System Release 7.17
ASTRO® 25
IINTEGRATED VOICE AND DATA

HPD Overlay System Infrastructure

NOVEMBER 2016

MN003298A01-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 Solution Support Center

The Solution 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 Parts organization. Your first response when troubleshooting your system is to call the Motorola 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
MN003298A01-A	Original release of the *HPD Overlay System Infrastructure* 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 HPD Overlay System Infrastructure

The High Performance Data (HPD) feature is designed for delivering mission-critical IP traffic between mobile data subscribers and customer host equipment.

This volume provides an introduction to the hardware and software components associated with the HPD Overlay System Infrastructure. Field service managers and field service technicians can use it after they have attended the Motorola Solutions formal training. Included are detailed procedures for installation, configuration, and maintenance.

What Is Covered in This Manual?

This booklet contains the following chapters:

- HPD Overlay Description on page 25 provides a high-level description of the HPD Overlay feature and the function it serves on your system.
- HPD Overlay Theory of Operations on page 29 explains how the feature works in the context of your system.
- HPD Overlay Installation on page 63 details the hardware and software installation procedures relating to HPD Overlay.
- HPD Overlay Configuration on page 69 details the system-level configuration procedures relating to HPD Overlay.
- HPD Overlay Optimization on page 79 contains the system-level optimization procedures and recommended settings relating to HPD Overlay.
- HPD Overlay Operation on page 81 details tasks that you perform once the HPD Overlay is installed and operational in an IV&D system.
- HPD Overlay Maintenance on page 91 describes periodic maintenance procedures relating to the HPD Overlay.
- HPD Overlay Troubleshooting on page 97 provides fault management and troubleshooting information relating to the HPD Overlay.
- HPD Overlay FRU/FRE Procedures on page 115 lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs, and includes replacement procedures applicable to the HPD Overlay.
- HPD Overlay Reference on page 117 contains supplemental reference information relating to the HPD Overlay.

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

Refer to the following documents for associated information about the radio system.

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 R56 manual. This may be purchased on CD **9880384V83** by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.

Chapter 1

HPD Overlay Description

This chapter provides a high-level description of the HPD overlay feature and the function it serves on your system.

1.1 HPD Overlay Overview

The High Performance Data (HPD) feature is designed for delivering mission-critical IP traffic between mobile data subscribers and customer host equipment. The HPD feature provides an efficient and reliable wireless transport medium for standard IP packet transfer, with raw data rates up to 96 kbps. This data rate allows service for medium bandwidth applications, including still image transfers, vehicle location services, and constrained web browsing services. The HPD system also supports delivery of traffic for user authentication, Dynamic Host Control Protocol (DHCP), and Domain Naming Server (DNS) services that can be implemented at the customer network.

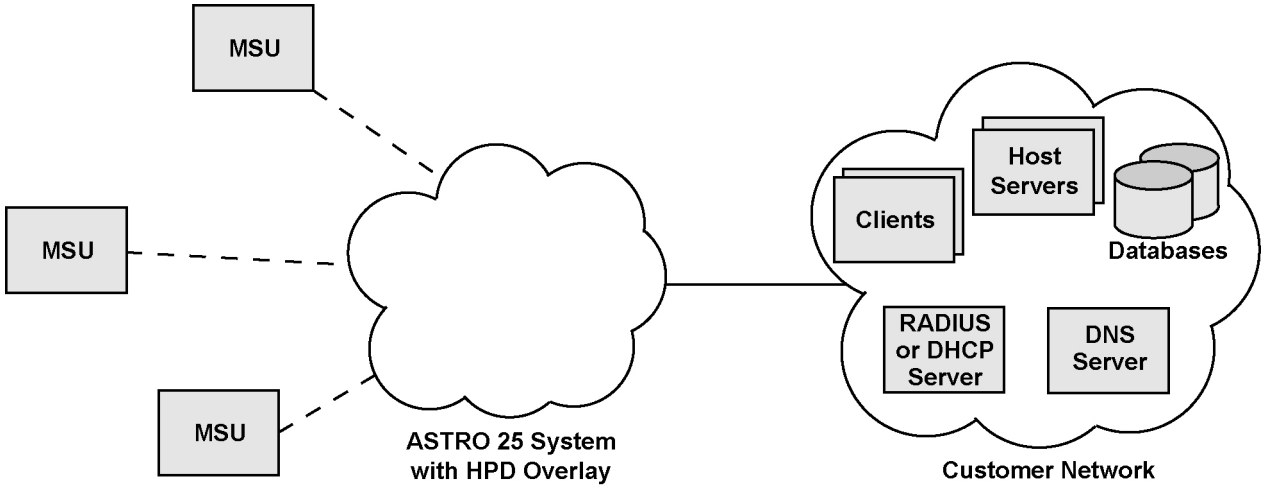
For a detailed description of HPD data services, refer to the *HPD - Packet Data Resource Management* manual.

The following figure shows a simplified diagram of the HPD feature in operation. The Mobile Subscriber Unit (MSU) consists of an HPD modem (which provides the RF interface) and a mobile data device (which is a computing device). MSUs register and context activate with the system to gain access to the resources at the customer network. The MSUs and customer network equipment can interact using standard IP-based applications and protocols, including web browsers, file-transfer software, messaging applications, and e-mail. Custom applications that utilize TCP/IP or UDP/IP can also be developed for the Mobile Data Devices (MDDs) and customer hosts.

After an MSU has been registered and context activated with the system, the MSU can interact with various hosts and clients on the customer network. It does so by sending and receiving IP traffic with the devices. Depending on the customer network configuration and the supported applications, the MSUs can access files or information from the host servers or databases. Likewise, clients on the customer network can interact with the MSUs for the text message service, Global Navigation Satellite System (GNSS) position tracking or other various applications.

The HPD system operator has the option to enable HPD modems to continue operating when a Mobile Data Terminal is not connected. When this feature is enabled, the HPD modem continues to send GNSS location coordinates through the HPD network to the central office (if it is requested to do so).

Figure 1: ASTRO 25 High Performance Data System



HPD_overview_simplified_overlay

1.2
System Capacity

The following system capacities are supported in an HPD system:

- seven zones
- 100 RF sites per zone
- five channels per HPD site
- 300 HPD channels per zone
- 64,000 provisioned users
- 20,000 active data users (trunking IV&D, conventional IV&D, and HPD users, total)
- ten points of presence for customer enterprise networks
- 1 million HPD messages/hour per system
- intermixed with unicast traffic, up to 300 broadcast messages per hour per zone

NOTICE: Channel capacity representing the number of users per channel must be based upon the applications used on the system.

1.3
Data Specifications

The following specifications apply to the data traffic supported by the HPD system:

- IP version 4 messaging
- Class A, B, and C addressing
- Unicast inbound/outbound HPD messaging
- 96/64/32 kbps raw data rates
- Motorola Solutions proprietary protocol transport mechanism for inbound GPS traffic
- 97% data message success rate

- Maximum delay of 20 seconds across coverage area
- Average delay of IP packets is 6 seconds
- 95% of successfully delivered packets are received within 20 seconds
- Confirmed delivery over an air interface
- Maximum air interface retries (configurable)
- Access control (registration, context activation, and user authentication supported)
- 1500 byte MTU maximum
- Inbound/outbound windowing over an air interface (configurable)
- Forward error correction over an air interface

1.4 Air Interface Specifications

The following general attributes apply to systems and subscribers using HPD services:

- 700/800 MHz public safety bands
- 25 kHz channel bandwidth
- 4x4.5 kHz subchannel signaling over four consecutive 6.25 kHz channel allocations
- 30 msec TDMA outbound channels
- 30 msec TDMA inbound reserved access channels
- 10 msec TDMA inbound random access channels
- Digital base station identifier broadcasting (configurable, broadcast every 15 minutes)
- Transmit power control
- Full-duplex BRs
- Full-duplex or Half-duplex MSUs
- 4/16/64-QAM RLA modulation
- Automatic site selection and mobility handovers
- 700 MHz interoperability capability for MSUs

1.5 Dynamic System Resilience Interactions

If the system with the Dynamic System Resilience features the HPD Overlay System Infrastructure, then the Backup Core also has an HPD Overlay. For information about the DSR interactions refer to the *Dynamic System Resilience* manual.

1.6 Trunking Subsystem Interactions

An HPD site may be overlaid at the Trunking Subsystem (Tsub) prime site. A Tsub may contain an HPD remote site. For Tsub configuration, see the *Edge Availability with Wireline Console for Trunking Subsystems* manual.

This page intentionally left blank.

Chapter 2

HPD Overlay Theory of Operations

This chapter explains how the feature works in the context of your system.

2.1 Access and Feature Controls

The ASTRO® 25 system with an HPD overlay includes access and feature controls to regulate system access and enforce the provisioned capabilities for legitimate subscribers. The system performs *unit registration* services when a subscriber powers up or roams into the network. Unit registration ensures that the subscriber is valid and that the appropriate services are available to the user (as defined by the Network Management configuration). MSUs must also *context activate* with the system to establish the connection for packet data services with hosts on the customer network.

If the customer network is implementing a RADIUS server, the system also supports transport of clear user authentication credentials.

2.2 Roaming and Mobility

The system supports automatic mobility between sites, allowing MSUs to roam throughout the system coverage area while maintaining the connection and services with the customer network. MSUs select the best site to use for service. MSUs continually monitor adjacent sites and automatically transition to the most advantageous site. The transition occurs according to some criteria (such as the state of the site and the signal strength of the home channel at that site).

MSUs can automatically switch between channels in both the 700 MHz and 800 MHz bands when roaming. An indication of the current site can be viewed through the Status Applet (which runs on the mobile data device). All mobility operation is transparent and does not require any user intervention.

When searching for adjacent sites, MSUs first scan through an internally stored adjacent site list (which is provided by adjacent site broadcast messages from the current site). If an available site is not found, the MSU then attempts to scan through its pre-programmed list of frequencies (provisioned through Customer Programming Software, CPS).

If a channel at the current HPD site fails, MSUs attempt to use another channel at the same site rather than roaming to another HPD site. However, if an HPD site enters local mode, the MSUs search for another HPD site that is in wide area mode so that the data services can continue.

Individual MSUs can be provisioned to access up to five ASTRO® HPD networks. The mobile computer operator can manually switch between the systems through the Status Applet extended display.

2.3 HPD Applications

The HPD feature supports the standard IP protocol for addressing and routing of traffic between the Mobile Subscriber Units (MSUs) and the hosts at a customer network. The mobile data devices run on the Microsoft Windows operating system: either Windows Vista with Service Pack 2 (SP2), Windows 2000 with SP2 and a PPPoE driver installed or Windows 7. If Windows power management features are desired (S3 Standby state) all operating systems require installation of additional Motorola Solutions provided software.

The HPD feature provides an IP bearer service that is suitable for tier 1 (9600 bps, low bandwidth) and tier 2 (96 kbps, medium bandwidth) applications. The applications on the mobile data devices can be

standard off-the-shelf applications or custom IP-based applications running on the Microsoft Windows operating system.

NOTICE: There is no longer on-going support for Microsoft Windows 2000. This strategy is consistent with the Microsoft lifecycle for the Windows 2000 operating system. Although Motorola Solutions makes no efforts to prevent Windows 2000 operation with HPD, an on-going support, or future development to support Windows 2000 based HPD systems can no longer be offered.

Examples of tier 1 (low bandwidth) applications:

- Text message service
- Database queries (vehicle records, identification queries, criminal database access)
- Dispatch and status messages

Examples of tier 2 (medium bandwidth) applications:

- Transmit/receive images (photographs, fingerprint identification)
- Transmit/receive files (incident reports, activity logs, citations)
- Automatic Vehicle Location
- Web server access (constrained)

Some common tier 1 and tier 2 application examples are explained in the following sections.

NOTICE:
The HPD feature does not work with the ISSI.1 Network Gateway or Public Safety LTE Push-to-Talk (PTT) Gateway features.

For additional configurations and any impact on HPD from the Dynamic System Resilience (DSR) feature, see the *Dynamic System Resilience* manual.

2.3.1
Database Inquiry

Database Inquiry is a common mobile data application allowing subscribers to obtain information from a real-time database. Applications commonly provide an inquiry form that allows the subscriber to enter the database search criterion and indicate the databases to be queried using the search criterion.

2.3.2
Database Update

Database Update provides the ability to submit new or revised information to a database. As with a database inquiry, the application would include a form to enter the field data to be submitted.

2.3.3
Dispatch and Status Reporting

In conjunction with a Computer Aided Dispatch (CAD) system, subscribers can be assigned tasks or jobs by using mobile data dispatching.

A dispatch message includes key information describing the assigned task or job:

- Where to go
- What to do
- Task or job priority relative to other work
- Notes and comments

Subscribers can indicate their progress on the task or job with pre-programmed status report messaging. Subscribers can use the following status reports:

- En route
- On site
- Work completed
- Available for next assignment

The **work completed** status may include subscriber data fields to indicate specifically what work was performed or the final disposition of the work. The work record can be further processed by other applications.

2.3.4
Broadcast Data

The HPD service enables unconfirmed delivery of small-sized broadcast data messages from a fixed host to a group or fleet of subscribers. (They all are part of a Broadcast Agency Group).This feature eliminates the need to generate a separate message for each individual recipient. Examples of broadcast types are text messages, text alerts, small images such as AMBER alert photos, and the GNSS coordinates of fleet members.

2.3.5
Location Reporting

Location Reporting applications provide the ability to track the location of subscribers. This information can be used to better assign appropriate resources to tasks or jobs, to enhance safety in the event of an emergency, and to manage field resources such as assisting with directions to a location. Location data is typically obtained using a GNSS receiver in the subscriber`s vehicle or in a portable device that automatically transmits location data periodically. It is also common to implement a mapping application in the customer network to display the subscriber's location graphically on a map.

IMPORTANT: Be careful implementing a location reporting application with a large fleet of mobile or portable subscribers. The location reporting is automatic and can generate a high amount of traffic loading on a wireless network.

2.3.6
Messaging

Messaging applications provide the ability to send a textual message to another subscriber or dispatcher and for the recipient to view the message. These applications may or may not provide the store and forward capability when a subscriber is temporarily unavailable to receive a message. It is common to present received messages in a list with the date and time received and the sender`s identity.

2.3.7
Electronic Mail

Like messaging applications, electronic mail applications (e-mail) provide the ability to send a textual message to another subscriber or dispatcher and for the recipient to view the message. However, e-mail always provides the store and forward capability so that subscribers can obtain messages sent to them when they are not connected to the network. Also, e-mail applications may be designed to allow e-mail messaging to and from customer network e-mail applications. E-mail applications on private wireless systems may or may not provide the ability to send attachments. Caution must be exercised when sending attachments, so that the available system capacity is not over utilized by subscribers sending e-mail attachments. Also, commercial e-mail solutions such as Microsoft Outlook/Exchange Server over private wireless systems may not perform due to their typical high-bandwidth utilization

characteristics. Performance of commercial e-mail applications may be less than the one experienced over a wired network.

2.3.8
Field Reporting

Like database update applications, field reporting allows a subscriber to complete reports electronically and submit the reports to a database for processing. Common public safety field reporting applications include the ability to support a supervisor review and approval of submitted reports.

2.3.9
Intranet Access

Intranet Access involves accessing customer network-based web servers for web-based applications or information. It also includes web browser access to applications servers that provide a web browser interface. Therefore, intranet access applications can be for numerous purposes. Examples include access to customer network online resources such as directories, records systems, databases, and bulletin boards.

2.3.10
File Transfer

General file-transfer applications are typically used to upload data collected from the field and may also be used to download updates to local client databases or applications. Secure File Transfer Protocol (SFTP) or Trivial File Transfer Protocol (TFTP) is commonly used as the transport layer protocol. Various file-transfer applications may include image downloads and document access.

2.3.11
HPD Broadcast Data

The HPD Broadcast Data feature builds on the existing HPD architecture by introducing broadcast data capability. It uses the best effort delivery, using over-the-air unconfirmed data over the UDP. The delivery of the broadcast data is a best effort. The HPD Broadcast Data feature is intended to distribute outbound only broadcast messages from a fixed host of relatively small data messages to an entire group or fleet of subscribers, each of which are part of a Broadcast Agency Group.

The smaller the message, the higher is the probability of a proper delivery. In the physical layer, the smaller number of microslots needed, the higher is the delivery probability; which is the intention of the term “small data messages” meant to convey here.

Various types of messages can be sent (text messages, text alerts, small images like AMBER alert photos, and the GNSS coordinates of all fleet members). Due to the lack of the confirmation and lack of the delivery guarantee, only small portions of the data should be delivered if no other means of delivery assurance is provided by the application.

Broadcast message initiated by a subscriber is not supported. Subscriber support of dynamic or static IP on the existing HPD architecture is unaffected by this feature. The HPD Broadcast Data feature is enabled or disabled at the system level on the UNC. Up to 20 Broadcast Data Agencies can be configured in the system by Provisioning Manager using reserved IP addresses. A standalone IV&D or HPD system supports up to 20 Broadcast Data Agencies. An IV&D and HPD overlay system supports up to 20 Broadcast Data Agencies combined.

In an overlay system, a given Broadcast Data Agency can only be used for IV&D Broadcast or for HPD Broadcast, but not both. Each HPD subscriber supports up to eight configured Broadcast Data Agencies. The configuration of the Broadcast Data Agencies and enabling or disabling of HPD Broadcast Data in a subscriber is done through CPS. Broadcast messages belonging to a particular Broadcast Data Agency are delivered to the zones and their sites that are part of the respective

Broadcast Data Agency. This delivery occurs regardless of whether there are Subscribers on the Sites or not. A site replicates the broadcast message for transmission over each HPD data channel upon receiving a broadcast data message. A site ensures that all subscribers have the opportunity to receive the message.

2.4 IP Bearer Service

The system provides the wireless interface and transport mechanism for the IP traffic between the MSUs and the customer network hosts. This IP bearer service enables end-to-end delivery of IP traffic, allowing mobile data devices to interface with fixed hosts using IP-based applications. End users can run commercial (off-the-shelf) applications and other customized applications that use standard IP interfacing. The mobile data devices and customer hosts interact through the IP bearer service transparently, as if they were both located on a wired IP network.

The HPD IP bearer service supports the unicast (point-to-point) IP datagram messaging using IP version 4. Multicast datagram messaging is not supported by the system. The service also supports layer 3 fragmentation and allows a Maximum Transmission Unit (MTU) size of 1500 bytes at the network edges. Class A, B, and C addressing may be used by the end-user applications. The system discards all other forms of addressing.

All IP traffic passes through a series of tunnels in the HPD network to isolate the user data from the system infrastructure. This tunneling also allows the reuse and transparency of the same IP addresses between the system and the customer networks.

MSUs must register with the system and context activate to establish the connection for datagram messaging over the HPD system. When an MSU is de-registered or context deactivated, the mobile data device cannot send end-to-end messaging over the system, and appropriate error notifications are returned to the mobile data device.

Data delivery is made on a best effort basis. If the delivery cannot be achieved for some reason (MSU is not registered, MSU out of range, and so on.) then the packet is discarded. The IP bearer service provides confirmed delivery of traffic over the air interface. So any packets lost over the air are retransmitted if the receiver does not send a confirmation.

Non-deliveries of data are reported back to the source through ICMP messages.

NOTICE: Certain types of failure conditions prevent the return of an ICMP response message, so ICMP responses are not guaranteed in all situations.

2.4.1 Confirmed Delivery Service (Air Interface)

The MSUs and HPD infrastructure confirm delivery for all Unicast traffic received over the air interface. This confirmation ensures that traffic is reliably received between the HPD base radio and MSU. If the system or an MSU sends traffic over the air interface, but does not receive a confirmation message (or if portions of the confirmation message are unrecoverable), then the sender retransmits the traffic. If the traffic has already been successfully received, the system automatically discards the duplicate effort.

For outbound traffic, the HPD modem sends confirmation for all control and user data messages. For inbound control traffic (such as registration and context activation traffic), the base radio sends the confirmation to the MSU. For inbound user data (IP traffic to the customer hosts), the Radio Network Gateway (RNG) provides the confirmation for the MSU. All inbound and outbound traffic (other than outbound broadcast messages) uses confirmed delivery.

The MSU codeplug, which is configured through CPS, defines the maximum number of retries that an MSU attempts during data transmission or initial connection with the system. The system is also configured with the maximum number of retries attempted during inbound/outbound HPD traffic. This configuration is applied in the Provisioning Manager application.

The confirmed delivery services include the buffered messaging, error reporting, data channel management, and automatic deletion of duplicate messages. Confirmed message delivery services promote channel efficiency, along with a high level of reliability for messages successfully transmitted across the HPD air interface. This capability enhances the net time for successful end-to-end data transfer.

The system provides confirmed delivery over the air interface only. Any other end-to-end acknowledgments that may be required between the mobile data devices and the customer network hosts have to be implemented through end-user applications on the mobile and host computers. Confirmed delivery does not apply to HPD broadcast data messages. Due to the small size of the messages and intensive nature of the broadcasts, delivery confirmations are not requested for these messages.

2.4.2
Buffered Messaging

The HPD Packet Data Router (PDR) and HPD modems queue traffic in an internal buffer. Since varying throughput and congestion levels may be experienced through the data path, this buffering allows the HPD PDR or HPD modem to regulate the data flow and prevent HPD traffic from being lost or bottle necked at the air interface.

The HPD modem can queue a total of ten datagrams at any one time. The HPD PDR can queue a total of 15,360 bytes of data at any one time. When the queue is full, any additional IP datagrams are discarded, and an ICMP message is sent back to the sender.

HPD datagram queues may be discarded under certain conditions. If the HPD PDR fails to successfully deliver an IP datagram, any remaining datagrams in the sending queue to or from the specific MSU are discarded. Also, when the HPD system removes a datagram from the queue to attempted delivery, it checks the age of the datagram. If the datagram is older than the SNDCP Queue Dwell Time, it is discarded and the queue is flushed. An ICMP `Destination Unreachable: Host Unreachable` message is returned to the source host for each discarded datagram. The SNDCP Queue Dwell Time is configured for the system through Provisioning Manager and can be configured for an HPD modem through Customer Programming Software (CPS).

2.4.3
ICMP Messages

The MSUs and fixed routing equipment may generate ICMP error messages when a packet cannot be successfully delivered to the destination. The ICMP messages indicate non-delivery events such as an unreachable network, unreachable host, fragmentation conflict, unknown network, or bad header condition. Typical causes for these messages can include component or link failure, routing problems, air interface confirmation not received, message lifetime expiration, MSU is not context activated, or the site is in local mode.

Any inbound ICMP messages from MSUs are forwarded through the system to the appropriate customer network as they are received. Outbound ICMP messages are filtered by the system according to the MSU settings in Provisioning Manager. If ICMP messages are disabled for the MSU, then the system discards any outbound ICMP messages intended for the MSU.

2.4.4
Support for IP Route Discovery Commands

To conceal the routing fabric of the infrastructure, the system infrastructure does not insert any internal routing information for IP route discovery queries (such as trace route commands or other network discovery requests). Instead, the system simply conveys the requests to the other end. Inbound discovery requests are conveyed to the border gateway of the appropriate customer network.

Outbound discovery requests are conveyed to the appropriate MSU. The path through the system is transparent to the end users.

2.4.5
Support for Logging Applications

Traffic between MSUs and customer hosts can be logged within the customer network by a logging application or server (no special interfaces are required). The logging server can become an access point for other clients on the network to generate reports that are specific for meeting the organization's needs. Since any MSU-to-MSU would require routing through a custom routing application on the customer network, that traffic could also be captured by a logging solution on the customer network.

The system also allows air traffic interface access (ATIA) messages to be forwarded to a logging host on the customer network. The ATIA messages indicate events such as registrations, location registrations (roaming), and de-registrations for MSUs on the system. Other data traffic between MSUs and the customer network do not generate any ATIA messages.

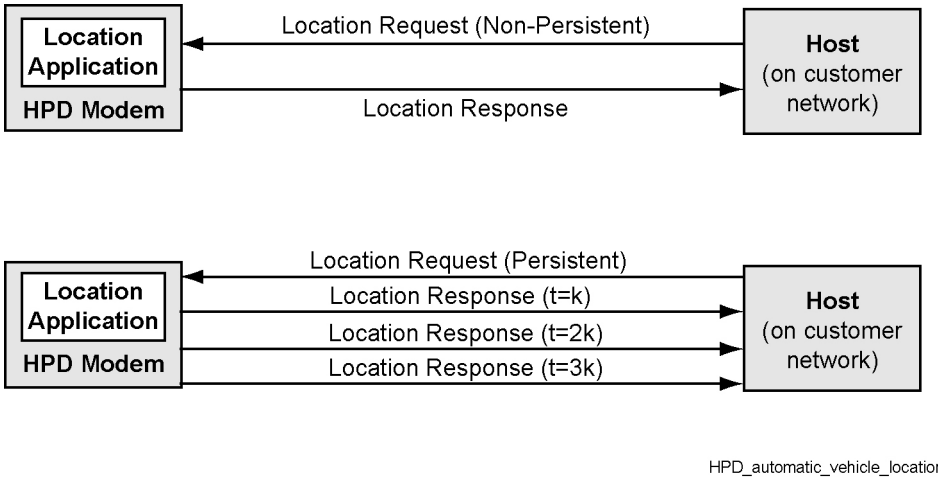
2.4.6
Multicast and Broadcast Messaging

The HPD system implements un-acknowledgement of broadcast packets over the radio channel with a fixed number of repeated transmissions for each broadcast data to increase the probability of their reception. The unconfirmed delivery of the broadcast data is considered non-mission critical. It is intended to distribute outbound only broadcast messages from a fixed host of relatively small data messages to an entire group or fleet of subscribers, each of which are part of a Broadcast Agency Group. This is because broadcast data is an unconfirmed service and the over-the-air delivery medium, making smaller broadcast data messages have higher probability of being received successfully than larger broadcast data messages.

2.5
Automatic Vehicle Location Service

HPD modems may include an optional GNSS application that supports Automatic Vehicle Location (AVL) services. Hosts on the customer network can request an MSU to send a one-time location response, or can request that the MSU send periodic location updates (which continue until canceled by the host). This allows a customer application to query the current location of an MSU (on a one-time polling basis), or continuously monitor the MSU location as it moves through the coverage area. Requests for continuous location updates are retained in non-volatile memory of the HPD modem so they are not lost when the HPD modem powers down. The following diagram illustrates how the one-time (non-persistent) and continuous (persistent) location requests are handled by the location application in the HPD modem.

