System Release 7.17
ASTRO ® 25
INTEGRATED VOICE AND DATA

Trunked Data Services Feature Guide

NOVEMBER 2016

MN003366A01-A

Copyrights

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

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

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

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a 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
MN003366A01-A	Original release of the *Trunked Data Services* manual	November 2016

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Trunked Data Services

This manual describes the implementation and use of Trunked IV&D services on ASTRO® 25 systems. It covers the Classic Data and Enhanced Data services, and the High Availability for Trunked IV&D (HA Data) feature.

For information on Conventional IV&D, see the *Conventional Data Services* manual.

For information on High Performance Data (HPD), see the *HPD Packet Data Resource Management* manual.

What Is Covered in This Manual?

This manual contains the following chapters:

- Data Services Description on page 23 introduces the following data features: Classic Data, Enhanced Data, High Availability for Trunked IV&D (HA Data), and Transit25 Data.
- Data Services Technical Overview on page 33 describes IV&D components and how they interact to provide the following data features: Classic Data, Enhanced Data, HA Data, and Transit25 Data.
- Data Services Configuration on page 65 describes how to configure radio communication system components for Classic Data, Enhanced Data, and HA Data operation.
- Data Services Optimization on page 81 covers fine-tuning of system parameters for optimal data service availability.
- Data Services Operation on page 83 describes Classic Data and Enhanced Data operation, HA Data-related procedures, and Transit25 Data operation.
- Data Services Troubleshooting on page 87 describes troubleshooting of Classic Data and Enhanced Data service issues.

Helpful Background Information

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

Related Information

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

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83 by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
Dynamic System Resilience	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature which may be implemented on your ASTRO® 25 system. This feature adds a

Table continued…

Related Information	Purpose
	geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
HPD Packet Data Resource Management	Describes how packet data transmissions are managed in the context of the High Performance Data (HPD) feature in an ASTRO® 25 system.
Conventional Data Services	Provides descriptive and procedural content relating to the ASTRO® 25 conventional data feature. The manual describes the feature and the components supporting the feature, and explains how conventional data call processing is implemented and how data messages are processed. Additional information provided includes procedures for installation, configuration, operation, and troubleshooting.
ASTRO 25 vCenter Application Setup and Operations Guide	Provides a description of the VMware vCenter application used to provide VMware fault tolerance and VMware high availability for virtual machines and includes process and procedures to support setup and operations for the VMware vCenter application in an ASTRO® 25 system.

Chapter 1

Data Services Description

This chapter provides a high-level description of data services and the function it serves on your system.

1.1 Introduction to Trunked IVD

Trunked data services are features available for implementation on ASTRO® 25 Integrated Voice and Data (IV&D) systems. The Trunked IV&D feature enables radio users to use client applications hosted in ASTRO® 25 subscriber units or in mobile data devices connected to subscriber units to have wireless access to server applications in fixed enterprise data networks through the trunking infrastructure.

ASTRO® 25 systems support the following features related to trunked data:

- Trunked IV&D services:
  - Classic Data
  - Enhanced Data
- High Availability for Trunked IV&D (HA Data)

The ASTRO® 25 system assigns resources (channels at sites) for data communications in response to a demand from a communications application in either a mobile subscriber/client, or a host in a Customer Enterprise Network (CEN). These applications can initiate packet data traffic from a host in either a land-based enterprise network, or from data devices such as mobile laptops connected to mobile radio subscriber units.

The data subsystem tracks subscriber location just as voice does, so that outbound (fixed end host to subscriber) Classic Data traffic can be routed to the right zone and site for delivery over one of the site's radio channels. The target subscriber is paged to an assigned data channel, and the data delivered to the mobile computer or other data terminal through the radio subscriber unit.

Enhanced Data does not support outbound messaging.

When a subscriber/client initiates inbound data traffic, the subscriber requests a channel at the affiliated site. When the channel is granted, the subscriber begins transmitting data. Once a channel at a site is assigned for data, it is advertised on the site's control channel so that other subscribers with data ready for transmission can switch to that channel immediately if needed, bypassing the request-and-grant process.

Any channel at a site can be assigned for Classic Data. Only channels configured as Reserved Access-capable can be assigned for Enhanced Data.

1.2 Classic Data Services

The Classic Data feature is a type of data service available for implementation on ASTRO® 25 Trunked Integrated Voice and Data (IV&D) systems. Classic Data and IV&D are synonymous terms.

Classic Data enables the transmission of data between fixed wireline networks that are part of the Customer Enterprise Network (CEN) and the wireless data clients connected through radio subscriber units to the ASTRO® 25 communication network.

Classic Data places office-centric capabilities in the hands of the mobile work force. Subscriber client applications can connect to server applications that reside in networks outside the boundary of a trunked radio system. Client applications can be hosted in the subscriber itself or in an attached mobile computer.

Typical uses of the Classic Data feature include:

- Dispatching mobile operators to incident scenes or job locations through wireless data services
- Making inquiries for information from centralized databases
- Sending messages to the mobile workforce over wireless data services

Data applications that use the Classic Data services to communicate include:

- ASTRO 25 Advanced Message Solution
- Over-the-Air-Rekeying (OTAR)
- POP25
- Premiere Mobile Data Communications (MDC)

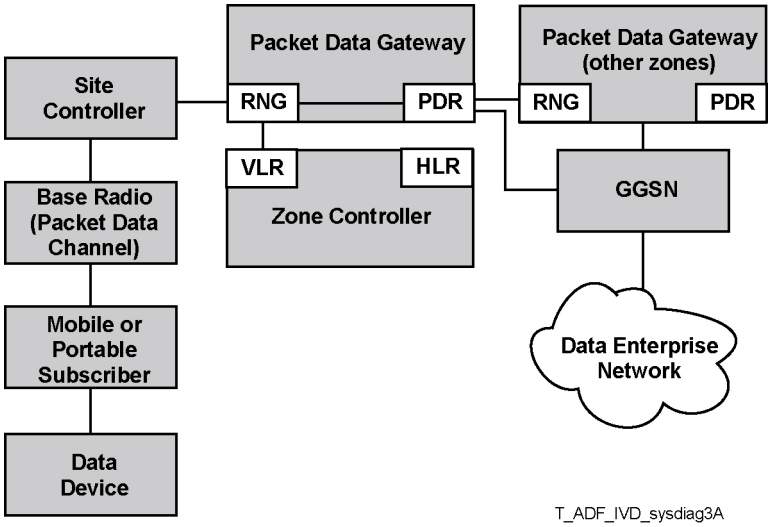
The IV&D data path supports broadcast data delivery service for up to 20 distinct agency destinations. A broadcast data message is originated from an application in the CEN. It is then delivered to every transmitting site within the coverage area of a zone. Each site in turn transmits the message to the destination subscriber units configured for data operation at each site.

The group of mobile subscribers receiving this message are typically aligned by agency within a fleet, especially in multi-agency IV&D ASTRO® 25 system deployments. Due to the broadcast nature of the message, messages are sent unconfirmed and message delivery is not guaranteed.

NOTICE: The IV&D data path does **not** provide group data delivery functionality. Group data delivery refers to the transmission of messages selectively to sites where the members of the group were last known to be associated.

The following figure shows the logical communication interface between ASTRO® 25 system components and the data enterprise network.

Figure 1: Integrated Voice and Data Communication Interface



1.2.1
Classic Data Services Capabilities

The Classic Data feature supports the following capabilities:

- Operation in the 700 MHz, 800 MHz, 900 MHz, UHF, and VHF frequency bands at 9600-baud

- Operation in up to seven zones
- Industry standard protocols: IPv4, Dynamic Host Control Protocol (DHCP), and Point-to-Point Protocol (PPP)
- Unicast IP datagrams
- Confirmed delivery of messages with IV&D service for unicast transmissions
- Broadcast data delivery service (with unconfirmed delivery)
- Tunneling: Virtual Private Network (VPN)
- Data-capable subscriber radios and other mobile data devices

1.3 Enhanced Data Services

Enhanced Data is a Manufacturer specific (not P25 standard) inbound-only packet data service optimized for applications that periodically send short messages from a subscriber or attached device to a host in the Customer Enterprise Network (CEN). Enhanced Data is only supported on ASTRO® 25 Trunked IV&D systems with GTR series site equipment and APX subscriber units. Datagrams carried via Enhanced Data must use UDP/IPv4 for network transport between the subscriber or attached device and the CEN. The subscriber uses the Enhanced Data service when the following conditions are met:

- The radio has the Enhanced Data option.
- Radio is enabled for Enhanced Data in the Provisioning Manager application.
- The UDP Destination Port number in an inbound datagram matches one of the Enhanced Data Port numbers in the subscriber, configured through Customer Programming Software (CPS).
- The site includes a channel enabled for Reserved Access capability, which means that the channel supports Enhanced Data.
- Message size does not exceed the maximum packet size allowed for Enhanced Data. If the message is over the limit, it can be sent via classic, depending on a radio setting.

Neither TCP nor IPv6 are supported for datagram transport. Optionally, either Header Compression (UDP/IP) or IPSec encryption via the Encrypted Integrated Data (EID) feature can be used together with Enhanced Data. An Enhanced Data message can contain a maximum of 384 bytes of data, including user payload and all headers. Any data messages larger than this size are sent using Classic Data.

Enhanced Data introduces a new type of data channel to support short, periodic inbound data messages, such as Location (supported systems: GNSS, BeiDou, Glonass, Galileo). The Enhanced Data channel is a trunked resource at a Radio Frequency (RF) site and is allocated on first request from an Enhanced Data subscriber, then dynamically based on a periodic evaluation of the Enhanced Data load at the site. The Enhanced Data channel is based on the timing and signaling characteristics of the Phase 2 TDMA channel. However, both logical TDMA channels are used in tandem to provide Enhanced Data service. It is not possible to run Enhanced Data on one logical channel and voice on the other logical channel. Only inbound packet data messaging is supported. No outbound packet data messaging is supported on Enhanced Data channels. Context activation on a Classic Data channel is required before Enhanced Data messaging can be performed.

An inbound datagram is sent using a reservation scheme where the subscriber computes the number of TDMA time slots required to send the message and makes a request to the infrastructure for the slots. The infrastructure schedules the requested slots, and the scheduling is communicated to the subscriber via outbound signaling on the Enhanced Data channel. The subscriber then sends its message using the assigned scheduling, and each slot is acknowledged by the infrastructure over the air. Any slots of data that are not successfully acknowledged are retransmitted by the subscriber.

Retries are performed until the infrastructure indicates the entire message has been successfully received or a predefined retry limit has been reached.

The Enhanced Data feature increases the safety of field users, by providing a practical outdoor tracking solution. The feature provides each active subscriber with an inbound data service for sending in periodic location and status updates. These short messages are used by dispatchers to track the radio users' status and location on Computer Aided Dispatch (CAD) consoles. Enhanced Data ensures a wide-area, mission-critical, portable and mobile coverage and offers a better utilization of the system resources. Enhanced Data is optimized for variable reporting rates and designed to support applications with message profiles similar to Location, such as PremierOne™ Responder Location.

The Enhanced Data feature can be used by Public Safety agencies, including police, fire, and EMS, as well as Transit agencies and city services, such as snow plow fleets.

1.3.1
Enhanced Data Services Capabilities

Enhanced Data Compatibility

The Enhanced Data feature is supported by the following system configurations, frequency bands, and devices:

- M and L zone cores
- Common Server Architecture (CSA)
- All redundancy configurations: Dynamic System Resilience (DSR), High Availability for Trunked IV&D (HA Data)
- All frequency bands: VHF, UHF, 700 MHz, 800 MHz, 900 MHz
- Trunked IV&D Radio Frequency subsystems: repeater, voting, simulcast
- GTR channels
- P25 Phase 2 (H-DQPSK, HCPM) modulation
- APX subscriber radios

Enhanced Data Channel Capacity

The capacity of an Enhanced Data channel varies depending on the data profile that includes the message size and cadence rate. Different message sizes and cadence rates are required for different data applications, which affects channel capacity. For example, 315 users per Enhanced Data channel can be supported with the message size of 60 bytes and the cadence rate of 90 seconds. 105 users can be supported at a 30-second cadence with the same message size.

When the Encrypted Integrated Data (EID) feature is used, Enhanced Data channels have different capacities. For example, if messages are encrypted, an Enhanced Data channel can support 180 users at a 90-second cadence rate and 60 users per channel at a 30-second cadence rate, based on an inbound message size of 120 bytes.

For location updates, the message typically contains the following location data: time, latitude, longitude, altitude, speed, and direction.

1.4
Data Services Capacity

For M3 systems, this capacity implies 7 zones and a GGSN at each zone.

NOTICE: The total data message traffic depends on

- Active data users number
- The maximum message rate for a channel
- The maximum number of channels in a zone
- The percent of channels in a zone that your organization is willing to dedicate to data traffic.

Table 1: Trunking IVD Data Services Capacity

	M3 Capacity	Other Systems Capacity (L and M1, M2 core)
	Per zone and per system	
Max number of active data subscribers sending/receiving data. This applies to both Classic and Enhanced Data combined. (cadence rate 120 seconds)	48,000	20,000
Max number of **Classic Data messages** per hour. This includes packet data registration messaging and any Motorola Solutions internal radio application messaging such as OTAR and broadcast messages	600, 000 (300,000 outbound messages, 300,000 inbound messages)	300, 000 (150,000 outbound messages, 150,000 inbound messages)
Max number of **Enhanced Data messages** per hour.	2,000,000 (cadence rate 30 seconds)	1,200,000 (cadence rate 30 seconds)
Max number of provisioned data users	Zone: 128,000 System: 250,000	Zone: 64,000 System: 128,000

Table 2: Trunking HPD Data Services Capacity

	Capacity for all M and L core Systems
Max number of active data subscribers sending/receiving data (cadence rate 120 seconds)	20,000
Max number of **trunking HPD clear messages** per hour	1,000,000
Max number of provisioned data users	Zone: 64,000 System: 128,000

Table 3: Hybrid System (Trunking IVD + HPD) Data Services Capacity

	M3 Capacity	Other Systems Capacity (L and M1, M2 core)
	Per zone and per system	
Max number of active data subscribers sending/receiving	48,000	20,000

Table continued…

	M3 Capacity	Other Systems Capacity (L and M1, M2 core)
data. This applies to both Classic and Enhanced Data combined. (cadence rate 120 seconds)		
Max number of **Classic Data messages** per hour. This includes packet data registration messaging and any Motorola Solutions internal radio application messaging such as OTAR and broadcast messages	600, 000 (300,000 outbound messages, 300,000 inbound messages).	300, 000 (150,000 outbound messages, 150,000 inbound messages).
Max number of **Enhanced Data messages** per hour.	2,000,000 (cadence rate 30 seconds)	1,200,000 (cadence rate 30 seconds)
Max number of **trunking HPD clear** messages per hour	1,000,000	1,000,000
Max number of provisioned data users	Zone: 128,000 System: 250,000	Zone: 64,000 System: 128,000

Table 4: Hybrid System (Trunking IVD + Conventional IVD) Data Services Capacity

	M3 Capacity	Other Systems Capacity (L and M1, M2 core)
Max number of active data subscribers sending/receiving data. This applies to both Classic and Enhanced Data combined. (cadence rate 120 seconds)	48,000 per zone and per system	20,000 per zone 40,000 per system
Max number of **Classic Data messages** per hour. This includes packet data registration messaging and any Motorola Solutions internal radio application messaging such as OTAR and broadcast messages	600, 000 (300,000 outbound messages, 300,000 inbound messages).	300, 000 (150,000 outbound messages, 150,000 inbound messages).
Max number of **Enhanced Data messages** per hour.	2,000,000 (cadence rate 30 seconds)	1,200,000 (cadence rate 30 seconds)
Max number of **Conventional messages** per hour	1,000,000	1,000,000
Max number of provisioned data users	Zone: 128,000 System: 250,000	Zone: 64,000 System: 128,000

1.5
Typical Trunked 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
- 10% using Enhanced Data at a 60 seconds cadence.
- 20% of users are sending a text message to the dispatch operator

1.6
High Availability for Trunking IV&D and Trunking HPD Description

High Availability (HA) for Trunking IV&D and Trunking HPD is an optional feature which introduces redundant components into the data subsystem to provide maximum data service reliability in case of hardware failure.

HA Data is available for:

- Trunking IV&D and Trunking HPD systems
- L2, M2, and M3 zone cores
- Common Server Architecture (CSA) systems only

Components needed for HA Data include:

- VMware vCenter application with Fault Tolerance
- Direct Attached Storage (DAS)
- Redundant Packet Data Gateway (PDG) virtual machines on two different Virtual Management Servers (VMS1 and VMS2)
- Redundant (GPRS Gateway Support Node) GGSN routers
- Redundant Customer Network Interface (CNI) path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers)

HA Data 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

Relation to Dynamic System Resilience (DSR):

- HA Data is a cost-effective alternative to DSR, deployed independently of DSR.
- HA Data provides on-site redundancy for quick recovery after hardware failure, while DSR provides off-site redundancy for recovery after loss of an entire site.
- HA Data and DSR can be implemented within a single system.

For more information on HA Data with DSR, see the *Dynamic System Resilience* manual.

PDG Redundancy

Redundancy for the 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 Trunking IV&D and Trunking HPD PDG, see the *ASTRO 25 vCenter Application Setup and Operations Guide*.

GGSN and CNI Path Equipment Redundancy

Redundancy for the GGSN and CNI path equipment is provided by installing redundant devices in the system and configuring them to switch over upon a component failure.

For information on how to set up GGSN routers and CNI path devices and configure them for redundancy, see the *System LAN Switches*, *System Gateways – GGM 8000* or *System Routers – S6000/S2500*, and *Fortinet Firewall*.

1.7 Transit25 Data Services

The Transit25 feature enables transmission of messages by a transit application provided by your organization through the ASTRO® 25 IV&D radio system to a fleet of vehicles. It provides integrated voice and data communications between the dispatch center and a large fleet of vehicles, and can be used to track the location of vehicles that belong to the fleet. Communications between vehicle and dispatcher are primarily carried out using data. Voice communication is also used, but to a lesser degree than data.

The Transit25 feature is supported on IP simulcast and ASTRO® 25 repeater sites.

