell interface command, “fips enable”, that results in only encrypted keyloading messages being sent to the CDEM by a KVL. A KVL 3000+ or later model KVL with the appropriate software load is required to operate in this mode.

1.4
ASTRO 25 Conventional with Integrated Data Capabilities

Table 3: ASTRO 25 Conventional with Integrated Data Capabilities

Capability	Description
Transport method	SCEP Conventional Packet Data
Frequency	700 MHz, 800 MHz, UHF, and VHF frequency bands, depending on site equipment
Zones	Operation in up to 7 zones
Conventional Packet Data SUs	• Maximum number of concurrently active Conventional Packet Data SUs in M1, M2 or K core: - 20,000 in a single zone - 40,000 across all zones in an entire ASTRO® 25 system. M3 systems, it is 48,000 in a single zone and 48,000 across all zones.
Manual Registration Type SUs	Manual SUs may be located in a single zone or distributed across zones. • Maximum concurrently active Conventional Packet Data subscribers for M1, M2 or K core: - 20,000 in a single zone - 40,000 across all zones • Maximum concurrently active Conventional Packet Data subscribers for M3:

Table continued…

Capability	Description
	- 48,000 in a single zone - 48,000 across all zones
Number of messages	Up to 1,000,000 clear (unencrypted) or 500,000 secure (encrypted) messages per hour per zone (with 512 byte packets Inbound and Outbound) and across all zones in an entire ASTRO® 25 system. **NOTICE:** The total data message traffic is based on the maximum message rate for a channel, the maximum number of channels in a zone and the percent of channels in a zone that your organization is willing to dedicate to data traffic. **NOTICE:** OTAR datagrams are encrypted at the application level, not by the ASTRO® 25 Conventional IV&D service. Therefore, OTAR datagrams are classified as unencrypted traffic.
Protocols	Industry standard – TIA, IPv4, DHCP, PPP, SSH, SNMPv3, SFTP, UDP, TCP
Tunneling	• IP-in-IP or VPN tunneling between the ASTRO® 25 network's entry point for CEN traffic (Border Gateway) and the Conventional GGSN • GTP tunneling between the Conventional GGSN and the Conventional PDG in the zone where an SU is receiving service
SU types	Data-capable SUs as well as attached Mobile Data Terminals All previously used 3.1 Conventional SUs as well as existing XTL/XTS 5000, XTS 3000/Spectra Plus, APX 7000, and APX 7500 SUs provide Conventional packet data support in SCEP mode.
Conventional SU mobility	• SU mode (channel) change within a zone and between zones in an ASTRO® 25 release 7.12 system, and to/from other Conventional systems • Dynamic, Data-Triggered, and Manual/Static Registration modes • SU Vote Scan and Data Scan • Data Site Steering • Conventional Radio Finder
IPv4 Datagram delivery (messaging) services	• Confirmed and Unconfirmed Unicast • Unconfirmed Group/Broadcast
Data encryption algorithms	DES-OFB and AES 256
Broadcast Data Agencies	Up to 20
GGSNs supported	One per system
PDGs supported	One Conventional IV&D PDG per zone or two PDGs to support High Availability for Conventional IV&D
CDEMs supported	One per PDG

Table continued…

Capability	Description
Contention	Audio call, supplementary signaling, station control and datagram contention mitigation
Over-the-Air Re-keying (OTAR)	Individual and group
Co-existing services	Trunked IV&D and HPD
Channel types	P25 Digital Conventional (V.24 and IP link types) and Mixed Mode (4-wire analog with V.24 digital link)
Modes of operation	Radio-to-Infrastructure and Repeated Data
Channel topologies supported	• Receive Only • Simplex • Control Station • Repeater • Remote DIU (RF link to DIU) • Wireline Comparator (voting, multicast, simulcast) **NOTICE:** The RF equipment used may limit functionality; not all versions of GTR 8000 Base Radios match all QUANTAR® station features.

1.5 Typical Conventional Data Services Usage

The estimated maximum number of messages is based on the typical data usage profile. Remember, that the usage and type of data messages can vary from system to system.

The most common data usage profile is the following:

- 1% of radios are in active POP25 session
- 10% of radios are in an active OTAR rekey transmission
- 20% using Outdoor location at a 60 seconds cadence.
- 1% of users are sending a text message to the dispatch operator

Chapter 2

Conventional Data Services Theory of Operation

This chapter explains how the ASTRO® 25 Conventional with Integrated Data feature works in the context of your system.

IMPORTANT: As discussed in ASTRO 25 K Core Configuration Functionalities on page 28, there are differences between M core and K core system functionality. In this chapter, any reference to the following items only applies to M core systems: Network Manager (Provisioning Manager, UEM, UNC, and ZDS), multiple zones, and zone controller.

2.1 How Datagrams are Transported

Since private IP addresses may be assigned to subscribers and hosts, an IP datagram generated by a subscriber/mobile computer or CEN host is not directly routable within the ASTRO® 25 network. For this reason, a user's IP datagram is encapsulated by protocols that transport the datagram from one end of the system to the other. The IP and transport protocol (typically UDP) headers generated by the originating subscriber or CEN host are encapsulated and transported across the system along with the application payload. This encapsulation is performed when the datagram is received at the ASTRO® 25 system's originating access point; in this case either the Border Gateway or the subscriber.

IMPORTANT: It is recommended that User Datagram Protocol (UDP) be used as the transport protocol for IP messaging between CEN hosts and subscribers (or attached mobile computers). Conventional IV&D's confirmed over-the-air delivery service addresses most of the reliability concerns a connection-oriented transport service such as TCP is intended to address, with less of a reduction in throughput.

After the datagram travels the ASTRO® 25 network and reaches its destination it is de-encapsulated and the original IP and transport headers are delivered to the destination along with the application payload. In this way, the subscribers and CEN hosts running an application may interact as though they are co-located on the same Local Area Network.

The process of encapsulating protocol headers and associated user data into a different protocol to route this information from one point to another is known as tunneling. The ASTRO® 25 system transports IP datagrams between a Conventional subscriber and a CEN host using three primary tunneling mechanisms:

- Simple CAI Encapsulation Protocol (SCEP)
- GTP
- IP-in-IP or VPN

Figure 5: Conventional IP Datagram Transport via ASTRO 25 Tunnels on page 40 shows tunneling between a conventional subscriber and a CEN host.

2.1.1 SCEP Tunneling

Unicast datagrams are transported in CAI format on the over-the-air link as well as on the ASTRO® 25 network links between the station equipment and the Conventional RNG using a SCEP tunnel. The confirmed and unconfirmed delivery services are implemented between the endpoints of this tunnel. When an IP datagram is sent by either a subscriber or the Conventional RNG, it is segmented into a

number of blocks whose format depends on whether confirmed or unconfirmed delivery is used as described in TIA-102.BAEB-A. When all blocks comprising the datagram have been received by either the subscriber or Conventional RNG the datagram is reassembled and checked for bit errors. Retransmission is requested if errors are detected and confirmed delivery is being used. For more information about confirmed and unconfirmed delivery, see Confirmed vs. Unconfirmed Message Delivery on page 56.

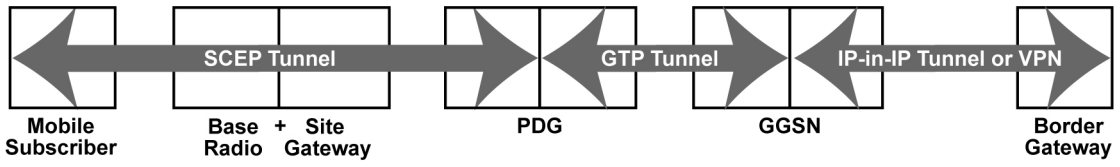
2.1.2
GTP Tunneling

Datagrams are transported between the Conventional PDR and the Conventional GGSN using a GTP tunnel. The two endpoints of this tunnel may be located in the same zone or in different zones. A separate GTP tunnel is created for each ASTRO® 25 Conventional IV&D subscriber during Packet Data Registration, and each subscriber's tunnel remains in place as long as the subscriber remains registered for Conventional integrated voice and data service.

2.1.3
IP-in-IP or VPN Tunneling

Datagrams are transported between the Conventional GGSN and the Border Gateway using either an IP-in-IP tunnel or a Virtual Private Network (VPN). As with the GTP tunnel, the two endpoints of this tunnel may be located in the same zone or in different zones. While separate GTP tunnels exist for each registered ASTRO® 25 Conventional IV&D subscriber, a separate GGSN-to-Border Gateway tunnel is only required for each combination of subscriber IP address ranges (subscriber address subnets) and CEN host IP address ranges (CEN host address subnets) that must be able to exchange IP traffic. If a single subscriber IP address range is used in an ASTRO® 25 system, and only a single CEN exists, then only a single GGSN-to-Border Gateway tunnel need exist. When an inbound datagram needs to be routed to a CEN, the Conventional GGSN selects the tunnel to use to route the datagram to the Border Gateway based on an Access Point Name (APN) configured by NM in the subscriber's record. The provisioned APN is associated with a subscriber's IP address and stored by the Conventional GGSN at the time the subscriber's GTP tunnel is created.

Figure 5: Conventional IP Datagram Transport via ASTRO 25 Tunnels



2.2
How Subscribers are Registered

To receive Conventional Packet Data service, a data-capable subscriber must be registered for the service. The registration process verifies the subscriber is eligible to receive ASTRO® 25 Conventional IV&D service, sets up internal data structures needed to provide this service, and establishes the GTP tunnel between the Conventional PDR and the Conventional GGSN.

The Conventional PDG is configured by the Network Manager with subscribers' records, each of which contains a Registration Type. To ensure a subscriber's data service functions correctly, it is important that each subscriber's Registration Type be configured correctly. There are three Unicast Registration Types:

- Dynamic Registration
- Data-Triggered Registration

- Manual Registration

NOTICE: Unlike Trunking IV&D, SCEP Conventional subscribers are not SNDCP-capable, are not aware of, and do not initiate packet data Context Activation. A Context Activation procedure is performed by the infrastructure on behalf of each subscriber, but the subscriber is not explicitly aware of this processing. Since it is an internal ASTRO® 25 system function for SCEP Conventional subscribers, Context Activation is not discussed in this document.

2.2.1 Dynamic Registration

Dynamic registration applies to subscribers that send Conventional Registration Connect and Disconnect messages to the infrastructure. This type of subscriber should be provisioned for Dynamic Registration unless they are expected to always be registered. If they are always expected to be registered they must be provisioned for Manual Registration.

These subscribers are designed to register with the infrastructure by sending a Conventional Registration Connect message upon power-up, mode change (which can be a channel change), and in certain other circumstances. In the case of a mode change from one data-capable channel to another, the subscriber automatically sends a Conventional Registration Disconnect message on the old serving channel (before leaving the channel) followed by a Conventional Registration Connect message on the new serving channel if it is compliant with TIA-102.BAAD-1. Once registered, these subscribers remain registered until they explicitly deregister (for example, by changing modes to a non-data capable channel or powering off) or their Standby timer expires. Dynamic subscribers may be provisioned to receive service in multiple zones within an ASTRO® 25 system. Dynamic Registration is performed using location and Scan Mode information provided with the Conventional Registration Connect message.

NOTICE: Previously used Motorola Solutions Conventional subscribers send a proprietary form of Registration Connect and Disconnect messages, and both the standard and Motorola Solutions proprietary messages are accepted. Subscribers that send proprietary messages should be provisioned for Dynamic Registration.