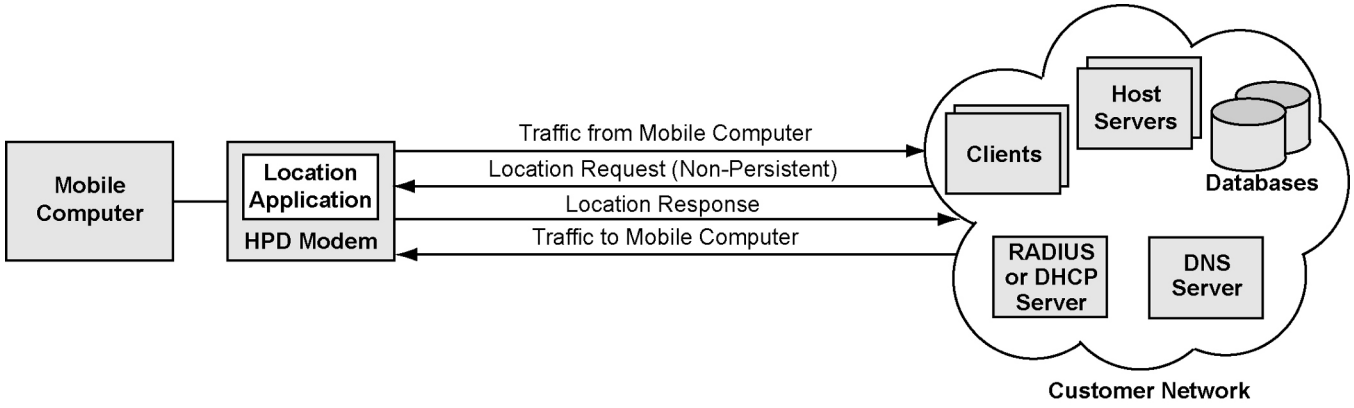
Figure 2: Persistent and Non-Persistent Location Requests



HPD_automatic_vehicle_location

Hosts on the customer network can simultaneously be connected with both the MSU's internal location application and the mobile data device that is connected to the HPD modem. Therefore, hosts can receive GNSS updates while other interactions are taking place with the mobile data device that is connected with the HPD modem. If only vehicle location services are required, the vehicle can be equipped with just an HPD modem. A mobile data device is not required for vehicle location services.

Figure 3: Simultaneous Location and Packet Data Activity



HPD_automatic_vehicle_location_simultaneous

The MSU internal location application can be configured to automatically context activate by itself after a power up, even if there is no active connection between the mobile data device and the MSU. The internal location application context-activates and begins sending updates for any pending location requests.

Parameters for the GNSS tracking feature are loaded into the HPD modem through Customer Programming Software (CPS). The CPS parameters define how the location application connects with the customer network and defines the maximum number of persistent location requests that can be serviced and retained in memory. If a customer network requires user authentication, then valid authentication credentials must be configured in the MSU for the location application to be used during context activation.

The HPD modem acquires its position using at least three (for 2D positioning) or four (for 3D positioning) satellites of the NAVSTAR satellite navigation system. Initially, the GNSS receiver takes up to 50 seconds (in an open sky condition) to lock onto the satellites and acquire its first position. Battery-backup of the GNSS receiver maintains satellite tracking when the MSU is powered down.

Position requests and responses are delivered using the Motorola Solutions proprietary Location Request Response Protocol (LRRP) over UDP/IP. Customer host applications can be developed using this protocol for automatic vehicle location tracking. Contact Motorola Solutions for more information about LRRP.

2.6 Data Rates

The HPD base radios and MSUs use adaptive modulation techniques to provide the greatest throughput and best performance for the HPD Unicast traffic over the air. The adaptive modulation methods contribute to more reliable data transactions over large coverage areas, providing data coverage that is comparable to standard ASTRO® 25 voice coverage capabilities.

If data errors are occurring and packets are being retransmitted, then the MSU or base radio automatically selects a more robust modulation method to ensure that the Unicast traffic is successfully received at the other end. The three supported modulation methods are listed along with the raw data rates for each method in the following paragraphs. The raw data rate decreases for more robust modulation methods since fewer bits per symbol are being communicated over the air. All adaptive modulation is performed dynamically as necessary by the MSU or base radio without any intervention from the user.

Table 1: Raw Data Rates

Raw Data Rate	Modulation	Description
96 kbps	64-QAM	Used for the first data transmission attempt.
64 kbps	16-QAM	Used for the second data transmission attempt (first retry).
32 kbps	4-QAM (QPSK)	Used for subsequent retries. Also used for control traffic, Broadcast Data and for requesting slot reservations.

When an MSU or base radio starts sending user data traffic, it first attempts to send the data at the 96 kbps data rate using 64-QAM modulation. If a retry is required, the MSU scales back to 16-QAM modulation, which yields a 64 kbps data rate. If additional retries are attempted, the MSU reverts to the more reliable QPSK modulation, which yields a 32 kbps data rate. In general cases, MSUs that are operating closer to the HPD remote site or in good coverage areas would potentially have most traffic delivered at 96 kbps, while MSUs that are in fringe coverage areas may experience a slower data rate.

All control signaling is sent using QPSK for reliability. When an MSU is requesting an inbound reservation slot (which is used to send inbound traffic), or if other control traffic is being transmitted by the MSU or by a base radio, then QPSK modulation is used.

All inbound/outbound HPD traffic uses enhanced forward error correction to promote better packet reconstruction and allow more packets to be accepted over the air interface. Additional error detection mechanisms are also used to ensure that no errors are in the traffic. If errors in user data traffic cannot be corrected, the system can request individual portions of a message to be retried (rather than having the entire message retried). This selective retry method helps reduce the number of large retransmissions and enhance overall channel efficiency when errors are only occurring in small portions of the received traffic.

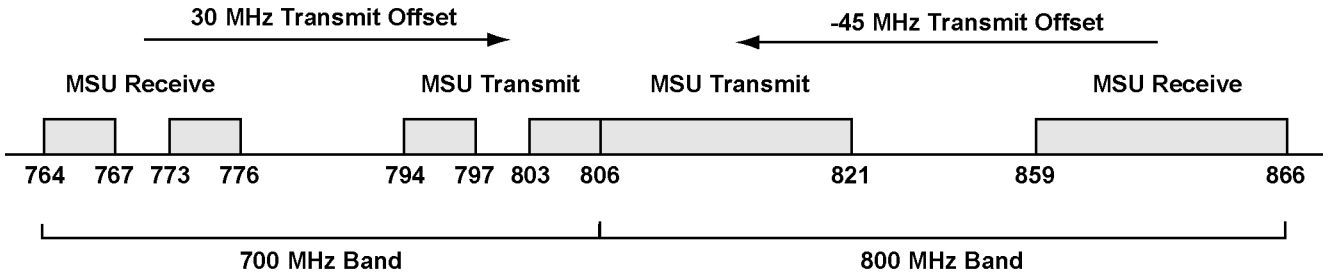
2.7 Frequency Bands

The HPD feature provides high speed narrowband data over standard 25 kHz channel allocations in the 700 MHz and 800 MHz private system frequency bands. The HPD signal performance provides quality wireless data service with a coverage footprint that is comparable with an 800 MHz voice coverage area. The 25 kHz HPD feature is a proprietary Motorola Solutions feature which closely

follows many of the wideband air interface standards defined by TIA, in a high speed narrowband medium.

The system and MSUs operate in public safety allocations in the 700 MHz and 800 MHz frequency band allocations illustrated in the following figure. NPSPAC frequencies (821 MHz - 824 MHz and 866 MHz - 869 MHz) may also be assigned by a waiver.

Figure 4: Frequency Bands



HPD_frequency_bands

Each HPD transmit and receive channel requires four contiguous 6.25 kHz allocations, providing a total of 25 kHz bandwidth for each channel (see the following table). 700 MHz interoperability channels require two contiguous 6.25 kHz allocations to provide a 12.5 kHz channel for 9600 bps interoperability.

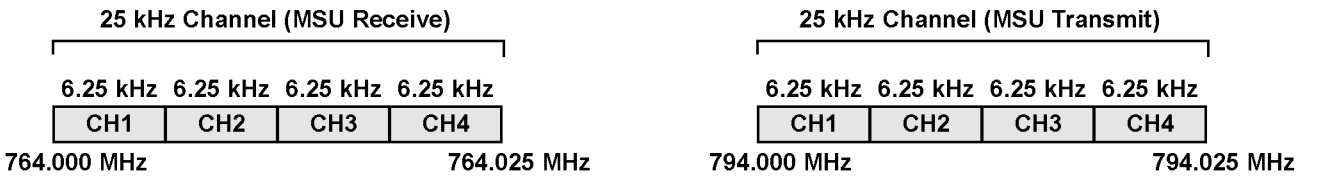
Table 2: HPD Channel Specifications

Band	MSU Receive	MSU Transmit	Tx - Rx Offset	Required Allocations
700 MHz	764-767	794-797	30 MHz	Four 6.25 kHz (25 kHz) for HPD
	773-776	803-806		Two 6.25 kHz (12.5 kHz) for interoperability
800 MHz	859-866	806-821	-45 MHz	Four 6.25 kHz (25 kHz) for HPD

MSUs operating in the 700 MHz band have a 30 MHz offset between the receive and transmit frequencies (see the following figure). MSUs operating in the 800 MHz band have a -45 MHz offset (with the transmit frequency being at the lower end of the 800 MHz spectrum).

For example, if an HPD site is using 764.000 MHz as the base frequency for the MSU receives (base radio transmit) channel, then four 6.25 kHz contiguous channels would have to be allocated to create a 25 kHz channel that spans from 764.000 MHz to 764.025 MHz. With the 30 MHz offset, the MSU transmit (base radio receive) channel would be a 25 kHz channel spanning from 794.000 MHz to 794.025 MHz.

Figure 5: HPD Channel – 700 MHz Example



HPD_aggregate_channels

The system complies with the emissions, spectral efficiency, frequency stability, and transmits power limitation requirements defined by the FCC for the supported frequency bands.

2.8 Interoperability

The HPD modem hardware is capable of APCO Project 25 data interoperability at 9600 bps to conform with the current 700 MHz narrowband interoperability requirements defined by the FCC. A total of 32 separate national interoperability data channels are available in the 700 MHz band for situations that require interagency cooperation. The interoperability channels designated by the FCC have 12.5 kHz channel spacing and operate at 9600 bps data rate. No interoperability rules currently exist for the 800 MHz band.

A mobile data user can select interoperability mode from the Status Applet that runs on the mobile data device. The mobile data device can only operate in one mode at a time. Switching between HPD and interoperability mode causes the connection for the current mode to be terminated before the connection for the new mode is established.

Since the Status Applet and HPD modem perform all the necessary operations to transition into the different modes, no other user intervention or custom applications are required. However, if the customer decides to develop any custom applications that can change the mode, the API provides the necessary hooks for switching between modes.

Interoperability mode only supports a 9600 bps data rate, so any medium bandwidth (tier 2) applications used in HPD mode may not experience the same performance when in interoperability mode. Instead, the 9600 bps interoperability mode is more suitable for lower bandwidth (tier 1) applications, such as the text message service and simple data queries. Any MSU operating in interoperability mode must be within the range of another MSU in interoperability mode for successful data communication.

2.9 Transmit Power Control

The transmit power control function permits the MSU to adjust its RF transmit power so the required quality of transmission is achieved with the least amount of radiated power. In this release, MSUs use an open loop power control calculation to adjust the transmit power.

Each HPD base radio is provisioned with an Open Loop Access Parameter (OLAP) and a Maximum MSU Transmit Power (MMTP) parameter through CSS. The HPD BR periodically sends these parameters to the MSUs at the site.

For the transmit power calculation, the MSU measures the received signal strength for a number of outbound time slots. The MSU then uses the OLAP value and the received signal strength to derive the transmit power. If the calculated transmit power exceeds the Maximum MSU Transmit Power, then the MMTP are used to limit the transmit power.

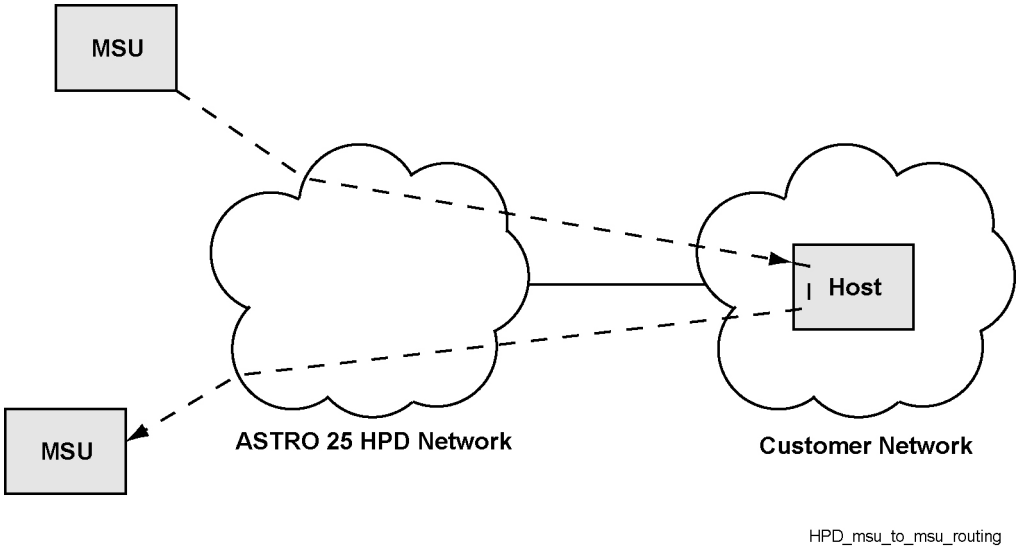
2.10 MSU-to-MSU Communication in HPD Mode

While the HPD modem hardware is capable of 9600 bps interoperability, the system does not support direct MSU-to-MSU communication or repeated data communication in HPD mode. When in HPD mode, MSUs only communicate with hosts on the customer networks (through the HPD system).

If MSU-to-MSU traffic in HPD mode is required for messaging or other purposes, then the customer must implement a custom application or routing function at the customer network. With this type of setup, a transmitting MSU would be able to send HPD traffic to the host on the customer network. The custom application or routing function at the customer network would then route the HPD traffic to the destination MSU. The custom routing application could define permissions, restrictions, and routing characteristics for any MSU-to-MSU data. The following figure illustrates how MSU-to-MSU traffic could be routed through a custom application on the customer enterprise network.

NOTICE: While MSU-to-MSU traffic can be supported in the routing table in the border gateway or other routers within the customer enterprise network, the user or client application would have to be aware of the other MSU address to use the routing fabric for this transfer.

Figure 6: MSU-to-MSU Communication in HPD Mode



2.11 User Authentication

The HPD system supports the exchange of user credentials (typically username and password) from the mobile data device to the destination CEN for user authentication. The credentials are validated within the CEN using a RADIUS server. The HPD system allows or denies access to the destination CEN based on the validity of the credentials.

In the GGSN configuration, user authentication may be either enabled or disabled individually for each CEN access point. If the authentication is configured for a CEN, all MSUs that are assigned to that CEN must have authentication enabled and must provide the appropriate credentials during the context activation process.

CAUTION:
If using CHAP authentication, disable the ability to store the password on the Radius server. If the server is configured to store the password, the subscriber is unable to context activate.

There is no authentication of the HPD Broadcast Agencies. For HPD customers that support Subscriber authentication, a separate border gateway is needed between the GGSN and CEN to route the non-authenticated Broadcast Data Agencies outbound Broadcast traffics. The existing pre-HPD Broadcast data border gateway continues to route the authenticated Subscribers inbound/outbound Unicast traffics. A Subscriber that requires authentication must not be provisioned with the APN that traverses the border gateway for the Broadcast traffics. For HPD customers that do not support Subscriber authentication, the same border gateway between the GGSN and CEN can be used to route the Subscribers inbound/outbound Unicast traffics and the Broadcast Data Agencies outbound Broadcast traffics.

User authentication settings must be configured in both the HPD modem and in the mobile data device. The HPD modem authentication settings are used for the internal application. These settings may be used to allow the optional location services application to automatically authenticate with the CEN without any required interaction from the mobile data device. HPD modem user authentication settings are configured using the Customer Programming Software (CPS) application. The authentication selections include PAP, CHAP, or no user authentication.

2.12
Dynamic and Static IP Addressing

The HPD feature supports both static and dynamic IP addressing for MSUs. For static addressing, the MSUs are configured with a fixed IP address. For dynamic addressing, the MSUs are assigned IP addresses dynamically from the HPD system or from the CEN during registration.

IP address settings are defined for each MSU through Provisioning Manager. Provisioning Manager includes a Radio Record for the MSU which must be configured with either static or dynamic addressing.

If the static addressing is used, then the static IP address for the MSU must be configured in Provisioning Manager. The assigned IP address for the MSU must be compatible with the IP plan for the associated CEN. If the dynamic addressing is being used, then the MSU may be assigned an IP address from either the system infrastructure or from the CEN.

If the Provisioning Manager setting for the MSU are configured for dynamic addressing, then the HPD system requests a dynamic address for the MSU from the GGSN. Depending on the configuration of the customer enterprise network, the GGSN contacts the DHCP server or RADIUS server on the CEN. It then supplies an address from a pool of predetermined addresses. The GGSN itself may also be configured to provide dynamic addresses to MSUs.

If an MSU attempts to context activate with static IP addressing and an invalid IP address, then the MSU is rejected. If the MSU attempts to use a duplicate IP address that is in conflict with another device, then the MSU is also rejected or context deactivated.

NOTICE: DHCP must be used if the system has the Dynamic System Resilience (DSR) capability. For information about the DSR refer to the *Dynamic System Resilience* manual.

2.13
Domain Name Service Updates

The HPD feature supports Dynamic Domain Name Service updates with a Name Authority DNS server on the customer enterprise network. This allows dynamic mapping of name strings, known as Fully Qualified Domain Names (FQDNs), to IP addresses that have been assigned or approved for an MSU. The DNS update also includes the reverse mapping of the IP address to the FQDN. These DNS services allow easily recognizable hostnames to be dynamically assigned to MSUs.

The GGSN can be configured to provide these updates to the DNS servers within each of the customer enterprise networks. When a context is successfully completed, the GGSN, (if so configured), pushes the DNS records to the DNS server at the appropriate CEN.

2.14
Security

The system provides a number of security features to protect against unauthorized access into the system. Only properly configured subscribers can register with the system. The customer network may additionally support user authentication, requiring subscribers to supply a valid user name and some form of valid passcode (such as a password or pin number).

The system may include an optional, yet highly recommended network interface barrier to provide isolation and security between the system and any external networks. The network interface barrier consists of a stateful firewall and an intrusion detection sensor. All traffic passing in or out of the system is scrutinized and filtered through the firewall. The firewall policy is defined to only accept services that are required by the customer networks and supported by the system infrastructure. The addition of the firewall does not change the operation of any supported services. An intrusion detection sensor monitors network activity at the network interface barrier and alerts the security management application of any intrusion patterns or signatures.

A core management security server can be installed to manage the network interface barrier, distribute antivirus updates to the system, and authenticate Network Management users that are remotely accessing the system.

Devices within the system have been provisioned with supplemental configuration to disable unnecessary services and to provide enhanced protection against unauthorized access or attacks.

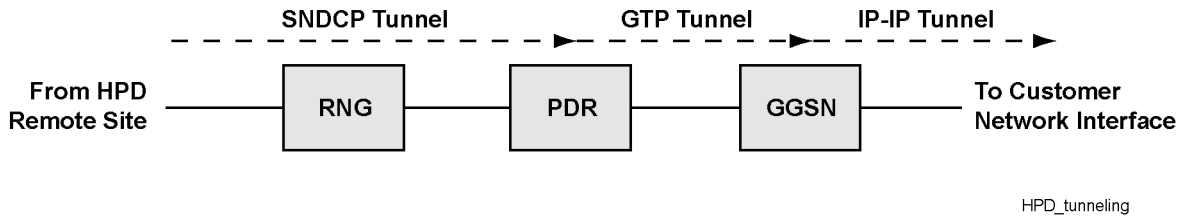
2.15 Encryption

The system does not currently provide encryption for HPD traffic between the customer network and the MSUs. If sensitive data packets must be encrypted, the encryption must be performed by applications or mechanisms outside the system.

2.16 Traffic Tunneling

HPD traffic is tunneled through the system to maintain system transparency and to keep the HPD traffic isolated from the routing fabric of the system (see the following figure). This tunneling is established for each MSU during context activation. Inbound traffic is delivered through a tunnel to the Packet Data Router (PDR) in the home zone of the MSU. Thereafter, the traffic is delivered through another tunnel to the GPRS Gateway Support Node (GGSN). The GGSN then sends the HPD traffic through an IP-IP tunnel to the appropriate customer network. This procedure provides isolation, separation, and security between the system and the HPD data.

Figure 7: Traffic Tunneling

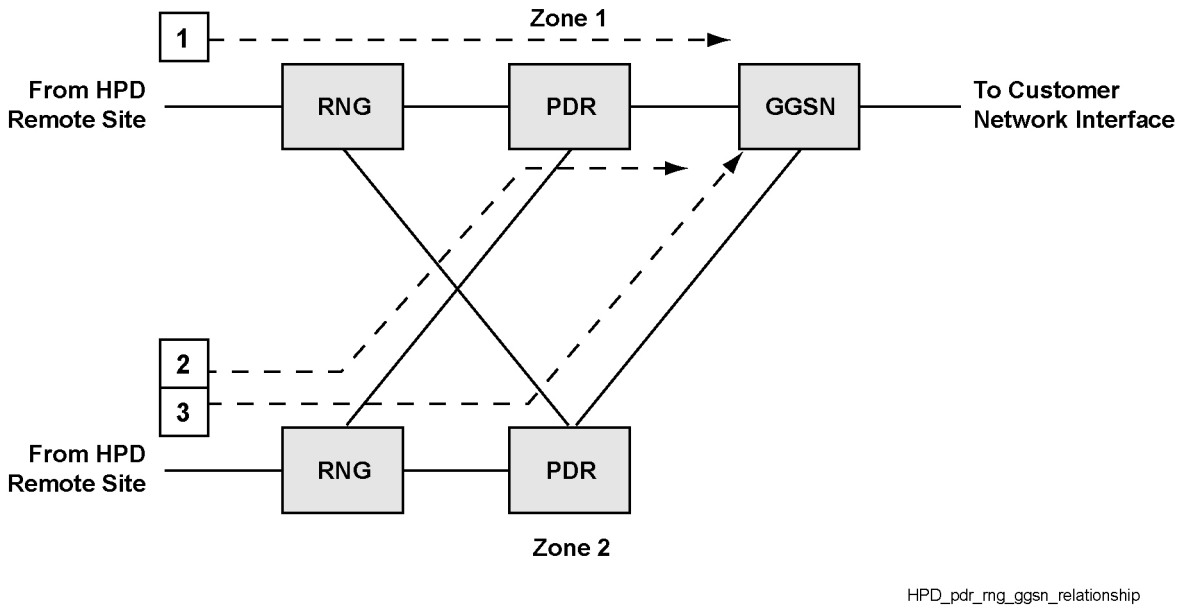


2.17 HPD Data Paths

HPD user data can potentially follow one of three general routes through the system. The route of the traffic depends on the location of the MSU, the home zone of the MSU, and the location of the GGSN. The following figure shows an example of three possible routing scenarios.

The first scenario shows an MSU transmitting traffic in its home zone, with the GGSN installed in the same zone. In this scenario, the MSU sends the HPD traffic over its assigned channel and timeslot. The HPD base radio forwards the traffic through the HPD site controller to the HPD RNG in the zone. The RNG sends the traffic to the home zone HPD PDR for the MSU, which is in the same zone. The PDR terminates the SNDCP tunnel and sends the traffic through a GTP tunnel to the GGSN, which also is in the same zone in this particular example. No interzone transactions have to occur in this scenario.

Figure 8: HPD Data Paths



The second scenario shows an MSU that has home zone mappings to zone 1, but is currently operating in zone 2. The traffic is delivered to the RNG in zone 2, which then forwards the traffic to the PDR in the MSU's home zone (zone 1). The PDR then sends the traffic to the GGSN, which is in the same zone.

The third scenario shows an MSU that is operating in its home zone (zone 2), with a GGSN located in another zone (zone 1). The traffic is routed through the RNG and PDR in zone 2, then sent to GGSN in zone 1.

In addition to the paths shown in preceding figure, there could potentially be more interzone transactions on the external DMZ before the traffic ultimately arrives at the customer network.