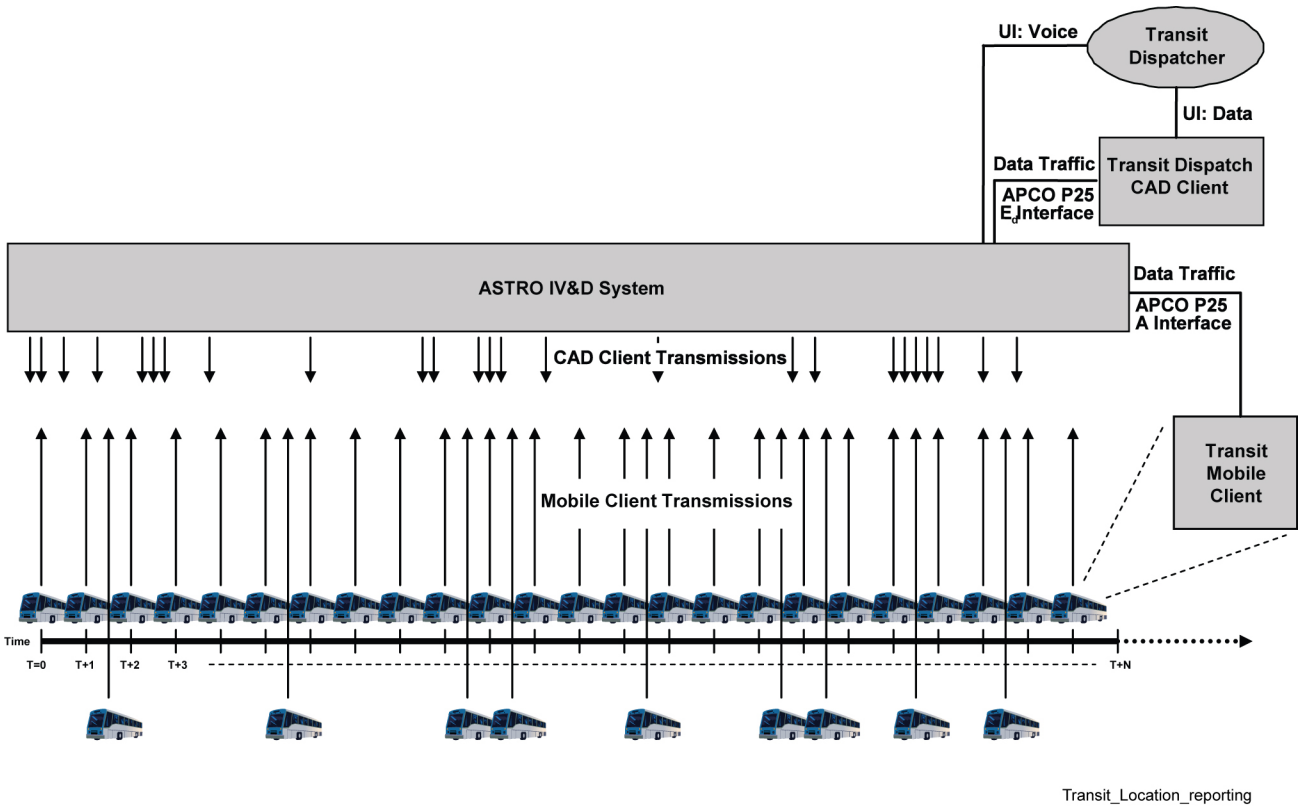
Typical usage scenarios for Transit25 include the following:

- Emergency alerts
  - AMBER alerts
  - Be-On-the-Look-Out (BOLO) alerts
- Informational notifications
  - Enabling fleet-wide audio paths for a general announcement on fare increases
  - In-vehicle digital signage updates for special event advertisements
  - Road condition updates
  - On-shift personnel updates (for example, policy change notifications, office procedure reminders, and so on).
- Operational notifications
  - Notify all vehicles to modify routes due to road blockage, such as in the case of accidents.
  - Instruct vehicle drivers of a particular fleet to bring their vehicle for maintenance at the end of a shift.

NOTICE:
Transit25 operates in wide area trunking mode for a single zone system. It does not support site trunking or failsoft modes.

The figure shows the high-level transit diagram with a fleet of vehicles interfacing with dispatch position through IV&D system.

Figure 2: Transit Location Reporting



1.7.1

Transit25 Data Service Capabilities

The Transit25 feature adds the following functions and capabilities to the data services provided by the ASTRO® 25 system:

- Allows transit users to access the 700 MHz spectrum range.
- Allows transit applications, used to track the location of a large fleet of vehicles, to operate on an ASTRO® 25 IV&D two-way radio system. Transit vendors can validate their applications for use on a Motorola Solutions ASTRO® 25 system.
- Supports up to 3000 transit users.
- The third-party transit application allows the radio to switch between voice mode and location tracking.
- Features Controlled Channel Access (CCA) mode of operation for channels assigned as packet data channels.
- Sends SNMP traps from the subscriber to the mobile computer for fault identification.
- Supports up to 16 channel partitioning groups.
- Simultaneously supporting up to 15 PDCHs per site for transit operation (adjustable from 1 to 15 channels).
- Simultaneously supporting up to 3 PDCHs per site for public safety operation (adjustable from 1 to 15 channels but only 3 PDCHs are supported).

Due to the intensive nature of broadcast data, Transit25 voice public address applications must be carefully planned to avoid system overload issues. Contact Motorola Solutions for more information on configuring system and subscriber parameters for optimal system performance.

Chapter 2

Data Services Technical Overview

This chapter describes the subsystem technology provided within the ASTRO® 25 System.

2.1 Trunked IVD Theory of Operation

The ASTRO® 25 trunking communication system involves the coordination of various system components designed and configured to successfully process data requests using available system resources. These system resources include packet data channels that are used for data transmission.

2.1.1 Trunked IV&D Components

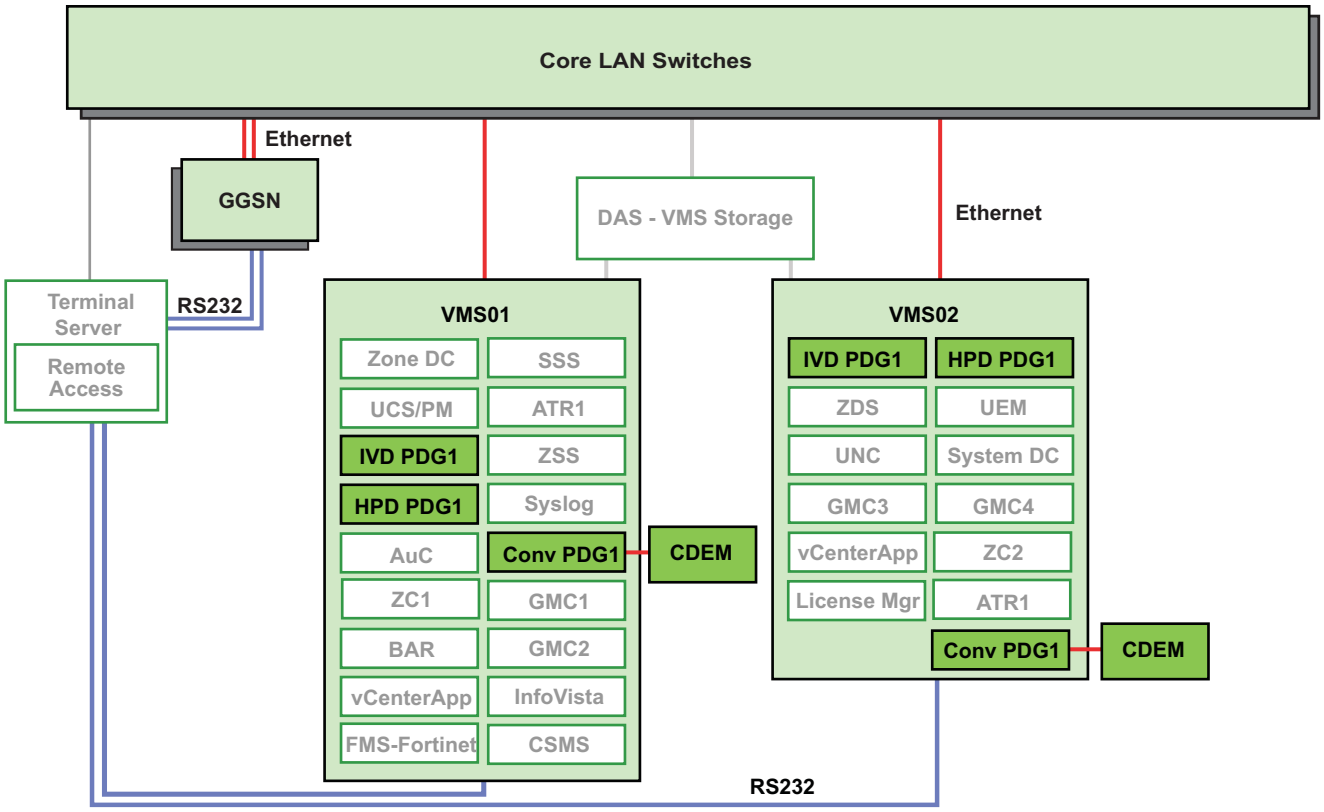
The following components are designed to support the Trunked Integrated Voice and Data (Trunked IV&D) feature:

- Zone Controller
- Trunked IV&D Packet Data Gateway (PDG)
- GPRS Gateway Support Node (GGSN) router
- Site Controller
- Border Router
- RNI-DMZ Firewall
- DMZ Switch
- Peripheral Network Router (optional)
- Subscriber units (data-capable)

The Customer Enterprise Network (CEN) is connected to the radio infrastructure through the GGSN router and the mobile data terminals are connected to the data-capable radio subscriber units.

The following diagram shows the data subsystem with redundant Trunked IV&D PDG and GGSN devices in an M3 zone core employing the Common Server Architecture (CSA) feature. For more information on the High Availability for Trunked IV&D (HA Data) feature that provides redundancy in the data subsystem, see High Availability for Trunked IV&D HPD Theory of Operation on page 56.

Figure 3: Data Subsystem



Note: Shadow and redundant elements are not specified

Data_M3_CSA_config_K

2.1.1.1 Zone Controller

The Zone Controller handles voice and data call processing functions for the ASTRO® 25 IV&D system. It performs the following functions on the system in the context of data services:

- Interacts with the Site Controller to manage Packet Data Channel resources. The Site Controller requests a Packet Data Channel from the Zone Controller. The Zone Controller grants, queues, or denies a request based on current channel availability and site status.
- Maintains the busy queue for data channel requests from a site. The Packet Data Channel requests follow the existing priority level scheme processing used for voice calls. Data busy queue priority is configured through the Unified Network Configuration (UNC) application.
- Tracks the number of active data channels at a site. (Active data users are tracked by the Site Controller.)
- Determines Packet Data Channel preemption based on preemption rules and current configuration. Packet Data Channel preemption parameters can be configured through the UNC and Provisioning Manager applications.
- Provides mobility information in the form of mobility pushes to the PDR. The PDR uses this information to keep the data system in sync with current subscriber unit mobility status. Information that the Zone Controller provides indicates activity of a subscriber unit with respect to registration, deregistration, site roaming, and zone roaming. Mobility pushes occur on every Zone Controller mobility update.

- Processes mobility queries from the Packet Data Gateway (PDG) between pushes. The components of the PDG (PDR and RNG) use the queries to verify subscriber unit location between pushes. The PDR queries the Zone Controller Home Location Register (HLR) database and the RNG queries the Visitor Location Register (VLR) database.

2.1.1.2
GPRS Gateway Support Node Router

The GGSN interfaces between the Motorola Solutions Radio Network and the Customer Enterprise Network (CEN). It performs the following support functions for IV&D:

- Isolates customer wireline and wireless network traffic from the Motorola Solutions RF network and customer agencies from each other.
- Facilitates the use of a customer's Dynamic Host Configuration Protocol (DHCP) servers.

The GGSN maintains routing information for all attached packet data users. This routing information is used to tunnel user datagrams to each subscriber unit's current point of attachment (the home PDR) and to customer hosts (through IP-IP tunnels).

2.1.1.3
Packet Data Gateway

The Packet Data Gateway (PDG) is used to link a customer's data network to the Motorola Solutions ASTRO® 25 RF network through the GGSN router. One trunking PDG is required for Trunking IV&D in each zone.

The PDG is a virtual machine running the following applications:

- Packet Data Router (PDR) application
- Radio Network Gateway (RNG) application

NOTICE: HPD and Conventional IV&D both require independent PDGs per zone.

For information relating to server hardware hosting the PDG platform, see the *Virtual Management Server Hardware* manual.

2.1.1.3.1
Packet Data Router (PDR)

The Packet Data Router (PDR) manages all aspects of the IP protocol and provides a logical interface between the GGSN router and the RNG module. It performs the following functions:

- Receives and maintains HLR information from the Zone Controller to identify a subscriber's home zone location for processing data calls.
- Interfaces with the RNGs within its zone and RNGs in other zones in the system.
- Maintains a database of all data-capable subscriber units that are in its home zone (based on home zone mapping).
- Controls routing of data messages. The PDR stores the routing information for the attached users. This routing information is used to tunnel user payload data to a subscriber unit's current point of attachment, which is the serving RNG.
- Manages context activation and deactivation. Authorizes and approves context activations based on provisioned, as opposed to requested value validation and other processing.
- Determines when a subscriber unit should be context deactivated. Some triggers for the PDR deactivating the subscriber unit are as follows:
  - Deactivation (context deletion) by the GGSN

  - Subscriber powers off
  - There is a change or deletion of the subscriber unit provisioning information
- Queries the Zone Controller's HLR to determine subscriber unit status and location affiliation. The term home PDR or servicing PDR refers to the PDR that contains provisioned information for a particular mobile subscriber radio.
- Supports RFC 2507 UDP/IP header compression to reduce the message size so that packet data channel bandwidth may be efficiently used. Header compression is not applied to broadcast data messages.
- Supports confirmed and unconfirmed message delivery to reduce the likelihood of shared channel transmission contention and collision on the packet data channel. Subscribers only send confirmed inbound data. Unconfirmed inbound messages are supported for few limited exceptions for control messaging.

2.1.1.3.2
Radio Network Gateway (RNG)

The Radio Network Gateway (RNG) provides a logical interface between the local RF resources and the PDR to support data calls to subscriber radios. It performs the following functions:

- Maintains a database of context activated subscriber units registered in the zone. The database is based on subscriber unit location and not home zone affiliation. For every subscriber unit location update, the local Zone Controller pushes the Visitor Location Register (VLR) information to the local RNG to provide routing information to the packet data service. The RNG uses VLR data to track subscriber unit mobility to the site.
- Processes and routes data messages. Processing involves fragmenting and reassembling data messages that the RNG then routes to the appropriate destination device (outbound to the Site Controller and inbound to the PDR).
- Communicates with subscriber units to ensure that data messages are sent and received without errors for confirmed mode messaging. For inbound data packets, the RNG checks data segments for errors and then sends an acknowledgment (ACK) or selective acknowledgment (SACK) to the transmitting subscriber. In the event the RNG receives damaged segments, it responds with a SACK, requesting that the transmitting subscriber retransmit those damaged segments.
- Supports header compression.
- Supports SNDCPv1 and SNDCPv3 data registration.
- Supports sending confirmed and unconfirmed outbound messages. Unconfirmed delivery removes the retries and acknowledgments. It is up to the application provider to manage acknowledgments, contention, and retries.

2.1.1.4
Site Controller

The Site Controller functions as a data Site Controller having trunked data resource allocation functionality. The Site Controller performs the following data service-related functions:

- Processes inbound and outbound data requests at the site.
- Requests Classic Data and Enhanced Data channel assignments and de-assignments from the Zone Controller. (The Zone Controller grants, queues, or denies data channel requests based on channel resource availability and site status.) For Enhanced Data, the Site Controller requests and releases channels based on Enhanced Data traffic load such that the load is balanced across an optimal number of channels.
- Provides routing between the Radio Network Gateway (RNG) and the Base Radio (Classic Data and Enhanced Data channels).

- Allows voice channel grants to preempt ongoing data calls (if the **Voice Grant Filter** parameter is appropriately configured).
- Interfaces with the Base Radios at the site to manage outbound RF channel queues and to allow prioritized access for control signaling over the Packet Data Channel.
- Determines and advertises the current status of the Classic Data and Enhanced Data channels at the site.
- Tracks and maintains a database of active data users at the site, including information on group affiliation.
- Maintains a busy queue for data users.
- Controls the number of users permitted on Classic Data and Enhanced Data channels.

Data channels are dropped and subscriber radios reactivate data requests with the Site Controller under certain conditions. Some examples are as follows:

- The Site Controllers at a site switch operating modes (active to standby or standby to active).
- A data channel failure occurs.

NOTICE: For the Dynamic Dual Mode features, configure the Frequency Reference for the GTR 8000 Base Radio to Integrated Reference A/B in order to accept the integrated site reference signal from the GCP 8000 Site Controller.

2.1.1.5
Mobile Subscriber Units

The subscriber unit provides an interface between an attached mobile computer and the radio network to enable use of communication system resources for data service. The subscriber unit performs the following functions in the context of data services:

- Monitors status of data service advertised by the Site Controller (voice and registration services, or voice, registration, and data services).
- Provides a platform to run Network Address Translation (NAT) service, which permits the subscriber unit to support multiple applications with one context.
- Communicates with a mobile computer through the Point-to-Point Protocol (PPP) or Remote Network Driver Interface Specification (RNDIS) protocol.
- Monitors the Packet Data Channel to determine its availability.
- Initiates a Packet Data Channel request, or uses a Packet Data Channel that is already open and available for use.
- Receives voice channel grants and updates on the outbound data channel while operating on a Packet Data Channel. The subscriber leaves the data channel and joins a voice call only if the Interrupt Data for Received Voice option is enabled. This option is configured by using Customer Programming Software (CPS).
- Moves off the packet data channel if the user presses the Push-to-Talk (PTT) button or moves to a different talkgroup.
- Supports RFC 2507 UDP/IP header compression to reduce the message size so that the packet data channel bandwidth may be efficiently used.
- Accepts broadcast messages addressed to the Broadcast IDs that it is configured for and forwards to terminal interface.
- Generates and sends Internet Control Message Protocol (ICMP) error notifications to the mobile computer for status and failure reporting (includes message lifetime expiration, context deactivation, site trunking notifications, and packet data transmission traps among others).

2.1.1.6
Mobile Data Terminal

The mobile data terminal provides a platform for data applications. It is situated in the vehicle and interfaces with the radio network through the radio subscriber unit.

2.1.1.7
Customer Enterprise Network

The Customer Enterprise Network (CEN) is where customer application servers are located. Customer applications include both server and client components. The CEN connects to the radio network through the GGSN.

2.1.1.8
Direct Attached Storage (DAS)

In Common Server Architecture (CSA) systems, the Virtual Management Server (HP DL380 Gen8 or Gen9 with ESXi OS) hosting the PDG and other virtual machines is configured to use the Direct Attached Storage (DAS) as a data storage for the virtual machines. DAS is an external storage solution used instead of an internal hard drive in the server.

