System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

HPD Packet Data Resource Management

NOVEMBER 2016

MN003299A01-A

Copyrights

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

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

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

Disclaimer

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

Trademarks

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

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

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

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

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

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

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

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

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

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola 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
MN003299A01-A	Original release of the *HPD Packet Data Resource Management* 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.

About This Manual

This manual provides an introduction to the ASTRO® 25 system High Performance Data (HPD) packet data resource management feature. It also provides an overview of the High Availability for HPD (HA Data) feature that supports redundancy in the data subsystem. Included are descriptions, technical information, and the Packet Data Gateways (PDG) switchover procedure.

This manual is intended to be used by field service managers and field service technicians after they have attended the Motorola Solutions formal training.

What Is Covered in This Manual?

This manual contains the following chapters:

- Packet Data Resource Management Description on page 19 – This chapter provides descriptive information for the ASTRO® 25 system High Performance Data (HPD) packet data resource management feature.
- Packet Data Resource Management Technical Overview on page 21 – This chapter provides technical overview information for the ASTRO® 25 system High Performance Data (HPD) packet data resource management feature.
- High Availability for HPD on page 53 – This chapter includes information relating to the purpose, configuration, and operation of the High Availability for HPD (HA Data) feature that supports redundancy in the data subsystem for high availability of HPD services.

Helpful Background Information

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

Related Information

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

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as 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 Documentation Overview	For an overview of the ASTRO® 25 system documentation, open the graphical user interface for the ASTRO® 25 system documentation set and select the **System Documentation Overview** link. A file opens that includes: • ASTRO® 25 system release documentation descriptions • ASTRO® 25 system diagrams

Table continued…

Related Information	Purpose
	For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.
Dynamic System Resilience	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature which may be implemented on your ASTRO® 25 system. This feature adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Trunked Data Services	Describes the implementation and use of data services on ASTRO® 25 systems, specific to the Classic Data (IV&D) and Enhanced Data functionalities, and the High Availability for Trunked IV&D and HPD feature.

Chapter 1

Packet Data Resource Management Description

This chapter provides a high-level description of Packet Data Resource Management and the function it serves on your system.

1.1 Packet Data Resource Management Introduction

This resource management document explains various aspects of the High Performance Data (HPD) operation in the system.

Topics explain the various settings, components, and system processes that must work together for HPD services in the system. Understanding this material helps when configuring, managing, and troubleshooting HPD services in a system.

1.2 Intended Audience

This document is intended for use by system managers and operators as a resource for understanding of the operation of High Performance Data (HPD) within a system.

The audience of this material is expected to attend an ASTRO® 25 system training and should have a basic knowledge of networking equipment and telecommunication systems.

This page intentionally left blank.

Chapter 2

Packet Data Resource Management Technical Overview

This chapter explains how the Packet Data Resource Management works in the context of your system.

2.1 Inbound and Outbound Traffic

For inbound traffic, the datagrams are originated at the Mobile Subscriber Unit (MSU) and are routed to the Customer Enterprise Network (CEN). For outbound traffic, the datagrams are originated from a host on the CEN and are routed through the system to the MSUs.

The High Performance Data (HPD) base radios provide the RF interface to the MSUs in the system. Each HPD base radio uses a transmit/receive carrier frequency pair for full-duplex interaction with MSUs. Time Division Multiplexing (TDM) is used on the inbound and outbound carriers to provide multiple time slots for traffic.

The inbound and outbound carriers are divided into frames, and each frame is subdivided into time slots. The following basic types of time slots are used on the inbound/outbound carriers:

- Inbound Reserved Access Time slot
- Inbound Random Access Time slot
- Outbound Time slot

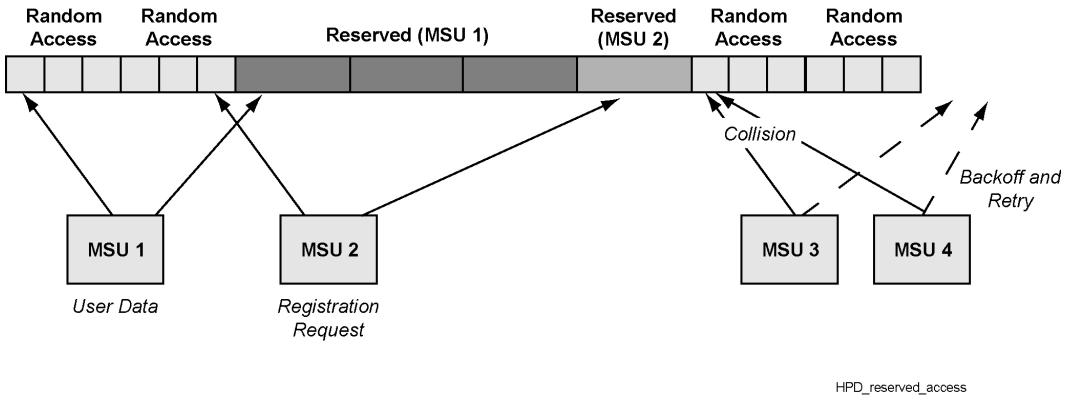
2.1.1 Inbound Reserved Access Time Slot

For the High Performance Data (HPD) operation, a system uses inbound reserved access. When a Mobile Subscriber Unit (MSU) has inbound traffic (registration request, packet data, and so on), it must first request a reservation over an inbound random access subslot. When a reservation request is received, the HPD base radio schedules an inbound reserved access slot and indicates that slot to the MSU.