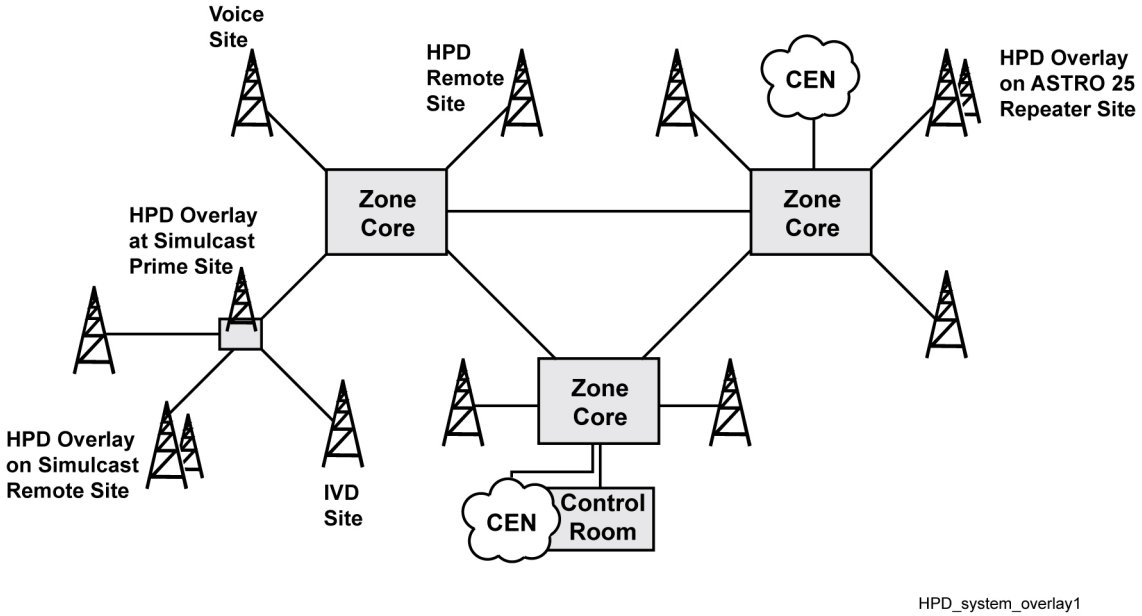
2.18 ASTRO 25 System with HPD Overlay

An ASTRO® 25 system with HPD overlay includes one or more zones, with a maximum of seven zones per system. Each zone includes a zone core which contains all the core infrastructure for controlling system access, processing traffic, and managing operations. In a multi-zone system, the zone cores are connected together to allow traffic to flow between the different zone cores as needed. Each zone may include a combination of up to 100 RF remote sites. This total may consist of various voice, 9600 bps data, and HPD capable sites. The valid HPD capable site configurations available in this release include the following:

- HPD remote sites
- HPD overlay on the simulcast prime site
- HPD overlay on the simulcast remote site
- HPD overlay on ASTRO® 25 repeater site

These sites provide the RF coverage to subscribers in the zone (see the following figure). The different overlay site varieties allow HPD channels to be colocated at an IV&D site. Each remote site is connected to the zone core within the zone. MSUs can roam between different HPD capable sites and zones with continued HPD service. HPD overlay can only be added to an RF site. It cannot be added to control room sites or other types of remote sites.

Figure 9: ASTRO 25 System with HPD Overlay



2.19

Zone Core

Each zone includes a zone core which contains all the core infrastructure for controlling system access, routing HPD traffic, managing system resources, and providing network security in the zone. The zone core also interacts with other zones as necessary to route traffic to appropriate devices. A zone core can include a customer network interface. This interface connects the system with the external customer networks. The zone core connects with all of the various remote sites in the zone through WAN connections. Zone cores connect with one another through WAN/Cooperative WAN Routing (CWR) links.

For the HPD overlay feature, an HPD Packet Data Gateway (PDG) is added to the zone core. This device is responsible for routing inbound/outbound traffic between the GGSN and the MSUs. The GGSN at the zone core interacts with the Customer Enterprise Networks (CENs).

Depending on your organization's needs, the following zone core configurations are available. All configurations employ the Common Server Architecture (CSA). See the *Master Site – Infrastructure* manual for details.

- Single zone non-redundant
- Single zone redundant
- Multi-zone capable

Figure 10: Zone Core with HPD Overlay – Single Zone Non-Redundant Configuration

The HPD PDG is included in the virtual machines labeled as **Various VMs**.

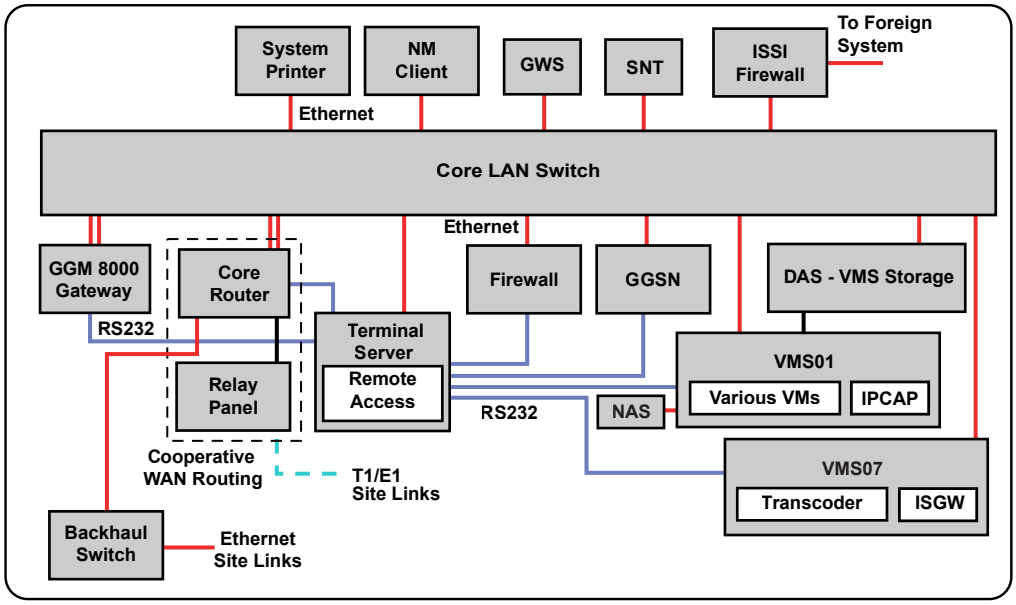


Figure 11: Zone Core with HPD Overlay – Single Zone Redundant Configuration

The HPD PDGs are included in the virtual machines labeled as **Various VMs**.

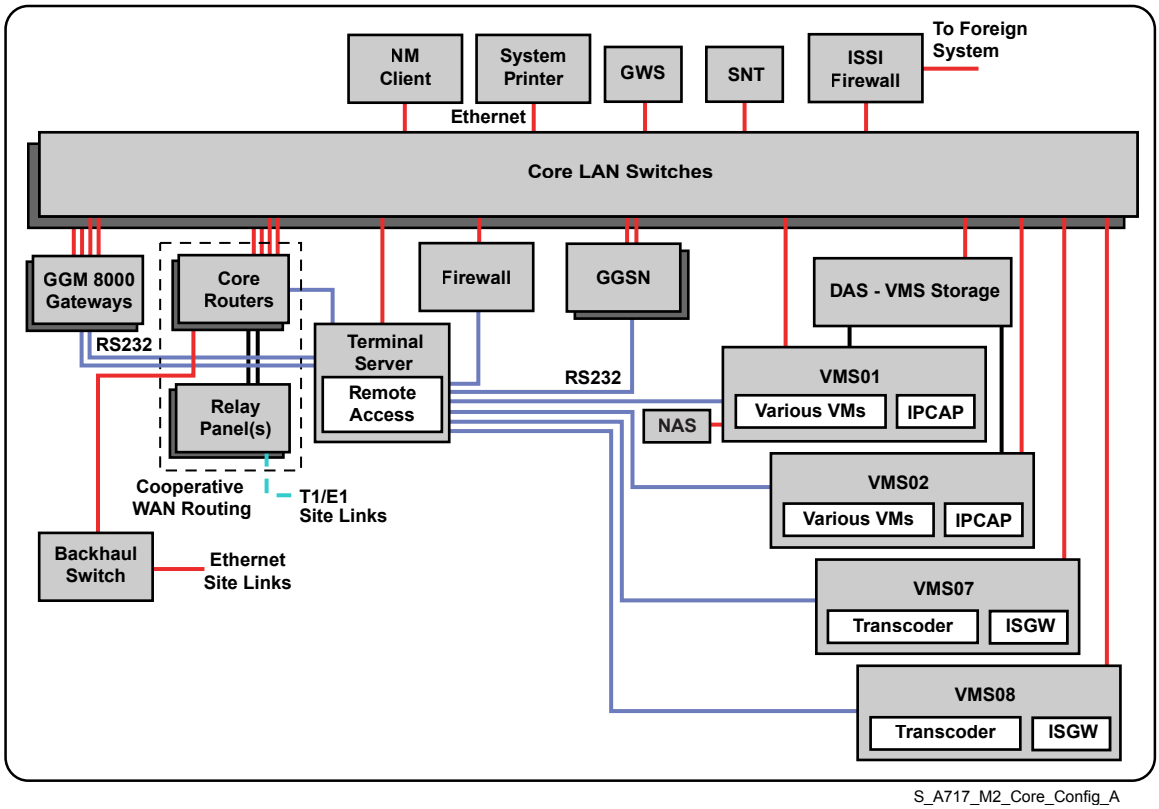
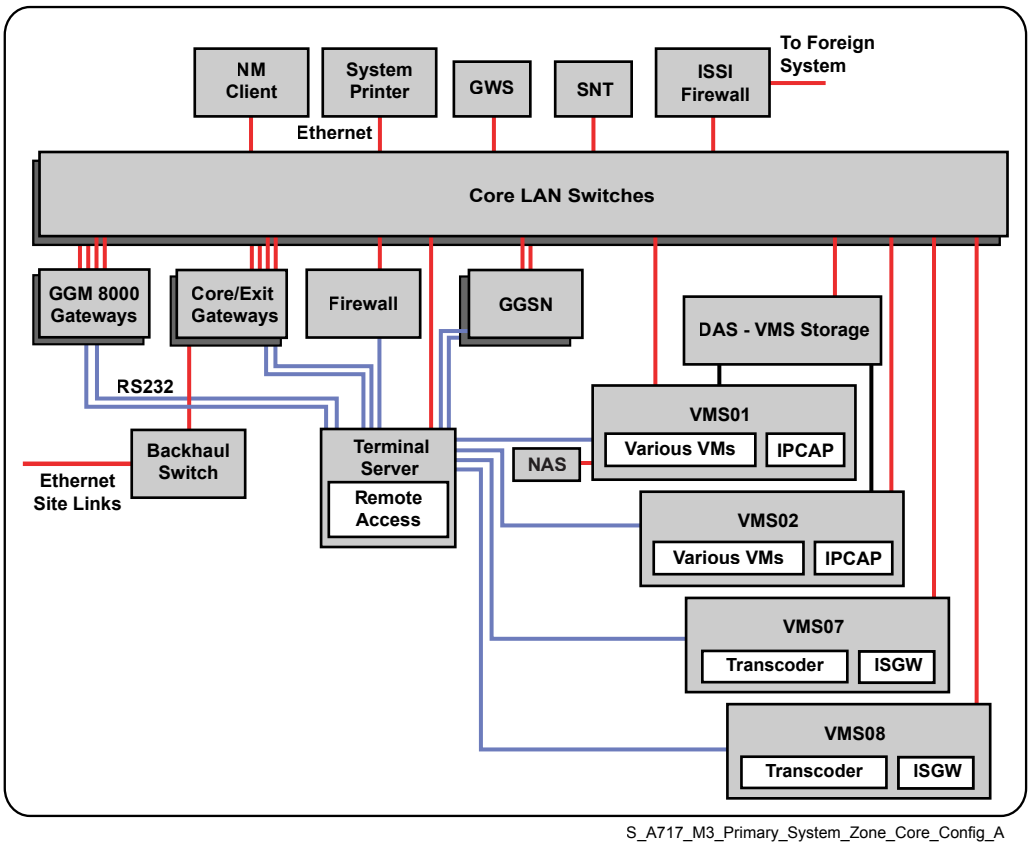


Figure 12: Zone Core with HPD Overlay – Multi-Zone Capable Configuration

The HPD PDGs are included in the virtual machines labeled as **Various VMs**.



NOTICE:
If you do not intend to install an HPD PDG at all zones in a multi-zone system, a filter needs to be created in UEM to filter out alarms sent by an HPD PDG when it cannot contact HPD PDGs in other zones. Please contact Motorola Solutions support for filtering UEM events.

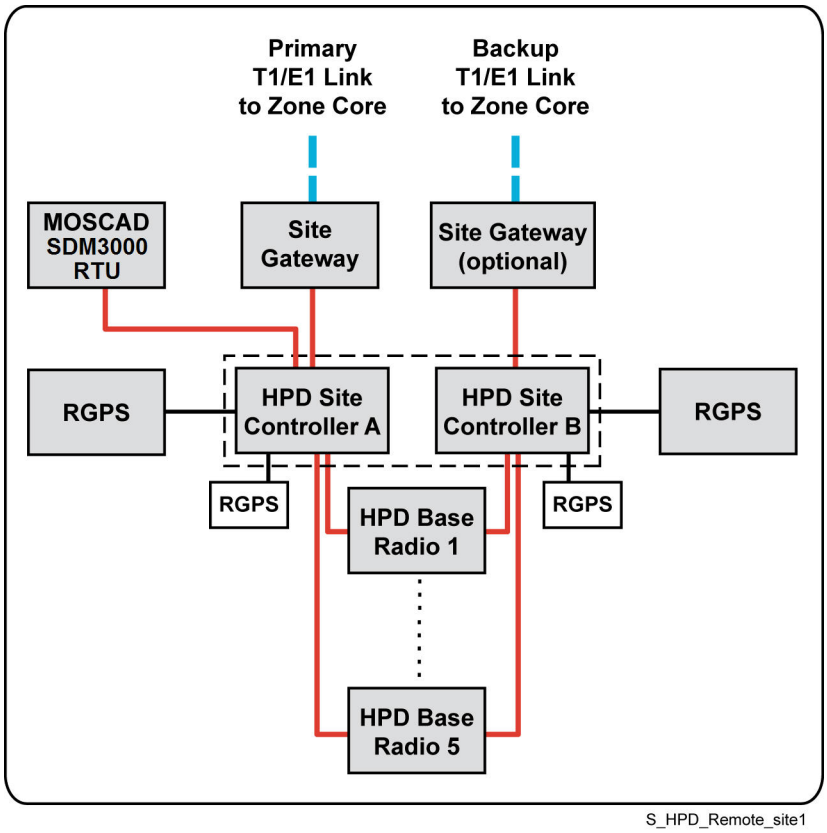
L2, M2 and M3 zone cores can be configured with the VMware vCenter application and redundant PDGs, GGSN routers, and CNI path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers) to support the High Availability for IV&D and HPD (HA Data) feature. See High Availability for HPD Installation on page 67 for more information.

For additional configurations, see the *Dynamic System Resilience* manual.

2.20 HPD Remote Site

HPD remote sites provide the RF interface for mobile data subscribers. Up to 100 HPD remote sites can be installed per zone to provide RF coverage throughout the region.

Figure 13: HPD Remote Site



Each remote site is connected to the zone core through a T1 or fractional T1/FT1 Wide Area Network (WAN) or Cooperative WAN Routing (CWR) connection. An optional redundant link configuration is also available, whicn allows two T1/FT1 WAN or CWR connections to the zone core. These connections link system control, Network Management, and HPD traffic between the remote site and the zone core.

A remote site can also be colocated with the zone core equipment.

For Ethernet interface alternatives, see the *Flexible Site and InterZone Links* manual.

Each HPD remote site includes a site controller with redundant modules, which locally manages the channels and mobile subscriber units that are active at the site. Up to five HPD base radios can be installed at each HPD remote site to provide the physical RF channels for HPD traffic.

The HPD remote site includes the following components:

- Site Gateway
- Site Controller with redundant modules
- Up to five Base Radios
- MOSCAD Network Fault Management (NFM) (optional)

Several site controller and base radio hardware configurations are available for the HPD remote site. The actual configuration selected depends on the number of channels supported or the type of RF distribution used at the site. The following platforms can be used:

GCP 8000 Site Controller
A standalone component, includes redundant modules.

GTR 8000 Base Radio
A standalone component.

GTR 8000 Site Subsystem
Includes redundant site controller modules, one base radio, and the RF distribution system (RFDS) in a single rack.

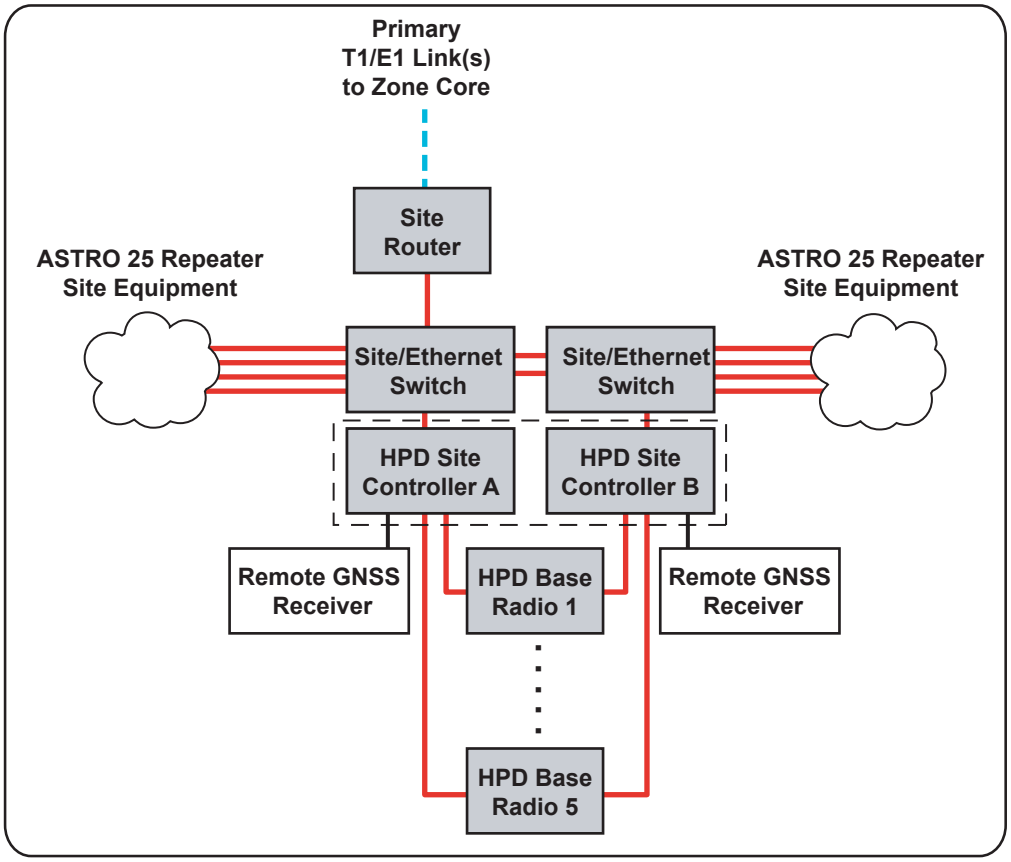
GTR 8000 Expandable Site Subsystem
A modular chassis that houses the redundant controllers, up to five base radios, and the RFDS equipment in a single rack.

2.21
ASTRO 25 Repeater Site with HPD Overlay

The ASTRO® 25 repeater site with HPD overlay allows an HPD site to be colocated with an ASTRO® 25 repeater site. Up to five HPD channels can be supported at each site.

Figure 14: ASTRO 25 Repeater Site with HPD Overlay

The HPD site controller connects to either an external site LAN switch installed or an internal Ethernet LAN switch embedded in IV&D site controller at the repeater site.



The HPD equipment installed at the site consists of the HPD site controller and up to five HPD base radios. The HPD site controller (with redundant modules) connects with the ASTRO® 25 repeater site LAN, and shares bandwidth with the other IV&D equipment on the T1/E1 site link to the zone core. The HPD site controller and HPD base radios operate independently from the other IV&D equipment at the site.

An HPD Overlay site can include the following equipment:

GCP 8000 Site Controller
A standalone component, includes redundant modules.

GTR 8000 Base Radio
A standalone component.

GTR 8000 Site Subsystem
Includes redundant site controller modules, one base radio, and the RF distribution system (RFDS) in a single rack.

GTR 8000 Expandable Site Subsystem
A modular chassis that houses the redundant controllers, up to five base radios, and the RFDS equipment in a single rack.

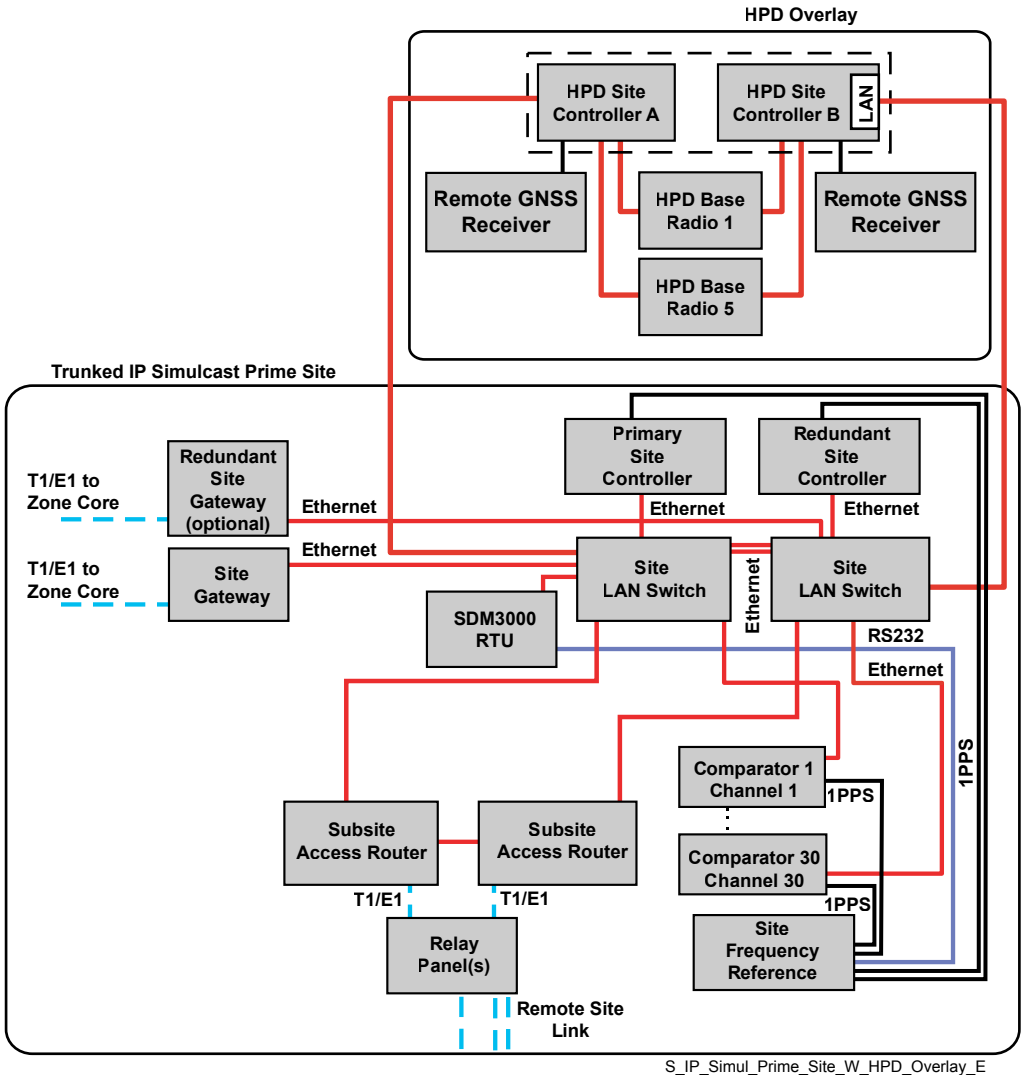
2.22 Simulcast Prime Site with HPD Overlay

A simulcast prime site with an HPD overlay allows an HPD site to be collocated with a simulcast prime site. The HPD equipment installed at the site consists of the HPD site controller and up to five HPD base radios. Up to five HPD channels can be supported at the site.

The HPD site controller (with redundant modules) connects with the prime site LAN, and shares bandwidth with the other IV&D equipment on the T1/E1 site link to the zone core. The HPD site controller and HPD base radios operate independently from the other IV&D equipment at the site.

All the different platforms listed for the HPD remote site can also be used in the overlay site (standalone GTR 8000, GCP 8000, site subsystem, or expandable site subsystem).

Figure 15: Simulcast Prime Site with HPD Overlay



Simulcast Prime Site with Geographical Redundancy and HPD Overlay

To provide a highly available trunked IP simulcast subsystem, a simulcast prime site can be split to two separate locations. Each half of a geographically redundant simulcast prime site is called a split prime site. Switchover to backup facilities and equipment occurs without operator intervention.

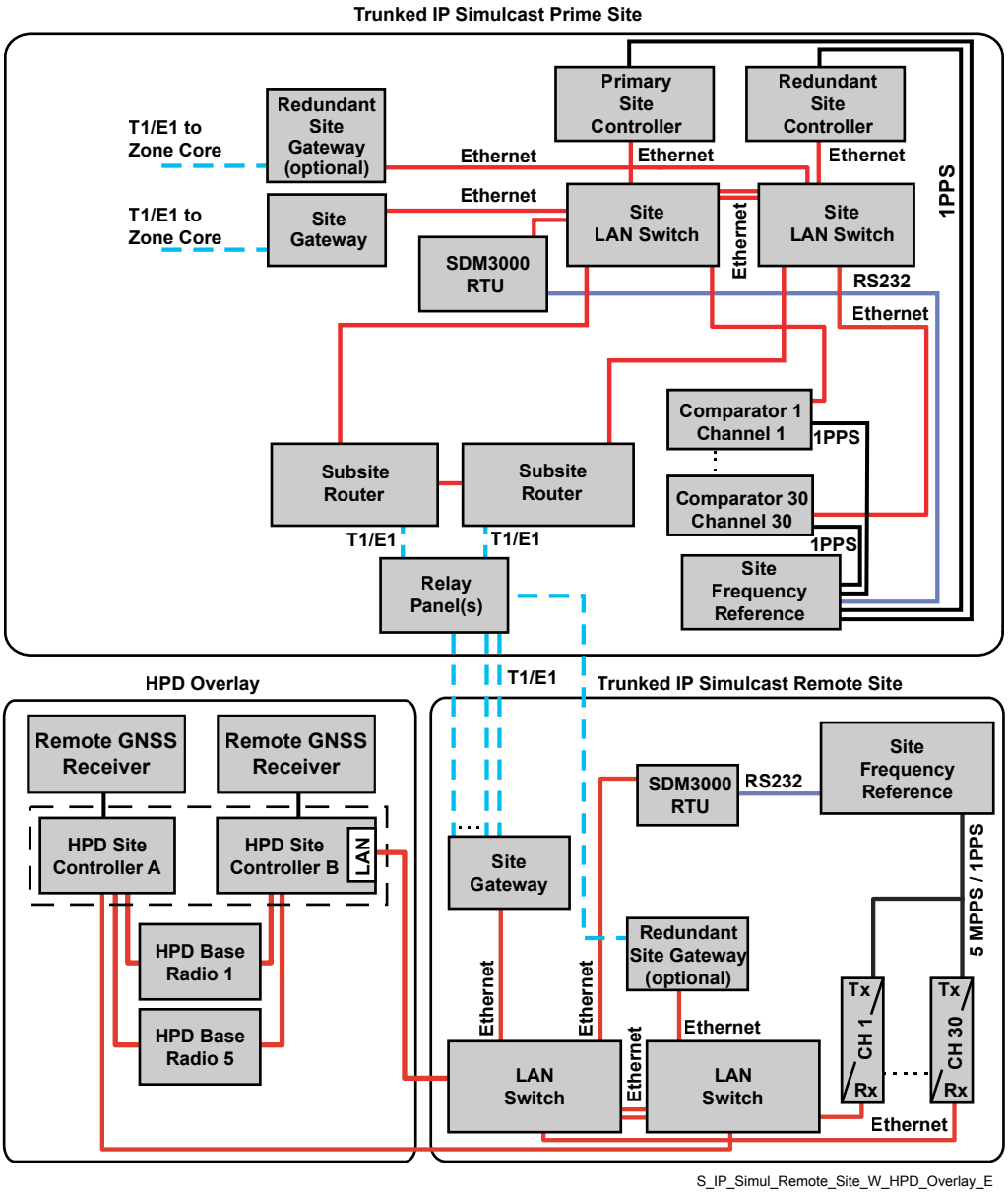
An HPD overlay site collocated at the prime site must reside only on the primary prime site. Both HPD site controllers are connected to the same split prime site LAN switch. This configuration results in lower availability for the collocated HPD overlay site since A LAN switch failure completely isolates the HPD site from the master site.