In a redundant system configuration with VMS1 and VMS2, required for the High Availability for Trunked IV&D feature (HA Data), both servers access the same DAS.

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

For more details regarding the DAS hardware, see the *Virtual Management Server Hardware* manual. For installation and configuration procedures relating to DAS, see the *Virtual Management Server Software* manual.

2.1.1.9
Virtual Management Server (VMS)

In Common Server Architecture (CSA) systems, the Packet Data Gateway (PDG) is hosted as a virtual machine on a Virtual Management Server (VMS). The VMS host is a hardware and software platform that consists of an HP DL380 Gen8 or Gen9 server with the ESXi operating system, VMware software, and virtual machine applications, including the PDG. Each virtual machine environment can be recognized as a separate server that can independently support its own operating system, configuration, and server application.

For more information about the hardware platform, see the *Virtual Management Server Hardware* manual. For more information about the software components, see the *Virtual Management Server Software* manual.

2.1.2
Encrypted Integrated Data

The Encrypted Integrated Data (EID) feature provides data encryption services to ASTRO® 25 Trunked Integrated Voice and Data (IV&D) IP Bearer services Classic Data and Enhanced Data, between the Customer Enterprise Network (CEN) and subscriber radios. The data transmitted in the system is encrypted, whether the data is sourced by a mobile application within the subscriber radio or an application external to the subscriber radio.

EID relies on the following system components:

- Subscriber radio
- PDEG Encryption Unit

- Key Management Facility (KMF) server
- Key Variable Loader (KVL)

NOTICE: Encrypted Integrated Data services are not applicable to ASTRO® 25 systems using High Performance Data (HPD).

2.1.3
Header Compression

The ASTRO® 25 system uses RFC 2507 header compression to reduce the number of bytes that need to be sent over the air in a data session. Header compression is implemented at the subscriber unit and at the Packet Data Gateway (PDG) to reduce the size of the User Datagram Protocol (UDP) and Internet Protocol (IP) datagram headers. Header compression reduces network overhead and speeds up the transmission of data packets. Most of the information contained in the UDP/IP headers in a given data session does not change from one datagram to the next. Once complete copies of the UDP/IP headers have been received, compressed copies can be sent thereafter. The receiver saves the complete copies of the headers and uses them to decompress subsequently received compressed headers. Sending compressed headers before complete copies of the headers have been received would result in those datagrams being discarded.

To minimize the risk of discarded datagrams in cases where full headers are not successfully received, two configuration parameters exist that regulate how often full headers are sent in relation to compressed headers:

Max Number of Compressed Headers Between Full Headers
Specifies the maximum number of compressed headers sent between full headers.

Max Time Between Full Headers
Specifies the maximum time between full headers. A full header is sent after this amount of time has expired, counting from the time that the last full header was sent.

These parameters are configured both in the Unified Network Configurator (UNC) and in the subscriber via Customer Programming Software (CPS). Setting the **Max Number of Compressed Headers Between Full Headers** to a non-zero value results in sending a full header after the specified number of datagrams with compressed headers. Setting the **Max Time Between Full Headers** to a non-zero value results in sending a full header at the specified time intervals. Setting both parameters to a value of zero results in only the first datagram in a data session being sent with full headers and all remaining datagrams in that data session being sent with compressed headers. This option is recommended only in cases where high confidence exists that all network links from the site to the Customer Enterprise Network (CEN) have a very low error rate. That is, when there is high confidence that a packet will not be discarded in transit from the site to the CEN.

Header compression is implemented at the subscriber unit and at the Packet Data Gateway (PDG) to reduce the size of the UDP/IP datagram headers.

The subscriber unit can request header compression during a packet data registration procedure. The PDG either accepts the received header compression parameter values or proposes new values. The subscriber unit accepts or rejects the values in its response. Each IP datagram to be sent or received is submitted to this supplementary data bearer service for compression, decompression, or no processing. For each parameter, the PDG selects the greater of the two values (between its value and the value sent in by the subscriber). The subscriber generally accepts the value because it should be equal to or larger than its own value. If the radio receives a value lower than its currently programmed value, it tears the context down. This should normally never happen.

An Enhanced Data message can contain a maximum of 384 bytes of data, including user payload and all headers. Full (uncompressed) IPv4, UDP, and SNDCP headers add up to 30 bytes. The size of a message including full headers is used to determine whether Enhanced Data can be used. Therefore, a message having 355 or more bytes of user payload is always sent using Classic Data, even if the size of the message with compressed headers would be less than 384 bytes. This is because at least

the first message must be sent with full headers, and that message size would be 355+30, or 385 bytes, which is too large to be sent using Enhanced Data.

Broadcast data does not employ header compression due to its one-way, outbound nature.

Inner and outer header compression is not supported for encrypted data.

2.1.4
Packet Data Channel

A Packet Data Channel refers to the radio frequency resource used for the transport of data in ASTRO® 25 trunked communication systems. This resource is comprised of a trunked RF channel that supports the transmission and receipt of data messages between the Radio Network Gateway (RNG) and the subscriber unit.

In trunked IV&D systems, two types of Packet Data Channel are available, depending on the type of data service that a channel is assigned to: Classic Data channels and Enhanced Data channels.

The Packet Data Channel accommodates a number of users, each carrying on separate packet data messaging transactions or threads. The RNG in each zone is responsible for managing each user thread separately – sending outbound packets to sites sequentially so that they do not interfere or overlap with one another.

The Packet Data Channel is not a dedicated resource, but is assigned based on need and priority. Any channel at a site can be assigned as a Classic Data channel, but not as an Enhanced Data channel. Since the system is sharing resources between the voice and data services, voice calls can preempt data calls if configured to do so.

A Classic Data channel utilizes unscheduled confirmed and unconfirmed data transmission. A channel at a data-enabled site has a number of users on it conducting data traffic. When the number of users on a single Classic Data channel reaches a pre-configured limit, the site requests another channel for Classic Data service. If another channel is available, the next subscriber is assigned to it, and the site now advertises that channel as the active Classic Data channel. If another channel is not available, the request for Classic Data service is busied or queued.

While the Zone Controller tracks which subscriber radios are using channel resources for voice calls, it is the Site Controller that tracks which subscribers are using data channel resources for data calls.

For information on Enhanced Data channels, see Enhanced Data Channel on page 49.

ASTRO 25 Repeater Site Packet Data Channel

In an ASTRO® 25 Repeater Site, the Packet Data Channel is a channel on a GTR 8000 Site Repeater or QUANTAR® Station Site Repeater.

Simulcast Packet Data Channel

In a Simulcast Subsystem, the Packet Data Channel can be supported by a GTR 8000 base radio employing the GCM 8000 Comparator or a QUANTAR® Station (V.24) base radio employing the ASTRO-TAC™ Comparator. In either case, the Packet Data Channel is a combination of the base radio and comparator. If the location of the subscriber is unknown, the comparator broadcasts the data payload to all subsites. When the comparator registers the activity of the subscriber at one or more subsites, it directs the data payload to the subsite with the best signal from the subscriber and remembers this location. Once the location of the subscriber is known, the data payload is site-steered to the subsite that the comparator remembered. If the comparator receives the best signal from a subscriber from a receive-only (Rx-only) subsite that has no transmitter, the comparator directs the data payload to a transmitter at another subsite that is assigned as the transmitter for that Rx-only subsite. The comparator simulcasts status (RFSS/Adj) and group activity notifications at least every 15 seconds. The subscriber units use these notifications to validate existence of the Packet Data Channel.

Packet Data Channel Access

There are two methods for accessing the Packet Data Channel, depending on its availability:

Requested Access

Occurs if the site does not advertise that a Packet Data Channel is currently assigned or available. In this case, the subscriber unit has to request access to the data channel.

Autonomous Access

Occurs when a Packet Data Channel is already assigned at a specific Site Controller and the system automatically grants the subscriber unit access to the Packet Data Channel. While a Packet Data Channel is assigned, the Site Controller periodically advertises the channel's availability to all subscriber units on the site. If a subscriber unit needs a Packet Data Channel, the system allows the subscriber unit to immediately access the Packet Data Channel specified in the advertisement, without an explicit request to the site.

Packet Data Channel and Data Service Timers

To maximize the efficient use and optimal performance of system components and channel resources, resource allocation timers, and data service timers monitor and react to system conditions to accomplish this objective. The Packet Data Channel resource allocation and data service timers are configured for the Site Controller and the Zone Controller.

2.1.5 Protected Data Channels

There is no pre-configured maximum limit to the number of data channels that can be in service at a site. Classic Data and Enhanced Data channels can be requested to support the demand for data services up to the limit of the number of channels at a site, excluding the Control Channel. To ensure that channel resources are always available for voice calls, the concept of protected data channels is used. The Zone Controller is provisioned with the number of both Classic Data and Enhanced Data channels to protect from preemption at each site. This provisioned number of channels is referred to as the *protected channel limit* or simply the *protected limit* for each type of data service (Classic or Enhanced).

The Zone Controller preempts a data channel for a group voice call only after the protected limit for that type of data channel, specified at the site by the Unified Network Configurator (UNC), is reached. The Zone Controller always preempts data channels, including protected data channels, for emergency voice calls. New individual voice calls do not preempt assigned data channels that are considered protected.

A request for a data channel received before the protected limit for that data channel type has been reached at a site (a request for a protected data channel) can cause the preemption of a data channel of the other type if the number of channels of the other data type is above the protected limit. Preemption is possible because there are unprotected data channels of that type.

A request for a data channel received before the protected limit for that data channel type has been reached at a site (a request for a protected data channel) does **not** cause the preemption of a data channel of the other data type if the protected limit for the other type has not been reached. Preemption of one type of data channel for another is possible when the requesting type has not reached its protected limit while the other type has already reached its limit.

Protected and unprotected data channels preempt scan channels used by subscribers in multigroups to listen for announcement calls.

The following UNC parameters are used to specify the number of protected data channels at a site:

Protected P25 Classic Data Channels

This attribute specifies the number of Classic Data channels protected from preemption by anything other than an Emergency Call.

Protected Reserved Access Data Channels

This attribute specifies the number of Enhanced Data channels protected from preemption by anything other than an Emergency Call.

2.1.6
Preferred Data Service

The **Preferred Data Service** option, available in the Unified Network Configurator (UNC), only distinguishes which type of data channel to preempt for a voice call. A non-preferred data channel is preempted before a preferred data channel.

New individual voice calls do not preempt assigned data channels that are considered protected. New non-emergency group voice calls preempt unprotected data channels according to the provisioned value for the **Preferred Data Service** parameter.

New emergency voice call requests attempt to preempt unprotected data channels according to the provisioned value for the **Preferred Data Service**. If there are no unprotected data channels to preempt, a non-emergency voice call is preempted. If there are no voice calls, protected data channels are chosen according to the provisioned value for the **Preferred Data Service** parameter.

The **Preferred Data Service** parameter is only relevant when both the Classic Data and Enhanced Data channel counts are above the protected limit, or both are below the limit. If one count is above and the other below, the one that is above the limit is preempted first regardless of the **Preferred Data Service** flag.

2.1.7
Busy Queue for Channel Requests

When there is no channel available to satisfy a data channel request from a site, the Zone Controller places the request in the busy queue for the requesting site. The Zone Controller puts all requests for data channels in the busy queue below emergency calls. If the number of active data channels of a particular type (Classic Data or Enhanced Data) is below the protected limit, requests for data channels of that type go in the busy queue above normal voice calls. Otherwise, data channel requests are placed in the busy queue above or below normal voice calls, according to the **Data Busy Queue Priority** settings.

When different data service requests are queued at the same level, the Zone Controller queues Enhanced Data channel requests and Classic Data channel requests based on the provisioned **Preferred Data Service** parameter.

Emergency calls, normal calls, protected data channels, and unprotected data channels are placed in the busy queue in the following order:

1. Emergency call requests
2. Protected data channel requests queued based on the preferred data service:
   - Classic Data channel requests needed to achieve the specified number of protected Classic Data channels at a site
   - Enhanced Data channel requests needed to achieve the specified number of protected Enhanced Data channels at a site

   NOTICE: Only one Classic Data channel request and one Enhanced Data channel request can be placed in the busy queue at a time.
3. Normal group voice call requests
4. Unprotected data channel requests queued based on the preferred data service:
   - Unprotected Classic Data channel requests
   - Unprotected Enhanced Data channel requests

NOTICE: Unprotected data channel and normal voice call requests have priorities that determine their relative locations in the busy queue. The table shows the default order, but it is possible to assign priorities such that normal voice falls below unprotected data.

2.1.8
Busy Queue for Data Messages

Motorola Solutions APX subscribers queue messages received from the mobile computer for transmission. When a message transmission attempt has been completed, successfully or unsuccessfully, the subscriber generates a trap to the mobile computer to notify the application that a message has been transmitted.

The Motorola Solutions APX subscriber queues a maximum of ten messages each of Enhanced Data and confirmed Classic Data for transmission to the Motorola Solutions ASTRO® 25 network with the Enhanced Data messages being higher priority than the Classic Data messages.

The APX subscriber can discard messages on the queue due to an excessive amount of time elapsing before the subscriber can attempt to transmit the message. The **SNDCP Queue Dwell Timer** governs how long a Classic Data message can reside in the queue before being discarded and is defaulted to 30 seconds. An equivalent **Enhanced Data Queue Dwell Timer** governs how long an Enhanced Data message is held in the Enhanced Data message queue before being discarded without a transmission attempt. The default value of this timer is 15 seconds.

Voice transmissions always take priority over data transmissions. The **Service Interaction Timer** is used by the Motorola Solutions APX subscribers and set to 1/3 of the **SNDCP Queue Dwell Timer**. If the data is sent during an active voice call, the **Service Interaction Timer** is used to determine if the message is transmitted or discarded. If the subscriber is still in an active voice call at the expiration of the **Service Interaction Timer**, up to ten queued messages of the same type are discarded.

IMPORTANT: The **SNDCP Queue Dwell Timer** and the **Enhanced Queue Dwell Timer** are configurable with Customer Programming Software (CPS). The **Service Interaction Timer** is **not** configurable, and is always 1/3 of the **SNDCP Queue Dwell Timer**.

If the Customer Programming Software (CPS) option to allow Enhanced Data to be sent on Classic Data channels is disabled, the **IVD Ready Time Delta** parameter configured for Classic Data channels impacts the amount of time an Enhanced Data message must wait before it can be sent. With this configuration, an Enhanced Data message that is queued for transmission due to the subscriber being on a Classic Data channel must wait for the Classic Data messaging to be completed and for the **IVD Ready Time Delta** to expire before the Enhanced Data messaging attempt can be made. Moreover, if additional Classic Data messages arrive for transmission after the Enhanced Data message has been queued, these additional Classic Data messages must wait for the Enhanced Data message to be sent since Enhanced Data is prioritized over Classic Data. This can lead to delays in sending Classic Data messages when Enhanced Data messages are queued even if the subscriber was already on a Classic Data channel.

The **Response Wait Timer** parameter is the amount of time that a subscriber waits for the Site Controller to grant or deny a Classic Data or Enhanced Data data channel request. When that time expires, the subscriber discards the message. The **Response Wait Timer** is **not** configurable and is 0.48 of the appropriate queue dwell timer.

2.1.9
Subscriber Management for Data Services

The Integrated Voice and Data (IV&D) network layer establishes and maintains connections for each trunked client/subscriber that is granted access to the system's data services. The connection properties can vary from subscriber to subscriber across the system. Examples of connection properties are the election of either static or dynamic IP address assignment for the client/subscriber, the assignment of the IP address, the binding of that IP address to the subscriber's link layer or CAI

address, data compression properties, and the establishment of a connection identifier that the client/subscriber uses every time it invokes the trunked data service.

2.1.9.1
Context Activation

Context activation is the process by which data call registration and service activation is implemented by the ASTRO® 25 IV&D communication system. It is similar to system affiliation or registration that all trunked radios perform for voice service in that the system must recognize subscribers before they can use the communications services of the system. Once known by the system, a subscriber can roam throughout the entire coverage area of the system, moving from RF site to RF site while maintaining both voice and data service. The subscriber registers for packet data service during context activation. Context activation can be triggered the first time a data packet is received from an attached data device.

During context activation, connection properties are established for each subscriber or data client. Each subscriber can have only one active context at a time, but the system can support many contexts. While all radio sites to which subscriber radios are affiliated connect to the data subsystem in the same way, the subsystem can provide different external network connections to different groups of subscribers. For example, the subsystem can provide a connection between a police unit and police network and databases or between a public utility unit and public utility databases and network. The connection properties are pre-configured for each subscriber and applied during context activation.

During context activation, a two-way request and response exchange of data occurs between a subscriber, the home Packet Data Router (PDR) of the subscriber, and the GGSN. The process is always triggered from the subscriber end of the system.

Context establishment requires pre-configuration in both the subscriber and infrastructure, as well as an over-the-air exchange to complete. The subscriber is configured with a link layer address (normal trunked CAI address) and an IP address. A specific IP address can be given to the subscriber (static IP assignment), or the subscriber can be given an address of 0.0.0.0 which signals the infrastructure that dynamic IP assignment is requested. Dynamic IP address (DHCP) assignment services can be provided by the GGSN or an address server located in the target Customer Enterprise Network (CEN).

Configuration management of the GGSN performs the following functions to provide the infrastructure end-of-context configuration:

- Binds the subscriber addresses to an Access Point configuration entity.
- Binds the Access Point configuration to an IP-to-IP tunnel into an external network where the application services of the subscriber reside.

2.1.9.2
Broadcast Data Messaging Context Activation

Broadcast data service context activation is initiated and managed by the Packet Data Gateway (PDG) and does not incur any over-the-air messaging to radio subscribers within the system.

The broadcast data messaging service follows a slightly different trigger for context activating broadcast data registrations. At system start-up, the PDG completes context activation for each broadcast ID configured into it after it verifies connectivity to the GGSN. For multizone system deployments, each PDG independently completes context activations for its configured Broadcast IDs.

If the GGSN-to-PDG link re-initializes, the PDG is responsible for re-establishing context activations for each broadcast ID.

2.1.9.3
Context Renewal

A standby timer is negotiated during context activation and this governs the time that the context is valid. Both the network infrastructure and subscriber unit maintain this timer.

The timer is reset when context is renewed. If the standby timer is greater than two hours, context renewal occurs 30 minutes prior to timer expiration. Retries may bet set to occur every five minutes if required. If the standby timer is less than two hours, no automatic context renewal occurs.