2.2.2 Data-Triggered Registration

Data-Triggered registration applies to subscribers that do not support sending Conventional Registration Connect and Disconnect messages to the infrastructure. This type of subscriber should be provisioned for Data-Triggered Registration unless they are expected to always be registered. If they are always expected to be registered they must be provisioned for Manual Registration.

When a subscriber provisioned for Data-Triggered Registration moves into or powers up in a zone, the infrastructure implicitly registers it on receipt of the first inbound datagram. Once registered, the subscriber remains registered until the Standby timer expires (Data-Triggered subscribers have no way to explicitly de-register). Data-Triggered subscribers may be provisioned to receive service in multiple zones within an ASTRO® 25 system. Data-Triggered Registration is performed using location information provided with the inbound message that triggered the registration, but with Scan Mode information provisioned via the Network Manager.

2.2.4 Automatic Re-Registration of Subscribers

Once a subscriber is successfully registered for ASTRO® 25 Conventional IV&D service, the Conventional PDG attempts to maintain the subscriber's registration state despite various types of failures such as Conventional GGSN reset/restart and failure/recovery of the network path between the Conventional GGSN and the Conventional PDG. Upon detection of a recovery from these types of events, the Conventional PDG attempts to automatically re-register those Dynamic and Data-Triggered

subscribers that were successfully registered before the failure. In addition, automatic registration of Manually registered subscribers is performed in these same instances.

Re-registration of previously registered Dynamic and Data-Triggered subscribers is performed in the same manner as automatic registration for Manually registered subscribers. While Dynamic and Data-Triggered registration is performed using the location from which the inbound messaging that triggered the registration was received, automatic re-registration of these subscribers uses the subscriber's last-known location recorded by the Conventional PDG (based on the last inbound datagram received from the subscriber). And, if a Scan Mode was received from any subscriber in a dynamic registration request (Registration Request Connect), that value is used instead of any provisioned value during re-registration. Re-registration of a previously registered Manually registered subscriber is performed in the same manner as automatic registration.

2.2.5
Subscriber Deregistration

Deregistration of a subscriber may occur for the following reasons:

- Loss of contact with the GGSN (temporary deregistration)
- Change or deletion of subscriber provisioning information
- Explicit deregistration request from subscriber
- Expiration of subscriber standby timer
- Implicit deregistration initiated by the GGSN designated for Conventional traffic to an old serving Conventional PDR upon receipt of a registration request from a new serving Conventional PDR (occurs when a subscriber moves from one zone to another and an explicit deregistration request was not received by the GGSN before the receipt of the new registration request)

2.3
How Subscribers are Assigned IP Addresses

The IP address of a subscriber is assigned and associated with its CAI ID as part of registration processing. A Conventional subscriber may be assigned an IP address in the following ways:

- Static IP assignment
- Dynamic IP assignment

2.3.1
Static IP Assignment

IP addresses must be statically assigned to subscribers that use IP-based applications (for example, text message service or a client/server application such as license plate lookup). This is because the host server in the Customer Enterprise Network (CEN) must know a subscriber's IP address to send outbound datagrams to an application running on the subscriber (or an attached mobile computer). A statically assigned IP address must be provisioned for the subscriber via NM in the infrastructure and via Customer Programming Software (CPS) in the subscriber itself. The values provisioned in both locations must match. These IP addresses must remain constant when the subscriber moves from one zone to another; this is not guaranteed when dynamically assigned IP addresses are used (see Dynamic IP Assignment on page 42).

2.3.2
Dynamic IP Assignment

For subscribers not running IP-based applications but requiring OTAR support, dynamically assigned IP addresses may be used. This is because the Conventional implementation of OTAR uses IP datagrams between the KMF and the PDR, but not between the RNG and the subscriber. The IP

address in this case is only used within the ASTRO® 25 system infrastructure to route datagrams to the PDR. It is not necessary in this case for the IP address assigned to the subscriber in the infrastructure (via the Network Manager) to match that assigned in the subscriber unit itself via CPS. Dynamically-assigned IP addresses are subnet dependent and are subject to change from one zone to another. This is not a problem for subscribers requiring only OTAR support because changing modes (channels) when leaving one zone coverage area and entering another causes a new IP address to be assigned. Since the dynamically assigned IP address always corresponds to the zone in which registration was performed, the infrastructure is always able to route IP packets for the subscriber to the correct PDR.

Dynamic IP Assignment in Border Router

The Border Router provides an onboard DHCP service for dynamic IP address allocation. Alternatively, the Border Router may be configured to use an external DHCP service. The Border Router's onboard DHCP service supports two methods for dynamic IP address assignment. In one method (the typical dynamic IP address assignment method) the Border Router assigns the next available IP address from a specified subnet range. The other method allows the operator to associate an IP address with a subscriber's MSISDN value such that the DHCP service returns the IP address specifically associated with that subscriber. This allows static IP address assignment to be performed via DHCP rather than by provisioning each IP address via the Network Manager.

2.4 Broadcast Data Agency Registration

Up to 20 Conventional Group/Broadcast Data Agencies may be provisioned in an ASTRO® 25 system. Similar to Manually registered subscribers, the Conventional PDG automatically registers any configured Broadcast Data Agencies for service upon initialization. An IP address and associated CAI ID are assigned to each agency in the same manner as for unicast subscribers. IP addresses for Broadcast Data Agencies must be statically assigned; dynamic IP address assignment is not supported. Each subscriber included in a particular agency must be configured with that agency's CAI ID via CPS. CEN hosts sending datagrams to a Broadcast Group must address the datagrams to the agency's IP address. Each agency is registered with a separate IP address (but the same CAI ID) in all desired zones of a multi-zone ASTRO® 25 system. These agencies remain registered for Conventional IV&D service – the Conventional PDR periodically renews Conventional Broadcast Data Agency registrations to ensure a transient fault does not result in more than a temporary loss of Broadcast Data Agency service.

Ensure that the IP address configured for an agency is valid within the sourcing CEN and that it matches the IP address used by the customer application for each zone that can be reached with the desired datagram. Failure to do so will prevent an application at the mobile computer from receiving the datagram and/or cause the wrong applications to receive it.

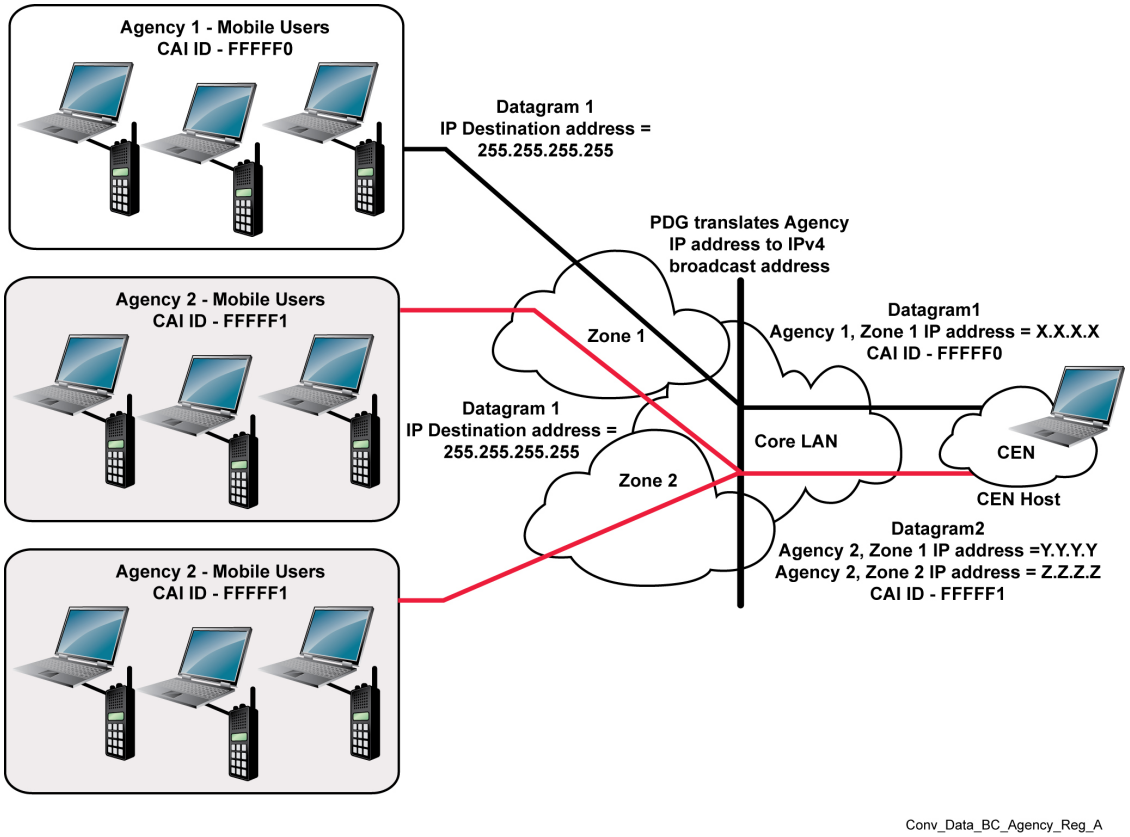
The ASTRO® 25 Conventional IV&D service transmits group/broadcast datagrams for an agency on all available Conventional channels after translating the agency's IP address to the IPv4 broadcast address (255.255.255.255). The agency's CAI ID is included in a header transmitted with each datagram. A subscriber identifies and receives any group/broadcast datagram addressed to one of its configured agency CAI IDs. All received group/broadcast datagrams are routed to an attached Mobile Computer. Any application-level routing of group/broadcast datagrams within the Mobile Computer is expected to be accomplished via UDP Destination Port addresses (since group/broadcast messages for all agencies are transmitted with the IPv4 broadcast address).

CAUTION: Use care when configuring and sending messages to the system-wide All-Call Broadcast ID (0xFFFFFF). When the All-Call Broadcast ID is used, all subscribers in range of the system receive the message. This may interfere with application-level messaging, especially in system configurations with multiple Agency Users and multiple connected CENs which are not intended to share messages through the Radio Network System.

NOTICE: The Broadcast ID value of 16,777212 (0xFFFFFC) is reserved for use within the ASTRO® 25 system infrastructure. Do not use this value to identify a Conventional Broadcast Data Agency.

The CEN host must send a broadcast message to all Agency 1 members in Zone 1 and another broadcast message to Agency 2 members in Zones 1 and 2. It does so by sending an IP datagram addressed to Conventional Broadcast Data Agency 1's Zone 1 IP address (associated with that agency's broadcast CAI ID). That message's destination IP address is replaced with 255.255.255.255 so the receiving mobile computer TCP/IP communication stacks accept the IP datagram for final routing to the applicable mobile application. The message is then transmitted to all agency subscribers in Zone 1's RF coverage area. Similarly, the CEN host sends an IP datagram addressed to Conventional Broadcast Data Agency's Zone 1 and Zone 2 IP addresses (both associated with that agency's CAI ID) so the Agency 2 subscribers in zone 1 and 2's RF coverage area can receive the broadcasted message.