2.23

Simulcast Remote Site with HPD Overlay

The Simulcast remote site with the HPD overlay allows an HPD site to be colocated with the simulcast remote site. Up to five HPD channels can be supported at the site. The HPD site controller (with redundant modules) connects with the remote site LAN, and shares bandwidth with the other IV&D equipment on the T1/E1 site link to the prime site. The HPD site controller and HPD base radios operate independently from the other IV&D equipment at the site.

Figure 16: Simulcast Remote Site with HPD Overlay



The HPD equipment installed at the site consists of the HPD site controller and up to five HPD base radios. All of the different platforms listed for the HPD remote site can also be used in the overlay site (standalone GTR 8000, GCP 8000, site subsystem, or expandable site subsystem).

2.24 Simulcast Subsystem Capacity and HPD Overlay

A simulcast subsystem supports up to 32 subsites (increased from 15 subsites in the previous releases of the ASTRO® 25 system). An HPD overlay site could be deployed at any of these subsites. However, the total number of HPD overlay sites and channel capacity are heavily dependent on the simulcast subsystem configuration and other features. System designers must consider the existing simulcast subsystem configuration and other capacity must ensure that existing capacity limits are not exceeded on the prime site links.

2.25
Customer Network Interface

The Customer Network Interface (CNI) is the common access point between the core infrastructure network and the external customer networks. The CNI provides Network Address Translation (NAT) services to keep the core IP addresses isolated and transparent to the CENs. The CNI also limits the IP routing advertisements from the core network.

If an optional network interface barrier is installed, then the firewall is the physical point where the core network ends. Otherwise, the customer network interface exists at the gateway router.

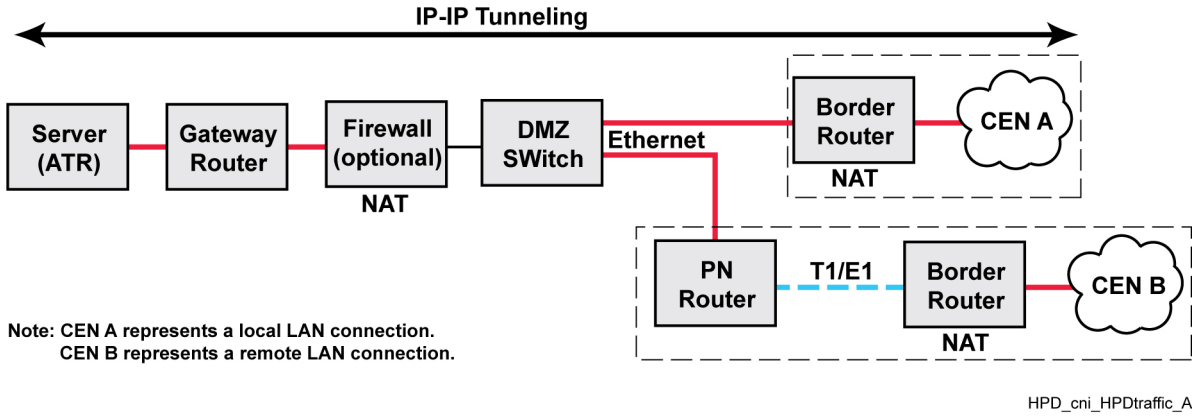
The customer network interface may support three general types of traffic. These include the following:

- HPD IP bearer services for subscriber data
- Air Traffic Information Access (ATIA) for unidirectional data
- Client/server (CADI and other applications) for bidirectional data

2.25.1
HPD Services

For HPD IP bearer services, the GGSN originates an IP-IP tunnel which passes through the CNI to the appropriate customer network or control room site (see the following diagram). The border gateway at the customer network or control room site terminates IP-IP tunnel and routes the traffic to the appropriate host. The IP-IP tunnel provides a VPN connection for the HPD traffic and provides IP address isolation between the core network and the customer network equipment.

Figure 17: Customer Network Interface – HPD IP Bearer Service



HPD_cni_HPDtraffic_A

2.25.2
Air Traffic Information Access

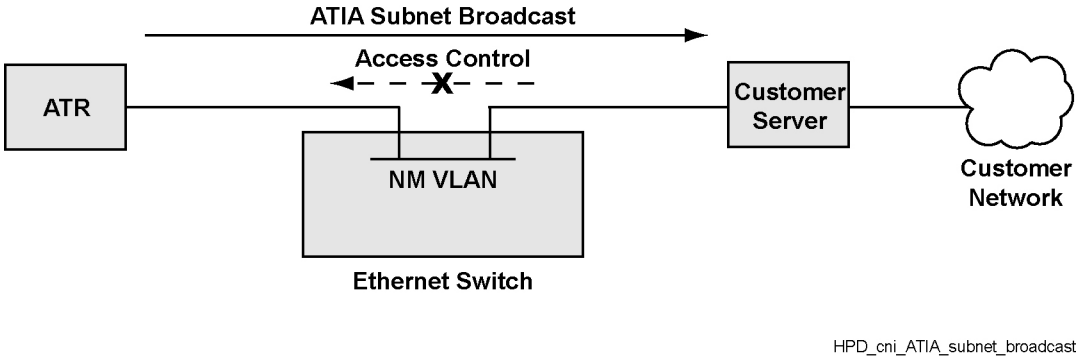
For streaming Air Traffic Information Access (ATIA) traffic, the Air Traffic Router (ATR) in each zone can be set up for unicast or subnet broadcast of the ATIA stream to a customer server. The customer server is typically a billing or accounting server. The ATR can be configured for redundancy to provide high availability of ATR services.

ATIA Subnet Broadcast Messaging

By default, the ATR sends ATIA traffic through subnet broadcast mode. The subnet broadcast is sent through the Network Management VLAN on the zone core Ethernet switch, and delivered to a locally connected customer server. In subnet broadcast mode, the ATIA packets include a short time-to-live value which causes the packets to be discarded if they are not immediately delivered to the customer server.

In addition to the connection to the NM VLAN, the customer server may have a second interface to the customer network, allowing clients on the customer network to access the billing or accounting information.

Figure 18: Customer Network Interface – ATIA Subnet Broadcast Messaging

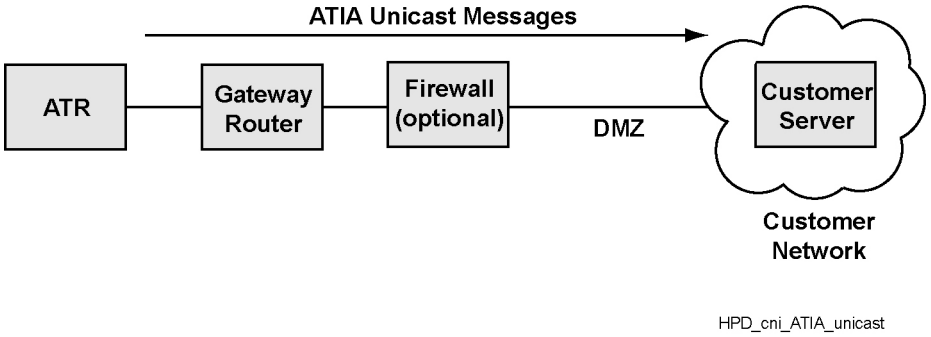


ATIA Unicast Messaging

When an ATR is set to unicast mode with an IP address of the customer server, the ATR sends the ATIA traffic through the Customer Network Interface (CNI) to the customer server, which exists on a customer network.

Unicast mode is preferred as it allows the network interface barrier to protect the core network and allows the billing server to be located on a customer network. When an ATR is set with an IP address, it cannot be returned to subnet broadcast mode.

Figure 19: Customer Network Interface – ATIA Unicast Messaging



High Availability for the ATR

L2, M2, and M3 zone cores can implement the Air Traffic Router (ATR) in a high availability, fault tolerant configuration. This configuration provides redundancy for the ATR to remove a single point of ATR failure and minimize recovery times of mission critical services: Computer Aided Dispatch (CAD), Air Traffic Information Access (ATIA), Mobility, Radio Control Manager (RCM), Provisioning Manager (PM), and Unified Network Services (UNS). In a high availability configuration, the ATR virtual machine runs in VMware Fault Tolerance mode on two Virtual Management Servers (VMS).

Fault Tolerance is a VMware feature that creates a standby ATR virtual machine on another VMS and keeps the standby ATR VM in sync with the primary device. At any given time, one of the two ATR VMs is the active device, streaming ATIA traffic in its zone, while the other ATR is the standby (inactive) device, providing redundancy. Only the active ATR is operating on the network and accessible by environment. Other devices in the system see the High Availability ATR pair as one ATR device.

The two ATR instances are continuously synchronized so that the standby ATR is able to assume the active role without loss of state. If the server hosting the active ATR fails, Fault Tolerance triggers a

switchover to the standby ATR, which becomes the active device, ensuring recovery of ATR services. The previously active ATR that experienced a failure becomes a standby device after the server recovers.

The active and standby ATR VMs share the same ATR IP address. Hence, the solution is transparent to external enabled ATR services in the event of switchover.

To implement HA ATRs, your system requires redundant Customer Network Interface (CNI) path equipment. If your system employs the High Availability for Trunked IV&D and HPD (HA Data) feature, which provides redundant CNI path equipment (in addition to redundant Packet Data Gateways [PDG] and GGSN routers), HA ATRs can reuse the redundant CNI path equipment provided by HA Data. The CNI path consists of the following devices:

- RNI-DMZ Firewall
- DMZ Switch
- Peripheral Network Routers
- Border Routers

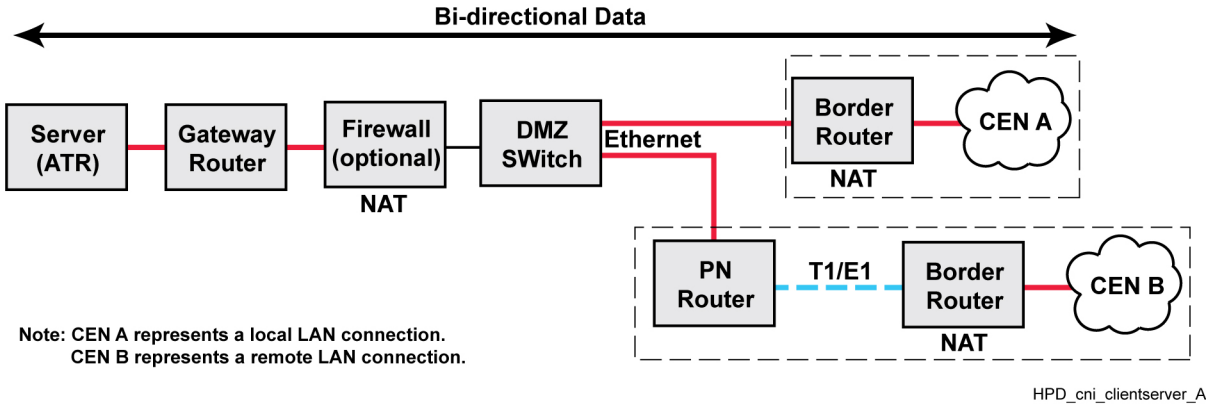
HA ATRs can be implemented in systems with the Dynamic System Resilience (DSR) feature. DSR is a system architecture that provides redundant zone core equipment by establishing a primary zone core and a backup zone core usually at two different master site locations. In DSR architectures, both the active core and the backup core must employ HA ATRs. Implementing HA ATRs either in the active core or the backup core only is not supported.

2.25.3
Client/Server Interface

For client/server applications between the customer network and the core network, NAT occurs at both the CNI (gateway router or firewall) and at the border gateway within the customer network or control room site.

Figure 20: Customer Network Interface – Client/Server

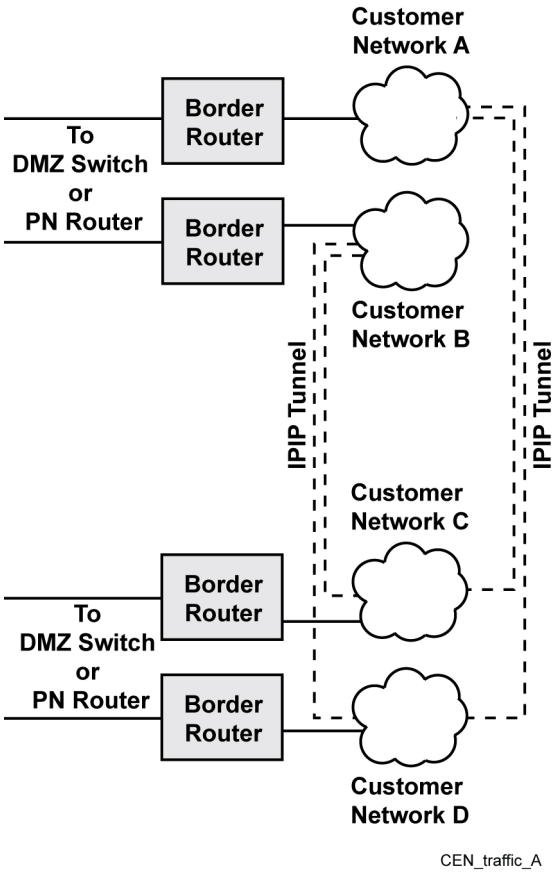
The following diagram shows the customer network interface in a client/server application.



2.25.4
Traffic Between Customer Networks

In addition to traffic through the CNI, traffic between customer networks is also supported. For this communication to occur, the border gateways use network address translation or IP-IP tunneling to isolate IP addressing between the separate networks. (This was previously handled by the peripheral network). See the following diagram.

Figure 21: Customer Network Traffic



2.26

Customer Enterprise Network

The Customer Enterprise Network (CEN) includes all the fixed customer host equipment. This may consist of various clients, servers, and networking devices that may interact with MSUs through the HPD wireless network. The equipment and applications at the CEN depends on your organization`s requirements. Some common types of equipment that may be supported at a CEN include:

- RADIUS server
- DHCP server
- DNS server
- Database servers
- Application servers
- Web servers
- File servers
- Billing/accounting servers
- Logging hosts
- Computer Aided Dispatch (CAD) hosts
- GNSS tracking hosts
- Routing application
- Client PCs

The HPD system supports up to ten points of presence to Customer Enterprise Networks (CENs). A CEN may be a complete separate customer network, or may be a separate set of customer hosts that are colocated at a control room site (on a separate VLAN from the Network Management clients at the site).

CENs may be connected locally to the DMZ, remotely over a WAN link, or remotely to the DMZ at another zone. The border gateway provides IP-IP tunneling for inbound/outbound HPD traffic. The IP-IP tunneling originates at the GGSN and terminates at the border gateway. The border gateway may also use either IP-IP tunneling or NAT when routing traffic to other CENs. Since the border gateway is considered part of the CEN, it is not managed by the Network Management applications in the HPD system. Instead, it should be managed by CEN Network Management applications.

Each CEN connection is called an access point and is referenced in the system by an Access Point Name (APN). This APN is associated to the border gateway for the CEN. While there may be more than one CEN, an individual HPD modem and attached mobile data device can only communicate through one statically configured CEN access point.

2.27 HPD Modem

The HPD1000 modem shown in the following picture is a radio transceiver that provides the RF interface between the mobile data device and the system infrastructure. When the HPD modem is turned on or enters the coverage area, it automatically registers with the system. When the mobile data device establishes a connection with the HPD modem, the HPD modem interacts with the system to perform a context activation. The context activation establishes the path for HPD traffic between the mobile data device and the customer enterprise network. This context activation can only be initiated by the HPD modem, and cannot be initiated by the HPD system or by any hosts on the CEN. The HPD modem provides the endpoint for the SNDCP tunnel (which is the established data transfer route to the home PDR). Any inbound or outbound traffic between the system and the mobile data device is passed through the HPD modem.

Figure 22: HPD Modem

HPD_1000_modem_front

When a Point-to-Point Protocol (PPP) link setup, internal application assertion, or IP configuration protocol setup from the mobile data device has been received, the HPD modem attempts to context activate with the system. The HPD modem also detects cases where it must context deactivate, including when a PPP link shutdown message, graceful shutdown, or connection loss with the mobile data device has occurred.

The HPD modem can operate in either HPD mode or interoperability mode. When in HPD mode, the modem communicates with the HPD infrastructure at rates up to 96 kbps. When using interoperability mode, the modem can communicate directly with other HPD modems at up to 9600 bps. When in HPD mode, the HPD modem uses adaptive modulation to provide reliable traffic delivery to the system throughout the coverage area.

The HPD modem is equipped with an optional GNSS receiver and internal location application (see the following diagram). This option can be used to send location information to Automatic Vehicle Location (AVL) applications on the customer enterprise network hosts. The internal GNSS receiver sends

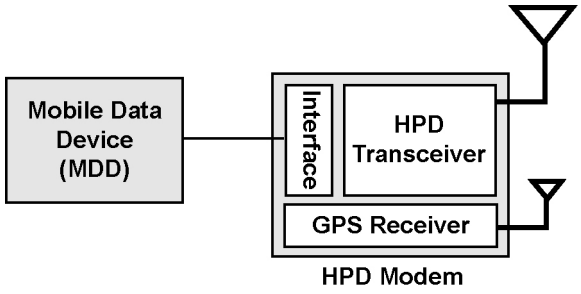
location information (if requested to do so) to the CEN, to the mobile data device, or to both. If the optional HPD Modem Enhanced Power Control Cable (FLN4215) is used between the modem and the mobile data device, location information can be sent to the CEN even when the mobile data device is off or disconnected from the modem.

Location services can be enabled or disabled through Customer Programming Software (CPS). The maximum number of location requests that are serviced by the HPD modem is also defined through CPS.

The HPD modem can transport user authentication credentials and acknowledgments between the mobile data device and the HPD system. Authentication credentials used exclusively for the internal location application can be configured through CPS. This allows the location application to independently context activate with the system when the authentication is required.

The HPD modem includes a USB port and an RJ45 Ethernet port. Either port can be connected to a mobile data device. A USB connection uses PPP. An Ethernet connection uses Point-to-Point Protocol over Ethernet (PPPoE). A GNSS antenna must be connected to support the internal GNSS receiver. Half-duplex and full-duplex capabilities are supported.

Figure 23: HPD Modem – Block Diagram



HPD_modem_block_diagram

The codeplug for the HPD modem is configured through CPS. The codeplug includes settings for the Radio ID, important IP addresses, authentication settings, RF characteristics, band and channel settings, internal location application settings, network address translation addresses, and infrastructure IDs that are used during registration and context activation.

Records and profile information are also defined for each HPD modem through Provisioning Manager. The records and profiles specify the Radio ID and define the access and permissions that are allowed for the HPD modem when it is operating in the HPD system. The Provisioning Manager and CPS settings must be coordinated for the HPD modem to operate on the system.

The user can control the HPD modem through the Status Applet on the mobile data device. The Status Applet can be used to reset, shutdown, or change the IP address of the modem. Switching between HPD and interoperability mode is also performed through the Status Applet.

NOTICE: The HPD 1000 MSU is capable of operation on a maximum of five different HPD networks. HPD Network selection is determined by manual user intervention.

2.28 Mobile Data Device

Motorola Solutions offers a number of full-featured computers with a rugged construction that would be suitable for HPD operation in mission-critical mobile environments. Motorola Solutions has tested and certified the following hardware platforms for HPD operation.

- ML 910 Rugged Notebook
- MW 810 Mobile Workstation

These platforms have been tested and certified using the following operating systems. If Windows power management features are desired (S3 Standby state), all operating systems require installation of additional Motorola provided software.

- Window Vista with Service Pack 2 (SP2)
- Windows 2000 with Service Pack 2 (SP2) and a PPPoE driver installed
- Windows 7

The mobile data device can connect with the HPD modem through either a USB or Ethernet connection. A PPPoE driver must be installed in a mobile data device if it is running Windows 2000 and uses an Ethernet connection to the HPD modem. To successfully connect with the system for HPD service, the mobile data device can be loaded with Connection Manager and Status Applet software provided by Motorola Solutions. Otherwise, other custom applications may be developed by your organization to manage the connection.

2.28.1
Communication Manager

The Communication Manager application can be installed on the mobile data device to manage and monitor the logical link to the HPD modem. The application, which resides in the system tray in the lower right portion of the screen, displays an icon showing the status of the connection to the HPD modem and indicates whether the mobile data device is context activated.

Figure 24: Communication Manager

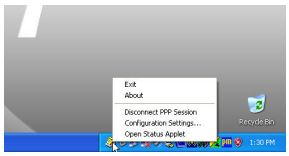


Table 3: Communication Manager – Icon Indications

Icon Color	Description
Red	A red icon indicates that the logical link to the HPD modem is not established. The mobile data device is not context activated.
Yellow	A yellow icon indicates that the logical link to the HPD modem is established. The mobile data device is not context activated.
Green	A green icon indicates that the logical link is established and the mobile data device is successfully context activated.
White	A white icon indicates that the logical link to the HPD modem is established. The mobile data device is out of range.

If the link to the HPD modem is lost or not established, the status icon changes to red, and the Communication Manager automatically attempts to re-establish a connection.

Right-clicking on the Communication Manager icon provides a pop-up menu, allowing the user to either open the Status Applet, the configuration window for the Communication Manager, or toggle the logical link state (connect/disconnect). The configuration window can be used to configure the following items:

- Select the type of the link option (USB/Ethernet).
- Configure link reconnection attributes.
- Configure SNMP connection attributes (used to communicate with the HPD modem).
- Configure the IP address for accessing the HPD modem.
- Indicate whether the Communication Manager should automatically start when Windows starts.

2.28.2

Status Applet Display – Simplified Mode

The HPD Status Applet has two modes of display called the Simplified and Extended Display. Only one mode of display can be active at a time. The ‘Simplified Mode’ and ‘Extended Mode’ buttons are used to switch between the desired mode of display. The Status Applet in minimized mode reveals the HPD system name and signal strength when pointed to by the mouse cursor.

Figure 25: HPD Simplified Status Applet

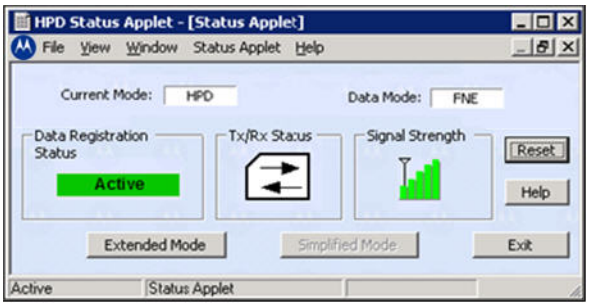
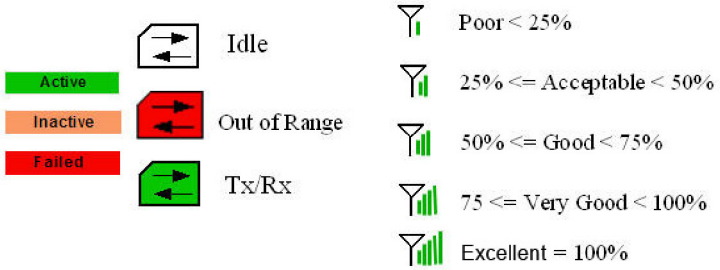


Figure 26: HPD Status Applet (Simplified and Extended) – Icons



2.28.3

Status Applet – Extended Mode

The Extended Status Applet displays a number of important characteristics about the operation and status of the HPD modem and mobile data device connection. It displays information about the current mode of the HPD modem, the registration status, GNSS status, signal strength, transmit/receive status, and important IP addresses.

The HPD Status Applet’s extended display enables a mobile user to select an ASTRO® System with HPD capabilities to roam to. The user is enabled to manually move the HPD 1000 MSU between a maximum of five ASTRO® networks that are provisioned in the MSU. The subscriber should use the extended Status Applet to switch between the systems and choose the system name from the list. If at least one of the systems requires authentication, a user should change Connection Manager settings before switching the systems. Refer to Troubleshooting HPD Services at the HPD Modem, Mobile Data Device, and Subscriber on page 97 for additional information on switching between authenticated and non-authenticated HPD systems.

Figure 26: HPD Status Applet (Simplified and Extended) – Icons on page 59 shows the icons used in the HPD Status Applet.