2.1.9.4
Context Deactivation

Context deactivation is the process used to remove a valid context, ending data service. Context deactivation can also occur for the following reasons:

- The standby timer expires
- Deactivation of context with the GGSN
- Loss of communication with RNG
- Change or deletion of subscriber provisioning information
- Updates to local RNG database based on mobility/provisioning updates

2.1.9.5
Inbound vs. Outbound Data Calls

The direction of packet data calls is always described from the subscriber unit's point of view as follows:

- Inbound call – Sourced from the subscriber unit and travels over the air and through the infrastructure to the host computer.
- Outbound call – Travels from the host, through the infrastructure, and over the air to the subscriber unit.

2.1.9.6
Data Roaming

Subscriber units maintain data service as they roam between sites. As a subscriber unit changes site affiliation, the data subsystem receives updated location information. The data subsystem can also request location information from the system in case it receives a request for service to/from a subscriber unit for which it does not have a current location record.

To manage the roaming process, the data subsystem uses subscriber unit identification records in much the same way as the voice system does. Each PDR in a zone maintains an HLR record of subscriber units that are data *homed* in that particular zone. Every data packet sent to or from a subscriber unit passes through that subscriber unit’s home PDR. Subscriber units may roam from zone to zone in the system, but the system always contacts the home PDR for service authorization. The RNG in each zone provides connectivity between the trunked sites in each zone and the PDRs. Each RNG holds VLR records for subscriber units that are currently affiliated with a site in the zone where the RNG is located. The record of each subscriber unit identifies its home PDR and allows packets from that subscriber unit to be routed to the home PDR.

2.1.9.7
Mobility Management

InterZone mobility (roaming) is based on mobility *pushes* from the Zone Controller Visitor Location Register (VLR) in the zone where the subscriber unit is currently affiliated. When a subscriber unit

enters a new zone, the RNG informs the PDR of the arrival of the subscriber unit and the PDR is responsible for *transferring* the subscriber unit from the old zone to the new zone.

The PDR queries a Zone Controller for location information of a given subscriber unit. The RNG queries the Zone Controller (VLR) for site information of a given subscriber unit.

2.1.9.7.1
Home Location Register (HLR) and Data Services

Home Location Register (HLR) is a database used by the Zone Controller and the Packet Data Router (PDR). A unique HLR database exists for each zone.

The HLR stores information for each radio user, including the home zone assignment of the radio. Home zone information refers to the zone assigned to a particular radio ID as its home zone.

Home zone data is entered into the Provisioning Manager application when the system is installed. Data from the Provisioning Manager is periodically downloaded to each Zone Database Server (ZDS) in the system (one per zone).

Each ZDS then transfers the records specific to its zone to the Zone Controller resident in its zone in the form of the HLR. The Zone Controller stores only the configuration information for those individual radio IDs that are home to that zone. The Zone Controller uses the HLR data with the Visitor Location Register (VLR) data for a particular subscriber to coordinate the assignment of channel resources and manage voice calls.

The same HLR information is also transferred to the Packet Data Router (PDR) module in the PDG. The PDR uses the HLR data to process data calls in a similar way that the Zone Controller uses the HLR information to process voice calls.

For more information on the HLR, see the *Call Processing and Mobility Management* manual.

2.1.9.7.2
Visitor Location Register (VLR) and Data Services

The Visitor Location Register (VLR) is a Zone Controller database that is used to track the activities of subscribers that are currently active. A unique VLR exists for each zone in the system.

The VLR contains subscriber database information, including access configuration data, and current site location information for each individual subscriber affiliated to sites in that zone.

The Zone Controller periodically updates the Radio Network Gateway (RNG) with changes in the VLR database related to subscriber registration at sites, de-registration, site roaming, and zone roaming. The RNG uses this information when processing data service requests from data-capable radios.

For more information on the VLR, see the *Call Processing and Mobility Management* manual.

2.1.10
Mobile Subscriber Units

Mobile Subscriber Units (MSUs) provide an interface between a mobile computer and the radio network. The MSUs perform the following functions:

- Monitor status of data service (that is, data channel announcement and system service class).
- Monitor the control channel for autonomous access status.
- Initiate context activation, based on configuration, and renew active context when needed.
- Communicate with a mobile computer through the Point-to-Point Protocol (PPP) or Remote Network Driver Interface Specification (RNDIS) protocol.
- Monitor voice call LCs for activity on affiliated talkgroups while on the Packet Data Channel.

- Depart the Packet Data Channel if the PTT is pressed or if the talkgroup changes. Packet Data Channel departure depends on MSU configuration (Rx voice interrupts data).
- Provide a platform to run Network Address Translation (NAT) service, which permits the MSU to support multiple applications with one context.
- Generate and send ICMP error notifications to a mobile computer.

2.1.11
System Component Configuration

The following applications are used to configure system components with the parameters necessary for them to provide data services:

- Customer Programming Software (CPS) to configure subscriber units.
- Network management applications: Provisioning Manager and Unified Network Configurator (UNC), to configure parameters for the Zone Controller and the Packet Data Gateway (PDG): Packet Data Router (PDR) and Radio Network Gateway (RNG).
- Configuration/Service Software (CSS) and UNC to program and manage the RF devices.

2.1.12
Inbound Classic Data Request Flow

This process describes the Classic Data flow in a transmission originated by a data device and directed to a host computer or application in the Customer Enterprise Network (CEN).

1. The radio subscriber unit establishes a link to a data device to which it is connected (for example, a mobile computer).
2. The data device uses this link to send the user-initiated request for data transfer (as an IP message) to the subscriber unit.
3. The subscriber unit receives the data request message from the data device and, while listening on the control channel, checks current data status at the site to determine the type of Packet Data Channel access required:
   - **Requested Access**: If a Packet Data Channel is not currently set up or not available at the site, the subscriber unit sends a request for a data channel to the Site Controller.
     1. The active Site Controller adds the subscriber's user record for data service to its database and requests a Packet Data Channel from the Zone Controller.
     2. The Zone Controller determines if a channel can be granted.
     3. If a channel is available, the Zone Controller grants the channel and communicates the same to the Site Controller.
     4. The Site Controller assigns the Packet Data Channel and sends the data channel grant notification to the subscriber unit. It also tracks the subscriber unit's granted access to the Packet Data Channel.
     5. The Site Controller updates the status of the channel indicating that subscriber units may use the open Packet Data Channel autonomously, that is, without expressly requesting a Packet Data Channel.
     6. The subscriber unit, upon notification that a data channel is available, moves to the assigned Packet Data Channel. It formats the IP message from the mobile computer in APCO Common Air Interface (CAI) format (that is, as an IP datagram) and begins the data transmission.
   - **Autonomous Access**: If the subscriber unit detects that the control channel at the site is advertising a Packet Data Channel currently set up and available at the site, the unit has

autonomous access to the open Packet Data Channel. It does not have to request a Packet Data Channel for data transmission. Since the channel is already available for transmission, the subscriber unit begins transmitting the data payload. The active Site Controller adds the subscriber's user record for data service to its database.

4 The Packet Data Channel carries the data payload to the Site Controller.

5 The active Site Controller checks and updates its database record, and forwards the segmented payload data to the RNG.

6 The RNG checks and updates its database, reassembles data segments, checks for errors in the message, acknowledges that the message was received without errors (ACK) or replies that only certain blocks were successfully received (SACK), and forwards the datagram to the home PDR. Acknowledgments and retries are applicable only for confirmed messaging services.

7 The PDR validates the subscriber unit's context activation status and, if valid, forwards the data message to the GGSN.

8 The GGSN router determines message destination based on routing tables and then extracts and routes the data message to an appropriate host in the Customer Enterprise Network (CEN).

9 The CEN host application receives the data message.

10 The call ends when resource allocation timers, data service timers, or data service configuration parameters dictate that the data call is to be deactivated. The subscriber remains on the Packet Data Channel for a short time after a data message transaction in case additional data must be sent or received soon after the transaction. That is why the data call does not end immediately after the one data message is transmitted and acknowledged. Context deactivation can also occur upon an equipment failure or other similar condition.

2.1.13
Outbound Classic Data Request Flow

The following process flow reflects a Classic Data transmission originating in the Customer Enterprise Network (CEN) and directed to a data device in the coverage area.

1 A host computer on a data enterprise network sends an IP datagram addressed to a data device through the peripheral network (or DMZ) to the GGSN router.

2 The GGSN router receives the datagram, determines the destination PDR, formats the message, and routes it to the destination PDR.

3 The PDR extracts the subscriber unit's ID and data message, validates the subscriber unit's context activation status, determines the destination RNG, serving the zone where the subscriber is known to be located, and forwards the message to this RNG.

4 The RNG checks its database for the subscriber unit's record to verify the radio's location, fragments the message for transmission, and sends a page request to the Site Controller. (If the radio is not in the current zone, the RNG queries the local Zone Controller and then reroutes the message to the appropriate zone's PDR.)

5 The active Site Controller checks its database for the subscriber unit's record, creates a subscriber unit record (if needed), and pages the subscriber unit on the control channel.

6 The subscriber unit verifies if it has an active context and notifies the Site Controller that it has received the page.

7 The active Site Controller checks Packet Data Channel status, requests, and receives a Packet Data Channel from the Zone Controller (if required), and makes the Packet Data Channel available to the subscriber unit.

8 The Site Controller notifies the servicing RNG that the subscriber unit has been granted a Packet Data Channel for use.

9 The subscriber unit moves to the Packet Data Channel.

10 The RNG requests data payload transfer using the site's Packet Data Channel.

11 The Packet Data Channel processes the RNG's request for payload transfer and grants the requests when airtime becomes available.

12 The RNG sends data segments to the Packet Data Channel for transmission to the subscriber.

13 The subscriber unit receives the data, reassembles the data segments, checks for errors in the message if any, replies with an acknowledgment that the message was received without errors (ACK) or that only some blocks were successfully received (SACK) which are forwarded from the site to the home PDR. Acknowledgments and retries are applicable only in cases of confirmed messaging.

14 The subscriber unit forwards the message to the data device that it is connected to.

2.2 Enhanced Data Theory of Operation

The Enhanced Data feature uses the same Trunked IV&D components as Classic Data. When you set up the components for Enhanced Data, it is recommended that you add dual diversity antennas if they are not already present. The antennas ensure that Enhanced Data has the same coverage as FDMA voice.

Enabling Enhanced Data requires setting a number of parameters at the system, site, channel, and subscriber level.

2.2.1 Enhanced Data Channel

The Enhanced Data feature introduces a new data channel that supports inbound transmission of short periodic messages, such as Location (supported systems: GPS, BeiDou, Glonass, Galileo), from subscriber units to applications in the Customer Enterprise Network (CEN). The Enhanced Data channel is a trunked resource at a Radio Frequency site. No outbound data transmission is supported on the Enhanced Data channel.

The first Enhanced Data channel at a site is allocated on request from a subscriber unit. From then on, the site monitors the Enhanced Data load and requests new channels or deassigns channels as needed.

All channels at a site, other than the Control Channel, can be used for Enhanced Data if they are Enhanced Data-capable and not otherwise occupied, for example with voice. A channel is marked as Enhanced Data-capable by provisioning it as **Reserved Access Data Capable** in the Unified Network Configurator (UNC) application.

A subset of outbound Control Channel messaging is transmitted on the outbound Enhanced Data channel. This mechanism allows a subscriber to receive call grants and other important control messaging while engaged in Enhanced Data operations. Subscribers operate in half duplex mode, which means that a subscriber can only transmit or receive at any moment, not both. Because of this, Control Channel messaging sent on the outbound Enhanced Data channel can be missed if the subscriber is transmitting (inbound) at the time the outbound message is sent

2.2.2 Enhanced Data Agency Groups

Data Agency Groups (DAGs) are used to partition Enhanced Data-capable subscribers into different administrative groups within a system. Only Enhanced Data-capable subscribers can belong to DAGs and all Enhanced Data subscribers must be members of a DAG.

DAGs are configured in Unified Network Configurator (UNC) and associated with subscribers in Provisioning Manager.

Up to six DAGs can be configured in a system. DAGs 1 through 6 are available for assignment to Enhanced Data-capable subscribers. DAG 1 is assigned as the default group. If you do not want to partition subscribers into multiple agencies, you can keep the default assignment to DAG 1.

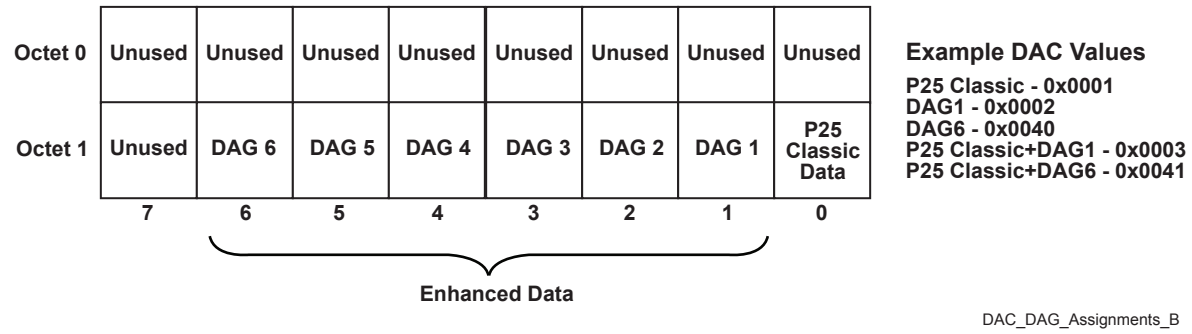
There is a fixed one-to-one correspondence between Data Agency Groups (DAGs) and Data Access Control (DAC) assignments. Each data-enabled subscriber is assigned to a DAC value during a successful context activation. The system derives the appropriate DAC value to assign to a subscriber based on its configuration: whether the subscriber is Enhanced Data-capable and which DAG it is assigned to. DAC values are then used between the subscriber and the infrastructure as part of data channel assignment.

Any changes to a context activated Enhanced Data subscriber's DAG assignment take effect the next time the subscriber context activates. The Packet Data Gateway (PDG) does not deregister an Enhanced Data subscriber based on a change in DAG assignment.

2.2.3
Enhanced Data Context Activation

A correspondence exists between an Enhanced Data Agency Group (DAG) and a Data Access Control group (DAC) defined for the Classic Data service. The following fixed assignment scheme is used to determine the DAC of the subscriber. As shown in the figure, a subscriber having only Classic Data capability has a DAC value of 0x0001. Subscribers with Enhanced Data capability must also have Classic Data capability and their DAC values have the Classic Data DAC bit set as well as the DAC bit corresponding to the DAG to which they are assigned.

Figure 4: DAC Assignments for Subscribers



SNDCPv3-capable subscribers support the Enhanced Data service while either SNDCPv1- or SNDCPv3-capable subscribers support Classic Data service. If an Enhanced Data-capable subscriber makes an SNDCPv3 context activation request and is denied, the subscriber makes a request using SNDCPv1. If the SNDCPv1 request is accepted and the subscriber is configured to allow Enhanced Data messages to be sent using the Classic Data service, the subscriber sends all packet data on the Classic Data channel, regardless of any UDP Port Mapping indicating Enhanced Data can be used.

Similarly, if an Enhanced Data-capable subscriber successfully context activates using SNDCPv3, but receives a DAC value indicating that only Classic Data channels can be used (that is, no DAC bits corresponding to an Enhanced DAG are received), the subscriber sends Enhanced Data messages using the Classic Data service if and only if the configuration of the subscriber indicates that Classic Data service can be used to send Enhanced Data messages.

2.2.4
Enhanced Data Channel Access

The availability of both Classic Data and Enhanced Data services are advertised separately at each site. A subscriber can only use each type of service when the site is advertising that the service is supported.

The subscriber determines that it needs to acquire an Enhanced Data channel based on the UDP Destination Port Number of the inbound data message. The subscriber attempts to acquire an Enhanced Data channel if the following three conditions are true:

- The UDP Destination Port Number indicates that an Enhanced Data channel is required.
- The Enhanced Data service is being advertised at the site, based on the Enhanced Data bit in the Motorola Solutions System Broadcast.
- The subscriber has been assigned a Data Access Control (DAC) group corresponding to an Enhanced Data Agency Group (DAG) during context activation.

The Zone Controller makes Enhanced Data channel assignments without regard to the DAG or DAC assigned to the requesting subscriber.

The subscriber dynamically builds and maintains a list of Enhanced Data channels that are advertised with Autonomous Access. If an application's UDP Port Number indicates that an Enhanced Data channel is required and one or more channels are present in the subscriber's dynamic channel list, the subscriber randomly chooses one of those channels and attempts to acquire it rather than making a channel request.

In a non-voted site configuration, the Base Radio receives Random Access requests, makes the decision as to whether to acknowledge the request, and factors this decision into the scheduling information sent on the outbound Enhanced Data channel. In a voted site configuration, the Base Radio sends the data as it is received to the Comparator. The Comparator makes the decision as to whether to acknowledge each request and factors these decisions into the scheduling information sent on the outbound Enhanced Data channel.

In a voted site configuration, duplicate copies of Random Access Reservation Requests can be received in a given subslot from the same subscriber. In addition, reservation requests from different subscribers can be received in a given subslot via different subsites. Since the design approach accepts only one Random Access Reservation Request per subslot, only a single subscriber's request is accepted in cases where multiple requests are received.

2.2.5
Enhanced Data Bandwidth Management

In a system where multiple Data Agency Groups (DAGs) share a site, DAGs can be configured for protected minimum bandwidth. This setting ensures that DAGs have Enhanced Data channel access during peak loading when all working channels are assigned as voice, Classic Data, or Enhanced Data. Access control is a method that allows DAGs to be provisioned to receive a certain portion of the site bandwidth when the site is fully loaded with Enhanced Data traffic and no additional channels can be allocated. A percentage of the available bandwidth is assigned to one or multiple DAGs on a per-site basis. Enabling access control allows the Site Controller to trigger access control enforcement when conditions warrant. Protected bandwidth is only available on Enhanced Data channels.

A site allows all DAGs to use the Enhanced Data channels in an unrestricted fashion as long as there are free channel resources available. If a new Enhanced Data channel has been requested from the Zone Controller but a busy or deny response is returned, the site triggers enforcement of access control on all currently active channels if at least one DAG is provisioned with a non-zero slot utilization percentage.

If DAGs provisioned with non-zero utilizations do not generate enough traffic to consume the available bandwidth at a site, those DAGs that do not have a provisioned bandwidth can use the remainder of the site bandwidth.