Figure 6: Broadcast Messaging in a Multi-Zone System



2.5 How Mobile Subscribers are Handled

When an ASTRO® 25 Conventional IV&D subscriber changes modes from one data-capable channel to another within the same zone, the channel may be served by the same or a different Site Gateway (Conventional Channel Interface). All Site Gateways (and therefore all Conventional channels) in a zone are served by a single Conventional RNG. The Conventional RNG tracks the last known Conventional site and channel on which an inbound datagram was received from each subscriber and uses that information when outbound datagrams must be sent to the subscriber. Thus, the Conventional RNG tracks subscriber mobility within a single zone.

Similar to Trunking IV&D, a conventional IV&D subscriber is homed to a zone in an ASTRO ® 25 system. When the radio user manually changes modes from a data-capable channel in one zone to a

data-capable channel in another zone, the new channel is served by the conventional RNG in the visiting zone. The visiting conventional RNG communicates with the Conventional PDR and GGSN in the subscriber's home zone for subscriber message delivery to and from the CEN

The Conventional Home zone map provisioning determines the Radio home zone affiliation. Each zone in the conventional home zone map is configured with the conventional unit ID ranges home to the zone. The mapping is provisioned at the Network manager and a conventional Unit ID can appear in no more than one zone of the Conventional home zone map.

2.6 How Subscribers Interface with Mobile Computers

The ASTRO® 25 Conventional IV&D SCEP tunnel originates (for inbound) and terminates (for outbound) IP datagram messaging at the subscriber. This is true regardless of whether an IP application is running on the subscriber itself or on an attached mobile computer. To support IP applications running on an attached computer, the computer must be connected to the subscriber with a serial interface, either RS232 or USB, depending on the interface on the computer and the subscriber.

The physical connection is managed by software running on both the subscriber and the computer, which sets up the serial connection and performs the exchange of datagrams. To perform these functions, the software must use a common set of messages known as the link layer protocol. Depending on the subscriber, one of the following link layer protocols is used:

- Serial Line Interface Protocol (SLIP)
- Point-to-Point Protocol (PPP)
- Remote Network Driver Interface Specification (RNDIS)

Early subscriber models require SLIP and a software package such as MWCS II running on the attached computer to provide the link layer protocol functions. Later subscriber models provide on-board support for PPP and may not require a separate software package running on the attached computer. However, Manual configuration of the serial interface is required. More recent subscriber models provide support for RNDIS and can connect to an attached computer in a “plug and play” mode where little manual configuration is needed. The capabilities of the various subscriber models and any attached mobile computers or other data devices to be used in a particular ASTRO® 25 system must be assessed to determine the link layer connectivity requirements.

Early models of Conventional subscriber units do not support on-board IP applications. These units simply allow a mobile computer to be connected and pass IP datagrams between the mobile computer and the SCEP tunnel, performing the datagram formatting required to interface with the tunnel. Later Conventional subscriber units contain their own IP stack and are capable of running on-board IP applications as well as passing IP datagrams between an attached mobile computer and the SCEP tunnel.

Three possible subscriber-side configurations exist for use with ASTRO® 25 Conventional IV&D:

- An IP-capable subscriber having no connected mobile computer runs one or more on-board IP applications. In this case the IP address assigned via CPS to the subscriber must also be configured for the subscriber in the infrastructure by the Network Manager.
- A subscriber, either not IP-capable or IP-capable but not running any on-board IP applications, is connected to a mobile computer that runs one or more IP applications. In this case the IP address assigned to the mobile computer must be configured for the subscriber in the infrastructure by the Network Manager.
- A subscriber that is not IP-capable and is not connected to a mobile computer runs OTAR. The Conventional OTAR implementation does not require the subscriber to support IP applications (for example, it does not exchange IP datagrams with the subscriber). However, OTAR Key Management Messages are sent between the KMF and the Conventional PDG as IP datagrams. In this case an arbitrary static or dynamic IP address from the subscriber IP address range may be

assigned to the subscriber since the IP address is not used to route datagrams to and from the subscriber.

For subscriber units without an on-board Network Address Translation (NAT) capability, it is only possible to route datagrams to and from the subscriber (only) or the mobile computer (only). The IP address of one of these devices must be configured as the subscriber's IP address in the ASTRO® 25 system infrastructure by the Network Manager. In this case, IP-based applications may only be run onboard the subscriber or on the mobile computer, not both. Therefore, if the onboard Presence, Location, ASTRO® 25 Advanced Message Solution, or POP25 applications must be supported then IP applications on an attached mobile computer cannot be supported. This includes any group/broadcast application since group/broadcast datagrams are always routed to the mobile computer. Conversely, if a mobile computer-based (external) location application or a group/broadcast application must be supported, then only OTAR may be supported onboard the subscriber.

NOTICE: At the time of this document's writing, Motorola Solutions Conventional subscriber units do not have the capability of concurrently routing IP datagrams to and from both an on-board application and an application running on an attached mobile computer.

2.7 Datagram Sizes and Fragmentation

ASTRO® 25 Conventional IV&D accepts outbound unicast and group/broadcast datagrams of up to 1500 bytes in length for delivery to subscriber units.

NOTICE: OTAR datagrams are an exception to this rule because they are limited to less than 512 bytes by the application (not fragmented).

The APCO air interface standard (TIA-102.BAAA-A, FDMA CAI) indicates the maximum transfer unit (MTU) size of an over-the-air datagram is 512 bytes plus a 13 byte encryption header if secure messaging is being used, resulting in an overall total datagram size of 525 bytes. The system supports this datagram size when confirmed delivery is used; for unconfirmed delivery the maximum datagram size is limited to 512 bytes including encryption header. To comply with these size constraints, the Conventional PDG performs IP fragmentation as needed on outbound datagrams. After all fragments are received, the subscriber reassembles them into the original datagram before passing the datagram to the intended application. For more information about confirmed and unconfirmed delivery, see Confirmed vs. Unconfirmed Message Delivery on page 56.

When confirmed delivery is used, datagrams larger than 512 bytes (including the IP and transport protocol headers created by the CEN host) are fragmented into multiple datagrams of no more than 512 bytes each. If secure delivery is used, a 13 byte encryption header is added to each fragmented datagram, resulting in each being no more than 525 bytes long over-the-air.

When unconfirmed delivery is used (including both unicast and group/broadcast datagrams), any datagram that is larger than 499 bytes (including the IP and transport protocol headers created by the CEN host) is fragmented into multiple datagrams no more than 499 bytes each. Since secure delivery adds a 13 byte encryption header, using a fragmentation size of 499 bytes allows the final over-the-air size of a secure unconfirmed outbound datagram to be no more than 512 bytes.

Conventional IV&D accepts inbound unicast datagrams of up to 525 bytes. For secure inbound datagrams, 13 bytes are devoted to an encryption header, leaving a payload size of 512 bytes (including the IP and transport protocol headers created by the mobile computer or subscriber). If IP datagrams larger than 512 bytes need to be sent inbound, IP fragmentation must be performed by the mobile computer's IP stack, as the subscriber does not perform IP fragmentation. Similarly, the Conventional PDG does not reassemble IP fragmented datagrams; reassembly must be performed by the receiving host in the CEN.

2.8
Secure Delivery of Inbound and Outbound Datagrams

The ASTRO® 25 Conventional IV&D service offers the option of secure delivery of inbound and outbound datagrams between the Conventional RNG and a subscriber using either DES-OFB or AES-256 encryption. Each subscriber may be provisioned via the Network Manager for secure inbound and/or outbound service and encryption type. Conventional Broadcast Data Agencies may be similarly provisioned (for outbound service only). A given subscriber or agency may be provisioned for either clear or secure outbound service by the Network Manager; all outbound datagrams are sent according to this provisioning. Conversely, a given subscriber may be provisioned by the Network Manager for strictly secure inbound service, strictly clear inbound service, or both secure and clear inbound service. The choice of whether secure or clear inbound datagrams are sent is determined by a definable CPS mode setting. It is recommended that all subscribers be provisioned via the Network Manager for both secure and clear inbound service; this allows the subscriber to send secure or clear inbound datagrams as programmed per mode.

NOTICE: Test new IV&D applications in clear mode to eliminate secure configuration and processing as variables while debugging application and network transport issues. Once successful functionality is demonstrated in clear mode, secure delivery of datagrams for the application can be tested.

The ASTRO® 25 Conventional IV&D service encrypts an outbound unicast or group/broadcast datagram before routing it to the Site Gateway (Conventional Channel Interface) if the target subscriber or group is provisioned for secure outbound service. Similarly, the ASTRO® 25 Conventional IV&D service decrypts an encrypted inbound unicast datagram before routing it to the Conventional GGSN if the originating subscriber is provisioned for secure inbound service. Secure delivery of datagrams between the Conventional GGSN and the Border Gateway may be provided if a VPN tunnel is used (rather than an IP-in-IP tunnel) between these points in the ASTRO® 25 network.

2.9
Support for MWCS II, RCP, and Radio IP MTG

The ASTRO® 25 Conventional IV&D feature supports existing IP-based applications written using the Motorola Solutions Wireless Communication Software (MWCS) II APIs, and new IP-based radio-aware applications may be written using these APIs. MWCS II may be used for ASTRO® 25 Conventional IV&D in the same way as it is used with ASTRO® 25 version 3.1 Conventional systems. Similarly, the RCP protocol and the Motorola Solutions Enhanced Radio Control Protocol (RCP) may be used to manage a subscriber unit in the same way as it is used for ASTRO® 3.1 Conventional systems.

The Radio IP MTG™ middleware package interoperates with the ASTRO® 25 Conventional IV&D system to provide subscriber VPN capabilities in the same way as for previous ASTRO® 25 Conventional and DataTAC releases.

2.10
Key Management

Encryption and decryption operations take precedence over key management activities in the CDEM. In cases where a Key Management Message requests that a Traffic Encryption Key currently being used to encrypt or decrypt a datagram be changed or deleted, the key remains unchanged until processing of the current datagram has been completed. This is true regardless of whether the key management request is conveyed via OTEK or KVL.

2.10.1
Conventional OTAR and OTEK

ASTRO® 25 Conventional IV&D provides centralized key management for its secure CAI Packet Data service for subscribers (and devices treated by the system as subscribers) via APCO P25 Over-the-Air

Rekeying (OTAR) and for the CDEM via Over-the-Ethernet Keying (OTEK). An OTAR- or OTEK-capable device must be seeded with some initial information via a Key Variable Loader (KVL) before OTAR/OTEK may be used. After this initialization procedure, all subsequent key management operations may be completed using OTAR or OTEK. OTAR and OTEK clients must be configured to receive these services both via the Network Manager and at the KMF.

2.10.1.1
Conventional OTAR

Unlike Trunking OTAR, which only supports Individual delivery of OTAR key management messages, OTAR over Conventional IV&D allows secure communication management for groups of subscribers (group OTAR) as well as for individuals. Although OTAR is not an IP application from the subscriber's perspective, OTAR datagrams are carried via IP transport between the KMF and the Conventional PDG. The Conventional PDG converts OTAR Key Management Messages (KMMs) between IP format and CAI (over-the-air) format. For this reason, some IP-related information such as the KMF IP address must be provisioned via the Network Manager for OTAR.

To receive OTAR service, a subscriber must be registered not only for ASTRO® 25 Conventional IV&D (Packet Data) service, but also for Conventional OTAR. SCEP Conventional subscribers, however, do not support OTAR Registration messaging. The Conventional PDG therefore proxies OTAR registration on their behalf. For subscribers who perform Dynamic or Data-Triggered registration, the PDG creates and sends an OTAR Registration message to the KMF upon receipt of the inbound message that triggers Packet Data registration for the subscriber. OTAR registrations for these subscribers are therefore distributed across time in the same way as ASTRO® 25 Conventional IV&D (Packet Data) registrations.