Figure 27: HPD Extended Status Applet

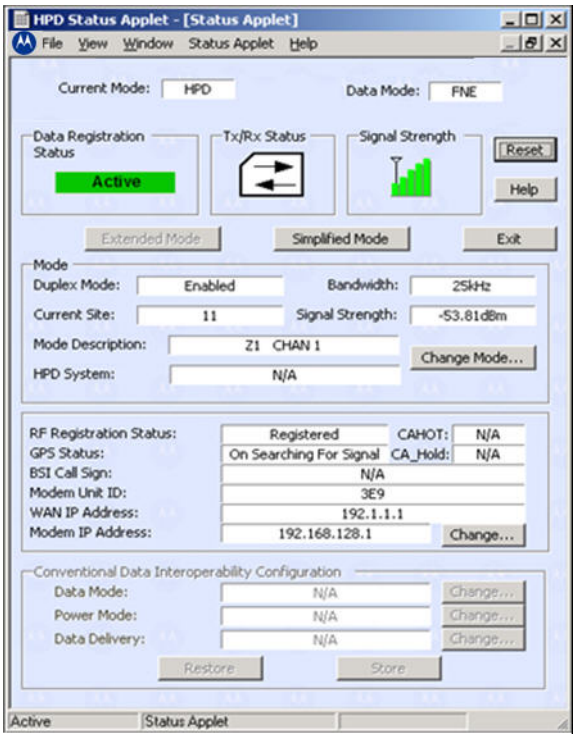


Table 4: Status Applet Fields and Buttons

Field/Button	Description
Current Mode	Indicates the current mode of the HPD modem. For HPD service, this field displays `HPD`.
Data Mode	Indicates the current data mode of the HPD modem.
Duplex Mode	Indicates whether the HPD modem is operating in duplex mode. This field may indicate `enabled` (Full-duplex) or `disabled` (Half-duplex).
Bandwidth	Indicates the bandwidth for the data service being used. For HPD services, the bandwidth displays `25 kHz`.
Current Site	Indicates the number of the site the HPD modem is affiliated to.
Signal Strength	Indicates the signal strength in dBm.
HPD System	The name of the system that the modem is provisioned/connected to.
Mode Description	Indicates the current mode that the HPD modem is operating in. For HPD service, this field displays `Zone Channel Assignment Name`.
RF Registration Status	Indicates whether the HPD modem has successfully registered with the system. The status may be registered or unregistered.
Change Mode	This button allows the user to select the mode that the HPD modem should operate in. HPD is the only mode supported in this release.

Table continued…

Field/Button	Description
Data Registration Status	Indicates the status of the context for this mobile data device. The context status may be active or inactive.
GNSS Status	Indicates the status of the GNSS receiver in the HPD modem.
Signal Strength	Indicates the signal strength of the outbound channel that this HPD modem is currently operating on.
BSI Call Sign	This is the Base Station Identification call sign that is transmitted by the HPD modem.
Reset Modem	Sends a reset command to the HPD modem, causing the HPD modem to restart.
Modem Unit ID	Indicates the unit ID for the HPD modem (as provisioned through CPS).
WAN IP Address	Indicates the address for the current SNDCP context. If the context is inactive, this address indicates 0.0.0.0.
Modem IP Address	Indicates the IP address of the HPD modem.
Change Modem IP Address	This button allows the user to change the IP address of the HPD modem. This IP Address is used by the Status Applet to communicate with internal status applications within the HPD modem. After changing the IP address, the HPD modem must be reset before the changes take effect.
Transmitter Status	Indicates the transmitter status for the HPD modem. Green indicates that the HPD modem is sending data to the system. Red indicates that the transmitter is idle.
Receiver Status	Indicates the receiver status for the HPD modem. Green indicates that the HPD modem is receiving data from the system. Red indicates that the receiver is idle.

2.28.4
Configuration Communication Manager

The HPD Communication Manager (also included with the Status Applet Tool) provides a logical link (PPP/PPPoE) connection between the mobile computer and the HPD MSU. The Communication Manager also monitors the logical link (PPP/PPPoE) as well as the Packet Data Service Registration status and displays it (through a color-coded icon) in the status bar.

This page intentionally left blank.

Chapter 3

HPD Overlay Installation

This chapter details the hardware and software installation procedures relating to HPD Overlay.

3.1 Site Links

The HPD remote sites and remote overlay sites connect with the zone core through T1/E1 WAN links. The following sections specify the site link requirements between the remote sites and the zone core.

NOTICE:
It is recommended to distribute all site links as evenly as possible over all access router pairs.

See the *Flexible Site and InterZone Links* manual for Ethernet interfaces alternatives.

3.1.1 T1 Links

There are different levels of T1 links supported by the various devices and different types of transport mediums supported between the various sites.

Unchannelized T1
The actual T1 format on the line is the same as channelized and fractional. The line supports a 1.544 Mbps bit stream with 192 bits of data and 1 framing bit per frame. In the unchannelized case, all 24 DS0s are used as a single serial bit stream of 1.536 Mbps.

Channelized T1
The actual T1 format on the line is the same as unchannelized and fractional. The line supports a 1.544 Mbps bit stream with 192 bits of data and 1 framing bit per frame. The channelized T1 link supports the ability to have many different serial bit streams of different speeds. Each Serial bit stream consists of one or multiple DS0s. The device that supports a channelized T1 link is able to split the physical 24 channels in groups and treat each group as a separate serial bit stream.

Fractional T1
The actual T1 format on the line is the same as unchannelized and channelized. The line supports a 1.544 Mbps bit stream with 192 bits of data and 1 framing bit per frame. The fractional T1 only uses a subset of the 24 DS0s on the link for one serial bit stream. There is no real difference between unchannelized T1 and fractional T1 except unchannelized T1 uses all 24 DS0s and fractional T1 uses from 1-24 DS0s.

NOTICE: They always start from the first DS0 of the T1. In both cases, the actual formatting of the link is the same.

3.1.2 E1 Links

There are different levels of E1 links supported by the various devices and different types of transport mediums supported between the various sites.

Unchannelized E1
The actual E1 format on the line is the same as channelized and fractional. The line supports a 2.048 Mbps bit stream with 1 or 2 time slots (Time slots 0 and optionally 16) used for framing and alarm and control signaling. Slot 16 may or may not be available depending on the Service

Provider. In the unchannelized case, 30 or 31 of the 32 DS0's are used as a single serial bit stream of 1.920 Mbps or 1.984 Mbps respectively.

Channelized E1

The actual E1 format on the line is the same as unchannelized and fractional. The line supports a 2.048 Mbps bit stream with 1 or 2 time slots (Time slots 0 and optionally 16) used for framing and alarm and control signaling. The channelized E1 link supports the ability to have many different serial bit streams of different speeds. Each Serial bit stream consists of one or multiple DS0's. The device that supports a Channelized E1 link is able to split the available physical 30 or 31 channels in groups and treat each group as a separate serial bit stream.

Fractional E1

The actual E1 format on the line is the same as unchannelized and channelized. The line supports a 2.048 Mbps bit stream with 1 or 2 time slots (Time slots 0 and optionally 16) used for framing and alarm and control signaling. There is no real difference between unchannelized E1 and fractional E1 except unchannelized E1 uses all available 30 or 31 DS0s and fractional E1 uses time slots 1-31 excluding timeslot 16 if used by carrier equipment for signaling (starting from the first DS0). In both cases, the actual formatting of the link is the same.

3.1.3
HPD Remote Site Links

Each HPD standalone remote site requires a full T1/E1 or fractional T1/E1 link to the zone core. The link must include bandwidth for one DS0 per HPD channel at the site. A minimum of two DS0s are required at the site, even if only one HPD channel is at the site. The following table shows the DS0s required for HPD remote site links.

Table 5: DS0s Required for HPD Remote Site Links

Number of HPD Channels	Number of DS0s Required
1	2
2	2
3	3
4	4
5	5

Fragmentation of HPD traffic is done at the Frame Relay layer using FRF.12 in the core and site gateways.

If the site is configured for redundant site links, then two separate links with the same minimum DS0s must be supplied between the HPD site and zone core. These links provide primary and backup connections for high availability.

The individual T1 or E1 lines should support the following recommended specifications in the following table.

Table 6: Recommended T1/E1 Line Specifications For HPD Remote Site Links

Link	Specification (bit errors per second)	Propagation Delay	Availability	Framing	Line Coding	Additional Information
Site Link T1	10e-6	5 msec	99.999%	ESF	B8ZS	• Signaling clear channel • Channelized or un-channelized • No compression
Site Link E1	10e-6	5 msec	99.999%	CRC4 , No CRC4	HDB3	• Signaling clear channel • Channelized • No compression • CCS only

3.1.4
Site Links for Voice/IV&D Sites with HPD Overlay

For remote sites with the HPD overlay, the HPD equipment shares the T1/E1 site link bandwidth to the zone core. The HPD equipment at the site requires one DS0 per HPD channel (with a minimum of two DS0s if only one HPD channel is installed at the site).

Adding HPD to a site increases the minimum bandwidth required at the site. In general, the bandwidth rules treat HPD as if it were being overlaid on top of an existing site. The bandwidth required for the site is first determined as if HPD were not present. Once that determination has been made, the incremental effect of adding HPD is determined.

At sites with a few voice channels, the bandwidth allocated for HPD must account not only for the HPD traffic, but also must ensure sufficient overhead to prevent excessive queuing of HPD packets. At high link speeds, queuing delay is not an issue for HPD packets, and bandwidth can be allocated on a worst case average traffic expected for an HPD channel. For this reason, one DS0 is required for every HPD site colocated at a site with less than 12 DS0s. An overlay site with more than 12 DS0s for voice/IV&D only require half a DS0 for each HPD channel added.

For ASTRO® 25 repeater sites with HPD overlay and Simulcast remote sites with the HPD overlay, the total number of DS0s required for the entire site does not exceed the capacity of one T1/E1 line. If a full T1/E1 line is already supported to the overlay site, then no additional bandwidth is required when the HPD equipment is added. If only a fractional T1/E1 line is supported at the overlay site, then the bandwidth of the site link may need to be increased to a larger fractional T1/E1 line or full T1/E1 line to support both the IV&D equipment and HPD equipment.

A Simulcast prime site with the overlay typically supports a larger volume of DS0s. The site link between the prime site and zone core has to support traffic for all the Simulcast remote sites (which may each include HPD overlay traffic) and additional traffic from HPD overlay equipment at the prime site itself. If the total bandwidth required for the prime site link to the zone core exceeds the capacity of a single T1/E1 link (24 DS0s for T1 or 30 DS0s for E1), then additional full T1/E1 links must be added using Multilink Frame Relay (MFR).

MFR is only implemented on full T1/E1 increments, and not on a fractional or DS0 level. If MFR is required, then fractional T1/ E1 links are not allowed. However, the actual bandwidth allocated to voice may still be a fractional amount of T1s/E1s, with the remaining bandwidth provided for non-voice

application traffic. For example, if a site requires 35 DS0's then two T1s (48 Ds must be used regardless whether the leftover bandwidth is needed or not.

3.2 Customer Enterprise Network

The installation of the Customer Enterprise Network depends on the customer requirements. The network may include various servers, clients, and network devices. Up to ten CEN connections are supported system wide. See the *Customer Network Configuration* documentation for CEN installation requirements.

3.2.1 Border Gateway

The CEN LAN must be connected to the DMZ through a border gateway. This gateway provides the access point into the CEN. The border gateway may either be supplied by Motorola Solutions or by your organization. If the border gateway is supplied by Motorola Solutions, the gateway is preconfigured for your system at the factory before it is shipped.

If the border gateway is supplied by your organization, it must support the following (at a minimum):

Border gateway protocol (BGP)
This protocol is used to advertise routes between the peripheral network router and the border gateway.

IP-IP tunneling
The border gateway must terminate IP-IP encapsulated tunnels provide IP-IP tunneling for HPD traffic from the GGSN. IP-IP tunneling may also be used for traffic between CENs for peer-to-peer type applications (many hosts to many hosts with no restriction on who initiates the traffic). IP-IP tunnels between CENs can only be used if the two CENs have coordinated their IP address plan and IP routing.

Network address translation (NAT)
Traffic between CENs can be sent using NAT or IP-IP tunneling. NAT can be used for client/server type applications. Any type of NAT mappings can be used (one-to-one, one-to-many, or many-to-many type translations), but an additional one-to-one NAT mapping is required in the border gateway for the server in a client/server configuration.

The following table shows typical minimum connections for a border gateway. If using a border gateway supplied by your organization, see the *Router and Customer* documentation for the proper installation and configuration.

Table 7: Border Gateway Connections

Device	Port	Device	Port	Notes
Border Gateway	LAN 1 port, RJ45	DMZ Switch	4-24, RJ45	Ports 4-24 on the DMZ switch are available for border gateway connection.
Border Gateway	LAN 2 port, RJ45	CEN Switch	RJ45	See *Customer Network Configuration* documentation for connection requirements.

3.2.2 DMZ Switch

A DMZ switch can be installed within each zone that supports a customer enterprise network or control room site. The DMZ switch provides the external LAN for connecting CENs, a peripheral network router, and the HPD system interface. Peripheral network routers and DMZ switches can be added as

required to support the interface to the customer enterprise networks. In general, there is one peripheral network router and one DMZ switch per zone where customer enterprise networks exist.

While IP-IP tunneling originates at the GGSN, the physical HPD system interface may either be at the firewall (if the network interface barrier option is selected), or it is on the DMZ VLAN port on the zone core Ethernet switch. The following table lists the standard port assignments for the DMZ switch.

Table 8: DMZ Switch Connections

Device	Port	Device	Port / Type	Notes
DMZ Switch	1	Firewall (optional)	NIC 4, RJ45	Connection to the optional network interface barrier. **NOTICE:** If the firewall is not installed, the connection is made to the DMZ VLAN on the zone core Ethernet switch.
DMZ Switch	2	Intrusion Detection Sensor (optional)	LAN port 2, RJ45	Mirror port for IDS traffic monitoring.
DMZ Switch	3	Peripheral Network Router	LAN 1 port, RJ45	Connection for the WAN routing of traffic on the peripheral network.
DMZ Switch	4-24	DMZ Devices	LAN port, RJ45	Connection for locally connected border gateways for customer enterprise networks.

3.2.3 Peripheral Network Router

Peripheral Router is only needed when a CEN is remote from a zone core over T1/E1 links, or IPv6 Ethernet Links (to terminate encryption endpoints).

3.3 High Availability for HPD 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 HPD (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 *GGM 8000 System Gateway* or *S6000 and S2500 Routers* 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

HPD Overlay Configuration

This chapter details the system-level configuration procedures relating to HPD Overlay.

4.1 Configuring UNC Wizard for HPD System

When and where to use: Follow this process to configure an HPD system using Unified Network Configurator (UNC).

Process:

1. Set data system parameters in the UNC Wizard. See “Updating a System-Level Setting” section in the *Unified Network Configurator* manual. See the parameter descriptions in Configuring the System for HPD Operation with Provisioning Manager on page 70.

   NOTICE: All parameters apply except the **Security Group**

2. Discover the HPD PDG by running a zone core discovery in the UNC Discovery Wizard. See the “Device Discovery” section in the *Unified Network Configurator* manual.
3. Discover the HPD site equipment by running a site or subsite discovery depending on where the site equipment exists. See the “Device Discovery” section in the *Unified Network Configurator* manual.
4. Configure adjacent sites through the UNC Adjacent Site Wizard. See the “Adjacent Site Management” section in the *Unified Network Configurator* manual.
5. Publish infrastructure data to Provisioning Manager. This operation pushes the APN Operator ID, site, and channel configuration to Provisioning Manager. See the “Publish Infrastructure Data Wizard” section in the *Unified Network Configurator* manual.

4.2 Provisioning Manager Configuration for HPD Operation

The following Provisioning Manager application objects must be properly configured for an HPD system. Since the HPD feature does not include telephone interconnect equipment, talkgroups/ multigroups, console equipment, or voice services, all the other Provisioning Manager objects typically do not need to be configured or changed.

Additional information for the following and other Provisioning Manager objects is provided in the *Provisioning Manager Online Help*.

- System
- Access Point Name
- Radio Site Access Profile
- HPD Radio
- Broadcast Data Agency
- Home Zone Map
- Security Group
- ZoneWatch profiles, watch windows, and filters

4.2.1
Configuring the System for HPD Operation with Provisioning Manager

Perform this process to configure the Provisioning Manager application records for HPD operation.

Process:

1. Set up security groups and Network Management user accounts:
   - **Security Group** – add Security Group records to partition user access if necessary.
2. Configure the system-level objects:
   - **System** – configure the system parameters.
   - **Access Point Name** – configure the APN Network IDs that identifies the IP network associated with a subscriber.
3. Configure subscribers:
   - **Radio Site Access Profile** – create profile records that define the sites that can be used by a number of radios.
   - **HPD Radio** – create radio records for each MSU that is operating on the system.
   - **Broadcast Data Agency** – configure users as part of a Broadcast Data Agency.
   - **Home Zone Map** – define the home zone mapping ranges for the individual radios (talkgroup and multigroup mappings are not required).
4. Configure ZoneWatch filters, watch windows, and watch profile settings.

4.2.2
Frequency Band Plan Settings for HPD Operation

The frequency band plan for HPD operation must be configured directly into each HPD site controller using the Configuration/Service Software (CSS) application. The Frequency Band Plan records in UNC apply to IV&D operation and do not have to be configured for HPD operation.

4.2.3
Home Zone Mappings for HPD Operation

For HPD operation, all the individual ID blocks must be assigned to home zones. Talkgroup and multigroup IDs do not apply to HPD operation. Use default settings for talkgroup and multigroup ID mappings.

4.2.4
Radio Site Access Profile for HPD Operation

The following Provisioning Manager application objects must be properly configured for an HPD system. Since the HPD feature does not include telephone interconnect equipment, talkgroups/ multigroups, console equipment, or voice services, all the other Provisioning Manager objects typically do not need to be configured or changed.

4.2.5
Configuring HPD Radio Settings for HPD Operation

An HPD Radio record must be created for each HPD radio operating in the system. The record defines a number of parameters related to the identity, data configuration and capabilities of a radio.

Procedure:

1. In Provisioning Manager, select the **HPD Radio** object in the **Subscriber** tab. Click **New** to add a new HPD radio record.
2. In the **Radio ID** field, enter the unique number that refers to a specific radio on the system. The Radio ID associates the radio with a home zone, according to the individual home zone mapping configuration.
3. In the **Radio Serial Number** field, enter the unique serial number of a specific radio on the system. This unique serial number is part of the radio's programming. The zone controller uses this number to link a radio ID to an alias.
4. In the **Radio User Alias** field, type a unique name for this radio user.
5. In the **Security Group** field, select the security group that this record should be associated with.
6. For the **IP Address Type** field, select either **Static** or **Dynamic**. Selecting dynamic addressing allows the GGSN or a RADIUS/DHCP server on the CEN to assign an IP address to the MSU during registration. Selecting static addressing requires the MSU to supply an IP address during registration. If the MSU does not supply a static address, the system assigns the MSU with the static address given in the next step.
7. If the static addressing was selected, enter a unique IP address for the radio user in the **IP Address** field.
8. For **Source Address Checking**, select whether the system should verify the source IP address for all traffic originating from this radio user. If **On** is selected, the system discards traffic with improper source IP addresses.
9. For **Generate ICMP Message**, select whether the system should generate ICMP response messages for failed delivery of messages that were originated by this radio user. If **Off** is selected, the radio does not receive any ICMP responses from the system for failed delivery of IP datagrams.
10. In the **Primary Core Access Point Name** and **Backup Core Access Point Name** fields, select the APN Network ID for the appropriate CEN that this radio is accessing.
11. In the **Radio Site Access Profile** field, select the Radio Site Access Profile to be used for this radio.

    IMPORTANT: The profile must include only HPD sites.

4.2.6
Configuring ZoneWatch Windows for HPD Operation

ZoneWatch filters and watch windows are configured in Provisioning Manager. Watch window records define how ZoneWatch operates, and may include a number of configurable filters to select the type of events to be displayed in ZoneWatch.

Procedure:

1. In Provisioning Manager, select the appropriate **Watch Window** object in the **Applications** tab.
2. Click **New** to add a new watch window.
3. In the **Radio Type Filter** field, select one of following options:
   - **HPD** to display events for HPD MSUs only
   - **All** to display events for all subscribers in the system (IV&D and HPD)
4. Enter the other filter settings and click **Apply**.

5 If any other filters should be applied to only view events from particular HPD sites, channels, or MSUs, first configure the necessary filters (Site Filter, Channel Filter, Radio ID Filter, or Radio Range Filter records). Then add the filters to the appropriate watch window and make any other related configuration changes. See the *Provisioning Manager Online Help* for more information about creating filters.

4.3 MSU Configuration Requirements

Configure properly each HPD modem and mobile data device for HPD operation. Any configuration performed for each device must be compatible with the settings made in the Provisioning Manager and CEN applications.

4.3.1 HPD Modem Configuration Requirements

The following table shows the typical configuration settings that are recommended for the HPD modem. Leave the default values for any CPS settings that are not listed. See the *CPS Online Help* for additional information about fields and settings.

Table 9: HPD Modem Configuration Requirements

Object	Tab	Field	Setting
Radio Wide	General	Power Button	Select checkbox.
Radio Wide	Modem Wide Data	Subscriber IP Address	Leave default address.
		SNMP Traps	Select checkbox.
		ICMP Echo	Select checkbox.
Radio Wide	Location	Location Enable	Select checkbox.
NAT List	NAT Entry - 1	WAN Port	4001
		LAN Port	4001
		Static NAT IP Address	`<IP address>`
Trunking	HPD Trunking Configuration	Operational Bandwidth	25 kHz
		Duplex Mode	Select appropriate duplex mode.
Trunking System - 1	General	Home System ID	Set the System ID (in hexadecimal format) as defined in Provisioning Manager.
		Home WACN ID	Set the Wide Area Communication Network ID (in hexadecimal format) as defined in Provisioning Manager.
		Unit ID	Set the Radio ID for this unit, as defined in Provisioning Manager.
		HPD System Name	Select the system name.

Table continued...

Object	Tab	Field	Setting
Trunking System - 1	Authentication Tab	Strict Authentication	Select checkbox if the authentication is required.
		Indicate Context Loss through PPP	Select checkbox.
		MC Authentication Type	Select CHAP, PAP, Both, or None.
		CAUTION: If using CHAP authentication, disable the ability to store the password on the Radius server. If the server is configured to store the password, the subscriber is unable to context activate.	
		MSU Authentication Type	Select None.
		MSU Authentication Username	Not required in this release.
		MSU Authentication Password	Not required in this release.
Trunking System - 1	Band Plan (add 800 MHz entry)	Band Plan Identifier	0
		Band Plan Channel Bandwidth (kHz)	25.000
		MSU Transmit Offset Sign	Minus (-)
		MSU Transmit Offset (MHz)	45.00000
		Channel Spacing (kHz)	6.250
		Base Frequency	851.01250
Trunking System - 1	Band Plan (add 700 MHz entry)	Band Plan Identifier	1
		Band Plan Channel Bandwidth (kHz)	25.000
		MSU Transmit Offset Sign	Plus (+)
		MSU Transmit Offset (MHz)	30.00000
		Channel Spacing (kHz)	6.250
		Base Frequency	764.01250
Trunking System - 1	Static Channels	TX Channel Frequency	Set to the actual transmit frequency for the MSU.
		RX Channel Frequency	Set to the actual receive frequency for the MSU.
		Static Channel Bandwidth (kHz)	25.000

Table continued…

Object	Tab	Field	Setting
Trunking System - 1	BW Preference	Bandwidth	25.000
		Preference Value	Select Always Preferred.
Trunking System - 1	HPD Advanced	All fields	No changes from the defaults are required.
Trunking Personality - 1	General	Protocol Type	HPD
		System & ID	1
Trunking Personality - 1	Preferred Sites	Site ID (Hex)	1
		Preferred Status	None
		System ID - RFSS ID	1
Zone Channel Assignment - 1	Zone	Zone	Type any desired zone name.
Zone Channel Assignment - 1	Channels	Channel name	Type any desired channel name.
		Personality Type	Trk
		Personality #	1
		Talkgroup #	Not applicable.
		Talkgroup	Not applicable.

IMPORTANT: You can preconfigure the HPD modem with several trunking systems with different Home System IDs. The requirement is that at least one system is predefined.

4.3.2
Configuring Mobile Data Device

Prerequisites: To support the Status Applet and Connection Manager applications, the mobile data device must be running either Windows Vista with Service Pack 2 (SP2), Windows 2000 or Windows 7 operating system. The Windows 2000 operating system also requires Service Pack 2 and requires a PPPoE driver to be installed (to support the PPPoE protocol if an Ethernet connection is made to the HPD modem). If Windows power management features are desired (S3 Standby state), the four operating systems require installation of additional Motorola provided software. SNMP/SNMP Trap Service must be enabled for the Status Applet to work properly (if not already configured).

When and where to use: The following procedure explains the overall process to configure a mobile data device for HPD operation with the Connection Manager and Status Applet on a Windows-based operating system. The Status Applet and Connection Manager are installed together as a single package onto the mobile data device. For additional details about installation and configuration requirements, see the *Status Applet Online Help*.

Procedure:

1 If you want to use the Status Applet and Configuration Manager applications, verify that the mobile data device has the appropriate operating system and required service pack or drivers as necessary.

- Window Vista with Service Pack 2 (SP2)
- Windows 2000 with Service Pack 2 (SP2) and a PPPoE driver for Ethernet connection to the HPD modem
- Windows 7

2 Verify that the SNMP Service and SNMP Trap Service are enabled.

   a In Microsoft Windows, select **Control Panel** → **Administrative Tools** → **Services**.

   b In the **Configuring SNMP Services** window, select **SNMP Service** from the list.

   c If the **Startup Type** is not set to **Automatic**, right-click the row and from the pop-up menu, select **Properties**. In the **Startup Type** field, select **Automatic**. Click **OK**.

   d In the upper left corner of the screen, select **Start** to start the service.

   e Configure the **SNMP Trap Service** item in the same manner. Configure the **Startup Type** as **Automatic** and start the service if necessary.

3 Run the setup program on the Status Applet CD to start the installation. When the first setup window appears, click **Next**.

4 Select a destination folder for the Status Applet files. Click **Next**.

5 In the **MSU IP Address** field, enter the IP address of the HPD modem.

   The Status Applet uses this IP address to send data traffic through the HPD modem.

6 Select your connection type.

   - If you are using a USB connection to the HPD modem, select **PPP**.
   - If you are using an Ethernet connection, select **PPPoE**.

7 If you want the Status Applet and Configuration Manager start automatically when the mobile data device starts up, select the **Select Autostart Status Applet on Windows Startup** check box.