As an example, say DAGs 1, 2 and 3 have provisioned slot utilizations of 33%, 33% and 34% at a site. These DAGs are given priority over others based on their configured bandwidth allowances when access control is being enforced. If each of these DAGs generates Enhanced Data traffic above their provisioned utilizations, each is limited to their provisioned site-wide utilizations (33%, 33%, and 34% in this example). This is necessary since the total slot utilization at a site cannot exceed 100%. However, if one or two of these DAGs' utilizations is lower than their provisioned value, then the third is allowed to exceed its provisioned utilization such that the site is as fully utilized as possible. Moreover, if the traffic generated by all three DAGs in this example does not fully load the site, other DAGs are allowed access on a first-come, first-served basis until all available bandwidth is used.

Access control enforcement is only necessary when fewer Enhanced Data channels are granted by the Zone Controller than are needed to meet the current requested bandwidth. A DAG is not limited to a provisioned utilization unless access control enforcement has been triggered.

Only subscribers that are part of a DAG configured for protected minimum bandwidth can access an Enhanced Data channel during peak loading. Some subscribers may be unable to access the Enhanced Data channel even if they are part of a properly configured DAG. This situation occurs when the bandwidth is allocated to other subscribers in the DAG. The affected subscribers must wait until the bandwidth is available.

2.2.6
Enhanced Data Load Balancing

An Enhanced Data channel is capable of supporting multiple subscribers. If no Enhanced Data channels are active at a site, the first subscriber that needs to send Enhanced Data causes a channel to be assigned. From that point, the site monitors the site-wide Enhanced Data load and requests an additional Enhanced Data channel when the load passes a configured threshold known as **Enhanced Data Channel Loading**, configured through the Configuration/Service Software (CSS) when Enhanced Data is deployed. Similarly, if the Enhanced Data site-wide load drops below a predetermined threshold, the site releases one of the assigned Enhanced Data channels.

Lower **Enhanced Data Channel Loading** values tend to reduce access collisions among subscriber requests on each Enhanced Data channel, resulting in a higher probability that each Enhanced Data messaging attempt is successful. Higher **Enhanced Data Channel Loading** values tend to allow more subscribers to compete for access to each Enhanced Data channel at a site. The trade-off is an increased chance that an Enhanced Data messaging attempt fails.

The Enhanced Data feature allows subscribers to be assigned to Data Agency Groups (DAGs) for the purpose of earmarking a portion of a site's Enhanced Data bandwidth for those subscribers. By default, all Enhanced Data subscribers are assigned to DAG 1, and DAG 1 is configured to receive 100% of a site's available Enhanced Data bandwidth. A maximum of six DAGs can be created within the system, and each DAG can be configured to receive a percentage of the available Enhanced Data bandwidth, known as that DAG's protected utilization.

An Enhanced Data subscriber's DAG assignment is represented in the DAC value sent to the subscriber during context activation. The subscriber sends their DAG assignment to the infrastructure when requesting slots for sending an inbound packet data message. This allows the site to track the site-wide load per DAG. Under heavy load conditions, the site restricts access to the Enhanced Data channel according to the protected utilizations configured for each DAG. DAGs with no protected utilization can only get access to an Enhanced Data channel when the DAGs that are configured with a protected utilization do not use all their protected capacity.

Load balancing is only used within a site. Load is not balanced across multiple sites.

2.2.7
Enhanced Data Roaming

The configuration of Enhanced Data channels at adjacent sites is not a factor in the site selection criteria used by roaming subscribers.

Enhanced Data-enabled subscribers roaming to another site can acquire an Enhanced Data channel if the site supports channels of this type.

If a subscriber roams from a site configured for Enhanced Data to a site that does not support this feature, the subscriber sends inbound data by using Classic Data channels if the site capacity and subscriber configuration permit.

2.2.8
Enhanced Data Encryption

A data subsystem operating in an Enhanced Data configuration can accept encrypted data from subscribers. The system provides the option to enable or disable data encryption for Enhanced Data.

Encryption of Enhanced Data messages is performed in the same way as encryption of Classic Data messages, using the PDEG Encryption Unit.

Inner and outer header compression is not supported for encrypted Enhanced Data.

For more information on encryption services, see the *Encrypted Integrated Data* manual.

2.2.9
Enhanced Data Behavior and Classic Data Interactions

Enhanced Data builds on the Trunked IV&D feature and can be used along with Classic Data. The Enhanced Data service displays the following behavior and interactions with the Classic Data service:

- If a site is advertising that the Enhanced Data service is available, an idle subscriber that has Enhanced Data to send moves to an Enhanced Data channel and transmits the message.
- If Enhanced Data becomes available to send while a subscriber is engaged in a voice call, the subscriber sends the Enhanced Data after the voice call ends.
- If Enhanced Data becomes available to send while a subscriber is on a Classic Data channel and the **Allow Enhanced Data On Classic Channel** option, provisioned in Customer Programming Software (CPS), is disabled, the subscriber sends the Enhanced Data after the subscriber's Classic Data ready timer expires and the subscriber leaves the Classic Data channel.
- If Enhanced Data becomes available to send while a subscriber is on a Classic Data channel and the CPS-provisioned **Allow Enhanced Data On Classic Channel** option is enabled, the subscriber sends the Enhanced Data message on the Classic Data channel after the Classic Data message is completed.
- If an Enhanced Data message remains queued longer than the CPS-provisioned **Enhanced Data Queue Dwell Time** parameter that message and any Enhanced Data messages queued behind it are discarded.
- A subscriber can use a Classic Data channel to send Enhanced Data only if sending Enhanced Data messages on Classic Data channels is enabled for the subscriber via CPS provisioning (the **Allow Enhanced Data On Classic Channel** option). This behavior occurs when a site supports the Classic Data service but not the Enhanced Data service, and when an Enhanced Data message needs to be sent at a time the subscriber is already on a Classic Data channel.
- If the CPS option to **Interrupt Data for Received Voice** is enabled and a subscriber receives a call grant while sending data on an Enhanced Data channel, the subscriber immediately aborts the Enhanced Data message and responds to the voice call grant. If that option is disabled, the

subscriber continues its data operation to completion. If the subscriber sees the voice grant or update at that time, it proceeds to join the voice call.

- If a subscriber is involved in Enhanced Data activity and the Push-To-Talk (PTT) button is activated or an emergency alarm is initiated, the subscriber immediately aborts the Enhanced Data message, returns to the control channel, and initiates the voice call.
- If a subscriber is involved in Enhanced Data activity when an outbound Classic Data message is initiated, the subscriber misses the Classic Data page sent on the control channel.
- If a subscriber is involved in Enhanced Data activity when an inbound Classic Data message is initiated, the subscriber holds off sending the Classic Data message until the Enhanced Data message is completed.

For information on timer and busy queue interactions between Classic Data and Enhanced Data, see Busy Queue for Channel Requests on page 42 and Busy Queue for Data Messages on page 43.

2.2.10
Enhanced Data Flow

The following process flow reflects an example Enhanced Data transmission. Enhanced Data traffic is inbound only, which means messaging originates in the subscriber and is directed to a host computer or application in the Customer Enterprise Network (CEN). Six timeslots are requested in this example, but in general the subscriber determines the number of timeslots to request based on the size of the message to be sent.

1 The subscriber determines six timeslots needed to send a message, acquires an Enhanced Data channel, and requests six timeslots.

2 The channel grants the request – timeslots will be scheduled.

3 The first three timeslots are scheduled.

4 The subscriber sends the first three timeslots' worth of data.

5 The channel acknowledges the receipt of the first three timeslots worth of data by sending an ACK response and schedules the next three timeslots.

6 The subscriber sends the next three timeslots' worth of data.

7 The channel acknowledges the receipt of two out of three timeslots' worth of data and schedules another slot for retransmission of the timeslot for which the channel sends a negative acknowledgement (NAK) response.

8 The subscriber retransmits the data in the NAK'd timeslot.

9 The channel acknowledges the receipt of the retransmitted timeslot.

10 The channel assembles the full message and forwards to the Site Controller.

11 The Site Controller forwards the full message to the Packet Data Gateway (PDG).

12 The PDG forwards the full message to the GPRS Gateway Support Node (GGSN) router.

13 The GGSN forwards the full message to the CEN.

2.2.11
Enhanced Data Performance Reporting

Statistics and information on Enhanced Data performance are obtained through the following applications:

- Genesis Enhanced Data Performance Reporting
- Zone Historical Reports
- ZoneWatch

Performance Reporting through Genesis Enhanced Data Performance Reporting

The Genesis Enhanced Data Performance Reporting application is a third-party product provided by the Genesis Group. The application generates reports for IV&D, HPD, and Enhanced Data. The purchase of this software is recommended.

The Genesis Enhanced Data Performance Reporting application resides in the Customer Enterprise Network (CEN) and monitors the ASTRO® 25 infrastructure through the Air Traffic Information Access (ATIA), GTP', and PMI interfaces.

Performance Reporting through Zone Historical Reports

The Zone Historical Reports application is part of the Private Radio Network Management Suite. It displays combined channel assignment statistics for Classic Data and Enhanced Data.

Performance Reporting through ZoneWatch

The ZoneWatch application displays the information on DAG Bandwidth and Channel Utilization per Site.

2.2.12 Subscriber Options for Enhanced Data Applications

To use Enhanced Data with the ASTRO® 25 Advanced Messaging Solution Responder Location application, a subscriber requires the Classic Data (IV&D), Enhanced Data, and Location solutions. Customers can purchase the required options in bundles or separately.

2.2.13 Public Address Voice Announcements Using Broadcast Data

While in Data Communications mode, the dispatch application can address messages to groups of subscribers to establish voice calls. Groups are formed in an improvised manner within the application layer, and can change over time. The dispatch application is responsible for creating and maintaining these messaging groups. The message is routed to all subscribers.

Public address voice communication mode is an example of the establishment of a voice call for a group of subscribers. This mode supports one-way voice communications (public announcements) from the dispatcher to a group of subscribers.

Public address voice communication mode is entered on command from the dispatcher through one or more broadcast data messages. Under normal operating conditions, this mode times out and the subscribers resume the data communications mode.

1. A dispatch position sends a broadcast data message addressed to a broadcast agency, indicating that members of that agency should start listening to a specific talkgroup uniquely associated with that dispatch console. The contents and format of this message are only known between the application in the dispatch position and the application in the mobile computer attached to the subscribers.
2. The subscriber radios that belong to that broadcast agency receive the message and forward it to their attached mobile computers.
3. The mobile computers instruct the subscribers to switch to a specific SB9600 mode that contains the requested talkgroup.
4. The subscribers switch to the mode and affiliate to the talkgroup.
5. The operator at the dispatch position starts the one-way voice call (announcement).
6. Eventually, the call times-out and the subscribers affiliate back to their original talkgroup.

2.3

High Availability for Trunked IV&D HPD Theory of Operation

L2, M2, and M3 zone cores in Common Server Architecture (CSA) systems can be configured with redundant components in the data subsystem to support High Availability for Trunked IV&D, including Classic Data and Enhanced DataHPD (HA Data). This optional feature provides automatic switchover in case of a component failure to ensure high availability of data services.

The following components support HA Data:

- Redundant Trunked IV&DHPD 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

Redundant Trunked IVDHPD PDG Virtual Machines

At any given time, one of the two PDG virtual machines is the primary device, actively supporting data services for its zone, while the other PDG is the secondary (inactive) device, providing redundancy. Only the primary PDG is active on the network and accessible by environment. Other devices in the system see the HA PDG pair 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 switchover 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.

The components supporting PDG redundancy include:

- VMware vCenter application – Fault Tolerance, configured through vCenter, creates a secondary PDG virtual machine on a different server and keeps it in sync with the primary device. If the server hosting the primary PDG fails, Fault Tolerance triggers an automatic switchover to the secondary PDG, which becomes active.
- VMS1 and VMS2 – Redundant Virtual Management Servers in L2, M2, and M3 zone cores support PDG redundancy and switchover. During a failure of VMS1 or VMS2, the secondary PDG running on the peer VMS becomes the primary PDG.
- Direct Attached Storage (DAS) – An external data storage solution for Virtual Management Servers. It is used to store the PDG data. VMS1 and VMS2 access the same Direct Attached Storage so that the failure of one host/server and switchover to the other VMS is possible and the PDG data is not affected.

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

Redundant GGSN Routers

At any given time, one of the two GPRS Gateway Support Node (GGSN) routers are 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, 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

HA Data is a redundancy-based, high availability solution, deployed independently of Dynamic System Resilience (DSR). Both features can be implemented within a single system to provide an extra high level of redundancy. To support HA Data in a non-DSR system architecture, redundant components are established in the data subsystem in a single zone core. To support HA 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.

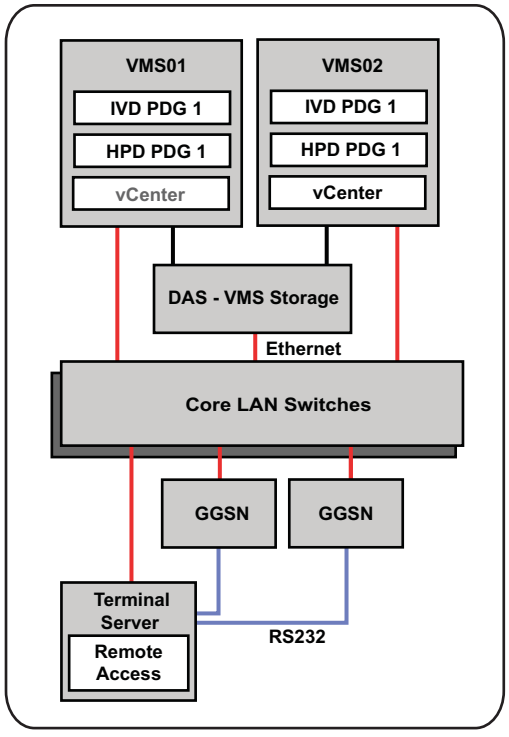
The following diagrams show the data subsystem in an HA Data configuration with redundant PDG and GGSN devices. The diagrams do not show other virtual machines which may reside on the VMS hosts in CSA systems.

The VMware vCenter application and the PDG use different technologies for redundancy. vCenter uses vSphere High Availability (HA) and the PDG uses vSphere Fault Tolerance (FT).

In the case of Fault Tolerance for the PDG, there is a primary PDG virtual machine (VM) and a shadow PDG VM. When you log on to individual servers, you see an instantiation of the PDG VMs on both servers although one is a shadow copy of the primary.

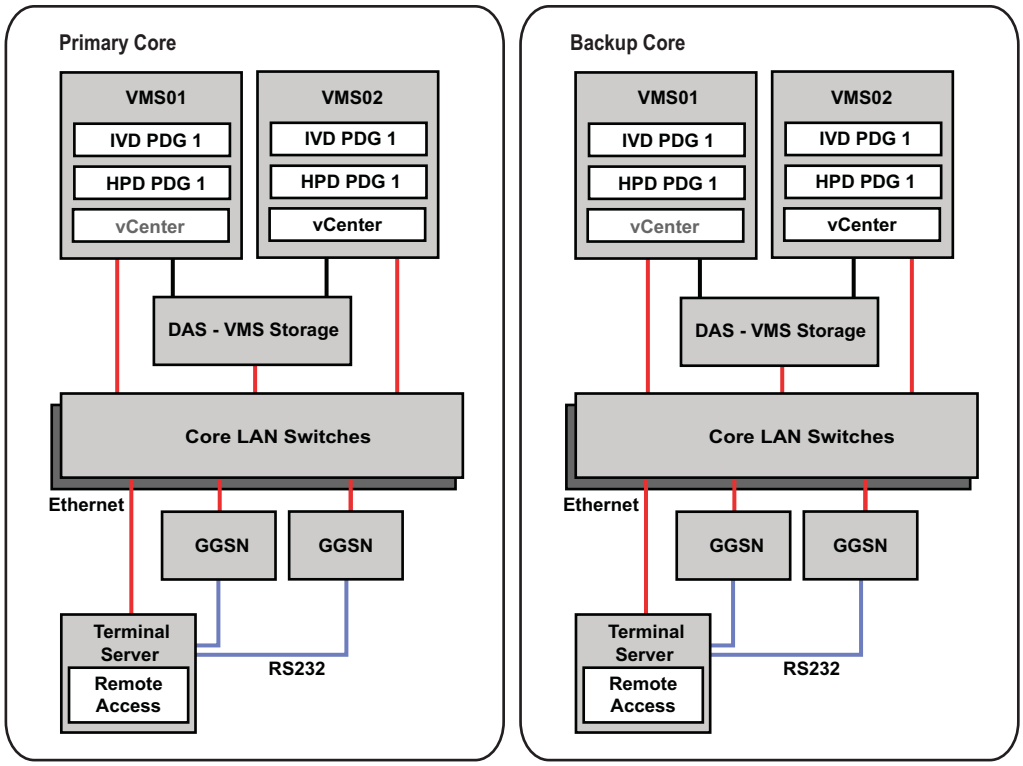
In the case of High Availability for vCenter, there is only one vCenter VM that is instantiated on one server. If that server fails, the vCenter VM moves to the secondary server. To show that the potential for this vCenter VM to reside on the secondary server exists if the primary server fails, one vCenter VM is grayed out in the following diagrams.

Figure 5: Data Subsystem in an HA Data Configuration without DSR



High_Avail_Data_Option_NonDSR_B

Figure 6: Data Subsystem in an HA Data Configuration with DSR



High_Avail_Data_Option_DSR_B

2.3.1
HA Data – Application Experience

Data bearer and non-data bearer applications benefit from the redundancy provided by the High Availability for Trunked IV&DHPD (HA Data) feature.

Data Bearer Service Applications

Packet data bearer service applications require packet data transfer between a Customer Enterprise Network (CEN) host and a subscriber (or attached device) via the Customer Network Interface (CNI), GPRS Gateway Support Node (GGSN), Packet Data Gateway (PDG), and site equipment. In a system with the HA Data feature, these applications experience up to 90 seconds of data loss due to any single failure between the Border Router and the PDG. Data service recovers automatically within 90 seconds after such a failure.

Non-Data Bearer Service Applications

Non-packet data bearer service applications include OTEK, CADI/ATIA, ASTRO® 25 Advanced Message Solution, UEM Email, and UEM NBI. Such applications require packet data transfer between a CEN host and a data application running in the Radio Network Interface (RNI). These applications benefit from the network transport redundancy provided by HA Data. Such an application is able to regain service after an HA switchover in the CNI or within a Master Site. Depending on which component failed, non-data bearer applications may need to re-establish their connection. A Dynamic System Resilience (DSR) switchover of the Network Transport is subject to the current DSR constraints (that is, application users may need to re-establish connections between the client/server in order to have its data flow again properly through the Firewall).

2.3.2

HA Data – Failure and Recovery

In case of a hardware failure, the High Availability for Trunked IV&DHPD (HA Data) feature provides automatic switchover to a redundant peer device. This section describes types of failures and how the system recovers from each. For any failure, the system will recover data service within 90 seconds.