As described in How Subscribers are Assigned IP Addresses on page 42, ASTRO® 25 Conventional IV&D registration for manually registered subscribers occurs automatically when the Conventional PDG starts up. To avoid sending OTAR Registration messages to the KMF at too high a rate if a large number of these subscribers are configured, the PDG introduces a random delay in their OTAR registration time, based on the setting of the Maximum OTAR Registration Delay parameter provisioned via the Network Manager. The delay takes into account the number of OTAR registration transactions outstanding between the Conventional PDG and the KMF so that the delay is longer when a large number of transactions are outstanding.

Failed OTAR registrations triggered by a Dynamic or Data-Triggered ASTRO® 25 Conventional IV&D registration are retried a maximum of 5 times at 15 second intervals. Failed OTAR registrations for Manually registered subscribers are retried indefinitely. The retry interval ranges from 15 seconds to 1 hour, and increases as the Maximum OTAR Registration Delay parameter increases.

OTAR registration is also performed in cases where a Dynamic or Data-Triggered subscriber is automatically re-registered. These OTAR registrations are performed in the same way as for Manually registered subscribers, with random delays between the Packet Data registration and the OTAR registration and with unlimited retries at intervals based on the Maximum OTAR Registration Delay value.

The KMF's Global Enhanced Security Parameter setting will not govern the encryption mode of OTAR messages the Conventional PDG proxies on behalf of a subscriber. These include the OTAR Registration, OTAR Retry Opportunity, and Unable to Decrypt messages.

2.10.1.1.1
Group OTAR

Unlike Trunking OTAR, key management operations that impact multiple OTAR-capable Conventional subscribers may be distributed via broadcast rather than via separate messaging to each impacted subscriber. To accommodate this, each OTAR-capable Conventional subscriber may be associated with an OTAR group at the KMF. Each OTAR group in turn is associated with one of the KMF's 6 Conventional Transport Services. Finally, each of the KMF's Conventional Transport Services is

provisioned with the IP address of one of the ASTRO® 25 system's Conventional Broadcast Data Agencies.

When the KMF operator initiates a key management operation such as a CKR Update, the KMF identifies all the OTAR-capable subscribers impacted by the operation, and by extension all impacted OTAR groups. The KMF then sends one or more group OTAR KMMs for the operation to each impacted OTAR group. This results in some number of group OTAR KMMs being sent to the Conventional Transport Services (and hence the associated Conventional Broadcast Data Agencies) associated with each impacted OTAR group. These KMMs will be delivered via the ASTRO® 25 Conventional IV&D group/broadcast service.

Compared to the ASTRO® 3.1 Group data implementation, where every KMM is preceded by a preamble sequence, sending KMMs in blocks via a High Capacity Broadcast Data Agency (with a preamble preceding the entire block) increases channel efficiency. For example, if 8 CKRs must be updated across 10 different OTAR groups, and the subscribers in all the groups are served by the same Conventional Transport Service (and hence the same Conventional Broadcast Data Agency), 80 CKR Update group KMMs must be sent to that agency for broadcast. Sending the KMMs in blocks of 10 results in 8 blocks of KMMs with 8 total preambles transmitted. In ASTRO® 3.1, sending the same 80 KMMs requires the transmission of 80 preambles.

2.10.1.1.2
OTAR Retry Opportunities

Attempts to perform OTAR updates to a subscriber may fail under certain circumstances (for example, the subscriber unit may be powered off or may not be tuned to a data-capable Conventional channel when the attempt is made). ASTRO® 25 Conventional IV&D supports sending Retry Opportunity messages to the KMF to allow such failed attempts to be tried again. When a Conventional subscriber finishes an inbound audio call on a data-capable channel, the Site Gateway (Conventional Channel Interface) sends a message to the Conventional PDG indicating the subscriber is on the channel. If the subscriber is OTAR-capable, the Conventional PDG sends a message to the serving KMF indicating an attempt may be made to rekey the subscriber. These notifications are only sent to the KMF if such a message has not already been sent for the same subscriber within the previous 10-minute period.

2.10.1.1.3
Decryption/Encryption Failure Indicators

When a subscriber encounters a decryption failure, it sends a Conventional Unable to Decrypt message to the Conventional IV&D PDG. The PDG then creates and sends an Unable to Decrypt KMM to the KMF on behalf of that subscriber if the subscriber is OTAR enabled.

The PDG also creates an Unable to Decrypt KMM and sends it to the KMF on behalf of a subscriber once every 10 minutes for either of the following reasons:

- an encrypted inbound Packet Data message is received from a subscriber that is not provisioned in the Data Subsystem to send secure inbound messaging
- an unencrypted inbound Packet Data message is received from a subscriber that is provisioned in the Data Subsystem to only send secure inbound messaging

When the CDEM encounters a decryption failure it creates and sends its own Unable to Decrypt KMM to the KMF via the PDG once every 10 minutes.

The PDG also sends a fault notification to the UEM once every 10 minutes for any of the following failure types:

- a Conventional "Unable to Decrypt" message is received from a subscriber
- failed attempts to encrypt outbound Packet Data messages to subscribers (who are provisioned in the Data Subsystem to send secure outbound messaging)

- failed attempts to decrypt inbound Packet Data messages from subscribers (who are provisioned in the Data Subsystem to receive secure inbound messaging)
- receiving an encrypted inbound Packet Data message from a subscriber not provisioned in the Data Subsystem to send secure inbound messaging
- receiving an unencrypted inbound Packet Data message from a subscriber provisioned in the Data Subsystem to only send secure inbound messaging

2.10.1.2
Conventional OTEK

Since the CDEM has no connectivity to the ASTRO® 25 network other than as a dedicated client device of the Conventional RNG, the CDEM is not able to perform OTEK procedures directly with the KMF. The Conventional RNG therefore proxies the OTEK connection to the KMF on the CDEM's behalf after detecting the CDEM has successfully connected via its dedicated link. Once the OTEK connection is established, the Conventional RNG passes OTEK Key Management Messages (KMMs) to and from the CDEM.

Some initial CDEM setup is required via both KVL and a serial connection before OTEK procedures may be performed. See the *CAI Data Encryption Module User Guide* manual for additional information.

If the CDEM receives an OTEK key management message it cannot decrypt from the KMF, it responds with an Unable to Decrypt KMM (sent via the Conventional RNG proxy). This allows the KMF to initiate additional key management operations with the CDEM if necessary to repair any problem that might hamper the CDEM's ability to provide secure service.

2.11
ASTRO 25 Conventional with Integrated Data Message Processing

Any P25 Digital or Mixed Mode channel at a Conventional Site served by an ASTRO® 25 system version 7.x Site Gateway (Conventional Channel Interface) may be designated as a Data Channel. However, the subscriber must be switched to a Conventional Packet Data-capable mode to transmit and receive datagrams. After the registration procedure completes for a subscriber (within the infrastructure), the subscriber can send and receive datagrams.

This section describes inbound (unicast) and outbound (unicast and group/broadcast) data messaging in the ASTRO® 25 Conventional with Integrated Data feature.

2.11.1
Conventional Inbound Data Messaging

When an inbound datagram needs to be sent to the ASTRO® 25 system infrastructure via the CAI interface (originated either from an on-board application in the subscriber unit or from the mobile computer) and the subscriber is registered for ASTRO® 25 Conventional IV&D service, the subscriber formats and sends the datagram to the infrastructure via the SCEP tunnel. The datagram's IP header Destination Address must be set to the IP address of the host in the CEN on which the desired peer or server application is running. Similarly, the Destination Port in the UDP header must be set to the desired application's port number. For confirmed inbound datagrams, the subscriber retransmits all or part of the datagram if no Acknowledgement or a Selective Acknowledgement is received.

Upon successfully receiving and reassembling the datagram, the Conventional PDG overwrites the Source Address in the datagram's IP header with the IP address configured for the subscriber via the Network Manager. The Conventional PDG uses this IP address to identify the subscriber's GTP tunnel and sends the datagram to the Conventional GGSN. The GGSN then examines the Destination Address field in the datagram's IP header to determine the IP-in-IP tunnel or VPN to use to route the datagram to the appropriate Border Gateway. From there, the datagram is routed to the destination

host in the CEN, based on the IP header Destination Address, using the existing network between the Border Gateway and the CEN host.

2.11.2
Conventional Unicast Outbound Data Messaging

When an application running on a host in the CEN has a datagram it needs to send to a peer or client application running either on a single subscriber or a mobile computer connected to a single subscriber, it must place the subscriber's IP address (as assigned via the Network Manager) in the Destination Address field of the outbound datagram's IP header. Similarly, the Destination Port in the UDP header must be set to the desired application's port number. Once sent from the host computer, the CEN is responsible for routing the datagram to the Border Gateway (the entry point into the ASTRO® 25 network) based on the Destination Address.

NOTICE: The subscriber's IP address is the (single) translated IP address presented to the ASTRO® 25 system infrastructure.

When the datagram arrives at the Border Gateway, the Destination Address is again used to select the proper IP-in-IP tunnel or VPN in order to route the datagram to the Conventional GGSN. The GGSN then uses the Destination Address to select the subscriber's GTP tunnel and sends the datagram to the Conventional PDG that is currently serving the subscriber.

Upon arrival at the Conventional PDG the datagram is queued, if necessary, for outbound delivery. A unicast outbound datagram is queued behind other undelivered unicast outbound datagrams that arrived previously for delivery to the same subscriber or to subscribers on the same Conventional channel. Even if no other such datagrams exist for delivery when a new unicast outbound datagram is received, the datagram is queued if the Conventional channel is currently Busy.

NOTICE: The Site Gateway (Conventional Channel Interface) indicates the state of a Data-Capable Conventional channel to the Conventional PDG. At any point, a Data-Capable Conventional channel may be Available (able to deliver outbound datagrams), Busy (unable to deliver outbound datagrams due to voice contention, co-channel interference, or another reason), or Withdrawn (not operational).

If the Conventional PDG is not able to initiate delivery of a unicast outbound datagram within a system-defined period of time, or if the datagram is received at a time when the Conventional channel is in the Withdrawn state, an ICMP failure message is returned to the originating host. Otherwise, the Conventional PDG formats and send the datagram to the subscriber via the SCEP tunnel.

2.11.2.1
Vote Scan and Data Scan

Any subscriber that explicitly registers for Conventional Packet Data service by sending a Conventional Registration Request Connect message into the infrastructure includes an indication in that message as to whether the subscriber is operating in Scan Mode. The operator is allowed to provision (via the Network Manager) a similar indication for subscribers that do not explicitly register. Additionally, each data-capable Conventional channel is provisioned to indicate whether Vote Scan is used by subscribers on the channel.

Data Scan is a mode of operation where the receiver in the subscriber unit rotates through a designated list of channels (the "scan list") looking for an outbound transmission. One channel within a Data Scan list may be designated as a data channel (channel on which datagrams may be received). Transmitting a preamble sequence immediately prior to an outbound datagram allows time for the subscriber to detect outbound activity and lock onto the data channel before the datagram is transmitted. The subscriber "hangs" on the data channel for an operator-configurable period of time before resuming its rotation through the scan list. The Conventional RNG requests the Site Gateway (Conventional Channel Interface) to transmit a preamble sequence prior to an outbound unicast datagram if the subscriber is operating in Data Scan mode and is not believed to be hanging on the target channel.