8 Click **Next** to continue to start the installation.

9 After the installation is complete, click **Finish** to close the setup program.

10 Install any other applications that are needed for the users on the mobile data device.

4.3.2.1
Configuring Communication Manager

When and where to use: The Communication Manager configuration defines how the Communication Manager connects and communicates with the HPD modem. These settings may be changed after the initial installation to configure a different IP address for the HPD modem, automatically start the Communication Manager, or reconfigure the link options. See the *Communication Manager Online Help* for additional details about these settings.

Procedure:

1 If the Communication Manager icon is not located in the system tray, open the Status Applet.

   The Status Applet opens and the Communication Manager icon is displayed in the system tray.

2 Right-click on the Communication Manager icon and select **Configuration Settings...** from the pop-up menu, or double-click the icon to open the configuration window.

   The Communication Manager Configuration window appears.

3 Check and update any necessary settings. See the following table and the *Communication Manager* online help for more information about these settings.

4.3.2.2

Communication Manager – Configuration Window Settings

The following table explains each of the fields that can be configured in the Communication Manager configuration window. For more information, see the online help that is supplied with the Communication Manager.

Table 10: Communication Manager – Configuration Window Settings

Field	Description
Link Options	Select **Use PPP Over USB** if connecting to an HPD modem through a USB cable. Otherwise, select **Use PPPoE** if connecting to the HPD modem through an Ethernet cable.
Link Reconnect – Reconnect Attempts	This setting defines the maximum number of retries (up to 10) that the Connection Manager tries when connecting with the HPD modem. After the maximum number of attempts, the Connection Manager considers the link to the HPD modem is not available and displays a pop-up window indicating the problem.
Link Reconnect – Time Between Reconnect Attempts	This setting defines the number of seconds that should elapse between retries when establishing a connection with the HPD modem. This setting can be configured for 1-300 seconds.
SNMP Options – SNMP Request Retries	This setting defines the maximum number of SNMP request retries (2-20) that the Communication Manager when establishing an SNMP session with the HPD modem. A pop-up window is displayed if the maximum number of retries fails during a session connection.
SNMP Options – SNMP Request Timeout	This setting defines the timeout length that the Communication Manager uses when establishing an SNMP session with the HPD modem.
Modem IP Address	This field should be configured with the IP address of the HPD modem.
Run this program when Windows starts	This checkbox can be selected if the Communication Manager should automatically be started when Windows is started.

4.4

Customer Enterprise Network Configuration Guidelines

The customer enterprise network configuration must be defined by your organization. The following sections explain a number of general guidelines that may be considered when setting up the customer enterprise network to work with the HPD system.

The CEN must include a border gateway that is configured with IP-IP tunneling to the GGSN. This requires a virtual port to be configured in the border gateway that maps to the IP address of the GGSN. If the optional network interface barrier solution is being used, then additional configuration considerations are required for the firewall. For routing traffic to other CENs, it is suggested that the border gateway use either NAT or IP-IP tunneling to the other CENs. The border gateway may be supplied by Motorola Solutions or by your organization. If supplied by Motorola Solutions, the border gateway is pre-configured at the factory.

The system infrastructure uses many addresses in the 10.x.x.x and 172.x.x.x networks. Ideally, these should not be used for translated addresses in the DMZ, and if they are, then considerable care should be taken in coordinating exactly which addresses are used. The best addresses to use would be in the 192.168.x.x range if they are available and not used in any of the CENs.

4.4.1
RADIUS Server Guidelines

The HPD feature supports user authentication between MSUs and a RADIUS server on the CEN. If configured, the GGSN can pass user authentication credentials and responses between the MSUs and RADIUS server during context activation. The type of RADIUS server used (if any) and the configuration of the server is left to your organization. The system can support PAP and CHAP authentication protocols.

CAUTION: If using CHAP authentication, disable the ability to store the password on the Radius server. If the server is configured to store the password, the subscriber is unable to context activate.

The GGSN should be defined as the Remote Authentication Server. The common secret key should be provisioned in both the GGSN and RADIUS server.

RADIUS users should be defined for each MSU assigned to the CEN. This condition includes both the mobile data devices and automatic vehicle location applications (optional) that are assigned to the CEN. The authentication credentials used must be coordinated between the MSU and the RADIUS server.

Both a primary and secondary RADIUS server can be defined in the GGSN configuration for each APN/CEN. The RADIUS server may also be designated as a DHCP server to assign dynamic IP addresses to MSUs.

4.4.2
DHCP Server Guidelines

The system can be configured to request dynamic IP addresses from a DHCP server on the CEN during MSU context activations. The GGSN may be configured with the addresses of both a primary and secondary DHCP server. The type of DHCP server used (if any) and the configuration of the server is left to your organization. The RADIUS server can be configured as a DHCP server to provide dynamic IP addresses.

If configured, the GGSN makes a request from the DHCP server with an IP address within the boundaries of the IP address pool. This IP address used by the GGSN must be coordinated with the provisioned pool of IP address pool in the DHCP server.

4.4.3
DNS Server Guidelines

The HPD feature supports Domain Name Service (DNS) updates with a name authority DNS server on the CEN. This provides dynamic mapping of a name string, known as a Fully Qualified Domain Name (FQDN) to the IP address that has been assigned or approved (in the static IP addressing case) for an MSU. This allows the customer network hosts to address MSUs using that MSUs domain name. The DNS update also includes the reverse mapping of the IP address to the FQDN.

The FQDN is formed from multiple components of statically configured information. Statically configured information includes a system owner prerequisite string (such as *hpd.cen20*) and what is called the Mobile Station International Subscriber Directory Number (MSISDN). The FQDN is in the form of <MSISDN>.<System Owner Prerequisite String>.

The MSISDN is assigned to a mobile host upon activation. The components of the MSISDN include the system ID, WACN ID, and digits from the MSU's layer 2 ID. These components are translated from their hexadecimal values nibble by nibble (half a byte or 4 bits at a time) into an ASCII character to form an ASCII MSISDN string. This is then combined with the system owner prerequisite string to create the FQDN (such as *c620100000e0df659f.hpd.cen20*).

The type of DNS solution used (if any) is left to your organization. The GGSN can be provisioned to provide updates during MSU context activations to one DNS server per CEN.

This page intentionally left blank.

Chapter 5

HPD Overlay Optimization

This chapter contains the system-level optimization procedures and recommended settings relating to HPD Overlay.

5.1 Enhancing Performance of TCP Applications

TCP is an end-to-end, connection-oriented protocol that is used by many services and applications. TCP-based services include SFTP, HTTP, telnet, and SMTP. Many off-the-shelf commercial applications also use TCP for flow control and end-to-end confirmation of packet delivery.

As a protocol, TCP was originally designed for use over wired networks. Wireless networks (like the HPD system) have different attributes such as random packet loss, latency, and variable bandwidth that can have an impact on the performance of TCP-based applications.

To enhance end-user performance and reduce radio channel bandwidth utilization, Motorola Solutions highly recommends installing the following software on the hosts and mobile data devices.

- TCP optimization software
- Web acceleration software
- Compression software

If TCP-based applications are running over the network, the optimization software optimizes packet transmissions for wireless transport and minimizes TCP acknowledgment traffic. Web acceleration software can provide enhanced performance for browsing and downloading content from web servers. Compression software helps file transfers to be made more quickly while using less total bandwidth on the system.

If custom applications are being developed, it is recommended that the applications use User Datagram Protocol (UDP) when possible. UDP is a simpler protocol that does not perform packet acknowledgments, congestion control, or retransmission of lost or damaged packets. It is a connection-less protocol that does not have any of the wireless performance issues that are experienced by TCP-based applications. Since UDP does not provide flow control, retransmission, and end-to-end confirmation of traffic, any UDP-based applications would have to perform this functionality at higher layers, if necessary.

Any handling or control of the TCP-based applications is outside the scope of the HPD system. The end-to-end TCP connections, flow control, and retransmissions are handled exclusively by the customer network hosts and the mobile data devices. The HPD system only provides the wireless medium between the MSUs and the customer hosts.

This page intentionally left blank.

Chapter 6

HPD Overlay Operation

This chapter details tasks that you perform once the HPD Overlay is installed and operational in an IV&D system.

6.1 Connecting a Mobile Data Device for HPD Service

When and where to use: The following procedure explains how to use the Connection Manager on a mobile data device to establish a connection with the customer enterprise network.

Procedure:

1. Turn on the HPD modem and mobile data device.

   The HPD modem registers with the system upon power-up. If the Connection Manager is configured to automatically start, it attempts to establish an active context with the system.

2. If the Connection Manager is not configured to automatically power-up, double-click the Status Applet icon or select the Status Applet from the Start menu.

   The Status Applet opens and the Connection Manager icon is displayed in the system tray. A login pop-up window appears.

3. Type the appropriate user name and password into the login window. If you wish to store the password, select the **Save Password** option. This option prevents you from entering the password during each login.

   CAUTION: If using CHAP authentication, do not store the password - it blocks the ability of the subscriber to context activate.

4. Click **OK** to initiate the context activation request.

   The Connection Manager icon turns green and a pop-up message appears indicating a successful context activation.

5. Click **OK** to close the context activation pop-up message.

   The Status Applet shows that the RF Registration Status is Registered and the Data Registration is Active.

6. If there are any problems, the Connection Manager makes additional attempts to context activate. After the maximum number of retries are made (according to the Connection Manager configuration), an error window indicates that the connection was unsuccessful. Check the Connection Manager and Status Applet for details.

6.2 Using MSU Applications with HPD Service

After a mobile data device has been context activated, the IP path to hosts on the CEN is available to the MSU. The MSU can begin using IP-based applications and sending inbound traffic over the IP bearer service transparently, as if the MSU were physically connected with the customer enterprise network.

6.3
Using CEN Applications with HPD Service

For a CEN host to send outbound traffic, the destination MSU must be context activated. If the MSU is not context activated with the CEN, then the host receives an ICMP response from the system. Otherwise, the CEN host can communicate with the MSU in a transparent fashion as if the MSU were physically connected on the customer enterprise network.

6.4
Terminating Connection with HPD Service

When and where to use: The following procedure explains how to terminate the context on the mobile data device using the Connection Manager and Status Applet.

Procedure:

1. Right-click on the Connection Manager icon and select **Disconnect PPP Session** from the pop-up menu.

   The Connection Manager icon turns yellow, indicating that the context is deactivated. A pop-up message indicates that the context is deactivated. The Status Applet indicates that the HPD modem is registered and the data registration service is no longer active.

2. Click **OK** to close the pop-up window.
3. To turn off the HPD modem, close the Status Applet and Connection Manager if HPD services are no longer required.

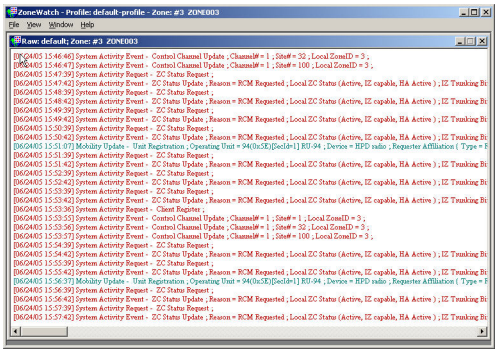
6.5
Checking for MSU Registration and Context Activation on the System

Operators using fixed network equipment may wish to check and monitor the online status of MSUs in the system. To determine if an MSU is registered, you can check for registration update messages in ZoneWatch. To check both the registration status and context status for an MSU, you can check the mobile device information through the PDG Local Configuration Interface at the home zone of the MSU.

6.5.1
Checking MSU Registration Status Through ZoneWatch

Registration events can be viewed through the Raw Display window in ZoneWatch. As shown in the following figure, mobility update messages can be used to display when an MSU has registered with the system. ZoneWatch only shows registration status messages for MSUs within the zone. Deregistration events for HPD modems within the zone and any other events for MSUs outside the zone are not displayed in the Raw Display window.

Figure 28: ZoneWatch – MSU Registration Messages



6.5.2
Checking MSU Registration Status Through Affiliation Display

When and where to use: The Affiliation Display application can be used to view MSUs that are affiliated within a zone. The following procedure explains how to check for affiliated MSUs using the Affiliation Display application.

Procedure:

1. Open the Affiliation Display application.
2. To display the status of an individual MSU, select **Radio Viewer** from the **View** menu. Type the radio ID or alias for the MSU in the text box of the Radio Viewer to display the status of that particular MSU within the zone.
3. To display MSUs that are affiliated with sites within the zone, select **Site Viewer** from the View menu.
4. In the Site Viewer, click the **Add All Sites** button to show all the sites within the zone. The number of affiliated radios (MSUs) is shown for each site.
5. To view all the MSUs at a site within the list, select the row for the site and click the **View Radios** button.

6.5.3
Checking MSU Context Status with PDG Local Configuration Interface

A Mobile Subscriber Unit (MSU) must be context activated before hosts on the Customer Enterprise Network (CEN) can send traffic to the MSU. The context activation status for MSUs can be viewed in the system through the PDG Local Configuration Interface. This interface displays the registration and context activation status only for MSUs that are provisioned and mapped to the same zone where the PDG is located. When logging into this interface, be sure to select the appropriate PDG that is in the home zone of the MSU.

Procedure:

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

   A dialog box appears prompting for an IP address, user name, and password.

2. Log on:

   a In the IP address field, type the IP address of the ESXi server where the PDG is located.

   b In the user name field, type `root`.

c In the password field, type the root password of the ESXi server.

d Click **Log in**.

The vSphere Client Inventory window appears

3 Select the PDG virtual machine from the left pane. Click the Console tab.

The Console tab appears.

4 Click on the screen. Press ENTER.

The Login screen appears.

5 Type the appropriate user name (`root`) and password. Press ENTER.

You are successfully logged in and the command prompt appears.

6 Type `admin_menu`. Press ENTER.

The main PDG administrator menu appears.

7 Select **Application Administration**. Press ENTER.

The Application Administration menu appears.

8 Select **Application Specific Management and Operations**. Press ENTER.

The Application Specific Management and Operations menu appears.

9 Select **PDG Local Configuration**. Press ENTER.

The PDG Local Configuration menu appears.

10 Select **View Mobile Device Information**. Press ENTER.

The View Mobile Device Information window appears.

11 Type the radio ID for the MSU to be checked. Select **Submit**. Press ENTER.

NOTICE: If the MSU is not registered or context activated, it does not display any active context information.

The mobile device information appears for the selected MSU. The window displays the registration status and context information, including the provisioned and currently used IP address for the MSU, and the APN for the CEN that the MSU is active with.

12 To exit from the administrator menu, type q and press ENTER.

The command prompt appears.

6.6 Verifying Performance

To verify HPD Overlay performance, perform the tests listed in Preventive Maintenance Procedures for HPD Overlay on page 91.

6.7 InfoVista Reports for HPD Devices

InfoVista is a customizable performance management application that interfaces with the HPD PDG and other equipment in the system. The application can produce a number of valuable reports for

monitoring different aspects of HPD network performance. The following sections describe the InfoVista reports that are available for HPD-related equipment.

6.7.1
HPD PDR InfoVista Reports

InfoVista can generate the following reports for the HPD PDR:

- Roaming and Registration Statistics Report
- ICMP Traffic Report
- IP Bearer Statistics Report
- Message Overload Protection Statistics Report

6.7.1.1
Roaming and Registration Statistics

The Roaming and Registration Statistics report shown in the following table indicates registration events, mobility queries, and InterZone roaming events.

Table 11: InfoVista – HPD PDR Roaming and Registration Statistics

Measurement	Description
SNDCP Registration Requests received by the PDR	Indicates the number of SNDCP registration requests received by the HPD PDR.
Queries sent to zone controller from the PDR	Indicates the number of mobility queries that the HPD PDR has sent to the zone controller.
Queries sent to zone controller with no Response	Indicates the number of queries sent to the zone controller from the HPD PDR with no response.
Number of the subscriber interzone roams	Indicates the number of the subscriber interzone roams being handled by the HPD PDR.

6.7.1.2
ICMP Traffic

The ICMP Traffic report displays the number of inbound/outbound ICMP messages being sent and indicates the total number of ICMP messages that have been generated and discarded by the HPD PDR.

The following table provides a description for the messages on the ICMP Traffic report.

Table 12: InfoVista – HPD PDR ICMP Traffic

Measurement	Description
Inbound ICMP messages	Indicates the number of inbound ICMP messages from MSUs that have been forwarded by the HPD PDR.
Outbound ICMP messages	Indicates the number of outbound ICMP messages forwarded to MSUs by the HPD PDR.
ICMP messages discarded	Indicates the number of ICMP messages that have been discarded.
ICMP messages generated	Indicates the number of ICMP messages that have been generated by the HPD PDR.

6.7.1.3

IP Bearer Statistics

The IP Bearer Statistics report displays inbound/outbound HPD activity and indicates the number of IP packets that have been discarded by the HPD PDR.

The following table provides a description of the statistics on the IP Bearer Statistics report.

Table 13: InfoVista – HPD PDR IP Bearer Statistics

Measurement	Description
Outbound IP Packets	Indicates outbound IP packets forwarded by the HPD PDR that are destined for MSUs.
Inbound IP Packets	Indicates inbound IP packets from the MSUs that have been forwarded by the HPD PDR.
IP Packets discarded	Indicates inbound/outbound IP packets that have been discarded due to ingress filtering or bad IP headers.
Broadcast IP Packets	The number of broadcast messages received by the PDR.
Broadcast Packets Discarded	The number of broadcast messages received by the PDR that were not deliverable (and were generated ICMP error messages).
Broadcast Packets Dropped	The number of broadcast messages received by the PDR that were not deliverable, due to buffer overload (and were not generated ICMP error messages).

6.7.1.4

Message Overload Protection Statistics

The Message Overload Protection Statistics report displays the number of dropped messages due to overload protection.

The following table explains each of the measurements shown in the report.

Table 14: InfoVista – HPD PDR Message Overload Protection Statistics

Measurement	Description
Dropped Inbound Messages	Indicates the total number of Dropped Inbound Messages that have been discarded by the HPD PDR due to message overload conditions.
Dropped Outbound Messages	Indicates the total number of Dropped Outbound Messages that have been discarded by the HPD PDR due to message overload conditions.
Dropped UDP Packets	Indicates the total number of Dropped UDP Messages that have been discarded by the HPD PDR OS due to message overload conditions.
Dropped Context Activation Requests	Indicates the total number of context activation requests discarded by the PDR due to message overload.

6.7.2

HPD RNG InfoVista Reports

InfoVista can generate the following reports for the HPD RNG:

- Context Activation Report
- HPD Packet Data Service – UP Connect Report
- HPD Packet Data Service – SDU Transmissions Report
- Channel Resources Report
- Inbound and Outbound Data Profile Report
- Mobility Report

6.7.2.1

Context Activation Report

The Context Activation report shown in the following table indicates the number of context activation requests and responses handled by the HPD RNG.

Table 15: InfoVista – HPD RNG Context Activation

Measurement	Description
Add User Requests received from PDRs (Add User Rx)	Indicates the number of Add User Requests received from all the HPD PDRs.
Delete User Requests received from PDRs (Delete User Rx)	Indicates the number of Delete User Requests received from all the HPD PDRs.
New User Responses received from PDRs (New User Res Rx)	Indicates the number of New User Responses received from all HPD PDRs.
Deactivate User Messages sent to PDRs due to Standby Timer expiration (Deactivate Tx STBY Exp)	Indicates the number of Deactivate User Messages sent to all HPD PDRs due to Standby Timer expiration.
Deactivate User Messages sent to PDRs due to Mobility Pushes (Deactivate Tx Push)	Indicates the number of Deactivate User Messages sent to all HPD PDRs due to Mobility Pushes.
Facility Indications sent to PDRs (Facility Tx)	Indicates the number of Facility Indications sent to all Packet Data Routers.

6.7.2.2

HPD Packet Data Service – UP Connect Report

This report has two graphs showing user plane connection events to MSUs in the zone. The first graph shows normal user plane connection activity. The second graph shows abnormal user plane connection activity. The first three measurements shown in the following table are normal activity. The last three measurements are abnormal activity.

Table 16: InfoVista – HPD Packet Data Service – UP Connect

Measurement	Description
Successful UP Connects Setup. (UP Connects)	Indicates the number of successful user plane connections (UP Connects) across all MSUs.

Table continued…

Measurement	Description
Number of UP Connects received from all MSUs. (UP Connects Rx)	Indicates the number of UP Connects received from all MSUs.
Number of UP Connects sent to all MSUs. (UP Connects Tx)	Indicates the number of UP Connects sent to all MSUs.
UP Connects received from all MSUs in OPEN (UP Connects Rx in OPEN)	Indicates the number of UP Connects received from all MSUs in OPEN state.
UP Connects sent to all MSUs in OPEN (UP Connects Tx in OPEN)	Indicates the number of UP Connects sent to all MSUs in OPEN state.
UP Disconnects sent to all MSUs. (UP Disconnects)	Indicates the number of UP Disconnects sent to all MSUs.

6.7.2.3
HPD Packet Data Service – SDU Transmissions Report

The InfoVista - HPD Packet Data Service – SDU Transmission report shown in the following table presents information about HPD RNG packet data channel access SDU transmissions.

Table 17: InfoVista – HPD Packet Data Service – SDU Transmissions

Measurement	Description
Tx and Rx Of 1 SDU from startup (Tx/Rx Of 1 from startup)	Indicates the number of transmissions and receptions of exactly 1 SDU from startup.
Tx and Rx Of 2 SDUs from startup Access (Tx/Rx Of 2 from startup)	Indicates the number of transmissions and receptions of exactly 2 SDUs from startup.
Tx and Rx Of 3 SDUs from startup (Tx/Rx Of 3 from startup)	Indicates the number of transmissions and receptions of exactly 3 SDUs from startup.
Tx and Rx Of 4 Or More SDUs from startup (Tx/Rx Of 4 Or More from Startup)	Indicates the number of transmissions and receptions of 4 or more SDUs from startup.

6.7.2.4
Channel Resources Report

The Channel Resources report shown in the following table presents information about HPD channel usage. The report includes two graphs. The first graph displays channel assignment activity and the second graph displays channel usage activity.

Table 18: InfoVista – Channel Resources

Measurement	Description
SRP Channel Requests sent to Sites (Chan Req Tx)	Indicates the number of SRP Channel Requests sent to all HPD remote sites.
SRP Channel Grants received (Chan Grant Rx)	Indicates the number of SRP Channel Grants received from all HPD remote sites.
SRP Response Messages received (Chan Resp Rx)	Indicates the number of SRP Response Messages received from all HPD remote sites.

Table continued...

Measurement	Description
Segments requested (Segs Requested)	Indicates the number of SRP Segments requested for transmission through SRP Channel Requests.
Segments granted (Segs Granted)	Indicates the number of SRP Segments granted for transmission through SRP Channel Grants.

6.7.2.5
Inbound and Outbound Data Profile Report

The Inbound and Outbound Data Profile report shown in the following table presents information about HPD RNG inbound and outbound data traffic. The report includes two graphs. The first graph displays the outbound data profile and the second graph displays the inbound data profile.

Table 19: InfoVista – Inbound and Outbound Data Profile

Measurement	Description
LLC Segments transmitted to MSUs (OB PDU Tx)	Indicates the number of LLC Segments transmitted to all MSUs.
LLC Segments retransmitted to MSUs (OB PDU Rtry)	Indicates the number of LLC Segments retransmitted to MSUs.
LLC ACKs received from MSUs (IB ACK Rx)	Indicates the number of LLC Response Messages (ACKs/NACKs/Selective ACKs) received from all MSUs.
LLC ACK Timeouts (IB ACK TMO)	Indicates the number of LLC Response Message Timeouts in the RNG.
PDGP SDUs transmitted to MSUs (OB SDU Tx)	Indicates the number of PDGP SDUs transmitted to all MSUs.
LLC Segments received from MSUs (IB PDU Rx)	Indicates the number of LLC Segments received from all MSUs.
LLC Segments retransmitted by MSUs (IB PDU Rtry)	Indicates the number of LLC Segments retransmitted by all MSUs.
LLC ACKs transmitted to MSUs (OB ACK Tx)	Indicates the number of LLC Response Messages (ACKs/NACKs/Selective ACKs) transmitted to all MSUs.
PDGP SDUs received from MSUs (IB SDU Rx)	Indicates the number of PDGP SDUs received from all MSUs.

6.7.2.6
Mobility Report

The Mobility report shown in the following table presents information about mobility queries and responses between the HPD RNG and the zone controller.

Table 20: InfoVista – HPD RNG Mobility

Measurement	Description
Queries sent to the zone controller (Query Tx)	Indicates the number of Mobility Queries sent to the zone controller.
Responses received from the zone controller (Response Rx)	Indicates the number of Mobility Responses received from the zone controller.

Table continued…

Measurement	Description
Queries sent to the zone controller that failed since query succeeded (Query Tx Fail)	Indicates the number of Mobility Queries sent to the zone controller that failed since last query succeeded.

6.8

Checking the Fault Tolerance Status of a High Availability PDG with UEM

If your system supports the High Availability for IV&D and HPD (HA Data) feature, perform this procedure to check the status of a Packet Data Gateway (PDG) in the Fault Tolerance application by using Unified Event Manager (UEM).

Prerequisites:
Ensure that VMware vCenter is discovered in UEM.

Procedure:

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

   In the **Type** column, the PDG is displayed as Fault Tolerant Virtual Machine. The **Managed Resources** column shows the name of the PDG virtual machine assigned during installation.
2. Select the PDG Fault Tolerant Virtual Machine.
3. From the top menu, select **View** → **Alarms**.
4. In the **Alarms** window, search for an alarm for the **Fault Tolerant Service**.

   NOTICE:
   If no alarm for the Fault Tolerant Service is displayed, it means that Fault Tolerance is enabled for the PDG and is not reporting any issues.

   UEM reports the state of the Fault Tolerant Service for each redundant PDG group separately.

   The status of the Fault Tolerant Service for the PDG virtual machine is displayed in the **Message** column.

Chapter 7

HPD Overlay Maintenance

This chapter describes periodic maintenance procedures relating to the HPD Overlay feature.