Virtual Management Server (VMS)

If the VMS on which the primary Packet Data Gateway (PDG) resides fails, the secondary PDG on the other Common Server Architecture (CSA) server becomes primary and resumes data service for the zone. When a failed VMS is restored, data service will be lost for 500 ms while the secondary PDG is synchronized with the primary PDG. Restoration of a VMS does not cause a switch in the primary PDG which is actively processing data for a zone.

VMS Network Interfaces

Each CSA server is equipped with redundant Network Interface Cards. If one of the Network Interfaces on a VMS fails, data to and from the PDG is routed via the redundant Network Interface.

GPRS Gateway Support Node (GGSN)

If the primary (active) GGSN fails, the secondary GGSN takes over data service for the zone. This can be caused by a hardware or critical software failure of the GGSN. Restoration of a failed GGSN does not interrupt data service and no switch in the active GGSN occurs. For systems which include the Genesis Charging Gateway to track individual user data usage, charging data is not synchronized between the HA GGSN pair. When there is a GGSN switchover, charging data that has not been reported to the Charging Server is lost for the duration of switchover. Once the secondary GGSN takes over, reporting of charging data resumes.

Customer Network Interface (CNI)

A CNI path consists of a Border Router, an optional Peripheral Network Router, a DMZ Switch, and an RNI-DMZ Firewall. If a component in the active CNI path fails, the next most desirable (highest priority) CNI path takes over transporting data to and from the Customer Enterprise Network (CEN). Data is always routed on the most desirable CNI path available. Restoration of a more desirable CNI path causes data to take the new path.

HA Data without DSR

Two CNI paths exist per Master Site:

- Between the Border Router and each GGSN via a local RNI-DMZ Firewall, DMZ Switch, and optional Peripheral Network Router.

HA Data with DSR

Four CNI paths exist per Master Site:

- Two between the Border Router and each GGSN via a local CNI path (RNI-DMZ Firewall, DMZ Switch, and optional Peripheral Network Router).
- Two between the Border Router and each GGSN via the network transport in the second Master Site. These tunnels exit one Master Site and enter another via the Exit Routers. In the second Master Site, the tunnels are routed via one of the CNI paths and ultimately to a Border Router. Dynamic System Resilience (DSR) is required for these inter-zone tunnels to be supported.

HA Data with Encrypted CEN links

The IP addresses of devices in the Radio Network Interface (RNI) are different depending on which CNI path is active:

- RNI Server IP Address – The IP address used by a client in the CEN to connect to a server in the RNI changes when there is a CNI path switchover. When there is a switchover of the HA

CNI path, new connections from the CEN client to the RNI server need to use an alternate RNI server IP address. It is recommended that the application develop a procedure to monitor the connection between the CEN client and the RNI server. When a broken connection is detected, the alternate RNI server IP address should be used. During a prolonged condition where the CEN client is unable to communicate with the RNI server, the CEN client will need to alternate between the two RNI server IP addresses until the connection is re-established. In a system with both HA Data and DSR, this procedure needs to execute in both the primary and backup zone cores.

- RNI Client IP Address – The IP address of a client in the RNI changes when there is a CNI path switchover. It is expected that servers in the CEN are able to recover from a change in the IP address of an RNI client.

Solutions Support Center (SSC) Connections

Although HA Data introduces multiple CNI paths at a Master Site, there is a single connection from the SSC to a Master Site for Service Access. The SSC connection benefits from the redundant CNI paths for access to the RNI, but the SSC Router and the link to the SSC Router are both single points of failure for Service Access. Failure of either of these components in the path to Motorola SSC results in loss of connectivity until the failure is repaired. The Service Automation server in the SSC network uses this SSC interface to access its satellite servers within the system.

2.4 Transit25 – Theory of Operation

The Transit25 data feature enables the use of the ASTRO® 25 IV&D data system infrastructure to provide location reporting functionality when used in combination with a transit application selected by your organization.

This section details Transit25 components and their interactions.

NOTICE: Transit25 operates in wide area trunking mode for a single zone system. It does not support site trunking or failsoft modes.

2.4.1 Transit25 Data – Components

There are three major components in the Transit25 data system in addition to the IV&D data subsystem components used for data routing:

- CAD server application installed on the transit Computer-aided Dispatch (CAD) server – Located in the Customer Enterprise Network (CEN). Provides communication services required for transfer of data between the Transit CAD client application used by the dispatcher and the transit client application on the mobile device used by the vehicle operator.
- Transit mobile terminal and client application – Located aboard the mobile computer on the vehicle. Used by the transit vehicle operator to receive messages from, and send messages to, the dispatch operator at the console site through the CAD server. The transit application may vary depending on the vendor selected by your organization. The radio subscriber unit connects to the USB port on the mobile terminal to provide connectivity to the radio communication system.
- CAD client application installed on the Transit CAD workstation – Located near the dispatch console site. Used by the dispatcher to communicate with the transit operator in the vehicle.

The Transit CAD Server application interacts with the Transit CAD Client application and the Transit Mobile Client application. Transit applications differ from classic data in the amount and persistence of data.

2.4.2
Transit25 Features

This section describes the following features which are important in the context of Transit25 data services:

- Header compression
- Unconfirmed message delivery
- Controlled channel access
- Data channel steering

2.4.2.1
Unconfirmed Message Delivery

Unconfirmed message delivery enables a more efficient use of packet data channels by reducing the size of messages to fit within an allocated transmission time slot. The reduction in the size is accomplished by removing the retry and acknowledgment phase of confirmed messaging. Unconfirmed messaging over the air reduces the likelihood of shared channel transmission contention and collision on the packet data channel.

TIA 102–specified unconfirmed message delivery is implemented at the radio subscriber, the fixed radio subsystem, and the PDG. The subscriber radio can send the unconfirmed messages on the Controlled Channel Access (CCA) channel as well as Classic channel.

When the RNG receives an inbound unconfirmed message, it does not acknowledge the receipt of the messages or request a retry of the message.

For inbound messages to be sent in unconfirmed mode, the subscriber must be configured with the Controlled Channel Access Protocol - Packet Filter on the mobile computer through SNMP. This filter contains the destination IP address and destination port used to determine if the inbound message from the mobile computer should have its header removed and sent in unconfirmed mode. When the subscriber unit receives an outbound unconfirmed message, it does not acknowledge the receipt of the messages or request a retry of the message.

Broadcast messages are exclusively transmitted in unconfirmed mode.

2.4.2.2
Controlled Channel Access

Packet data channels can operate in one of two modes – classic PDCH and Controlled Channel Access (CCA) PDCH. The classic PDCH operates with unscheduled, confirmed data transmissions whereas a CCA PDCH operates with scheduled, unconfirmed data transmissions.

To provide a high level of efficiency for Transit25 applications, a scheduled transmit PDCH is employed such that a subscriber transmits its data message within its transit transmission slot. All data subscriber radios are synchronized through a time and micro-slot synchronization message announced on a site’s control channel. An application that is synchronized with the system time base specifies a specific point in time for the subscriber radio to transmit a user message. Scheduled message transmissions are accomplished in this manner through a transit application operating on a mobile computer attached to a subscriber radio.

The exact occurrence of the transmission is derived (minimally) by the transit application resident at the vehicle, and is calculated based on the following information:

- Configured report rate for all users on a PDCH
- Synchronization in time received on the control channel
- Assigned “slot” for the transit application mobile terminal

CCA applies to inbound transmissions only, not outbound transmissions.

2.4.2.3
Data Channel Steering

Data channel steering allows subscriber units to be directed to either a classic or Controlled Channel Access (CCA) packet data channel. A classic PDCH exercises unscheduled confirmed and unconfirmed data transmissions. A CCA PDCH employs scheduled unconfirmed data transmissions.

Channel steering occurs when the site controller tags each packet data channel to a data steering group. The Data Access Control (DAC) ID associated with a data steering profile within the group is used to identify PDCHs used for scheduled (classic) or unscheduled (CCA) transfers. During packet data registration (context activation), the subscriber unit receives the DAC from the PDR. The DAC indicates which of the 16 possible data steering profiles are enabled for the subscriber unit.

The subscriber unit matches the received DAC with its internally provisioned DAC. Each internally provisioned DAC bit or data steering profile in the subscriber unit contains additional parameters that identify the mode of operation, classic versus CCA, and the slot size associated with a particular profile.

The site controller can maintain up to five data steering groups and 16 data steering profiles. Each group is associated with a mode of operation, slot size, maximum number of users assigned to the data channel, and a profile list that defines the profiles that are members of that group.

On receiving a PDCH request from a subscriber unit, the site controller checks if the data steering profile specified in the DAC is a member of a configured data steering group. If it is, the site controller checks to see if a PDCH has been assigned for the group. If a PDCH has been assigned, the site controller grants the channel to the requesting subscriber unit. Otherwise, the site controller requests a PDCH for the group following the normal request process. The subscriber unit request is denied by the site controller if the data steering profile is not a member of any of the enabled data steering groups.

The subscriber unit DAC operational mode that is associated with an enabled data steering profile must match the operational mode provisioned for the corresponding data steering profile at the site controller. If the operational mode is provisioned differently at each end, severe performance degradation is likely to occur on the PDCH that is associated with the active data steering group and data steering profile.

Since a CCA PDCH has an allotted message size, an uncompressed UDP/IP datagram that does not fit in the slot is transmitted by the subscriber on the classic packet data channel. The subscriber unit decides on the use of a CCA or classic channel based on the contents of the message header and the size of the message.

Data steering profile updates must be made in both site provisioning through the Unified Network Configurator (UNC) or the Configuration/Service Software (CSS) for the site controller and through Provisioning Manager in all affected radio records. If a profile is deleted from a data steering group in the site controller through UNC/CSS, that profile must also be deleted from all the affected radio records in the PDR. Otherwise, when the subscriber requests a channel with that profile, it is denied by the site controller.

2.4.3
Outbound Broadcast Data Transmission

The following process flow describes how broadcast data messages are delivered to subscriber radios that are tuned to a site's control channel. Subscribers that are already active on a packet data channel at the occurrence of a broadcast message receive that broadcast message on the packet data channel at the end of this process flow.

1. The GGSN receives a datagram for broadcast delivery. The destination is identified in the destination IP address of the message.
2. The GGSN forwards the message to the PDR associated with the destination IP address.

3. The PDR replaces the destination IP address with 255.255.255.255 and forwards the message to RNG with the associated Broadcast ID.
4. The RNG receives and queues the broadcast message, sends a request to all sites within its zone to notify subscribers that a message has arrived for the associated Broadcast ID. It then de-queues and sends the broadcast message to all sites within the zone.
5. The sites send “classic” packet data channel requests to the zone controller if needed. If a “classic” packet data channel is already active, it is reused and no channel requests are necessary.
6. Once the channel is available, the site controller transmits an unsolicited data channel grant over the control channel including the Broadcast ID as the target ID and the appropriate packet data channel ID. Subscribers configured with a matching Broadcast ID respond to the unsolicited data channel grants.
7. Each packet data channel sends the broadcast message in unconfirmed mode with the destination air address set to the Broadcast ID the message.
8. The subscribers receive the message and move to the indicated packet data channel. They then receive the message and forward it to the mobile computer interface.
9. The RNG sends an acknowledgment to the PDR indicating the broadcast message has been delivered to the packet data channels.
10. On receiving the acknowledgment, the PDR transfers the next message in queue for the Broadcast ID in question. Each Broadcast ID is transferred independently in terms of queuing.

This page intentionally left blank.

Chapter 3

Data Services Configuration

This chapter details configuration procedures relating to data services.

3.1 Configuring Data Services

This process lists the high-level steps required to configure the system components for ASTRO® 25 Classic Data and Enhanced Data services. The following objects need to be configured to enable data services in your system:

- Packet Data Gateway (PDG): Packet Data Router (PDR) and Radio Network Gateway (RNG)
- Zone Controller
- Links between the PDR, RNG, Zone Controller, and GGSN router
- Site
- Channel

The following applications are used to configure the system components to implement data services:

Provisioning Manager
Used to configure parameters for the PDG and the Zone Controller.

For more information, see the *Provisioning Manager* manual.

Unified Network Configurator (UNC)
Used to provision parameters for the PDG and the Zone Controller, to configure and manage the site infrastructure equipment, including the Site Controller, Base Radios, and Packet Data Channels.

For more information, see the *Unified Network Configurator* manual.

Configuration/Service Software (CSS)
Used to configure and manage the site infrastructure equipment, including the Site Controller, Base Radios, and Packet Data Channels.

For more information, see the Configuration/Service Software (CSS) online help.

Customer Programming Software (CPS)
Used to configure subscriber units.

For more information, see the *Configuration Programming Software (CPS)* Online Help.

Process:

1. Discover the IV&D PDG for the zone in UNC and publish the infrastructure data to Provisioning Manager.

   For procedures, see the *Unified Network Configurator* manual.

2. Configure the data parameters for the Site Controller in CSS.

   See Configuring Classic Data and Enhanced Data Parameters in the Site Controller with CSS on page 66.

3. When configuring the Base Radio with CSS, leave the default value of the **Enhanced Data Max Wait** parameter unchanged.
4. Configure the parameters for Classic Data in UNC.

See Configuring Classic Data in UNC on page 67.

5 Configure the parameters for Classic Data in Provisioning Manager.

See Configuring Classic Data in Provisioning Manager on page 69.

6 Optional: Configure the parameters for Enhanced Data in UNC.

See Configuring Enhanced Data in UNC on page 70.

7 Optional: Configure the parameters for Enhanced Data in Provisioning Manager.

See Configuring Enhanced Data in Provisioning Manager on page 72.

8 Configure the data parameters for subscriber units in CPS.

For procedures, see the appropriate subscriber documentation.

For information on the data parameters in CPS, see Data Parameters in CPS on page 76.

3.1.1
Configuring Classic Data and Enhanced Data Parameters in the Site Controller with CSS

Perform the following procedure to configure the Site Controller to support the Classic Data and Enhanced Data features in your system. Use the Configuration/Service Software (CSS) application to perform this procedure.

For more information, see the Configuration/Service Software (CSS) online help and the *GCP 8000 Site Controller* manual.

Prerequisites: Complete the initial configuration of the Site Controller. See “Initial Configuration of a Device in CSS” in the *GCP 8000 Site Controller* manual.

Procedure:

1 Connect to the Site Controller through an Ethernet port link.

See “Connecting Through an Ethernet Port Link” in the *GCP 8000 Site Controller* manual.

2 From the navigation tree on the left, select **Site** → **Data Configuration**. Click the **Primary Core** tab.

3 In the **Data Capability** field, leave the default value unchanged.

The **Data Capability** parameter can be configured in the Unified Network Configurator (UNC) application. It is recommended to configure this parameter by using UNC.

4 In the **Page Wait Timer** field, enter the time the Site Controller waits before resending a page.

5 In the **Data Service Activation Rate** field, enter the appropriate value.

6 In the **Max Users per Data Channel** field, enter the maximum number of users per data channel at the site.

7 In the **Voice Grant Filter** field, disable or enable the Voice Grant Filter capability for the channel.

8 In the **RNG Link IP Address** field, enter the IP address for a specific Radio Network Gateway (RNG).

9 Optional: In the **Broadcast Data** pane, configure the broadcast data capability:

a In the **IVD Data Broadcast Capability** field, select **Enabled**.

b In the **IVD Broadcast Data Multicast IP Address 1** and **IVD Broadcast Data Multicast IP Address 2** fields, enter the multicast IP addresses for broadcast connection with the RNG.

10 In the **Enhanced Data Configuration** tab, in the **Enhanced Data Channel Loading** field, leave the default value unchanged.

   The other Enhanced Data parameters available in this tab can be configured in UNC. It is recommended to configure these parameters by using UNC.

11 Perform one of the following actions to save the configuration data.

   - To save the configuration data to a new archive file, from the menu, select **File** → **Save As**.
   - To overwrite the existing archive file, select **File** → **Save**.

   IMPORTANT: Be sure to save any configuration changes to a local or network drive so that if the device module fails, you can load your settings to a replacement device module. If the configuration file is not saved to a local or network drive, you will need to repeat the set-up steps after replacing a device module.

12 Write the configuration data to the device. From the menu, select **File** → **Write Configuration to Device**.

3.1.2
Configuring Classic Data in UNC

Perform the following procedure to configure the infrastructure to support the Classic Data feature in your system. Use the Unified Network Configurator (UNC) application to perform this procedure.

For more information on the Classic Data parameters that you configure with this procedure, see Classic Data Parameters in UNC on page 73.

Procedure:

1 Log on to the UNC Wizard. See the *Unified Network Configurator* manual.

2 Select the **System Configuration** wizard and click the **Data Configuration** tab.

3 In the **General Settings** pane, in the **APN Operator ID** field, enter the ID that represents the APN Operator for the data system.

4 Configure the parameters in the **Trunked Integrated Data** pane:

   a In the **IVD Broadcast Data Capability** field, select **Disable** or **Enable**.

   b In the **Maximum Users Per Data Channel (IVD Only)** field, enter the maximum number of users per data channel.

5 Configure the parameters in the **IP Header Compression** pane:

   a In the **Enable Compression** field, select **Yes** or **No**.

   b In the **Max Time Between Full Headers (sec)** field, enter the maximum number of seconds between full headers.

   c In the **Max Number of Compressed Headers Between Full Headers** field, enter the maximum number of compressed headers between full headers.

   IMPORTANT: To send one full header at the beginning of a data session and all compressed headers after that, configure both the **Max Time Between Full Headers** and the **Max Number of Compressed Headers Between Full Headers** to a value of 0.

   d In the **Max Non-TCP Contexts Per Subscriber** field, enter the number of non-TCP contexts per subscriber.

   e In the **Max Header Size That May Be Compressed** field, enter the maximum header size that can be compressed.