The full reserved access time slot is dedicated to the requested MSU. The MSU assembles a header block along with any pending inbound traffic that fits within the time slot. The MSU can reserve multiple time slots.

The diagram illustrates how the random access subslots are used and how time slots are reserved for inbound traffic. In this example, MSU 1 has user data to send, so it sends a reservation request over a random access subslot. Afterwards, MSU 2 has a registration request, so it sends a reservation request over a random access subslot. The system reserves some inbound slots for MSU 1 to send its user data. The system then reserves a slot for MSU 2 to send its registration request.

Figure 1: Inbound Reservation-Based Access



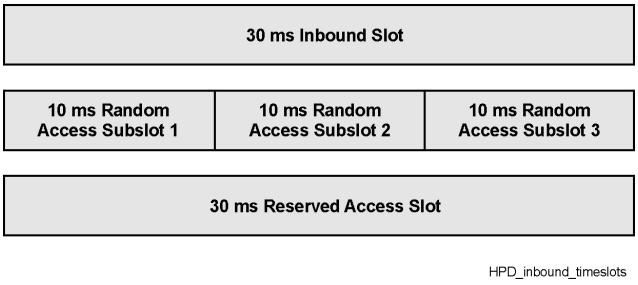
MSU 3 and MSU 4 are shown contending for a random access subslot and having a collision. Both MSUs run their backoff algorithm and retry their requests during later random access subslots.

2.1.2
Inbound Random Access Time Slot

The inbound random access time slot is divided into three separate subslots that are accessible to the Mobile Subscriber Units (MSU). MSUs use these random access subslots request a reservation on an inbound packet data channel. The subslots are random access, so multiple MSUs can contend for a subslot and collisions can occur. If collisions do occur, and the MSUs do not receive a response from the system, then the MSUs use a backoff algorithm to schedule retry attempts.

The High Performance Data (HPD) base radio advertises when random access time slots are available to the MSU population. The diagram shows how three consecutive random access subslots consume a full inbound slot.

Figure 2: Inbound Slot Structure



The HPD base radios periodically broadcast some random access parameters to the MSUs. Each HPD base radio is configured with a Random Access Response Timer, Maximum Random Access Attempts, and Wait for Cluster Timer in the Configuration/Service Software (CSS). MSUs run the response timer when sending information over a random access subslot. If the system does not respond before this timer expires, the MSU runs its backoff algorithm and retry its random access transmission. After the maximum number of retries, the MSU considers that the channel is unavailable and can seek another channel.

MSUs also run the Wait for Cluster Timer. A random access cluster represents one full random access time slot (three sub slots). If a random access cluster is not made available on the channel before this timer expires, the MSUs can seek another channel for services.

2.1.3
Outbound Time Slot

The outbound carrier from the High Performance Data (HPD) base radio is continuously keyed. A continuous stream of outbound time slots is sent to the Mobile Subscriber Unit (MSU) population.

The first outbound time slot of every frame is designated as the Broadcast Control Slot. This time slot is used to broadcast information to the MSUs. In addition, MSUs use this slot as an opportunity for scanning adjacent sites (to avoid missing outbound traffic during other time slots). In addition to the Broadcast Control Channel, the HPD base radio schedules control traffic, packet data traffic, and other types of broadcasts for the MSUs on the outbound carrier.

2.2
Broadcasts

The Broadcast Control Slot is used to send Time Division Multiplexing (TDM) synchronization, basic access information, random access parameters, power control information, and other such information to the Mobile Subscriber Unit (MSU) population at the site. The Broadcast Control Slot is sent as the first outbound slot of every frame.

In addition to the Broadcast Control Slot, the High Performance Data (HPD) base radios provide the following broadcasts to MSUs at the site:

- Adjacent Status Broadcast
- Additional Channel Broadcast
- Channel Identifier Update Broadcast
- System Identifier Broadcast
- Time and Date Broadcast
- Base Station Identifier Broadcast
- Channel Access Information Broadcast

2.2.1
Adjacent Status Broadcast

The High Performance Data (HPD) base radios periodically send the Adjacent Status Broadcast to inform the Mobile Subscriber Unit (MSU) population of the presence and status of the home channel at an adjacent site. The broadcast includes home channel information and indicates whether the adjacent site is in local mode or wide area mode.