Vote Scan is a mode of operation where the subscriber expects to receive the same outbound transmission on multiple channels in a Multicast topology (each outbound channel transmits on a different frequency). The subscriber assesses the quality of the signal received on each channel in the Vote Scan list and locks onto the channel with the strongest signal. Transmitting a preamble sequence immediately prior to an outbound datagram allows time for the subscriber to detect and lock onto the channel with the strongest signal before the datagram is transmitted. The subscriber “hangs” on the data channel for a short, non-configurable period of time before resuming its assessment of the Vote Scan channel list. The Conventional RNG requests transmission of a preamble prior to each outbound unicast datagram and inbound packet acknowledgment if the subscriber is operating in Vote Scan.

2.11.3
Conventional Group/Broadcast Outbound Data Messaging

Conventional group/broadcast datagrams are sent using unconfirmed delivery. When an application running on a host in the CEN has one or more datagrams to send to a peer or client application running on mobile computers connected to a group of subscribers (or the entire subscriber population), it must place the IP address of that group’s Conventional Broadcast Data Agency (as assigned via the Network Manager) in the Destination Address field of each outbound datagram’s IP header. Similarly, the Destination Port in the UDP header must be set to the desired application’s port number. These datagrams are routed from the CEN host to the Conventional PDG based on the IP Destination Address in the same way as unicast outbound datagrams are routed.

As described in the previous section, a single queuing mechanism is provided for unicast outbound datagrams. In the case of group/broadcast datagram delivery, two types of queuing mechanisms are provided – Time Sensitive queuing and High Capacity queuing. Each Conventional Broadcast Data Agency is provisioned via the Network Manager to use one of these two queuing types.

When the InterBroadcast Delay Time parameter of the infrastructure is less than the hang time value of the conventional site equipment, it will appear that the conventional subscribers on a conventional channel continuously receive data without pause. In actuality, the conventional channel will be available for outbound transmissions during the inter-broadcast delay time, even though hang time is active on the channel.

2.11.3.1
Time Sensitive Queueing

The Time Sensitive broadcast data service is intended for applications needing to deliver one (or a small number of) group datagrams at a time with as little delay as possible. It is not designed to accommodate large volumes of data. Time-Sensitive queuing is meant for broadcast applications that are characterized as follows:

- A single datagram (or a small number of datagrams) is sent to a group on a frequent basis, where “frequent” means a new datagram needs to be sent anywhere from every few seconds up to once every two minutes.
- The group data becomes “stale” quickly, meaning if a group/broadcast datagram has remained in the Conventional PDG’s queue longer than an operator-provisioned amount of time it is desirable to discard the datagram in favor of a more recently received datagram for the same group.

2.11.3.2
High Capacity Queueing

High Capacity queuing is meant for broadcast applications that are characterized as follows:

- A large number of “one time” datagrams are sent from one or more broadcast applications to a group. “One time” as used here implies an application sends datagrams relatively infrequently to the group (anywhere from every few hours to every few months).

- The group data does not “age” or become “stale” quickly. Depending on the amount of broadcast data to be sent to the group, the data may be queued for up to several hours.

If a single group of subscribers is to receive broadcast datagrams from multiple applications, where at least one of these applications sends datagrams in the Time Sensitive category while at least one other application sends datagrams in the High Capacity category, the group must be assigned two separate CAI IDs. Two Broadcast Data Agencies are needed, each with its own IP address mapped to one of these two CAI IDs. One agency is configured for Time Sensitive queuing while the other is configured for High Capacity queuing. Each application must address group datagrams to the IP address corresponding to the agency using the desired type of queuing.

Upon arrival at the Conventional PDG, the datagram is queued, if necessary, for outbound delivery according to the queuing discipline associated with the Conventional Broadcast Data Agency. A group/broadcast datagram is queued behind undelivered datagrams that arrived previously for delivery to the same group. If the Conventional PDG is not able to initiate delivery of a group/broadcast datagram before it expires, an ICMP failure message is returned to the originating host.

The Conventional PDG does not use the SCEP Tunnel for delivery of group/broadcast datagrams. Instead, ASTRO® 25 Conventional IV&D uses the same broadcast multicast tree used by Trunking IV&D. The transmission only happens from the PDG to the sites, no messages are sent from any of the sites back to the PDG. Group/broadcast datagrams are delivered on all available data-capable Conventional channels; the Conventional PDG does not delay delivery of group/broadcast datagrams based on any channel's Busy or Withdrawn conditions.

Group/broadcast datagrams associated with a Time Sensitive Broadcast Data Agency are delivered one at a time, separated by an operator-provisioned inter-broadcast delay interval. Since group/broadcast messages are sent to many subscribers, some of which may be using vote scan or data scan while others are not, the Conventional PDG requests the site equipment to transmit a Preamble sequence before transmitting all group datagrams sent to a Time Sensitive agency.

The primary goal of a High Capacity Broadcast Data Agency is to transmit a large number of datagrams to a group of subscribers as quickly as possible. To achieve this goal, group/broadcast datagrams associated with a High Capacity Broadcast Data Agency are delivered in contiguous blocks consisting of a specified number of datagrams (maximum of 15 datagrams per block). Each block is separated by an inter-broadcast delay interval, and the Conventional PDG requests the site equipment to transmit a Preamble sequence (only) before the first datagram of each block. This delivery scheme takes advantage of the fact that once a scanning subscriber locks onto a channel, it will remain on that channel for a duration known as the “hang time”. The fact that transmitting a contiguous block of datagrams requires only a single Preamble maximizes channel efficiency and minimizes the amount of time taken to transmit the complete set of group/broadcast datagrams for a High Capacity agency.

When using High Capacity Queuing, the full range of Conventional IV&D Broadcast Data Block Size may be used on all channels except ATAC 3000 comparator channels. On ATAC 3000 comparator channels, if broadcast packets of over 500 bytes (including 28 byte IP/UPD header, and 12 byte Esync for secure data) are used, a Conventional IV&D Broadcast Data Block Size of 9 or less must be used. If more than 9 is used, one or more packets in each block will not be transmitted over the air. Broadcast packets of less than 500 bytes may use Conventional IV&D Broadcast Data Block Sizes up to and including 15 on ATAC 3000 comparator channels.

NOTICE: Hang time is configurable via CPS for Data Scan mode. Hang time for Vote Scan is fixed at 200 ms. Large blocks of datagrams prevent radios from scanning for the duration of the block of messages for the length of the block of data (nearly a second per 512 byte block). Therefore, radios receiving many large blocks scan less than normal (possibly for hours).

2.11.4
Concurrent Group/Broadcast and Unicast Outbound Delivery

If multiple CEN applications have group/broadcast data to send to several Broadcast Data Agencies at the same time, the Conventional PDG rotates among all agencies that have datagrams queued for

delivery, sending one datagram (for Time Sensitive agencies) or one block of datagrams (for High Capacity agencies) for delivery each time an agency is reached. The Conventional PDG pauses broadcast delivery for the duration of the operator-configured inter-broadcast delay after sending the datagram or block of datagrams for an agency. When group/broadcast datagrams are received by the site equipment, they are transmitted on all available data-capable channels (operational and not already occupied with voice, previously sent data, co-channel interference, etc.). If a group/broadcast datagram is received at the site equipment when a data-capable channel is not available, the datagram is discarded. By definition, broadcast is a “best effort” delivery service. No ICMP failure message is returned to the originating CEN host in this case. For more information about ICMP messages, see Internet Control Message Protocol (ICMP) Messaging on page 75.

At the same time group/broadcast datagrams are being delivered, the Conventional PDG may also have unicast outbound datagrams to be delivered to individual subscribers. The Conventional PDG does not synchronize the group/broadcast delivery mechanism with the unicast outbound delivery mechanism. However, for unicast outbound delivery, the Conventional PDG does attempt to determine whether the Conventional channel serving the target subscriber is available before sending the datagram to the site equipment. If the channel is not immediately available (already occupied with voice, group/broadcast data, co-channel interference, etc.) the Conventional PDG waits for the channel to become available for an operator-configurable time period before assuming the datagram has become too “stale” to be delivered and discarding it. Unicast outbound datagrams that are discarded result in an ICMP failure message being returned to the originating CEN host.

The typical combined delivery pattern of group/broadcast and unicast outbound datagrams is that unicast datagrams are delivered during the inter-broadcast delays after sending one agency’s datagram(s) and before sending the next agency’s datagram(s). However, depending on the timing of events in the system, it is possible that a unicast outbound datagram might be transmitted between the group/broadcast datagrams within a block.

Applications intending to use the ASTRO® 25 Conventional IV&D group/broadcast and/or unicast datagram delivery mechanisms should make provisions for receiving ICMP failure notifications, and/or include application-level end-to-end reliability and monitoring facilities. The application developer must be aware of Conventional data service characteristics to ensure that any upper-layer operations are compatible with the service.

2.11.5
General Service Interaction Rules

Audio is given precedence over packet data in the ASTRO® 25 Conventional IV&D system. Outbound data service is suspended while outbound audio is active. However, if outbound audio is presented for delivery to a Conventional SU when the Conventional channel is busy with a datagram, the audio is buffered up to one second to allow the datagram to be delivered. When datagram transmission is complete, the system presents the delayed audio to the SU in its entirety.

The following general rules outline system behavior between Data and Audio calls to a subscriber. Both unicast and group/broadcast datagram transmission may be interrupted by audio. Typically, these rules apply only after a subscriber is registered for ASTRO® 25 Conventional IV&D service. However, some are pertinent for registration processing on a Conventional Channel.

The system can buffer one outbound audio call at a time; if contention for a Conventional channel is such that the system would need to buffer more than one audio call, the Zone Controller is notified that the additional call is not granted (no lightning bolt appears on the console channel resource) because the Conventional channel is busy. This condition lasts no longer than 1 second and if the console transmit button is pressed longer than 1 second the outbound call is granted after the second.

The following table displays the general service interaction rules, where the items in the top row occur first, followed by the items in the first column.

Table 4: General Service Interaction Rules

	Outbound activity on Conventional Channel Prior to Contention		
Source of Contention	**Unicast Data/ Broadcast Data**	**CAI Ack**	**Delayed Audio**
Outbound audio	Complete PDU - Buffer Audio for TX	Complete PDU - Buffer Ack for TX	Reject new audio call temporarily*
Outbound Supplementary Request/Acknowledgement	Reject Req/Ack	Reject Req/Ack	Reject Req/Ack
Outbound Emergency Ack	Complete PDU - Buffer Ack for TX	Complete PDU - Buffer Ack for TX	Complete Audio – Buffer Ack for TX
Station Control	Reject Station Control	Reject Station Control	Reject Station Control
Inbound Audio on Voice Repeat	Complete PDU – Truncate Repeated Audio	Complete Ack – Process Repeated Audio	Process Audio according to station priority settings
Inbound Audio or Data on Simplex/Control Station	Possible interference due to collision of inbound and outbound data transmission	Possible interference due to collision of inbound and outbound data transmission	Possible interference due to collision of inbound and outbound data transmission

* New audio call granted upon completion of buffered audio.

The following table displays the interaction rules for data during audio services, where the items in the top row occur first, followed by the items in the first column.