6 Select the **Advanced Data Configuration** tab.

7 Configure the parameters in the **Trunked Integrated Data and HPD** pane:
   a In the **Broadcast Data Ack Time (sec)** field, enter an appropriate value.
   b In the **Mobility Query Timer (sec)** field, enter an appropriate value.
   c In the **Outstanding Queries** field, enter an appropriate value.
   d In the **LLC User Plane Window Size** field, enter an appropriate value.
   e In the **LCC User Plane Response Timer (msec)** field, enter an appropriate value.
8 Configure the parameters in the **Trunked and Conventional Integrated Data** pane.
   a In the **Broadcast Data Wait Time (sec)** field, select an appropriate number.
   b In the **LLC Timer (sec)** field, select an appropriate number.
   c In the **LLC Number of Attempts** field, select an appropriate number.
9 Configure the parameters in the **Trunked Integrated Data** pane:
   a Leave the **Packet Data Channel Slot Time (microslots)** field at the default value.
   b In the **Data Busy Queue Priority** field, enter the priority level that a data channel has in the busy queue.
   c In the **IVD FNE SNDCP Queue Dwell Time (sec)** field, enter the appropriate number.
   d In the **IVD Ready Time Delta (sec)** field, enter the appropriate number.
   e In the **Page Wait Timer (sec)** field, enter the appropriate number.
   f In the **IVD Standby Timer (hours)** field, enter the appropriate number.
   g In the **Preferred Data Service** field, select the data service to be given priority when a channel is preempted or a busy conversion occurs.
      • To give priority to Classic Data, select **P25 Classic**.
      • To give priority to Enhanced Data, select **Reserved Access**.
10 Click **Submit**.
11 Configure the Access Point Name (APN):
   a Select the **APN** wizard.
   b Click **Add Row**.
   c In the **Zone ID** field, enter the zone number.
   d In the **APN** field, enter the APN Network ID.
12 Configure an unconfirmed message filter or filters for the APN:
   a In the **Source IP Address** field, enter the source IP address for the selected APN.
   b In the **Destination Port Number** field, enter the destination port number for the selected APN.
   c Save the APN and unconfirmed message filters by clicking **Submit**.
13 Configure the GGSN Zone ID for the PDG:
   a Select the **Zone Configuration** wizard and click the **PDG GGSN Configuration** tab.
   b In the **Primary Core PDG GGSN Zone ID** field, enter the Zone ID of the Primary Core GGSN.
   c In the **Backup Core PDG GGSN Zone ID** field, enter the Zone ID of the Backup Core GGSN.
   d Click **Submit**.

14 Configure the site-level parameters for Classic Data:

a Select the **Site** wizard.

b In the **Zone ID** field, select a zone.

c In the **Site ID** column in the table, double-click the number of a site that you want to configure for Classic Data.

d In the **Data Capability** field, perform one of the following actions:

- To enable Classic Data in the system, select **P25 Classic Data Service**.
- To enable Classic Data and Enhanced Data in the system, select **P25 and Reserved Access Data Services**.

e In the **Protected P25 Classic Data Channels** field, enter the number of Classic Data channels that you want to be protected from preemption by anything other than an Emergency Call.

NOTICE: You can update **Data Capability** and **Protected P25 Classic Data Channels** parameters for multiple sites in a zone by using the **Multiple Update Configuration** option in the UNC Wizard. For more information, see the *Unified Network Configurator* manual.

f Click **Submit**.

15 Approve the remedy job in EMC Smarts Network Configuration Manager.

See “Approving Configuration Changes” in the *Unified Network Configurator* manual.

16 To distribute the configuration changes to the network devices, click **Publish Infrastructure Data**.

IMPORTANT: Plan updates and distribute them in batches when the updates are completed.

3.1.3
Configuring Classic Data in Provisioning Manager

Perform the following procedure to configure the infrastructure to support the Classic Data feature in your system. Use the Provisioning Manager application to perform this procedure.

Procedure:

1 Log on to Provisioning Manager.

See the *Provisioning Manager* manual.

2 Configure subscriber units for Classic Data:

a Select **Subscriber** → **IVD Radio**.

b Select an IVD Radio record and click **Edit**.

To update parameters for multiple subscribers, you can select a number of records at a time.

c In the **Data Capability** field, perform one of the following actions:

- To enable the radio or radios for Classic Data, select **P25 Classic Data Service**.
- To enable the radio or radios for Classic Data and Enhanced Data, select **P25 Classic and Reserved Access Data Services**.

d Click **Update**.

3 Optional: Configure Broadcast Data Agencies for subscribers:

a Select **Subscriber** → **Broadcast Data Agency**.

b Click **+ (New)** to add a Broadcast Data Agency.

c In the **Radio ID** field, enter a number that refers to a specific radio on the system.

d In the **Broadcast Data Agency Alias** field, enter a name that is unique among all Broadcast Data Agencies, radio users, and console users in the system.

e In the **Broadcast Data Agency Type** field, select IVD.

f In the **Security Group** field, select the security group for this Broadcast Data Agency.

g In the **IP Identity** pane, click the arrow to add a new record.

h In the **Zone** column, select the zone configured to broadcast data for the Broadcast Data Agency.

i In the **Access Point Name** column, select the APN that can be used by the Broadcast Data Agency.

The APN Network ID identifies the home network of the Broadcast Data Agency.

j In the **IP Address** column, enter the IP address associated with the Broadcast Data Agency configured for the zone.

k Click **Save**.

4 Distribute the configuration changes to the network devices. See the *Provisioning Manager* manual.

IMPORTANT: Plan updates and distribute them in batches when the updates are completed.

Classic Data is enabled in your system.

3.1.4
Configuring Enhanced Data in UNC

Perform this procedure to configure the infrastructure to support the Enhanced Data feature in your system. Use the Unified Network Configurator (UNC) application to perform this procedure.

You can make the following configuration changes at the same time as Classic Data configuration and distribute the changes in a batch after you complete all updates.

Perform this procedure before enabling subscribers for Enhanced Data in the Provisioning Manager application.

For more information on the Enhanced Data parameters that you configure with this procedure, see Enhanced Data Parameters in UNC on page 77.

Prerequisites:
Ensure that the parameters for Classic Data services are configured.

Obtain the *Unified Network Configurator* manual.

Procedure:

1 Log on to the UNC Wizard. See the *Unified Network Configurator* manual.

2 Enable at least one channel at a site for Enhanced Data:

a Select the **Channel** wizard.

b Select the appropriate zone and the site that you want to configure for Enhanced Data.

c For the channels that you want to enable for Enhanced Data, set the **Reserved Access Data Capable** parameter to **Yes**.

IMPORTANT:
At least one channel at a site must be marked as **Reserved Access Data Capable** before the site can be enabled for Enhanced Data. Only G-series channels can be configured as **Reserved Access Data Capable**.

You can update multiple channels at a site by using the **Multiple Update Configuration** option in the UNC Wizard. For more information, see the *Unified Network Configuration* manual.

d Click **Submit**.

3 Optional: Create Data Agency Groups (DAGs):

a Select the **Data Agency Group** wizard.

DAG 1 exists in the system by default.

b To add a Data Agency Group, click **Add Row**.

c In the **ID** field, enter a unique number associated with the DAG.

d Optional: In the **Alias** field, enter a unique name associated with the DAG.

e Click **Submit**.

4 Optional: Configure Enhanced Data Utilization Profiles:

a Click the **Enhanced Data Utilization Profile** wizard.

Enhanced Data Utilization Profile 1 exists in the system by default.

b To add a new Enhanced Data Utilization Profile, click **Add Row**.

c In the **ID** field, enter a unique number associated with the Enhanced Data Utilization Profile.

d Optional: In the **Alias** field, enter a unique name associated with the Enhanced Data Utilization Profile.

e In the **Data Agency Group Utilization** column, perform one or more of the following actions:

- For DAGs that you want to have a minimum configured bandwidth allocation, select a utilization percentage of 1–100.

  You do not have to enter a number for all DAGs. The sum of utilizations must add to less than or equal to 100%.

- For DAGs that you want to keep enabled for Enhanced Data access at the site but which may not get any access during peak loading periods, select a utilization percentage of 0.
- For DAGs that you want to disable for Enhanced Data access at the site, select **Disabled**.

f Click **Submit**.

5 Configure the site-level parameters for Enhanced Data:

a Select the **Site** wizard.

b In the **Zone ID** field, select a zone.

c In the **Site ID** column in the table, double-click the number of a site that you want to configure for Enhanced Data.

d In the **Data Capability** field, select **P25 Classic and Reserved Access Data Services**.

e In the **Enhanced Data Utilization Profile** field, select an Enhanced Data Utilization Profile to be used for this site.

f In the **Protected Reserved Access Data Channels** field, enter the number of Enhanced Data channels to be protected.

NOTICE:
Do not count a channel as both a Protected P25 Classic Data Channel and a Protected Reserved Access Data Channel. The sum of Protected P25 Classic Data Channels and Protected Reserved Access Data Channels should be less than or equal to the total number of channels at the site minus one (the Control Channel).

You can update the **Data Capability**, **Enhanced Data Utilization Profile**, and **Protected Reserved Access Data Channels** parameters for multiple sites in a zone by using the **Multiple Update Configuration** option in the UNC Wizard. For more information, see the *Unified Network Configuration* manual.

g Click **Submit**.

6 Approve the remedy job in EMC Smarts Network Configuration Manager.

See “Approving Configuration Changes” in the *Unified Network Configuration* manual.

7 To distribute the configuration changes to the network devices, click **Publish Infrastructure Data**.

IMPORTANT: Plan updates and distribute them in batches when the updates are completed.

The infrastructure in your system is configured for Enhanced Data.

3.1.5
Configuring Enhanced Data in Provisioning Manager

This procedure describes how to configure subscribers for the Enhanced Data feature by using the Provisioning Manager application.

Perform this procedure after configuring the infrastructure for Enhanced Data and distributing the configuration to the network devices by using the Unified Network Configurator (UNC) application.

You can perform these steps at the same time as Classic Data configuration and distribute the changes in a batch after you complete all updates.

Prerequisites:
Ensure that the parameters for Classic Data are configured.

Obtain the *Provisioning Manager* manual.

Procedure:

1 Log on to Provisioning Manager. See the *Provisioning Manager* manual.

2 Enable subscribers for Enhanced Data and add them to Data Agency Groups:

a Select **Subscriber** → **IVD Radio**.

b Select an IVD Radio record and click **Edit**.

To update parameters for multiple subscribers, you can select a number of records at a time.

c In the **Capabilities and Settings** pane, in the **Data Capability** field, select **P25 Classic and Reserved Access Data Services**.

d In the **Data Agency Group** pane, select a Data Agency Group for the subscriber or subscribers.

e Click **Update**.

3 Optional: Configure ZoneWatch to display Site Data Load information:

a Select **Applications** → **Raw Data Filter**.

b Select a Raw Data Filter record and click **Edit**.

c In the **Infrastructure Data** pane, set the **Site Data Load Update** parameter to **Yes**.

d Click **Update**.

4 Distribute the configuration changes to the network devices. See the *Provisioning Manager* manual.

IMPORTANT: Plan updates and distribute them in batches when the updates are completed.

Enhanced Data is enabled in your system.

3.1.6
Classic Data Parameters in UNC

Table 5: Classic Data Parameters in UNC

The following table provides the names and descriptions of the parameters relating to Classic Data service that can be configured in the Unified Network Configurator (UNC) application.

Parameter	Description
APN Network ID	Access Point Name Network IDs that can be used by the radio user. The APN identifies the home network of the radio user.
APN Operator ID	Alias that represents the APN (Access Point Name) Operator for this data system.
Backup Core PDG GGSN Zone ID	Used by the PDG to calculate the GGSN IP address based on the GGSN zone ID and the IP plan.
Broadcast Data Ack Time (sec)	The time in seconds that the RNG waits after sending the last segment of the Broadcast Data message before sending an ACK to the PDR to indicate it has finished the transmission.
Broadcast Data Wait Time (sec)	The time in seconds that the RNG waits for the sites to allocate a Packet Data Channel for Broadcast and for the subscribers to move to the newly allocated channel.
Data Busy Queue Priority	Priority level that an unprotected data channel has in the busy queue. That is, the priority associated with a data channel request when the number of already-assigned data channels of the same type at the site is above the protected limit. The protected limit is the provisioned number of protected channels of that type.
Data Capability	Specifies the type or types of data service available at a site.
Destination Port Number	A radio destination port number for an unconfirmed message filter for the selected APN Network ID. Unconfirmed message filters allow sending messages from the application host source IP address to the destination radio port as unconfirmed.
Enable Compression	Allows the use of IP Header Compression in the system.
IVD Broadcast Data Capability	Enables Broadcast Data Capability in the entire system.

Table continued…

Parameter	Description
IVD FNE SNDCP Queue Dwell Time (sec)	The time in seconds that a message is allowed to wait in the PDR outbound queue before it is discarded.
IVD Ready Time Delta (sec)	Both the subscriber and the Packet Data Gateway (PDG) run a Ready Timer to determine when the subscriber should leave a Classic Data channel after a period of no data activity. The PDG subtracts this delta value from the actual Ready Timer value and uses the result to determine when to send a message telling the subscriber to leave the channel. If the PDG waits the full duration of the Ready Timer before sending a message, the subscriber's Ready Timer expires by the time the PDG sends the message over the air.
IVD Standby Timer (hours)	Monitors the time an MSU can retain its context following data service activity. Value in seconds.
LLC Number of Attempts	The number of times the RNG sends the same message to the MSU before giving up.
LLC Timer (sec)	The number of seconds the RNG waits before retrying the message to the MSU. Value in seconds.
LLC User Plane Response Timer (msec)	The amount of time the User Plane waits to receive an acknowledgement before sending the next attempt.
LLC User Plane Window Size	The number of messages allowed into the LLC User Plane window, before an acknowledgement must be received to continue.
Max Header Size That May Be Compressed	Threshold header size in bytes after which the system does not use compressed headers. Headers larger than this size are not compressed.
Max Non-TCP Contexts Per Subscriber	Maximum number of Non-TCP header compressions contexts per subscriber used by system devices to allocate system and memory resources.
Max Number of Compressed Headers Between Full Headers	Specifies the maximum number of compressed headers sent between full headers. Setting this parameter to a non-zero value results in sending a full UDP/IP header after the specified number of datagrams with compressed headers. Setting this parameter and **Maximum Time Between Full Headers** to a value of 0 results in sending one full header at the beginning of a data session and all compressed headers thereafter. This setting is recommended only in cases where high confidence exists that all network links from the site to the Customer Enterprise Network (CEN) have a very low error rate.
Max Time Between Full Headers	Specifies the maximum time between full headers. Setting this parameter to a non-zero value results in sending compressed headers for that time interval, then sending a full UDP/IP header.

Table continued…

Parameter	Description
	Setting this parameter and the **Max Number of Compressed Headers Between Full Headers** to a value of 0 results in sending one full header at the beginning of a data session and all compressed headers thereafter. This setting is recommended only in cases where high confidence exists that all network links from the site to the Customer Enterprise Network (CEN) have a very low error rate.
Maximum Users Per Data Channel	Used to limit the number of radio users that can be present on one Classic Data channel. If the system reaches this limit, it assigns another Classic Data channel to service the additional data users.
Mobility Query Timer (sec)	The time a mobility client waits for a given query response.
Outstanding Queries	The maximum allowed mobility queries to the mobility server at one time.
Page Wait Timer (sec)	The maximum time to wait for Packet Data Channel access. Value in seconds.
Preferred Data Service	This attribute specifies which data service is given priority when a channel is preempted or a busy conversion occurs.
Primary Core PDG GGSN Zone ID	Used by the PDG to calculate the GGSN IP address based on the GGSN zone ID and the IP plan.
Protected P25 Classic Data Channels	This attribute specifies the number of P25 Classic Data channels protected from preemption by anything other than an Emergency Call.
Source IP Address	A Customer Enterprise Network (CEN) application host source IP address for an unconfirmed message filter for the selected APN Network ID. Unconfirmed message filters allow sending messages from the application host source IP address to the destination radio port as unconfirmed.

3.1.7
Classic Data Parameters in Provisioning Manager

Table 6: Classic Data Parameters in Provisioning Manager

The following table provides the names and descriptions of the parameters relating to Classic Data services that can be configured in the Provisioning Manager application.

Parameter	Description
Broadcast Data Agency	The Broadcast Data Agency object allows you to configure the ability to send data messages to a large set of users within the entire system coverage area. Before configuring the Broadcast Data Agency, it is necessary to ensure that GGSN and APN are configured in the Unified Network Configurator (UNC) and synchronized to the Provisioning Manager, and that a respective IVD Radio object exists.

Table continued…

Parameter	Description
Data Capability	Specifies the data service type for a subscriber. The available values include **No Data Service**, **P25 Classic Data Service** for Classic Data, and **P25 Classic and Reserved Access Data Services** for Classic Data and Enhanced Data.

3.1.8
Data Parameters in CPS

Table 7: Data Parameters in CPS

The following table provides the names and descriptions of subscriber parameters relevant for data services that are configured by using the Customer Programming Software (CPS).

Parameter	Description
Allow Enhanced Data On Classic Data Channel	Allows you to send Enhanced Data as Classic Data when a Classic Data channel is already in use or when an Enhanced Data channel is not available.
Common Air Interface, Timers and Threshold	Established to set limits on CAI threshold timers.
Context Deactivation Alert Tone	When selected, an alert tone is generated if the radio has context deactivated.
CQPSK	Compatible Quadrature Phase Shift Keying for narrowband simulcast operation and non-simulcast operation. This selection is only available to radio models equipped with Common Air Interface (CAI) Digital Operation. This digital modulation type is required for any data service on a Simulcast channel.
DAC Operational Mode	Classic APCO 25, Enhanced Data, or Controlled Channel Access.
Disable NAT	Keep enabled. When NAT is enabled, the system supports data applications running on an attached mobile computer.
Enhanced Data Port List	This list includes the UDP ports used for sending Enhanced Data. By default, the list has a port entry of 1031. To send Enhanced Data for the ports specified in the list, select the Enhanced Data Port List for the corresponding data profile. By default, the port list is disabled for the data profile.
Enhanced Data Queue Dwell Timer (sec)	The amount of time that an Enhanced Data IP datagram remains in the SNDCP queue.
IP Header Compression Enable	Indicates if RFC2507 UDP/IP Header Compression is enabled.
Max # Compressed Headers Between Full Headers	Specifies the maximum number of compressed headers sent between full headers
Maximum Time Between Full Headers	Specifies the maximum time between full headers. Setting this parameter to a non-zero value results in sending com-

Table continued…

Parameter	Description
	pressed headers for that time interval, then sending a full UDP/IP header.
Mobile Computer IP Address	The IP address of the mobile computer when the link is set up between the subscriber unit and mobile computer. Network Address Translation (NAT) is to be enabled, not disabled.
Packet Data Capable System	Enables or disables packet data.
Packet Data Registration Version	Indicates the SNDCP version used by the subscriber unit. SNDCPv3 is required for Enhanced Data.
Port List Selection	Allows you to select the Enhanced Data Port List. You can send Enhanced Data to the ports specified in the port list.
Ready Timer	The duration for which a subscriber remains on the Packet Data Channel after data service activity.
Rx Voice Interrupts Data	When enabled, Rx voice has a higher priority than data and interrupts the data session. When disabled, the Rx voice does not interrupt a data session.
Queue Dwell Timer (sec)	The amount of time that a Classic Data IP datagram remains in the SNDCP queue.
SNMP Traps	When selected, status messages are sent to the mobile computer.
Subscriber IP Address	The IP address used by the radio when communicating to a mobile computer while running CPS or when NAT is disabled.
Terminal Data	Enables or disables terminal data.