7.1 Preventive Maintenance Procedures for HPD Overlay

The following tests are recommended for preventive maintenance:

- The Site Controller reference oscillator should be checked for proper operation with the RGPS disconnected.
- Transmit Power should be verified annually.
- Transmit Modulation (EVM) should be verified annually.
- Receive sensitivity should be verified annually.
- Fans should be cleaned periodically.

In addition, the following tests are recommended to verify system performance:

- Transmit Power
- Transmit Frequency
- Transmit Modulation
- Transmit Effective Radiated Power
- Receive Levels
- Receive BER Calibrate
- Receive BER Floor
- Receive BER Sensitivity
- Receive Effective Sensitivity

7.2 Testing Site Controller

When and where to use: The reference oscillator on the GCP8000 Site Controller (SC) should be checked in order to verify that the site can operate on the SC internal reference. The following procedure describes the steps to perform the test on Site Controller.

Procedure:

1. Start the CSS application on the laptop computer.

   The CSS main screen opens.

2. Select **File** menu, then click **Read Configuration From Device** or press CTRL + R keys simultaneously.

   The CSS Connection Screen opens.

3. Perform steps 4 to 6 in the CSS Connection Screen window.
4. Set the Connection Type to **Ethernet**.

5 Set the Ethernet Settings Device IP Address to the IP address of the SC.

6 Select the **Connect** button.

NOTICE: You may need to read the SC twice to be successful.

The system presents the IP addresses for the SC. The IP address should be 10.101.<site_number>.91 for a stand-alone SC A and 10.101.<site_number>.92 for SC B.

7 Review the SC codeplug.

7.3 Transmit Tests

This section describes performance tests for transmission.

7.3.1 Setting Up for Transmit Tests

The following procedure describes how to set up the system for transmit tests.

Procedure:

1 Start the CSS application on the laptop computer.

The CSS main window opens.

2 Select the **Service** menu, then point to **Test and Measurement**.

The **CSS Test and Measurement** window opens.

3 Select the **Change to Service Mode** button.

The Base Radio goes into service mode.

4 Wait for the Base Radio to reset.

5 Verify that the Base Radio is configured as described in the Setting CSS Configuration Parameters for the GTR 8000 Base Radio (HPD) section of the *GTR 8000 Base Radio* manual.

6 Verify that the Aeroflex 3901 or 3902 Communications Analyzer is configured correctly for HPD Base Radio testing.

7 Set the Communications Analyzer for external reference:

a Select **Utils** → **Utils** → **Reference**.

b Change the **Reference** to **External**.

c Press the **TEST** button and select **HPD**.

d Press TAB until the **Rx Meter Display** tile is highlighted.

7.3.2 Testing Transmit Rated Power

The following procedure describes how to test transmit rated power. The specification calls for the Base Radio to produce Rated Power ±10% after accounting for **all** losses in the transmit path. The internal PA Output cable at 800 MHz adds 0.2 dB loss (4%).

Procedure:

1 Key the Base Radio with a V.52 16 QAM test pattern.

2 Start the CSS application on the laptop computer.

The CSS main screen opens.

3 From the **Service** menu, select **Test and Measurement**.

The **CSS Test and Measurement** window opens.

4 Set the **CSS Select Pattern To Transmit** field to **V.52**, **16-QAM**, then select the **Start Pattern Transmission** button.

Pattern transmission starts.

5 On the Communications Analyzer, press the **Reset/Acquire** button.

The wattmeter displays the forward power, frequency error, and transmit Bit Error Rate (BER).

6 Record the power reading displayed. A wattmeter reading corrected for **all** cable losses indicate the rated power ±4.6%.

7.3.3
Testing Transmit Frequency Error

The following procedure describes how to test transmit frequency error. The specification calls for Tx Frequency Error of < ±20 ppb. Multiply transmit band center frequency in MHz by 0.02 to obtain the allowable Frequency Error. For the 700 band, 770 x 0.02 = 15.4 Hz.

NOTICE: The Communications Analyzer **must** obtain a suitably accurate external 10 MHz reference such as a portable Rb standard or a Trak 9100 FDM.

Procedure:

1 Key the Base Radio with a V.52 16 QAM test pattern.

2 Start the CSS application on the laptop computer.

The CSS main screen opens.

3 From the **Service** menu, select **Test and Measurement**.

The **CSS Test and Measurement** window opens.

4 Set the **CSS Select Pattern To Transmit** field to **V.52**, **16-QAM**, then select the **Start Pattern Transmission** button.

Pattern transmission starts.

5 On the Communications Analyzer, press the **Reset/Acquire** button.

The wattmeter displays the forward power, frequency error, and transmit Bit Error Rate (BER).

6 Record the frequency error displayed.

3900 Freq Error is less than ±20ppb from the assigned transmit frequency.

7.3.4
Testing Transmit Bit Error Rate

The following procedure describes how to test transmit Bit Error Rate (BER). The specification calls for Transmit Bit Error Rate (BER) of ≤ 0.01%.

NOTICE: Tx BER is only specified for 16-QAM. QPSK reading meets the specification. 64-QAM reading is higher than specified.

Procedure:

1. Key the Base Radio with a V.52 16 QAM test pattern.
2. Start the CSS application on the laptop computer.

   The CSS main screen opens.
3. From the **Service** menu, select **Test and Measurement**.

   The **CSS Test and Measurement** window opens.
4. Set the **CSS Select Pattern To Transmit** field to **V.52**, **16-QAM**, then select the **Start Pattern Transmission** button.

   Pattern transmission starts.
5. On the Communications Analyzer, press the **Reset/Acquire** button.

   The wattmeter displays the forward power, frequency error, and transmit Bit Error Rate (BER).
6. Record the 3900 Rx BER reading.

   3900 Rx BER ≤ 0.01% (1x10-4)

7.3.5
Testing Transmit Modulation

Prerequisites: The specification calls for a Transmit EVM (RMS) average value of ≤ 10%.

NOTICE: The Communications Analyzer measures Tx EVM about 2% higher than the factory test equipment. There is enough margin in the normal operation of a Base Radio that it should pass the 10% EVM specification using the Communications Analyzer.

When and where to use: The following procedure describes how to test transmit modulation.

Procedure:

1. On the Communications Analyzer, qualitatively assess the Constellation plot.

   You should see the points cluster around the blue + marks.
2. Expand the Rx Meter Display.
3. Press the **Reset Acquire** softkey and wait for 30 seconds.

   The Communications Analyzer displays the average EVM, maximum EVM, Symbol Clk Err, and Occupied BW values. EVM average should be ≤ 10%. There are no specifications for the other values.
4. Record the values displayed.
5. Minimize the RX Meter Display.
6. Maximize the Constellation tile.

   The Communications Analyzer displays the Carrier Feed, average Ampl Imbal, and Phase Mis values.
7. Record the values displayed.
8. Minimize the Constellation tile.

7.4
Receive Tests

This section describes performance tests for reception.

NOTICE: If you have dekeyed the transmitter, it must be rekeyed with a 16-QAM Test Pattern.

7.4.1
Setting Up for Receive Tests

The following procedure describes how to set up the system for receive tests.

Procedure:

1. Start the CSS application on the laptop computer.

   The CSS main screen opens.

2. From the **Service** menu, select **Test and Measurement**.

   The **CSS Test and Measurement** window opens.

3. Verify the configuration of the Base Radio and the Aeroflex 3901 or 3902 Communications Analyzer, as described in Setting Up for Transmit Tests on page 92.

7.4.2
Receive BER Calibration Test

Prerequisites: The specification calls for a CSS BER = 1.0% ±0.001%.

When and where to use: The following procedure describes how to test-receive BER calibration.

Procedure:

1. Set the RF Generator input level into the GTR8000 at –70 dBm. Account for your test cable loss.
2. On the Communications Analyzer, set the RF Gen Level to –70 + Cable Loss. As an example, for a 1.5 dB cable loss, the RF Gen Level would be – 68.5 dBm.
3. On the **CSS Test and Measurement** screen, set the **Sampling Period** to 10 seconds.
4. In CSS, click the **Start BER Measurement** button and wait for 30 seconds.
5. Record the CSS Bit Error Rate (%) value.

   CSS BER = 1.0% ±0.001%.

6. In CSS, click the **Stop BER Measurement** button.

7.4.3
Receive BER Floor Test

Prerequisites: The specification calls for a CSS BER ≤ 0.01%.

When and where to use: The following procedure describes how to test-receive the BER floor.

Procedure:

1. Set the Communications Analyzer so that PATTERN=O.153 Std.
2. In CSS, click the **Start BER Measurement** button and wait 30 seconds.

3 Record the CSS Bit Error Rate (%) value and the CSS Received Signal Strength (dBm) value for the Branch you are connected to. (RxA = Branch1, RxB = Branch2).

   CSS BER ≤ 0.01% ; CSS RSSI = -70 dBm ± 5 dB.

4 In CSS, click the **Stop BER Measurement** button.

7.4.4
Testing Receive Sensitivity for Stand-alone Base Radio

Prerequisites: The specification calls for RF Gen Level – Cable Loss ≤ -104 dBm.

When and where to use: The following procedure describes how to test a receive sensitivity for Stand-alone Base Radio.

Procedure:

1 Change the CSS Sampling Period (sec) to 1 second.

2 On the Communications Analyzer, set the RF Gen Level to -100 dBm.

3 In CSS, click the **Start BER Measurement** button.

4 Wait a few seconds for the CSS Bit Error Rate (%) to update and stabilize. Start dropping the RF Gen Level in 1 dB increments until the CSS Bit Error Rate (%) approaches 1%. Remember to wait a few seconds after each level change for the CSS Bit Error Rate (%) to update.

5 Adjust the RF Gen Level in 0.1 dB increments to achieve as close to a 1% BER as possible, again waiting for the BER to update before changing the RF Gen Level.

6 Record the RF Gen Level and the CSS Received Signal Strength (dBm) value.

   RF Gen Level corrected for cable loss ≤ -104 dBm.

7 In CSS, click the **Stop BER Measurement** button.

8 In CSS, select **Service** menu, then point to **Test and Measurement**.

   The CSS Test and Measurement screen opens.

9 Ensure that transmit test patterns are turned **off**.

10 Disconnect all test cables from the Base Radio. Reconnect all normal Base Radio cables.

11 Repeat the tests in this section on all HPD channels at the site until all HPD channels are completed.

Chapter 8

HPD Overlay Troubleshooting

This chapter provides fault management and troubleshooting information relating to HPD Overlay.

8.1 Troubleshooting Tools

The following tools and applications may be available for viewing monitoring HPD equipment and troubleshooting suspected problems.

- InfoVista
- Status Applet and Connection Manager

NOTICE: For failure and recovery procedures of the Dynamic System Resilience feature, refer to the *Dynamic System Resilience* manual.

8.1.1 InfoVista

InfoVista provides detailed statistics for many High Performance Data (HPD) events. When troubleshooting HPD services or individual components, analyze alarms in the network fault management application and any related InfoVista reports to determine the cause of the problem.

The following reports related to HPD operation can be checked through InfoVista:

- Channel Resources Report
- Context Activation Report
- HPD Packet Data Service – SDU Transmissions Report
- HPD Packet Data Service – UP Connect Report
- ICMP Traffic Report
- Inbound and Outbound Data Profile Report
- IP Bearer Statistics
- Message Overload Protection Statistics
- Mobility Report
- Roaming and Registration Statistics

8.1.2 Troubleshooting HPD Services at the HPD Modem, Mobile Data Device, and Subscriber

The Status Applet resides on the mobile data device and provides diagnostic information for mobile subscribers that have communication difficulties. The applet displays the registration status of the High Performance Data (HPD) modem, the context activation status, the received signal strength from the base radio, and HPD modem operating parameters. The Connection Manager provides an icon in the system tray that indicates the status of the connection to the HPD modem and the status of the context.

Procedure:

1. Verify that the HPD modem is powered and the mobile data device is connected.
2. Check the color of the Connection Manager icon in the system tray. If the icon is yellow, the mobile data device has an active Point-to Point Protocol (PPP) connection to the HPD modem, but is not registered and context activated with the system. If the icon is red, there is no active PPP connection with the modem. Try to connect to the HPD modem.
3. Check the Connection Manager configuration settings.
   - When switching from a non-authenticated to authenticated system, clear the **Enable Auto-Dialer Feature** option and select **Enable Authentication**. Then select **Connect PPP session**. When the login screen appears, enter your login credentials.
   - When switching from authenticated to a non-authenticated system, clear the **Enable Authentication** option and select **Enable Auto-Dialer Feature**.

   Verify the link options. If necessary, increase the reconnection attempts or reset the HPD modem and/or mobile data device.
4. In Customer Programming Software (CPS), check the HPD modem configuration.
5. In the Status Applet, check the signal strength on the received channel. If there is a weak or no signal within the coverage area, determine whether there is a problem with the MSU or with the system (HPD base radio).
   - If the mobile subscriber unit (MSU) can receive good signals from other sites or channels, check the status and configuration of the HPD base radio. If necessary, check the frequency alignment and output power characteristics for the HPD base radio.
   - If the MSU cannot receive good signals from other channels, check the HPD modem configuration and consider checking the receiver sensitivity for the HPD modem if necessary.
6. If the signal strength is nominal, check the **RF Registration Status** field.

   If the HPD modem is not registered, the modem may be trying to register with one of the following parameters that is not compatible with the settings in Provisioning Manager:
   - Radio ID
   - WACN ID
   - System ID

   If the MSU is not registered, it may be due to one of these reasons:
   - The MSU is at a site in local mode.
   - The MSU is attempting to register at a restricted site (site access denial).
   - The MSU does not receive any response from the system before its timeout expires.
7. Check the **Data Registration Status** field.

   If the status is not active, it may be due to one of the following reasons:
   - The MSU has improper authentication credentials.
   - The site is in local mode.
   - The local RNG or home PDR has failed.
   - The dynamic IP address pool is empty.
   - The MSU is not configured for HPD service in the system.
   - An incorrect Access Point Name (APN) has been used.
   - A static address conflict has occurred.

8.2

Wide Area and Local Area Modes

High Performance Data (HPD) sites can operate in two modes: wide area or local area mode.

Wide area mode

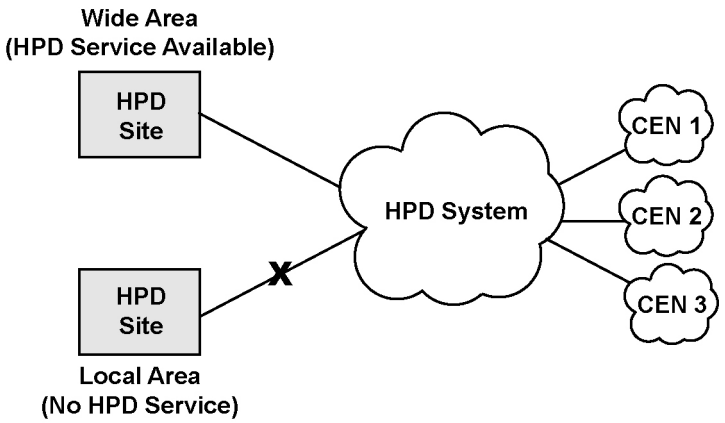
The normal operating mode for the HPD site. When an HPD site is operating in wide area mode, the site has connection with the zone controller and the serving HPD Radio Network Gateway (RNG) that is in the zone. The HPD site can handle registration requests and provide data services to the registered mobile subscriber units (MSU).

Local area mode

When an HPD site is operating in local area mode, registration and data services are not available at the site. An HPD site can be in local area mode before site initialization, during link or component failures, or when requested by a network management user through Unified Network Configurator (UNC).

NOTICE: MSUs always try to remain in wide area coverage. When an HPD site goes into local area mode, MSUs that were operating at this site try to register at a valid HPD remote site that is operating in wide area mode.

Figure 29: Wide Area and Local Area Modes



8.3

Registration Failures

A Mobile Subscriber Unit (MSU) attempts to register when powered up or when entering the coverage area of the system. If a registration request is unsuccessful, a reject message is sent to the MSU indicating the general reason for the failure.

Three categories of registration failures can occur.

Registration Refused

When an MSU receives a Unit Registration Refused response, the MSU remains unregistered and does not attempt to find another site or channel. The MSU does not attempt to register again until the user performs a specific action such as shutting down and turning the radio back on. An MSU may be refused due to one of the following reasons:

- The MSU sent an invalid radio ID or duplicate radio ID.
- The zone controller cannot create or retrieve the individual record for the MSU.

Registration Denied

Upon receiving a Unit Registration Denied response, the MSU remains unregistered and leaves the site immediately. The MSU invalidates the site and looks for another site. The MSU then attempts to register again when it finds another site. The Unit Registration Denied condition occurs due to one of the following reasons:

- The MSU is trying to access the wrong system (a wrong WACN or system ID is sent).
- The MSU is trying to register at an invalid site according to the site access denial settings in Provisioning Manager.

Registration Timeout

If an MSU sends a registration request and does not receive a response from the system within a specified time (10 seconds by default), the MSU automatically decides to either stay on the current channel or try a new channel. The MSU then tries to register again. If seven failed registration attempts have been made on a particular channel, the MSU marks the channel and temporarily removes it from its stored list of available channels.

8.4 Context Activation Failures

If a context activation is unsuccessful, the system denies access to High Performance Data (HPD) services and sends the mobile subscriber unit (MSU) a reject message. The context activation reject indicates the reason for the reject (if any).

Depending on the type of reject, the MSU behaves in the following ways:

- The MSU attempts another context activation immediately.
- The MSU waits 5 minutes before attempting another context activation.
- The MSU does not attempt context activation until the MSU is powered down and restarted.

When the following reject message is received, the MSU performs another context activation immediately. Additional attempts are allowed.

User authentication failed
The user authentication has failed.

When any of the following reject messages are received, the MSU holds off for 5 minutes before attempting another context activation. These reject messages may indicate that codeplug settings need to be updated in the MSU.

Any reason
The MSU has been rejected for some general reason.

MRC not provisioned for packet data
The MSU is not configured for HPD service in Provisioning Manager.

Dynamic address pool empty
The MSU has requested a dynamically assigned IP address, but the DHCP server does not have any available.

Static address not correct
The MSU has sent a static IP address that does not match the static IP address assigned for the radio record in Provisioning Manager.

Static address not allowed
The MSU has sent a static IP address that is not allowed by the system.

Temporary rejection
The system has temporarily rejected the context activation request.

Maximum number of contexts exceeded
The system is servicing the maximum number of contexts.

Access point name incorrect
The MSU has requested connection with an access point name that does not exist in the system.

When either of the following reject messages are received, the MSU disables any context activation attempts until the MSU is restarted. These reject messages may indicate significant codeplug or firmware issues that need to be updated in the MSU.

MRC DSUT (Data Subscriber Unit Type) not supported
The MSU has provided context activation information for a unit type that is not supported by the system.

SNDCP version not supported
The system has determined that the SNDCP version being used by the MSU is not supported.

8.4.1
Context Deactivation Conditions

An existing context between a mobile subscriber unit (MSU) and the customer network may be deactivated due to normal or failure conditions.

Some typical causes for a context deactivation or context renewal failure include:

- The MSU has moved out of range and the HPD Standby Timer has been exceeded.
- The HPD modem has received a discrete PPP Link Shutdown message from the mobile data device.
- The physical connection to the mobile data device has been lost.
- The HPD modem has performed a graceful shutdown.
- The Terminal Data Enabled option has been set to Disabled for the MSU.
- The HPD PDR has deactivated its context with the GGSN for some reason.
- The connection with the RNG has been lost.
- Provisioning information for the MSU has been changed or deleted.
- The GGSN or home HPD PDR has failed.
- A provisioning change or record deletion in Provisioning Manager.
- The maximum number of context renewal retries have failed.

8.5
Data Delivery Failure

IP bearer services may not be available for various reasons including component failure, registration failure, context activation failure, or deactivation of an existing context. The system or mobile subscriber unit (MSU) may also discard individual packets in certain situations. In some cases, ICMP responses are sent to the sender.

A partial list of the possible causes for IP failure or loss of individual packets includes:

- A critical component or path for HPD service has failed.
- The registration request has failed or has been rejected by the system (denied, refused, or timed out).
- Context activation was not successful or the context has been deactivated for some reason.
- The MSU has not been successfully assigned with a proper IP address.

- The maximum number of retries for the HPD traffic over the air interface has occurred (the MSU may be out of range).
- The MSU or PDR queue is full. Additional packets delivered to the queue may be discarded.
- A Network Address Translation (NAT) problem exists between the HPD modem and mobile data device.
- The individual packets do not conform to IP version 4.
- The packet address does not conform to Class A, B, or C addressing.
- The packet is larger than the Maximum Transmission Unit (MTU) allows (1500 bytes) and the `Do Not Fragment` bit has been set for the packet.

The system infrastructure does not store user datagrams beyond the time it takes to make a best attempt delivery of the datagrams. If the best effort attempt delivery fails, the datagram is discarded and an Internet Control Message Protocol (ICMP) message `Destination Unreachable: Host Unreachable` is returned to the sending host. If additional IP datagrams were queued within the HPD system for the host that was not accessible, they are discarded and ICMP `Destination Unreachable: Host Unreachable` messages are returned to the sending host.

NOTICE: ICMP messages are returned under normal operation, but some failure conditions may result in no ICMP message being returned and applications must be able to recover from that situation.

Host-generated ICMP messages are not treated the same as other IP datagrams. The HPD system does not return an ICMP message to the originating host when it fails to deliver the host-generated ICMP message. Instead, the host generated ICMP message is discarded without further processing. One exception to this is for ICMP information request messages directed to HPD system components for which an ICMP response is provided.

8.5.1
Broadcast Data Failures

The base radio reports overflow condition to the Unified Event Manager (UEM) application through the site controller (if it receives a broadcast message and there is already a previous broadcast message buffered). This occurs if the outbound buffer allocated (approximately 15 kb) for the Broadcast Agency involved is full. The PDR allocates outbound buffer on a per-subscriber basis. For the Broadcast Data, it is on a per Broadcast Agency basis.

If the PDR was unable to send the broadcast message to the RNG, or if the PDR received a negative acknowledgment for a broadcast message the PDR sent to the RNG – the PDR sends an ICMP message notifying the application initiating the broadcast message of non-delivery.

NOTICE: There is no ICMP for broadcast messages discarded due to overflow at the BR or at the PDR. Indication of such event is the overflow condition reported by the base radio or PDR to the UEM.

8.5.2
MSU is Not Authenticated

If an MSU is configured to require user authentication with a customer network RADIUS server, IP datagrams other than those associated with the authentication process are discarded until authentication is achieved. An ICMP `Destination Unreachable: Network Unreachable` message is returned for each IP datagram sent.

8.5.3
MSU is Out of Range

If an MSU goes out of coverage range of the HPD system, any datagrams sent to that MSU are not received successfully. An ICMP `Destination Unreachable: Host Unreachable` message is returned to the sending host after the delivery attempt has failed.

If an MSU remains out of range for a configured time called the (HPD Standby Timer), the HPD infrastructure deactivates the context for the mobile host. The default value of this timer is 12 hours. Any datagrams sent to that MSU after the context deactivation are discarded and an ICMP `Destination Unreachable: Network Unreachable` message is returned to the sending host. An MSU that attempts to send data after its context has been deactivated receives an ICMP `Destination Unreachable: Network Unreachable` message until context activated again. The mobile data device can maintain its PPP connection with the HPD modem while the MSU is out of range or unable to context activate at a site.

8.5.4
Full Datagram Queue

The system allows hosts to send multiple IP datagrams to the same destination and queues them pending delivery attempt. For inbound communications, the MSU limits its queue for ten datagrams. For outbound communications, the HPD infrastructure limits the queue to 8192 bytes of data, inclusive of IP headers.

If a host exceeds the queue limit, an ICMP message `Destination Unreachable: Host Unreachable` is returned to the host for each datagram received while the queue is at its limit.

NOTICE: ICMP messages are returned under normal operation, but some failure conditions may result in no ICMP message being returned and applications must be able to recover from that situation. Also, no ICMP message is returned for host sent ICMP messages that are directed to another host.

System datagram queues can be discarded under certain conditions. If the system infrastructure fails to successfully deliver an IP datagram, any remaining datagrams in the sending queue to or from the specific MSU are discarded. Also, when the HPD system removes a datagram from the queue to attempted delivery, it checks the age of the datagram. If the datagram is older than the SNDCP Queue Dwell Time, it is discarded and the queue is flushed. An ICMP `Destination Unreachable: Host Unreachable` message is returned to the source host for each discarded datagram.

The SNDCP Queue Dwell Time is defined for the HPD PDR through Provisioning Manager. The parameter is set for HPD modems through Customer Programming Software (CPS).

8.5.5
Static and Dynamic Addressing Scenarios

Table 21: Static and Dynamic Addressing Scenarios

If a radio record for an MSU is defined with dynamic addressing in the Provisioning Manager (PM) application, but the MSU sends a registration request with a static IP address, the system sends a reject to the MSU. Additional static and dynamic addressing scenarios are explained in the following table.

PM Setting	MSU Setting	Description
Static	Static	During registration, the system verifies that the MSU address matches the address provisioned for the MSU in Provisioning Manager. If the addresses match, the MSU is successful-

Table continued…

PM Setting	MSU Setting	Description
		ly registered to the system. If the addresses do not match, the MSU receives a reject.
Dynamic	Dynamic	During registration, the MSU receives an address from a DHCP or RADIUS server on the customer enterprise network.
Dynamic	Static	The system sends a reject response to the MSU.
Static	Dynamic	During registration, the system assigns the MSU with the static address that is defined for the MSU record in Provisioning Manager. This scenario allows the IP addressing for the MSUs to be defined and maintained centrally through Provisioning Manager.

8.5.6
Bandwidth Limitations

The bandwidth of radio channels is a limited shared resource that is used to support HPD MSUs and IV&D subscribers that are operating in the system. Varying environmental conditions make the path to and from an MSU different from an Ethernet connection, and even different from a dial-up modem connection. The reason for this difference is not only that the bandwidth is limited, but the bandwidth and data delivery delay can also vary with radio signal conditions and network loading. MSUs can also become unexpectedly unreachable for periods of time or may become disconnected without notice.

8.5.7
System Messaging Overload Protection

If messaging services on the system exceed 100% capacity, an overload protection mechanism temporarily suspends certain low-priority and non-critical services in the system. This protection mechanism allows the system to recover from the overload condition without requiring major system reset conditions. The system automatically resumes normal operations within 2 minutes after overload condition subsides.