Table 5: Interaction Rules: Data During Audio Services

	Activity on Conventional Channel Prior to Contention				
Source of Contention	**Outbound Audio**	**Outbound Supplementary Request/Ack**	**Outbound Emergency Ack**	**Station Control**	**Inbound Audio on Voice Repeat and Inbound Audio/ Data on Control Station**
Outbound Unicast Data	Continue Audio - Buffer Unicast	Discard Unicast	Continue Emergency Ack – Discard Unicast	Process Unicast after Station Control	Continue Audio - Buffer Unicast
Outbound Broadcast Data	Continue Audio - Discard Broadcast	Discard Broadcast	Continue Emergency Ack – Discard Broadcast	Process Broadcast after Station Control	Discard Broadcast
Outbound CAI Ack	Buffer Ack	Buffer Ack	Buffer Ack	Buffer Ack	Buffer Ack

2.11.6
Confirmed vs. Unconfirmed Message Delivery

Outbound datagrams may be delivered using either confirmed or unconfirmed delivery. If the system is unable to deliver a confirmed datagram an ICMP failure message is sent to the originator. Unconfirmed delivery reduces the likelihood of channel contention and saves bandwidth by eliminating the retries and acknowledgments associated with confirmed delivery. Upon receipt of an inbound unconfirmed datagram, the system neither sends an acknowledgment nor requests a retry if the datagram is received with errors. Delivery of unconfirmed datagrams is not guaranteed. Subscribers served by channels participating in audio conversations or already occupied with data might not receive unconfirmed datagrams. Moreover, subscribers in poor RF coverage areas might miss these messages. The sending application is not informed of such failures when unconfirmed delivery is used.

The system determines that unconfirmed delivery is to be used for an outbound unicast datagram based on the IP Source Address and UDP Destination Port of the datagram. Up to three [Source Address + Destination Port] combinations per Conventional IV&D PDG may be configured via the Network Manager for unconfirmed outbound unicast datagram delivery. Broadcast Data messages are exclusively transmitted using unconfirmed delivery.

Conventional subscribers send all inbound application datagrams using confirmed messaging. (Though certain Conventional non-application messages such as Registration Request – Disconnect (deregistration) are sent using unconfirmed delivery.) There is no CPS configuration available to select an unconfirmed mode of inbound delivery. However, unconfirmed inbound messaging can be configured in a limited fashion if desired through the use of a special configuration tool known as an SNMP MIB browser. Using this tool, the value of an internal parameter can be modified to cause unconfirmed inbound messages to be sent. This change must be made when the link between the subscriber and attached computer has already been established and when the subscriber is on the Conventional channel where unconfirmed inbound messaging is desired. The parameter change remains in effect until a subscriber mode change is performed or the subscriber is power cycled.

2.12
Site Steering of Packet Data

Site steering of outbound datagrams is supported in connection with Voting topologies. It is supported for both Simulcast and Multicast channels, but is not recommended for use on Multicast channels where subscriber Vote Scan is being performed. Since packet data is more sensitive than audio to distortions caused by minor Simulcast phase variances, steering outbound unicast datagrams to a particular Simulcast subsite can improve delivery reliability relative to Simulcasting.

Channels must be provisioned as site steered via the Network Manager. For each subscriber being served by a site steered channel, the Conventional PDG tracks the subsite from which the most recent inbound datagram was received. Subsequent outbound unicast datagrams for that subscriber are routed to that subsite for transmission. In cases where receive-only subsites exist in a Voting topology, each receive-only subsite is mapped to a transmit-capable subsite in the system. Site steered outbound datagrams are then routed to the transmit-capable subsite mapped to the subsite that received the most recent inbound datagram.

The system cannot track sub-site information for Conventional Broadcast Data Agencies; as such Broadcast Data messages are not site steered. Each Simulcast or Multicast sub-site receives a single copy of every Broadcast Data message.

2.12.1
Radio Finder

Radio Finder is an ASTRO® 25 Conventional IV&D function invoked when normal delivery of a confirmed outbound datagram sent to a Conventional subscriber operating on a subsite steered channel is unsuccessful. When Radio Finder is invoked, the system transmits the failed datagram to the subscriber at all the channel's subsites. If the subscriber acknowledges this transmission at a

particular subsite, the system stores the new subsite location for future site steered datagram transmissions.

2.13 Differences Between ASTRO 3.1 Conventional IV&D and ASTRO 25 7.x Conventional IV&D

The following table lists the differences between ASTRO® 3.1 and ASTRO® 25 7.x Conventional IV&D.

Table 6: ASTRO 25 7.x Conventional IV&D Capabilities

Status	ASTRO 25 7.x Conventional IV&D Capability
Encryption Redundancy	Redundant CDEM devices are not supported. Failure of the CDEM device results in the loss of the zone's ability to send or receive encrypted data.
Encryption Algorithms	DES-XL, DVP-XL, and DVI-XL algorithms are not supported. Data can be encrypted using AES-256 and DES-OFB.
Data Redundancy	Partially redundant data equipment (such as the equipment used in ASTRO® 3.1 Conventional IV&D) is not supported. Channels in a zone can only receive data service from the PDG in that zone. Failure of a PDG results in the loss of the zone's ability to send or receive data.
Broadcast Data	Broadcast data is a best effort service. Only channels that are idle at the time of broadcast transmission receive broadcast data.
Information Assurance (IA)	An array of optional IA features are available. None of these features apply to previously used ASTRO® 3.1 system components.
Configuration, Fault, & Performance Management	Centralized configuration, fault, and performance management functions are available. These functions are not available in the ASTRO® 3.1 system.

2.14 Migration from ASTRO 3.1 Conventional IV&D to ASTRO 25 7.x Conventional IV&D

The ASTRO® 3.1 combination of the RNC and the WNG are replaced in ASTRO® 25 7.12 Conventional IV&D by the combination of a GGSN designated for use with ASTRO® 25 Conventional IV&D, the Conventional PDG, and the Site Gateway (Conventional Channel Interface). These system elements are described throughout this document. Many elements of an ASTRO® 25 7.12 Master Site are required to provide Conventional IV&D service.

When migrating an ASTRO® 3.1 system to an ASTRO® 25 7.x system to add ASTRO® 25 Conventional IV&D, the migration engineer must install and configure the ASTRO® 25 7.x system devices needed to enable this service, including the following:

- Conventional channels are connected one by one to the Site Gateway (Conventional Channel Interface) directly or via an ATAC-3000 to provide parallel console operation as well as the ASTRO® 25 7.12 Conventional IV&D service.
- The Transport Network must be configured to enable communication between the Conventional PDG and the Site Gateway (Conventional Channel Interface).
- Install the Conventional PDG.
- Determine which existing GGSN to use for Conventional Packet Data, or whether a new GGSN needs to be added.
- The CDEM (optional) must be installed and configured to communicate with the Conventional RNG.
- An ASTRO® 3.1 KMF must be upgraded to the ASTRO® 25 7.x KMF and existing OTAR records migrated to the new IP Conventional transport service required by this feature.
- The DIU-to-Conventional Channel connection can be disconnected and the new Site Gateway-to-Conventional RNG link can be enabled (via the Network Manager) in its place on a channel-by-channel basis. Only one data infrastructure (ASTRO® 3.1 or ASTRO® 25 7.x) can be in control of a conventional channel at any time.

2.15 High Availability for Conventional IVD Theory of Operation

Conventional IV&D can be established for High Availability by employing redundant components for the conventional data subsystem. This feature provides automatic switchover in case of a component failure to ensure high availability of conventional data services.

The following components support the High Availability for Conventional Data feature:

- Redundant Conventional IV&D PDG virtual machines
- Redundant GPRS Gateway Support Node (GGSN) routers
- Redundant Customer Network Interface (CNI) path equipment, including the RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers, and Redundant Trunked IV&D PDG Virtual Machines

At any given time, one of the two Conventional PDG virtual machines is the primary device, actively supporting conventional data services while the other Conventional PDG is the secondary (inactive) device providing redundancy. Only the primary Conventional PDG is active on the network and accessible by environment. Other devices in the system recognize the pair of Conventional PDGs as one PDG device. The two PDG instances are continuously synchronized so that the secondary PDG is able to assume the primary role without loss of state (including active subscriber context information). If the server hosting the primary PDG fails, Fault Tolerance triggers a switch-over to the secondary PDG, which becomes primary, ensuring recovery of data services. The previously primary PDG that experienced a failure becomes a secondary device after the server recovers.

Components supporting PDG redundancy include the following:

- VMware vCenter application – The vCenter application provides fault tolerance support to manage the switchover between redundant PDGs and it keeps the PDGs in sync. If the VMS hosting the primary PDG fails, the vCenter fault tolerance function triggers an automatic switchover to the secondary PDG, which becomes active.
- Redundant Virtual Management Servers – A redundant Conventional PDG VM (Virtual Machine) is hosted on a separate VMS (Virtual Management Server). A failure of a VMS host triggers an automatic switchover to the secondary PDG running on a separate VMS host.
- Direct Attached Storage (DAS) – An external data storage solution for the Virtual Management Servers hosting the PDG Virtual Machines is used to store PDG data. Both VMS hosts access the same DAS so that the PDG data is not affected by a failure of one host/server and switchover to the other VMS is possible.

Redundant GGSN Routers

At any given time, one of the two GPRS Gateway Support Node (GGSN) routers is active, handling IP traffic for the master site, while the other GGSN remains inactive, providing redundancy. If the primary GGSN fails, the system automatically switches over to the secondary GGSN, which becomes active, ensuring quick recovery of data services. The previously primary GGSN that experienced a failure becomes a secondary device after recovery.

Redundant CNI Path Equipment

The Customer Network Interface (CNI) path equipment consists of the RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, and Border Routers. At any given time, one of the devices in a redundant pair is active, handling transport between the radio network and the Customer Enterprise Network (CEN), while the other device remains inactive, providing redundancy.

Data Subsystem with HA Data

High Availability for Conventional IV&D is a redundancy-based, high availability solution, deployed independently of the Dynamic System Resilience (DSR) feature. Both features can be implemented within a single system to provide an extra high level of redundancy. To support High Availability for Conventional Data in a non-DSR system architecture, redundant components are established in the data subsystem in a single zone core. To support High Availability for Conventional Data in a DSR system architecture, redundant components are established in the data subsystem at the primary zone core as well as the backup zone core. See *Packet Data Gateways* for details.

This page intentionally left blank.

Chapter 3

Conventional Data Services Configuration

This chapter provides high-level configuration processes for components of the ASTRO® 25 Conventional with Integrated Data feature for ASTRO® 25 M core and K core systems.