3.1.9
Enhanced Data Parameters in UNC

Table 8: Enhanced Data Parameters in UNC

The following table provides the names and descriptions of the parameters relating to Enhanced Data service that can be configured in the Unified Network Configurator (UNC) application.

Parameter	Description
Data Capability	Specifies the type or types of data service available at a site.
Data Agency Group	An organizational group for Enhanced Data subscribers. All Enhanced Data subscribers must be members of one and only one Data Agency Group (DAG). Each DAG has a unique ID and alias.
Data Agency Group Utilization	A utilization percentage assigned to Data Agency Groups (DAG) that you want to have a minimum configured bandwidth allocation. The sum of utilizations must add to less than or equal to 100%. DAGs with a zero percentage are enabled to use Enhanced Data at the site but may not get any access during peak loading periods. DAGs for which

Table continued…

Parameter	Description
	Disabled is selected are not allowed Enhanced Data access at the site.
Enhanced Data Utilization Profile	Identifies the bandwidth utilization enforced for each defined Data Agency Group (DAG) at a site. An Enhanced Data-capable site has one and only one Enhanced Data Utilization Profile associated with it. The bandwidth utilizations defined in the profile of a site are enforced when access protection is being performed at the site.
Protected Reserved Access Data Channels	Specifies the number of Enhanced Data channels protected from preemption by anything other than an Emergency Call.
Reserved Access Data Capable	Specifies whether a channel is capable of supporting Enhanced Data.

3.1.10
Enhanced Data Parameters in Provisioning Manager

Table 9: Enhanced Data Parameters in Provisioning Manager

The following table provides the names and descriptions of the parameters relating to Enhanced Data services that can be configured in the Provisioning Manager application.

Parameter	Description
Data Capability	Specifies the data service type for a subscriber. The available values include **No Data Service**, **P25 Classic Data Service** for Classic Data, and **P25 Classic and Reserved Access Data Services** for Classic Data and Enhanced Data.
Data Agency Group	A Data Agency Group (DAG) is an organizational group for Enhanced Data subscribers. All Enhanced Data subscribers must be members of only one DAG. Contention for Enhanced Data site utilization is based on DAG membership.
Site Data Load Update	Setting this parameter to **Yes** allows you to view Site Data Load Information in ZoneWatch. Setting this parameter to **No** filters out all Site Data Load Update data, so you do not see this information.

3.2
High Availability for Trunked IVDHPD Configuration Installation

L2, M2, and M3 zone cores in Common Server Architecture (CSA) systems can be configured with redundant devices in the data subsystem to provide high availability of data services and automatic switchover in case of a component failure.

Enabling the High Availability for Trunked IV&D, including Classic Data and Enhanced DataHPD (HA Data) feature requires:

- Installing the VMware vCenter application and enabling the Fault Tolerance feature for PDGs. See the *ASTRO 25 vCenter Application Setup and Operations Guide*.
- Installing redundant GGSN routers. See the *System Gateways – GGM 8000* or *System Routers – S6000/S2500* manuals.

- Installing redundant CNI path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers). See the *System LAN Switches*, *GGM 8000 System Gateway* or *S6000 and S2500 Routers* , and *Fortinet Firewall* manuals.

For a description of HA Data and operations related to this feature, see the *HPD Packet Data Resource Management* manual.

This page intentionally left blank.

Chapter 4

Data Services Optimization

This chapter contains optimization procedures and recommended settings relating to data services.

4.1 Optimization for Data Services

Optimization of classic IV&D and Enhanced Data services is performed at the time of system planning. Typical message sizes and frequency of broadcast messages are added to the messaging profile of the system to determine the system size.

NOTICE: While no routine optimization is required, Motorola Solutions has engineering application tools to model performance of wireless communications systems for coverage prediction and traffic analysis. See your Motorola Solutions system planner or field engineer for details.

This page intentionally left blank.

Chapter 5

Data Services Operation

This chapter describes the operation of Classic Data and Enhanced Data, and provides the procedure for a manual Packet Data Gateway (PDG) switchover when the PDG is in a high availability configuration.

5.1 Classic Data Operation

The Classic Data services are used in one of the following ways:

- The user initiates and receives data transmissions using an application resident on the radio subscriber itself.
- The user connects a mobile data device, such as a laptop, to the radio subscriber unit and uses an application installed on the data device to transmit and receive data.

For more information, see the relevant user guides, data accessory guides, or software manuals.

Classic Data is a P25 standard packet data service supporting general inbound and outbound datagram transfer over Trunked channels. It is strongly recommended that UDP/IPv4 be used for network transport between the subscriber (or attached device) and the Customer Enterprise Network (CEN). IPv6 datagram transport is not supported. Both Header Compression (UDP/IP) and Network layer encryption (IPSec, via the Encrypted Integrated Data feature) is supported with Classic Data.

ASTRO® 25 supports inter-zone roaming for Classic Data. A roaming subscriber is served by the Radio Network Gateway (RNG) in the zone they are currently in, and that RNG communicates with the Packet Data Router (PDR) and the GPRS Gateway Support Node (GGSN) in the subscriber's home zone for message delivery to and from the CEN. Confirmed unicast datagram delivery is supported both inbound and outbound. In addition, unconfirmed unicast outbound datagram delivery is supported.

5.2 Enhanced Data Operation

The Enhanced Data services are used in one of the following ways:

- The user initiates data transmissions using an application resident on the radio subscriber itself.
- The user connects a mobile data device, such as a laptop, to the radio subscriber unit and uses an application installed on the data device to transmit data.

Enhanced Data is a Motorola Solutions proprietary (not P25 standard) inbound-only packet data service optimized for applications that periodically send short messages from a subscriber (or attached device) to a Customer Enterprise Network (CEN) host. Enhanced Data is only supported on Trunked ASTRO® IV&D systems with GTR-series site equipment and APX subscriber units. Datagrams to be carried via Enhanced Data must use UDP/IPv4 for network transport between the subscriber (or attached device) and the CEN. (The subscriber uses the Enhanced Data service when the UDP Destination Port in an inbound datagram matches one of the CPS-configured Enhanced Data Port Numbers in the subscriber and the site supports Enhanced Data). The port configured in the subscriber radio and the port configured in the server in the Customer Enterprise Network (CEN) need to match. Neither TCP nor IPv6 are supported for datagram transport. Optionally, either Header Compression (UDP/IP) or IPSec encryption (via the Encrypted Integrated Data feature) can be used together with Enhanced Data.

The Enhanced Data channel is based on the timing and signaling characteristics of the Phase 2 TDMA channel. However, both logical TDMA channels are used in tandem to provide Enhanced Data service;

it is not possible to run Enhanced Data on one logical channel and voice on the other logical channel. Only inbound packet data messaging is supported – no outbound packet data messaging is supported on Enhanced Data channels. Context activation on a Classic Data channel is required before Enhanced Data messaging can be performed.

An inbound datagram is sent using a reservation scheme where the subscriber computes the number of TDMA time slots required to send the message and makes a request to the infrastructure for the slots. The infrastructure schedules the requested slots, and the scheduling is communicated to the subscriber via outbound signaling on the Enhanced Data channel. The subscriber then sends its message using the assigned scheduling, and each slot is acknowledged by the infrastructure over the air. Any slots of data that are not successfully acknowledged are retransmitted by the subscriber. Retries are performed until the infrastructure indicates the entire message has been successfully received.

5.3 High Availability for Trunked IVDHPD Operation

In case of a hardware failure, the High Availability for Trunked IV&D, including Classic Data and Enhanced DataHPD (HA Data) feature provides automatic switchover to a redundant peer device. A switchover can also be initiated manually on a PDG and GGSN.

Manual PDG switchover
Performed with Unified Event Manager (UEM). The procedure is described in Performing a Manual Switchover between High Availability PDGs on page 84.

Manual GGSN switchover
Executed from the Unified Network Configurator (UNC) by performing a reboot of the primary GGSN router. The reboot causes the redundant GGSN to take over. See the *Unified Network Configurator* manual for the router reboot procedure.

For more information on the use of VMware vCenter, see the *ASTRO 25 vCenter Application Setup and Operations Guide*.

For more information on the use and operation of the Direct Attached Storage (DAS) device, see the *Virtual Management Server Software* manual.

5.3.1 Performing a Manual Switchover between High Availability PDGs

If your system supports the High Availability for Trunked IV&D (including Enhanced Data) and HPD (HA Data) feature, use this procedure to control which Packet Data Gateway (PDG) is active by initiating a switchover from the primary to the secondary PDG. This operation is available to the user, but not performed in a regular scenario.

Prerequisites: Ensure that VMware vCenter is discovered in Unified Event Manager (UEM).

Procedure:

1. From the **Navigation View** pane in UEM, select **Network Database** and find the PDG Fault Tolerant Virtual Machine on the list of managed resources.

   NOTICE: In the Type column, the PDG is displayed as Fault Tolerant Virtual Machine. The Managed Resources column shows the name of the PDG virtual machine.

2. Right-click the PDG Fault Tolerant Virtual Machine and select **Issue Command**.

   The **Command** window appears.

3 Select **Switchover** and click **Apply**.

A switchover is performed. The secondary PDG becomes active, and the previously active PDG becomes redundant.

5.4 Transit25 Data Operation

In a Transit 25 implementation, the transit (vehicle) operator has a data terminal mounted in the vehicle and connected to the subscriber radio. The transit operator uses the transit client application on the data terminal to view broadcast data messages sent to the fleet or fleet subgroup by the dispatcher. The dispatcher is also able to broadcast voice messages to the fleet.

In case of emergencies, the transit operator may initiate voice transmissions to the dispatch position. In most cases, the operator must first place a request for a voice transmission request to the dispatch position. Once the request is accepted, the operator may begin speaking.

Transit operation varies based on the application chosen by your organization. For details, see the user guides that shipped with your vendor transit dispatch and client applications.

This page intentionally left blank.

Chapter 6

Data Services Troubleshooting

This chapter provides fault management and troubleshooting information relating to data services failure.

6.1 Failure Scenarios and Solutions

Table 10: Data Service Troubleshooting Scenarios and Solutions

The following table lists problems that you can encounter with data services, possible causes, and troubleshooting steps.

Symptoms	Possible Causes	Solution
Messages are not received by the infrastructure	RF collisions Subscriber is in a poor coverage area. Overloaded channel causes messages to be timed out.	Assess channel loading and performance at the site where problems are detected.
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, Site Controller, Zone Controller, 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, see 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 (UEM) that the link is down. The RNG context de-activates the subscriber unit.	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 UEM.

Table continued…

Symptoms	Possible Causes	Solution
	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.	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 context creation message from the PDR. Link up states are reported to the UEM.
	PDR link failure with RNG in a different zone – PDR detects link failure within 15 seconds of inactivity and notifies the fault management application (UEM) that the link is down. If the PDR receives a message from the GGSN, it replies with an ICMP message to the host application in the CEN indicating the message could not be delivered. Messages are queued until message timer expiration. After this point, the PDR generates another notification to the host application indicating the message could not be delivered.	Determine the root cause and fix the link failure. Link up states are reported to the UEM.
	RNG link failure with PDR in a different zone – RNG detects link failure and waits for link to be reestablished by the PDR. When the RNG receives a message from the Site Controller, it sends the data to the PDR in its home zone. The PDR responds with an unknown ID message. The RNG sends a context deactivation command to the radio subscriber.	Determine the root cause and fix the link failure. Link up states are reported to the UEM.
	Local RNG to PDR link failure – The local RNG detects the link failure and stops responding to the base station and the PDRs that it is connected to. The RNG then waits for the link to be reestablished with the PDR.	Determine the root cause and fix the link failure. Link up states are reported to the UEM.
	PDR failure – This scenario is like a link failure between the RNG and the GGSN. All radios served by the failed PDR lose data service during the PDR failure. The fault management application (UEM) detects the failure after a timeout of its polling interval.	Check in UEM for the state of the PDR and any events or alarms reported to it by the PDR before the failure. Determine the root cause and fix the link or hardware issue as appropriate. Link up states are reported to the UEM.

Table continued…

Symptoms	Possible Causes	Solution
	Zone Controller - PDG link failure – This link is used for mobility pushes and queries. After a maximum number of failure counts is reached, the fault management application is notified.	Check in UEM for the state of the PDR and Zone Controller and any events or alarms reported to it by these devices. Determine the root cause and fix the link or hardware issue as appropriate. Link up states are reported to the UEM.
	For radios whose records exist in the RNG, the record is updated with inbound data and the message reaches the destination. Outbound data is sent to the last-known Base Radio and this may result in a failure to reach the proper site until the RNG is able to query the Zone Controller again. The RNG sends delivery notification failure to the PDR if all Zone Controller query retry attempts have failed. The PDR sends an ICMP message to the host.	
	For radios whose records do not exist in the RNG, inbound data causes a new radio record to be created and data reaches its destination. Outbound data is sent to the last-known RNG and this results in a failure to reach the proper site until the PDR is able to query the Zone Controller again. The PDR sends an ICMP message to the host application if the message cannot be delivered.	
Data is not delivered to the CEN or to the subscriber unit ZoneWatch/UEM indicates Site Trunking state. Data service is unavailable at the site (as reported on the subscriber unit)	Zone Controller has failed or link to Zone Controller is lost. Site enters site trunking and data service is lost. This scenario has symptoms like a ZC-Base Radio, ZC-PDR, or ZC-RNG failure. Failure of the active Zone Controller causes a switchover to the standby Zone Controller. All sites in the zone enter “local area” operating mode until the standby Zone Controller becomes active and indicates that the sites can go into wide trunking. The Zone Controller mobility database is lost due to the failure since the standby Zone Controller does not have the mobility information. Site mo-	Determine why the site is in site trunking state and address the cause of the failure. Check the status of the Zone Controller and the Zone Controller-to-site link.

Table continued…

Symptoms	Possible Causes	Solution
	bility upload occurs after the standby Zone Controller is up and functioning. When a Site Controller enters site trunking, it sends Packet Data Channel termination information to the subscriber unit, terminates all Packet Data Channels at the site, and disconnects the link to the RNG. The RNG senses the link disconnection and cancels any pending data for subscriber units at that site. Subscriber units also cancel any pending data. Service is restored once the site re-enters wide area trunking.	
Data is not delivered to the CEN or to the subscriber unit due to Site Controller switchover.	Site Controller switchover – If a Site Controller switches over to its redundant counterpart, data service is lost, and the system notifies the RNG, deassigns all Packet Data Channels at that site, and notifies the Zone Controller. Data service re-initializes after the Site Controller successfully switches. During the switch over, only data calls are terminated. Voice calls continue.	Check the status of the Site Controllers.
Data is not delivered to the CEN or to the subscriber unit and site is busy (ZoneWatch shows busy queue).	Data channels are being preempted at a site.	Zone Controller and subscribers may be configured to give priority to voice communication over data transactions and voice channels are in high demand at the site. Adjust these parameters if it is not desirable for data to be preempted.
Data is not delivered to the CEN or to the subscriber unit.	Channels at a site are not becoming available soon enough to permit a data transaction to commence.	Determine if site capacity for voice and data is sufficient.
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.	Packet Data Channel failure – If the Site Controller detects that a Packet Data Channel has failed, it informs the home Zone Controller. The Zone Controller de-assigns the Packet Data Channel. The Site Controller indicates this failure to the RNG and the RNG cancels any pending data for all subscriber units assigned to that Packet Data Channel. The subscriber unit has the capability of detecting when the Packet Data Channel fails and upon detection, cancels any pending data transaction.	Verify the operation of the Base Radio (Packet Data Channel). Check channel condition in ZoneWatch and events or alarms reported to Unified Event Manager (UEM).
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 in the UEM displays the reported status of the logical link between the PDR and the GGSN router.	Check the condition of the GGSN and any traps reported by PDR in UEM 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 establish context activation for a subscriber unit is lost.	Check the traps reported by PDR in UEM 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.	GGSN router, Border Router, or Peripheral Network Router failure – Prevents data messages originating in the CEN from reaching subscriber units and vice versa.	Check the condition of the GGSN router, Border Router, and Peripheral Network Router 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	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	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.

Table continued…

Symptoms	Possible Causes	Solution
non-redundant Border Router reset at a CEN.	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.	
Subscriber is generating errors to the data device	Subscriber reports the following as ICMP messages to the data device: • Message Lifetime Expiration • Not Context Activated – Subscriber is not registered with the system. • Site Trunking – Site has entered site trunking and data services are not available. • Service Interaction • Time Trap: Indicates system time received from the site equipment. • Sync Status Trap: Indicates if the subscriber unit has lost or regained time base synchronization with the system. The trap is originated if no communication has occurred with the site equipment for more than 2 minutes. • Packet Data Transmission Status Traps: Generated when the subscriber is not synchronized with the system for more than two minutes, or the message received from the mobile computer is larger than 500 bytes. • Site Change Trap: Sent when the subscriber roams from zone to zone and/or site to site. Indicates the latest zone ID and site ID once the subscriber has registered at the new site (caused by automatic site selection or user forced roaming events).	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.
Broadcast data messages fail to deliver	The system may not be able to deliver broadcast messages due to the following reasons:	Review the traps sent by the PDR to the UEM application located in the same zone as the PDR.

Table continued…

Symptoms	Possible Causes	Solution
	• 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.	Check UEM 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 The specific remedies vary 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 subsequent dynamic (individual radio user) context activations, 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 UEM 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.

For the Header Compression functionality, the PDR tracks the number of compressed header errors and sends the fault information to the Fault Manager.

6.2 Performance Management and Troubleshooting Tools

This section covers the tools that you can use to performance manage and troubleshooting data services on an IV&D system.

6.2.1 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 IV&D system components, network connectivity failures, CPU overload conditions, and so on.

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

6.2.2
InfoVista

InfoVista is a performance monitoring tool for the ASTRO® 25 IV&D systems that can be installed if required. This application 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

For more information on these reports, see the *InfoVista User Guide* manual.

6.2.3
Genesis Enhanced Data Performance Reporting

The Genesis Enhanced Data Performance Reporting application is a third-party product provided by the Genesis Group. The application generates reports for IV&D, HPD, and Enhanced Data. The purchase of this software is recommended.

The Genesis Enhanced Data Performance Reporting application resides in the Customer Enterprise Network (CEN) and monitors the ASTRO® 25 infrastructure through the Air Traffic Information Access (ATIA), GTP', and PMI interfaces.