8.6
ICMP Messages

The system infrastructure and High Performance Data (HPD) modems can both generate Internet Control Message Protocol (ICMP) responses for unsuccessful delivery of IP datagrams and other failure conditions. ICMP messages indicate non-delivery events such as an unreachable network, unreachable host, fragmentation conflict, unknown network, or bad header condition. Typical situations that may generate ICMP messages include component or link failures, routing problems, no confirmation of air interface traffic, message lifetime expiration, MSU not context activated, or the site is in local mode. In some cases, an ICMP message cannot be successfully returned to the sender.

ICMP responses contain the first 32 bytes of the data portion of the IP datagram sent by the host. Any inbound ICMP messages from HPD modems are forwarded through the system to the appropriate Customer Enterprise Network (CEN). The ICMP messages are forwarded in the same form as when they were generated by the HPD modem. Outbound ICMP messages are filtered by the system

according to the MSU settings in Provisioning Manager. If ICMP messages are disabled for the MSU, the system discards any outbound ICMP messages intended for the MSU.

Table 22: ICMP Messages

The following table outlines the ICMP responses that may be returned to the sending host.

Type	Code	Description	Potential Reject Reasons
3	0	Destination Unreachable: Network Unreachable	• Service has been rejected by HPD infrastructure. • The mobile host has not yet successfully context activated or authenticated with the system. • The mobile data device has sent an inbound datagram to the HPD modem after a context deactivation has been initiated.
3	1	Destination Unreachable: Host Unreachable	• The response wait timer has expired. • The MSU is in another service at time of IP datagram. • The MSU has exhausted the maximum number of radio interface retry attempts. • End of data has been received before the MSU can transmit the message on the radio channel. • The MSU is out of range from the system. • The IP datagram queue on a device is full. • The IP datagram SNDCP Queue Dwell Time has expired. • The MSU has experienced a PPP exception error when delivering an outbound message to the mobile host. • The MSU is in the process of context deactivation when an outbound message is received. • The MSU is not able to receive datagrams from the mobile data device due to an internal software issue within the HPD modem. • The MSU does not have an active PPP connection with the mobile data device and is not able to receive datagrams from internal MSU applications.
3	4	Destination Unreachable: Fragmentation Needed But Do Not Fragment Bit Set	A properly formatted IP datagram is received at a system interface point for IP bearer service that exceeds the system wide MTU limit with the **Do Not Fragment Bit** set in its header.
3	6	Destination Unreachable: Destination Network Unknown	A properly formatted IP datagram is received indicating a destination network class not supported by the system (that is, not part of Class A, B, or C).
12	0	Parameter Problem: IP Header is Bad	An IP datagram has been received with an improper formatting of its IP header and does not conform to IP version 4 format at the MSU.

8.7
Link Failures

The following sections describe the system reaction and behavior during various link failures in the HPD system. The sections also include the system operation during link recovery when applicable.

- HPD PDR-GGSN Link Failure
- GGSN-HPD PDR Link Failure
- GGSN-RADIUS/DHCP Server Link Failure
- HPD PDR-Remote HPD RNG Link Failure
- Remote HPD RNG-HPD PDR Link Failure
- HPD PDR-Local HPD RNG Link Failure
- HPD RNG-HPD BR Link Failure
- HPD BR-HPD RNG Link Failure
- ZC-HPD BR Link Failure
- HPD BR-ZC Link Failure
- ZC-HPD PDG Link Failure

8.7.1
HPD PDR-GGSN Link Failure

Under normal conditions, the PDR sends an echo request to the GGSN once per minute. If the PDR does not receive a response, the PDR performs up to five additional retries (4 seconds apart each). If PDR does not receive an echo response within the total of 80 seconds, the PDR reports the event to Unified Event Manager (UEM) application.

The HPD PDR maintains the GTP tunnel to the GGSN for an additional 4 minutes while continuing to send echo requests each minute. Contexts is only deleted if the MSUs attempt to use HPD data services during the GGSN failure.

From the perspective of the PDR, the following events and behaviors take place during a GGSN-PDR link failure.

1. The HPD PDR detects the link failure within 80 seconds.
2. Upon detection of the link failure, the PDR delays the tunnel deletion to the GGSN for 4 minutes.
3. The PDR sends an echo request to the GGSN every 60 seconds without retries.
4. The PDR notifies the network fault management application that the link is down.
5. The PDR only deletes contexts when MSUs try to initiate traffic. Idle contexts remain.
6. For context deletions, the PDR sends a delete user command to the RNG. The RNG then notifies the MSU that its context is deactivated.
7. If the HPD modem is configured to indicate the context loss over the PPP link, then the PPP link to the mobile data device is taken down.
8. Any outbound data from the CEN is not delivered. The GGSN sends ICMP notifications back to the CEN hosts.

8.7.1.1
HPD PDR-GGSN Link Recovery

The HPD PDR recovers a link when a response (positive or negative) is received for an echo request or a tunnel management message is received from the GGSN. Upon recovery, the PDR notifies the

network fault management application. Once the link is available, recovery should occur in less than 1 minute.

If the link is recovered before the failure is detected by the GGSN, then existing MSUs that have not been context deactivated can send data traffic to the CEN. If the link is recovered after the failure is detected by GGSN, then the contexts are torn down and the MSUs request a new context activation. To alert the MSUs to perform context activation again, the PDR sends a Context Activation Status message after flipping the CA bit, to the local RNG. The RNG forwards the message to sites which is broadcast over the air. The message targets subscribers, which are home to this zone and are currently registered in the zone. Those subscribers detect a different value of the CA bit, than what was received before, and would re-initiate the context activation process.

8.7.2
GGSN-HPD PDR Link Failure

Under normal conditions, the GGSN sends an echo request to the HPD PDR once per minute while the GTP tunnel exists. If there are no GTP tunnels established, the GGSN does not send an echo request to the PDR. From the perspective of the GGSN, the following events and behaviors take place during a PDR-GGSN link failure.

1. The GGSN detects a link failure within 4 minutes.
2. The GGSN deletes the tunnels with the PDR. All active contexts are deleted for MSUs with the affected home PDR.
3. For any outbound messages from the CEN, the GGSN responds with ICMP notifications.

8.7.2.1
GGSN-HPD PDR Link Recovery

The GGSN recovers the link upon receiving a context create message from the HPD PDR. MSUs with existing PDR contexts (which were not deleted during the failure) may send inbound traffic to the GGSN, but the traffic is rejected and the GGSN sends a context deactivation to the MSUs (since the GGSN had already deleted the contexts during the failure). The MSUs may initiate another context activation request and begin sending data.

8.7.3
GGSN-RADIUS/DHCP Server Link Failure

The GGSN does not perform explicit link failure detection on the link to the RADIUS/DHCP server. Instead, the GGSN uses a timeout and retry mechanism to detect link failures and try a switchover to a secondary RADIUS/DHCP server.

After the GGSN has timed out and maximum number of attempts have been made to a RADIUS/DHCP server, the GGSN determines that no RADIUS/DHCP server is available for IP address allocation from either the primary or secondary DHCP servers on the Customer Enterprise Network (CEN). The GGSN responds to the HPD PDR with a message that indicates no resources are available (for a failed DHCP server) or a system failure has occurred (for a failed RADIUS server).

8.7.4
HPD PDR-Remote HPD RNG Link Failure

An HPD Packet Data Router (PDR) may interact with HPD Radio Network Gateways (RNG) in other zones to route inbound and outbound traffic from mobile subscriber units (MSU). When the PDR detects a failure with the remote RNG, the following sequence of events takes place from the PDR perspective.

1. The PDR detects a link failure within a few seconds of inactivity through a keep-alive mechanism within the RNG.

2 The PDR notifies the network fault management application that the RNG link has failed.

3 The PDR attempts a link reestablishment with the RNG every few seconds.

4 The PDR continues to service inbound and outbound HPD traffic from other connected RNGs.

5 If the PDR receives outbound HPD traffic from the GGSN that is destined for the remote RNG with the link failure, the PDR generates an ICMP response and send it back to the host indicating that the message could not be delivered.

6 The PDR queues any messages that are already in progress until the message timer expires. Upon expiration, the PDR issues an ICMP response to the host indicating that the message could not be delivered.

8.7.5
Remote HPD RNG-HPD PDR Link Failure

An HPD Radio Network Gatteway (RNG) routes High Performance Data (HPD) traffic between mobile subscriber units (MSU) operating in the zone and the home Packet Data Router (PDR) for each MSU. The following series of events takes place when an RNG loses its link with a PDR in another zone.

1 The remote RNG detects a link failure with the PDR within 2 minutes. The detection is made through a keep-alive mechanism with the PDR or inactivity of data from the PDR.

2 The remote RNG waits for the link to be established by the PDR.

3 The RNG continues to service inbound and outbound HPD traffic with other connected PDRs.

4 The RNG continues to service Zone Controller (ZC) mobility pushes.

5 Inbound HPD traffic is sent to the serving RNG which is destined for the PDR with the failed link.

6 The RNG forwards the message to the local PDR. The PDR responds with an Unknown ID message. The RNG sends a context deactivation command to the MSU.

8.7.6
HPD PDR-Local HPD RNG Link Failure

An HPD Radio Network Gateway (RNG) relies on the local Packet Data Router (PDR) for certain critical services. The local RNG detects a link failure with the PDR within 3 minutes. The RNG handles the link failure in the following way.

1 After the link failure has been detected, the RNG stops responding to the HPD base radios and other PDRs. HPD services are not available for mobile subscriber units (MSU) operating in the zone.

2 The RNG continues to service Zone Controller (ZC) mobility pushes.

3 The RNG waits for the link to be established by the PDR.

8.7.6.1
HPD PDR-Local HPD RNG Link Recovery

The connection has to be established by the Packet Data Router (PDR). Expected link recovery time is within a few seconds after the establishment of link. Once the link is recovered, the Radio Network Gateway (RNG) can begin reestablishing its links to the High Performance Data (HPD) base radios in the zone and links to other PDRs in the system.

8.7.7
HPD RNG-HPD Base Radio Link Failure

The HPD Radio Network Gateway (RNG) maintains a logical link with High Performance Data (HPD) base radios in the zone. This link is used for inbound/outbound delivery of HPD traffic. The Radio Network Gateway (RNG) handles a failure on this link as described.

1. Upon detection, the RNG informs the local PDR of the link failure. The local PDR reports the failure to the network fault management application.
2. When outbound HPD traffic is routed to the RNG, the RNG responds to the PDR with a delivery failure notification. The PDR then generates an ICMP message to the sender.
3. The RNG continues to process mobility pushes from the Zone Controller (ZC).

8.7.7.1
HPD RNG-HPD Base Radio Link Recovery

The HPD Radio Network Gateway (RNG) waits for the link establishment request from the High Performance Data (HPD) base radio. Once the link is established, the RNG notifies the Packet Data Router (PDR) of the recovery, and the PDR reports the event to the network fault management application.

8.7.8
HPD Base Radio-HPD RNG Link Failure

The High Performance Data (HPD) base radio delivers all registration requests, context activation requests, and HPD traffic to the Radio Network Gateway (RNG) in the zone. An HPD base radio handles a loss of connection to the RNG in the zone in the following way.

1. The HPD base radio detects a link failure within a few seconds of the failure.
2. Upon detection, the HPD BR notifies the Zone Controller (ZC) of the failure condition and transition to local area mode.

8.7.8.1
HPD Base Radio-HPD RNG Link Recovery

The High Performance Data (HPD) base radio continuously attempts to establish the link with the Radio Network Gateway (RNG) after being commanded to do so by the Zone Controller (ZC). Upon recovery, the HPD base radio notifies the ZC that it is wide capable. The HPD BR transitions to wide area mode when a grant is received from the zone controller.

8.7.9
Zone Controller-HPD Base Radio Link Failure

The path between the zone controller and High Performance Data (HPD) base radio consists of an active site link and a standby site link. The active site link and standby site link are logical links that utilize one of two physical paths (if configured) between the zone controller and HPD base radio. These physical paths are referred to as the primary and secondary site control paths. The Zone Controller (ZC) dictates which site control path is to operate as the active site link at any given time.

The zone controller detects an active site link failure within a couple seconds. The zone controller expects to see keep-alive messages from the site every 300 msec. If five keep alive messages are missed, then the ZC declares the link down.

1. Upon detection of the failure, the zone controller notifies the network fault management application that the active site link is down.

2 The ZC attempts to switch over to the standby site link (if configured) without impacting call processing.

3 The ZC waits for the link establishment request from the HPD base radio.

8.7.9.1
Zone Controller-HPD Base Radio Link Recovery

The recovery process is triggered when the zone controller receives link-up requests from the High Performance Data (HPD) base radio. If one link is up and the other recovers, then the recovering link may be activated if it is on the preferred path. Otherwise, the other link remains as the active site link. If neither link is up and one link recovers, then the recovered link is activated. The Zone Controller (ZC) notifies the network fault management application of the recovery and performs actions to bring the site to wide area mode.

8.7.10
HPD Base Radio-Zone Controller Link Failure

The High Performance Data (HPD) base radio detects an active site link failure within a couple seconds. The HPD base radio waits an additional 2 seconds before assuming that the standby site link is also down.

1 The HPD base radio waits (up to 2 seconds) for the Zone Controller (ZC) to activate the secondary site link.

2 During the two second wait, the HPD base radio remains in wide area mode.

3 If both the active and secondary site links have failed, then the HPD base radio transitions into local area mode. HPD services are not available on the channel.

4 Mobile subscriber units (MSU) attempt to move to another channel at the site, or search for another HPD site that is in wide area mode.

8.7.10.1
HPD Base Radio-Zone Controller Link Recovery

The High Performance Data (HPD) base radio waits for the activation command from the Zone Controller (ZC) after the link is re-established. The zone controller also specifies the active site link for call processing. The HPD base radio waits for the ZC to issue commands to transition back to wide area mode.

8.7.11
Zone Controller-HPD PDG Link Failure

The ZC-HPD PDG link is used for records queries and mobility pushes. If the RNG has an existing record for an MSU, it continues to process inbound and outbound HPD traffic in the following way.

1 Inbound HPD traffic from the HPD base radios allows the RNG to update its mobility information. The RNG is able to continue handling inbound HPD services without any problems.

2 Outbound HPD traffic is sent to the last known HPD base radio. This may result in a failure to reach the proper site.

3 If all attempts to retry the ZC query have failed, the RNG sends a delivery notification failure to the PDR. If outbound data cannot be delivered to the intended MSU the PDR sends an ICMP response to the originating host.

If the RNG does not have an existing record for an MSU while the ZC-PDG link is down, the RNG is able to continue handling inbound HPD traffic. Outbound HPD traffic is sent to the last known location of the MSU.

1 Inbound data causes the RNG to create a record. The RNG is able to route the HPD traffic to the intended destination.

2 Outbound data is sent to the last known RNG associated with the MSU. This may result in a failure to reach to proper RNG/site since the mobility queries are not available.

3 If the message could not be delivered, the PDR sends an ICMP response to the originating host.

8.7.11.1
Zone Controller-HPD PDG Link Recovery

The PDG sends a successful indication to the network fault management application after a certain number of successful queries have been achieved. The HPD PDG attempts to self-correct as it receives inbound and outbound HPD traffic.

8.8
Component Failures

Many components in the High Performance Data (HPD) system are designed for high availability to allow continued operation during failure conditions. Certain devices in the system, such as the zone controllers and HPD site controllers (with redundant site links), include full redundancy. A failure to these devices causes a switchover which results in HPD services to be lost for a short time.

Several network transport devices in the zone core (zone core Ethernet switch, standalone core routers and exit routers or combine core/exit routers, gateway, and routers) support multiple paths or some level of fault tolerance to allow continued network services during individual failure conditions. While path redundancy allows continued service, the system capacity may be diminished if an individual switch or router fails.

Apart from the network transport devices, a number of components perform critical roles for HPD service in the system. The following sections describe the behavior and reaction of the system during the failure of these key devices.

- GGSN Failure
- HPD PDG Failure
- Zone Controller Failure
- Active Site Controller Failure
- Active and Standby Site Controller Failure
- HPD Base Radio Failure

8.8.1
GGSN Failure

In a High Availability configuration, two redundant GGSN routers provide automatic switchover in case of a component failure. If the active GGSN fails, the backup GGSN immediately takes over, ensuring continuous availability of HPD services. The following GGSN failure scenario applies to configurations without redundant GGSNs or situations where both GGSNs in a High Availability configuration fail.

A GGSN failure halts all inbound and outbound HPD traffic between the MSUs and customer network hosts. Individual contexts are not deactivated during a GGSN failure unless MSUs attempt to send HPD traffic.

During a GGSN failure, the system exhibits characteristics that are like a GGSN-PDR link failure. The general sequence of activities during a GGSN failure is explained as follows:

1 The HPD PDR periodically polls the GGSN. If the GGSN does not respond, the PDR reports the failure condition to the system. No explicit notification of the failure is sent to either the MSUs or customer network hosts.

2 Behavior for other devices in the system is like the behavior during a PDR-GGSN link failure.

3 If an MSU sends inbound HPD traffic, the PDR deletes the context and sends a context deactivation message to the MSU. The PDR does not delete idle contexts during the GGSN failure.

4 If the GGSN recovers, the GGSN gradually recovers its database. During the recovery, any messages with unrecognized tunnel IDs are rejected (resulting in context deactivations).

8.8.2
HPD PDG Failure

To avoid the loss of High Performance Data (HPD) services caused by a Packet Data Gateway (PDG) failure, the system can be configured to support PDG redundancy. The two features providing PDG redundancy, are DSR (Dynamic System Resilience) and HA Data (High Availability for Trunked IV&D and HPD).

- HA Data introduces redundant components in the data subsystem within a single zone core. In this configuration, the Fault Tolerance feature enabled for the HPD PDG establishes a redundant HPD PDG on a separate server. If the primary PDG fails due to a hardware failure, the backup PDG immediately takes over, ensuring continuous availability of HPD services.
- DSR is a system architecture feature that provides redundant zone core equipment by establishing a primary zone core and a backup zone core usually at two different master site locations. An HPD PDG failure in the primary core forces a switchover to the backup data subsystem, ensuring a quick recovery of HPD services.

In a system without PDG redundancy, an HPD PDG failure causes all HPD services to become unavailable for all MSUs that are mapped to the zone with the failed PDG. The general sequence of activities during an HPD PDR failure is explained as follows:

1 The system detects the PDG failure.

2 Behavior for other devices in the system is like the behavior during PDG-BR and PDG-GGSN link failures.

3 Any MSUs that are home zone mapped to the zone with the failed PDG lose HPD service

4 When the PDG recovers:

   - The PDR uses its existing database if it is not corrupted. The system communicates any changes that have occurred during the failure. If the database is corrupted, the PDR re-synchronizes with the system.
   - Contexts are restored in the PDR through normal message traffic.
   - The RNG database is gradually rebuilt through mobility pushes, context activation requests, and inbound/outbound data. The PDR notifies Network Management when the RNG has recovered.

8.8.3
Zone Controller Failure

When the active zone controller fails, the standby zone controller initiates a switchover. All High Performance Data (HPD) sites in the zone transition to local area mode, and mobile subscriber units (MSU) attempt to find wide area mode HPD sites. After the switchover has completed, MSUs attempts to register with the individual sites within the zone

During the zone controller switchover process, the system exhibits characteristics that are like ZC-BR, ZC-PDR, and ZC-RNG link failures. The general sequence of activities during a zone controller failure is explained as follows:

1 The standby ZC detects that the active ZC has failed and initiates a switchover. The mobility database of the HPD MSUs is lost since the standby ZC does not contain mobility information.

2 Behavior for other devices in the system is like the behavior during a ZC-BR, ZC-PDR, and ZC-RNG link failure.

3 All sites in the zone enter local area mode during the ZC switchover process.

4 MSUs attempt to find an HPD site that is in wide area mode during this time. However, no wide area HPD sites are available in the zone. Any MSUs that are roaming near adjacent sites in other zones may be able to register with wide area HPD sites in the other zones.

5 The RNG sends delivery failure notifications for any outbound messages received from local or remote PDRs. The home PDRs generate appropriate ICMP messages to the customer network hosts.

6 The new active zone controller gradually brings the entire zone into wide area mode within 2-3 minutes. The ZC receives mobility uploads from the HPD site controllers in the zone. The ZC then sends commands to the HPD SCs to transition into wide area mode.

7 MSUs that transitioned to other zones are required to remain registered in the other zones until the InterZone debounce timer has been completed.

8.8.4
Active Site Controller Failure

If the active site controller fails, and the standby site controller has a connection with the zone core, then an SC switchover occurs. During the switchover period, the standby SC must reinitialize and the site temporarily enters local mode. MSUs that are active on the site attempt to find an adjacent wide area site. After the switchover has completed, the HPD site resumes normal operation. MSUs can register with the site and data services can resume.

During the site controller switchover process, the system exhibits characteristics that are like SC-RNG, SC-BR, and SC-ZC link failures. The general sequence of activities during an HPD SC failure is explained as follows:

1 The standby SC detects the loss of the active SC within 150 ms. The standby SC begins sending TSP messages immediately after switchover. The TSP contains new active SC info.

2 Behavior for other devices in the system is like the behavior during an SC-RNG, SC-BR, and SC-ZC link failure.

3 The new active SC performs an initialization process like the power up initialization. During this initialization process, the base radios advertise that the site is in local area mode. MSUs leaves the site and search for a wide area site.

4 After the base radios receive the TSP messages from the new active SC, the BRs clean their database, but do not dekey. The BRs then begin to accept registration requests.

5 Adjacent sites broadcast that the site is in wide area mode. MSUs can begin to register with the site. Any existing MSUs that have not already registered with another site still has to perform another registration since the standby SC and active SC do not share databases. Hold off timers (RRHOT and FRHOT) are used to prevent a large volume of MSUs from trying to register with the recovered site simultaneously.

8.8.5
Active and Standby Site Controller Failure

If both the active and standby HPD Site Controllers (SC) fail, or if the active SC fails and the redundant SC is isolated from the system, then all the HPD channels at the site dekey. MSUs leaves the site and attempts to register with another site that is in wide area mode.

During the HPD SC failure, the system exhibits characteristics that are like SC-RNG, SC-BR, and SC-ZC link failures. The general sequence of activities when both active and standby SCs have failed is explained as follows:

1 Channels detect the link failure within 500 ms (since TSP messages are not received from the site controllers). All the channels at the site dekey and broadcast information ceases.

2 Behavior for other devices in the system is like the behavior during an SC-RNG, SC-BR, and SC-ZC link failure.

3 MSUs that were operating on the HPD site scan through their adjacent site list and attempt to register with another site that is in wide area mode.

4 If one or both SCs recover, the first SC to recover initializes and become the active SC. The HPD BRs at the site will then begin to accept registration requests and handle HPD traffic after the site initialization has completed. Hold off timers (RRHOT and FRHOT) are used to prevent a large volume of MSUs from trying to register with the recovered site simultaneously.

8.8.6
HPD Base Radio Failure

If the HPD base radio is isolated from the active site controller, then the base radio dekeys and does not handle any MSU traffic. Again, MSUs attempts to operate on another HPD channel at the site. If another channel is not available, the MSUs attempt to register at another HPD site.

During the base radio failure, the system exhibits characteristics that are like ZC-BR and RNG-BR link failures. The general sequence of activities during a base radio failure is explained as follows:

1 The active HPD SC periodically pings each of the HPD BRs at the site. If a BR does not respond to a certain number of attempts, or if the SC does not receive a response to other messages that require acknowledgment, then the SC declares that the channel has failed.

2 Behavior for other devices in the system is like the behavior during a ZC-BR and RNG-BR link failure.

3 If the HPD base radio was the home channel at the site, the site controller assigns another base radio as the home channel

4 If the HPD base radio was the home channel at the site, the site controller assigns another base radio as the home channel.

5 The SC updates the Additional Channel Broadcast so that the failed BR is not advertised to the radio population.

6 The SC continues to send outbound data to the failed channel throughout the duration of the failure.

7 MSUs that were operating on the failed channel attempts to move to another HPD channel at the site.

8 LLC Timeouts causes the RNG in the zone to send delivery notification failures to the home PDR(s). The home PDRs sends ICMP responses that indicate the failed delivery to the hosts on the customer enterprise network.

Chapter 9

HPD Overlay FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to HPD Overlay System Infrastructure.

9.1 Field Replaceable Entities (FRE)

Table 23: Field Replaceable Entities (FRE) for HPD Overlay System

The following table provides reference information about the Field Replaceable Entities (FRE) for the HPD Overlay feature.

Component	Reference
Master Site	See the *Master Site – Infrastructure* manual.
HPD Remote Site	See the *GTR 8000 Expandable Site Subsystem* manual.
ASTRO® 25 Repeater Site	See the *GTR 8000 Expandable Site Subsystem* manual.
Simulcast Prime Site	See the *Trunked IP Simulcast Subsystem Prime Site* manual.
Simulcast Remote Site	See the *Trunked IP Simulcast Subsystem Remote Site* manual.
Data Subsystem (PDG, GGSN)	See the *Packet Data Gateways* and *GGM 8000 System Gateway* or *S6000 and S2500 System Routers* manuals.

This page intentionally left blank.

Chapter 10

HPD Overlay Reference

This chapter contains supplemental reference information relating to HPD Overlay System.

10.1 System Scalability

The system is designed for scalability, allowing some zones, sites, and channels to be configured as required to support the entire coverage area. Systems in dense urban areas may include more sites and channels to provide appropriate coverage and services for numerous local subscribers. Statewide systems may include more zones that are spread out to provide service over larger geographical areas. The system scalability also supports future growth, allowing additional zones, sites, and channels to be added over time as needed.

To expand HPD services within the system, additional HPD remote sites can be added to the system or HPD overlay sites can be added to other existing IV&D RF sites (ASTRO® 25 repeater site, simulcast prime site, or simulcast remote site).

10.2 Wideband Migration

The equipment for the HPD feature is designed for easy and economical migration to future wideband data solutions. These future solutions provide higher data rates and additional features for more intense mobile applications. HPD modems are software upgradeable to support these future wideband offerings.

This page intentionally left blank.