For detailed configuration procedures and field descriptions about system components, see the following application manuals or online help:

- *Packet Data Gateways* manual
- *CAI Data Encryption Module* manual
- *S6000 and S2500 Routers* manual
- *Conventional Operations* manual
- *Provisioning Manager* manual (M core systems only)
- *Configuration Manager for Conventional Systems User Guide* manual (K core systems only)
- *Configuration/Service Software (CSS)* online help
- *Key Management Facility User Guide* manual
- *KVL 3000 and KVL 3000 Plus Key Variable Loader User's Guide* or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*
- *ASTRO 25 Customer Programming Software (CPS)* Online Help
- ASTRO® 25 subscriber radio User's Guide for your specific model

3.1 ASTRO 25 Conventional with Integrated Data Component Configuration for M Core Systems

Prerequisites: For M core systems, the following applications are used to configure ASTRO® 25 Conventional IV&D communication system components to implement data services:

- Provisioning Manager and Unified Network Configurator (UNC) to configure parameters for the PDG (PDR and RNG), GGSN, Site Gateway (Conventional Channel Interface), and CDEM (for systems utilizing data encryption/decryption)
- PDG local configuration tool to set the PDG to the active state the first time only, and to configure optional parameters
- Configuration/Service Software (CSS) and Unified Network Configurator (UNC) to configure and manage Conventional site infrastructure equipment (base radios/PDCH)
- Customer Programming Software (CPS) to configure subscriber units
- KVL and KMF to load keys into the CDEM
- KMF Client to configure the KMF for conventional data services

Process:

1. Load the Conventional IV&D PDG.
2. Configure the GGSN.

3. Use the UNC Wizard Conventional Subsystem discovery type to discover system devices.
4. Use the UNC System Configuration Wizard to configure the System: System ID and Wide Area Communications Network (WACN) ID. Then use the APN wizard to configure the Access Point Name (APN).
5. Use the UNC System Configuration Wizard to configure the GGSN Zone ID. Use the UNC Zone Configuration Wizard to configure primary and backup (if backup is required) core GGSN Zone ID.
6. Use the UNC Wizard System Configuration Wizard to configure the Conventional IV&D Broadcast Data Block Size.
7. Use Voyence to enforce the policy to the PDG.
8. Use Provisioning Manager to set up and submit the conventional home zone map to all initialized devices in the system, including PDG.
9. Use Force Initialize in Provisioning Manager to initialize subscribers' configuration sets to all initialized devices in the system, including PDG. This creates a baseline of subscriber information.
10. Use Distribute Changes in Provisioning Manager to send only the changes to subscribers' configuration sets to all initialized devices in the system, including PDG.
11. Use Provisioning Manager to configure Conventional Channel Group, Conventional Unit, Conventional Broadcast Data Agency, and Digital Conventional Channel Record. Then use Provisioning Manager to publish the changes to UNC.
12. Configure the CDEM (for data encryption/decryption only).
13. Configure the KMF for OTAR/OTEK (optional).
14. Log on to the PDG and access the Local Configuration interface. Change the Redundancy State to Active. The NMA Application Redundancy State must show Active Operable.

3.2 ASTRO 25 Conventional with Integrated Data Component Configuration for K Core Systems

Prerequisites: For K core systems, the following applications are used to configure ASTRO® 25 Conventional IV&D communication system components to implement data services:

- Pdgconf Command Line Interface (CLI) to configure system parameters such as sites, channels, and GGSN configurations
- PDG local configuration tool to set the PDG to the active state the first time only, and to configure optional parameters.
- Configuration Manager to configure SU records and broadcast data information in the PDG.
- Configuration/Service Software (CSS) to configure and manage Conventional site infrastructure equipment (base radios)
- Customer Programming Software (CPS) to configure subscriber units
- KVL and KMF to load keys into the CDEM
- KMF Client to configure the KMF for conventional data services

Process:

1. Load the Conventional IV&D PDG.
2. Configure the GGSN.

3 Use the Configuration chapter and the Appendix in the *Packet Data Gateways* manual to configure the PDG.

4 Log on to the PDG and access the Local Configuration interface. Change the Redundancy State to Active. The NMA Application Redundancy State must show Active Operable.

5 Use Configuration Manager to configure subscriber information.

6 Use Configuration Manager to configure broadcast data information.

7 Configure the CDEM (for data encryption/decryption only).

8 Configure the KMF for OTAR/OTEK (optional).

3.3 Conventional Channel Groups

For the Conventional audio service, Conventional Channel Groups allow public safety agencies sharing a system to reuse Conventional Unit IDs and Conventional Channel IDs across agencies. A Conventional Unit or Conventional Channel is only unique within its Conventional Channel Group. The concept of Conventional Channel Groups does not exist for the Conventional Data Service, for example, each Conventional Unit or Channel that is made data capable is automatically assigned to the same Conventional Channel Group (Conventional Channel Group 2001). This means that the ID space for data capable Conventional Units and Channels is shared among agencies, and that coordination between agencies is needed when assigning IDs in a shared system.

Conventional Units and Channels that are not data capable may also be assigned to the Conventional Channel Group 2001. If a Conventional Unit is not data capable, but needs to communicate on a data capable Conventional Channel, it should be assigned to Conventional Channel Group 2001 in order to be properly identified by the system.

3.4 Windows Registry Value Requirements for Mobile Computers

NOTICE: This section only applies to mobile computers running the Microsoft Windows XP operating system.

For the ASTRO® 25 Conventional with Integrated Data feature, the following Windows registry values must be modified for mobile computers:

- EnablePMTUDiscovery
- MTU

The registry values are located under the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

To modify these values, use the Registry Editor tool (Regedit.exe). For detailed information about modifying the registry, see Microsoft Windows help for the version of Windows used on your mobile computer.

3.4.1 EnablePMTUDiscovery

The Valid Range for EnablePMTUDiscovery must be set to 0 (False).

- Key: Tcpip\Parameters
- Value Type: REG_DWORD - Boolean
- Valid Range: 0,1 (False, True)
- Default: 1 (True)

- Description: If you set this parameter to 1 (True), TCP tries to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and causes network congestion. If you set this parameter to 0, an MTU of 576 bytes is used for all connections that are not to computers on the local subnet.

3.4.2
MTU

The Valid Range for MTU must be set to 512.

- Key: Tcpip\Parameters\Interfaces\ID for Adapter
- Value Type: REG_DWORD Number
- Valid Range: 68 - the MTU of the underlying network
- Default: 0xFFFFFFFF
- Description: This parameter overrides the default Maximum Transmission Unit (MTU) for a network interface. The MTU is the maximum packet size in bytes that the transport transmits over the underlying network. The size includes the transport header. An IP datagram can span multiple packets. Values larger than the default value for the underlying network cause the transport to use the network default MTU. Values smaller than 68 cause the transport to use an MTU of 68.

Chapter 4

Conventional Data Services Operations and Optimization

This chapter outlines the tasks to perform once the ASTRO® 25 Conventional with Integrated Data feature is installed and operational on your system.

4.1 Operating ASTRO 25 Conventional with Integrated Data Components

The ASTRO® 25 Conventional with Integrated Data feature relies on several pieces of hardware, which have general operating procedures covered in their own manuals. For more information, see the following ASTRO® 25 system documentation:

- *Provisioning Manager* manual (M core systems only)
- *Configuration Manager for Conventional Systems User Guide* manual (K core systems only)
- Configuration/Service Software (CSS) online help
- *Packet Data Gateways* manual
- *CAI Data Encryption Unit* manual
- *Key Management Facility* manual
- *KVL 3000 and KVL 3000 Plus Key Variable Loader User's Guide* or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*
- ASTRO® 25 subscriber radio User's Guide for your specific model

4.2 Maintaining Software

Software and firmware updates to the ASTRO® 25 Conventional IV&D components must be installed as and when they become available for optimal operation.

CDEM software is installed with a KVL. For upgrade information, see the *CAI Data Encryption Module User Guide* manual.

The subscriber radios receive their software updates through Customer Programming Software (CPS) or FLASHport™. For your specific radio model for more information, see the user guide.

4.3 Managing Keys

Encryption keys are stored on both the CDEM and in the subscriber radio within the ASTRO® 25 system.

Installing encryption keys to the CDEM or subscriber radios is called loading. Erasing the keys is called zeroizing.

For details about managing keys on the CDEM, see the *CAI Data Encryption Module* manual. For details about managing keys on the subscriber radio, see the ASTRO® 25 subscriber radio User's Guide for your specific model.

4.4
CDEM Reporting in the Key Management Facility

If your system includes a Key Management Facility (KMF) for centralized key management, you can generate summarized and detail CDEM reports using the KMF client. The summarized report displays the name, RSI, and state of the CDEM. The detail report displays the assigned CDEM group, CDEM status, and pending actions in addition to algorithms and keys associated with the CDEM, and its keyset status. For more information, see the “KMF Operation” chapter in the *Key Management Facility User Guide* manual.

4.5
Performance Management Using InfoVista

NOTICE: Performance management is not supported for K Systems.

Performance management covers various applications that report system statistics via the InfoVista network management console, an optional performance monitoring tool for the ASTRO® 25 Conventional IV&D system. The ASTRO® 25 Conventional IV&D feature provides reports for zone level data traffic monitoring. For a description of the Conventional RNG and PDR reports and how to access them via the InfoVista console, see the *InfoVista User Guide* manual.

InfoVista provides reports for usage statistics applicable to voice only, data only, or for both voice and data. Reports are available at the channel, site, and zone level. Specific information in the reports includes the following:

- Amount of time channel allocated for data
- Percent of time channel allocated for data
- Number of data channel requests
- Total busies for data channel requests
- Total busy duration
- Max busy duration
- Average busy duration
- Total number of data allocations
- Total time duration for data
- Total time in use for voice and data

The following reports are available for broadcast data usage analysis:

- Number of broadcast messages sent to the sites
- Number of broadcast messages sent to each broadcast agency/ID
- Number of dropped broadcast messages per site
- Number of dropped broadcast messages overall

4.6
Event Reporting for Subscriber Radios

The subscriber radio provides the ability to report exception events (failure to encrypt/decrypt) to the user display and to a connected mobile computer through SNMP trap messages (per Project 25 Radio Management Protocol, also known as Radio Control Protocol – RCP), ANSI/TIA-102.BAEE-B). Consult the specific subscriber radio user manual used in your ASTRO® 25 system for details about these event reporting capabilities.

4.7

Conventional Data Services Optimization

Optimization of ASTRO® 25 Conventional IV&D data services are performed at the time of system planning. Typical message sizes and frequency of broadcast messages are added to the systems messaging profile to determine of system sizing. No routine optimization procedures are required.

This page intentionally left blank.

Chapter 5

Conventional Data Services Troubleshooting

This chapter provides fault management and troubleshooting information relating to ASTRO® 25 Conventional IV&D service failures.

5.1 Troubleshooting ASTRO 25 Conventional IV&D Components

Failure Scenarios and Solutions on page 70 lists some high-level troubleshooting scenarios for ASTRO® 25 Conventional IV&D services. For detailed troubleshooting procedures, see the following application manuals or online help as appropriate:

- *Provisioning Manager*
- *Packet Data Gateways* manual
- Configuration/Service Software (CSS) online help
- *CAI Data Encryption Module* manual
- *Key Management Facility* manual
- *ASTRO 25 Customer Programming Software (CPS)* Online Help
- *KVL 3000 Plus Key Variable Loader User's Guide* or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*

IMPORTANT: As discussed in ASTRO 25 K Core Configuration Functionalities on page 28, there are differences between M core and K core system functionality. In this chapter, any reference to the following items only applies to M core systems: Network Manager (Provisioning Manager, UEM, UNC, and ZDS), multiple zones, and zone controller.

5.1.1 Fault Management

The ASTRO® 25 Conventional IV&D feature requires fault management of the following:

- Conventional PDG (PDR and RNG) – PDR to RNG local link
- CDEM (optional)
- GGSN
- Site Gateway (Conventional Channel Interface)
- Conventional PDG – KMF link (optional)
- Site Gateway (Conventional Channel Interface) – Conventional RNG link
- Conventional PDR – GGSN link
- Site Gateway (Conventional Channel Interface) – Conventional RNG state of broadcast (Gateway Router) link
- Conventional PDG – Gateway Router link
- Conventional RNG – CDEM link (optional)

NOTICE: In K core systems the PDG does not support fault notifications sent to the Network Manager.

5.1.2 Loss of Master Site Connectivity

In the event that a Conventional Site loses connectivity to the Conventional RNG in the Master Site, ASTRO® 25 Conventional IV&D service is lost. The service is restored once the site regains connectivity to the Conventional RNG. Loss of Conventional RNG connectivity is detected by both the Site Gateway (Conventional Channel Interface) and the RNG. The RNG senses the link disconnection and cancels any pending data for SUs at that site. The Site Gateway (Conventional Channel Interface) discards all pending data as well as any new inbound data received from SUs.

While a loss of connectivity exists between the Conventional RNG and a Site Gateway (Conventional Channel Interface) configured with at least one data-capable channel, the Site Gateway (Conventional Channel Interface) continuously attempts to reestablish the link to the RNG. These attempts persist until either the link is reestablished or the Site Gateway's configuration is changed to eliminate any data-capable channels.

5.1.3 Conventional Channel Failure

In the event the Site Gateway (Conventional Channel Interface) detects that a link to a base radio or Comparator has failed, it informs the Conventional RNG and the RNG then cancels any pending data for all SUs assigned to that conventional channel. The SU has the capability of detecting when the conventional channel fails and upon detection, cancels any pending data transaction.

5.1.4 Redundant PDG

ASTRO 25 Conventional IV&D supports Dynamic System Resilience for all M1 and M3 Conventional system configurations. K Core and M2 system configurations do not support DSR operations. For more information about DSR, see the *Dynamic System Resilience* manual.

5.1.5 CDEM Replacement

The CDEM is a Field Replaceable Unit. A failed CDEM may be swapped for a backup unit in the field.

5.1.6 Failure Scenarios and Solutions

The following table lists problems that may be encountered with data services, possible causes, and troubleshooting steps.

Table 7: Data Service Troubleshooting Scenarios and Solutions

Symptoms	Possible Causes	Solution
Messages are not received by the infrastructure	• RF collisions • Subscriber is in a poor coverage area	Assess channel loading and performance at the site where problems are detected.

Table continued…

Symptoms	Possible Causes	Solution
	• Overloaded channel causes messages to be timed out	
Data is not delivered to the CEN or to the subscriber unit	Potential failure on the communication path	• Ensure network connectivity along the path. • Check the status of all the devices in the data communication path (data device, subscriber, base radio, PDG, GGSN router, and other networking components) in the fault management application located in the zone. Ensure that they are exhibiting normal function. If the failure can be isolated to a specific device, refer to the respective hardware manuals for detailed troubleshooting procedures.
	PDR-GGSN link failure – If the GGSN does not respond to a PDR echo request (sent every 60 seconds), PDG detects the link failure and notifies the fault management application that the link is down. The Conventional PDR deregisters all subscribers after a four-minute delay.	Determine the cause of the problem by examining links to the GGSN from the PDR and the physical device if necessary. When the link is reestablished, the PDR sends notification of recovery to the fault management application. Link up states are reported to the fault management application.
	GGSN-PDR link failure – If the PDR does not respond to the GGSN echo request, the GGSN detects the link failure. If a data message is received from the CEN, the GGSN responds with an ICMP message to the host application in the CEN. The Conventional PDR deregisters all subscribers after a four-minute delay.	Determine the cause of the problem by examining links to the PDR from the GGSN and the physical device if necessary. The GGSN recovers the link when it receives a registration message from the PDR. Link up states are reported to the fault management application.
Data is not delivered to the CEN or to the subscriber unit and data host application in CEN receives ICMP from PDG or mobile data terminal receives ICMP message from subscriber unit.	GGSN Hostname to IP address Resolution Failure – If the system cannot resolve the GGSN Hostname to IP address (that is, hostname entry in the /etc/hosts file is missing), the PDR rejects the registration request and notifies the RNG of the failure. The RNG deletes the subscriber unit record.	Ensure that there is a GGSN associated with the network/country codes in the Access Point Name (APN).

Table continued…

Symptoms	Possible Causes	Solution
Data is not delivered to the CEN or to the subscriber unit and mobile data terminal receives ICMP message from subscriber radio or CEN host application receives ICMP message from GGSN router.	GGSN router failure – System loses the ability to provide data messaging from your data network to mobile data devices in your system, and all IP services are dropped. The PDR sends “link down" status information to fault management server in that zone. The GGSN Link object displays the reported status of the logical link between the PDR and the GGSN router in the fault management application.	Check the condition of the GGSN and any traps reported by PDR in the fault management application and take remedial action.
Data is not delivered to the CEN or to the subscriber unit	PDR failure – Results in a disconnect of the data path between the data communication system and the subscriber units. The ability to register a subscriber is lost.	Check that the traps reported by PDR in the fault management application to pinpoint the problem.
Data is not delivered to the subscriber unit and the CEN application host receives a “Host unreachable” message, or data originating in subscriber unit is not delivered to the CEN application.	Border Gateway failure – Prevents data messages originating in the Customer Enterprise Network (CEN) from reaching subscriber units and vice versa.	Check the condition of the Border Gateway and take remedial action in case of a failure.
Data delivery loss for a maximum of 7 minutes to all connected CENs or to the Subscriber Unit due to a non-redundant Border Router reset at a CEN.	In a system with a non-redundant data configuration and when data services to multiple CENs are handled by a single GGSN, if one of the connected CEN Border Router restarts, it results in a restart recovery of the GGSN for all subscribers across all the connected CENs. This results in a data service downtime of 7 minutes or less. Data from the subscriber units are not delivered to the destination CEN hosts and data from the CEN applications are dropped. Data service re-initializes with the GGSN restart recovery. Data delivery resumes with the service re-initialization.	Determine the reason for the Border Router reset. High availability is recommended as a solution for the Border Router single point of failure to the data service.
Subscriber is generating errors to the data device	Subscriber generates one of the following error messages to the data device: • Message Lifetime Expiration • Service Interaction	Some conditions are temporary whereas others need intervention to resolve. Review the other scenarios listed to determine the appropriate troubleshooting step, if one is required.

Table continued…

Symptoms	Possible Causes	Solution
Broadcast data messages fail to deliver	The system may not be able to deliver broadcast messages due to the following reasons: • One or more CEN-based applications attempts to deliver a large number of IP data messages to the system intended for broadcast delivery within a short period. The PDR becomes overloaded with messages and discards messages due to buffer overflow. • The PDR does not detect if the rate of message arrival exceeds the system delivery capacity because the interface with the GGSN is UDP. • Gateway Router or Multicast Tree Failure	Review the traps sent by the PDR to the fault management application located in the same zone as the PDR. Check the fault management application to see if the site was unable to participate: • Site did not join the multicast tree • Channel was busy • Site did not receive the broadcast page • Check status of Gateway Router The specific remedy varies based on the root cause. Judge this on a case-by-case basis using the other information provided in this table.
Broadcast message delivered to single user only	If the DHCP server is not correctly configured, it could potentially assign broadcast IP addresses to individual subscribers, preventing broadcast messages from being sent to the agencies.	Create separate IP address spaces for broadcast agencies and radio users. It is critical that the static and dynamic configured IP addresses specified for radio users and broadcast agencies do not conflict within a CEN address. IP Address conflicts may also result in loss of data messaging service for the conflicting subscribers.
Broadcast message gets ICMPed from PDG.	Broadcast IDs were not context-activated automatically upon PDG start-up. Typical of a PDG (PDR) failure.	Check PDG status in the fault management application and messages written by the PDG to syslog if the Centralized Event Logging feature is implemented on your system.
Broadcast message is incorrectly routed	Radio ID is the same as a provisioned broadcast ID	Assign radio IDs that are not the same as the provisioned broadcast ID.
Conventional site loses connectivity to the Master Site; data service is lost	Loss of connectivity is detected by both the Site Gateway (Conventional Channel Interface) and the RNG. The RNG cancels any pending data for SUs at that site. The Site Gateway (Conventional Channel Interface) discards all pending data as well as any new inbound data received from SUs.	Data service is restored once the site regains connectivity to the Master Site.
Conventional channel failure	Site Gateway (Conventional Channel Interface) detects channel failure and	Restore channel.

Table continued…

Symptoms	Possible Causes	Solution
	informs the RNG, which cancels any pending data for SUs assigned to that channel. SUs can also detect channel failure and cancel any pending data transactions.	
Unintended users can listen to broadcast messages	SUs with incorrect broadcast agency IDs.	Configure SUs with correct broadcast agency ID. If information is highly sensitive, implement encryption for applications in the CEN and mobile computer.
Excessive traffic due to responses to broadcast data; response to broadcast message degrades performance	Inbound responses must be sent as a result of broadcast transmission.	The application must do random back-off retry messages (over several hours), or allow the host to do polling.
CDEM stops processing data. When the CDEM re-establishes communication with the PDG, it tells the PDG it has no keys and the PDG does not assign the CDEM any data for encryption/decryption. The No Keys status is reported to the UEM.	The Erase button on the CDEM was pressed, causing the CDEM to be reset.	Reload all key material into the CDEM.
	The Ethernet link between the CDEM and the PDG is broken.	Check and re-establish the Ethernet connection between the CDEM and the PDG.
CDEM cannot encrypt or decrypt messages to or from one or multiple subscribers. CDEM keyfail messages are sent to the PDG and the PDG communicates the keyfail messages once every 10 minutes to the UEM.	The CDEM contains some keys, but does not have the one used by the subscriber or is assigned a CKR for transmit to the subscriber which has no key loaded for it.	Reload all key material into the CDEM.

5.2

Internet Control Message Protocol (ICMP) Messaging

The ASTRO® 25 Conventional IV&D network does not store application data. If the Conventional IV&D PDG is unable to deliver an IP datagram, the PDG drops the datagram and sends an ICMP message to the originator. ICMP messages are a typical response to errors in IP datagrams or for diagnostic or routing purposes. The application can be designed to use ICMP messages, in which case the originator can decide what action to take. The returned ICMP message provides reason codes about why the message was not delivered.

If an ICMP “host unreachable” message is received for a packet, the network has done its best to deliver the packet. Simply resending the packet when an ICMP message has been received may not result in delivery success. In this case, the application should implement a kind of “back-off” and suspend sending packets for a while.

5.3

Troubleshooting with Unified Event Manager

The Unified Event Manager (UEM) is a network fault management tool. Each zone has a UEM server that receives fault notifications (traps) from devices in the zone. UEM is a useful troubleshooting tool for determining problems with ASTRO® 25 Conventional IV&D system components, network connectivity failures, CPU overload conditions, and so on.

For more information about UEM, see the *Unified Event Manager* manual.

NOTICE: UEM is not available for K core systems. To view traps from the PDG in K core systems, open the PDG local configuration tool and access PDG logs in /var/log/messages or use the Administration menu. For more information, see the *Packet Data Gateways* manual.

5.4

Contacting Motorola Solutions for Technical Support

The Motorola Solutions Support Center (SSC) provides technical support, Return Material Authorization (RMA) numbers, and confirmations for troubleshooting results. Call the SSC for information about returning faulty equipment or ordering replacement parts. North America: 1-800-221-7144 / International: 001-302-444-9800.

This page intentionally left blank.