The MSUs store the received information in a list of adjacent site information. An MSU uses this internal list to monitor adjacent sites, select new sites, or change sites during failure scenarios. If the present site fails or the adjacent site signal strength becomes greater than the signal received at the current site, the MSUs can register at an adjacent site.

2.2.2
Additional Channel Broadcast

The additional Channel Broadcast is sent out as a background message from each High Performance Data (HPD) base radio to inform the Mobile Subscriber Unit (MSU) population of the presence and status of other channels at the same site. The HPD site controller provides each HPD base radio at the site with the information needed for this broadcast.

The MSUs store the information for the other channels at the site in an internal list. If an MSU is operating on a channel that fails, or if an MSU has made the maximum number of failed retries on a channel. The MSU then tries to select a new channel at the site according to its internal list. If no other channel is available at the site, then the MSU attempts to register with another site.

2.2.3
Channel Identifier Update Broadcast

The Channel Identifier Update Broadcast is sent as a periodic background message to inform the Mobile Subscriber Unit (MSU) population of the band plan parameters configured at the site. These parameters include channel identifiers, base frequencies, channel bandwidth, channel spacing, and transmit offset settings.

In this release, MSUs check whether the band plan parameters match the internally provisioned band plan settings within the MSU. If there is a mismatch, the MSU logs an error and continues normal operation.

2.2.4
System Identification Broadcast

The System Identification Broadcast is sent periodically to inform Mobile Subscriber Units (MSU) on the channel of the system identification information. This broadcast includes the Wide Area Communication Network (WACN) ID, System ID, zone ID, site ID, current channel, and site status (local mode or wide area mode). The MSUs use this broadcast for mobility purposes.

2.2.5
Time and Date Broadcast

The Time and Date Broadcast informs the Mobile Subscriber Unit (MSU) population of the current date (day/month/year) and time (hours/minutes/seconds). The broadcast includes the local time offset and has flags which indicate whether the time and date values are valid. It allows the MSU population to support common real-time clocking for the time stamping of logging messages. The GNSS/NTP functionality within the High Performance Data (HPD) site controller provides this service.

2.2.6
Base Station Identifier Broadcast

The High Performance Data (HPD) base radios periodically send out the Base Station Identifier Broadcast to indicate a digital call sign to any device listening on the channel. The Base Station Identifier (BSI) is enabled and configured for each channel through Unified Network Configurator (UNC). A call sign of up to 20 characters is provisioned. The BSI is broadcast every 15 minutes on the channel.

2.2.7
Channel Access Information Broadcast

The Channel Access Information Broadcast is periodically sent out to inform the Mobile Subscriber Unit (MSU) population of Context Activation Hold-Off Time (CAHT), Channel Access Hold-Off Time (CAHOT), and Recovery Random Hold-Off Time (RRHOT) parameters out of which CAHOT and RRHOT that have been provisioned for the site through Unified Network Configurator (UNC).

MSUs use these time values during site failure and recovery situations. During a site failure, an MSU waits for a random amount of time (up to the CAHOT value) before attempting a new registration or location registration with another High Performance Data (HPD) site. During a site recovery, an MSU waits for a random amount of time (up to the RRHOT value) before attempting to register with an HPD site that has recovered. In the Packet Data Gateway (PDG) failure and recovery scenario, MSU waits before sending Context Activation/Renew message (Context Activation Hold-Off Time). This message helps to speed up the context reactivation rate of MSU.

2.3 Channel Hunt

When a Mobile Subscriber Unit (MSU) is powered up or enters a coverage area, it begins a search for an available channel. This operation is called a channel hunt.

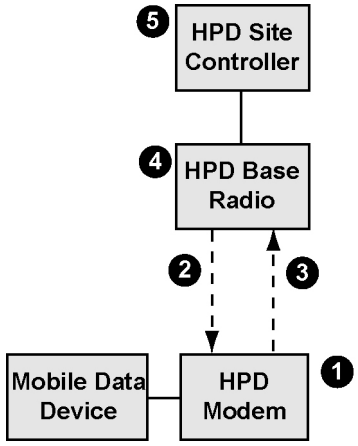
MSUs search for an available channel by browsing the channels in the following sequence:

1. Home channel on the home site (from the persistent memory)
2. Additional channels on the home site (from the persistent memory)
3. Adjacent site list (from the persistent memory)
4. Pre-programmed list of channels (from the MSU codeplug)

The first three items are stored in memory in a dynamic list that is updated during MSU runtime. The pre-programmed list of channels is configured through CPS and remains in the codeplug. A full spectrum scan is not supported in this release.

Figure 3: Channel Hunt

The following diagram shows the MSU channel hunt sequence.



HPD_channel_hunt

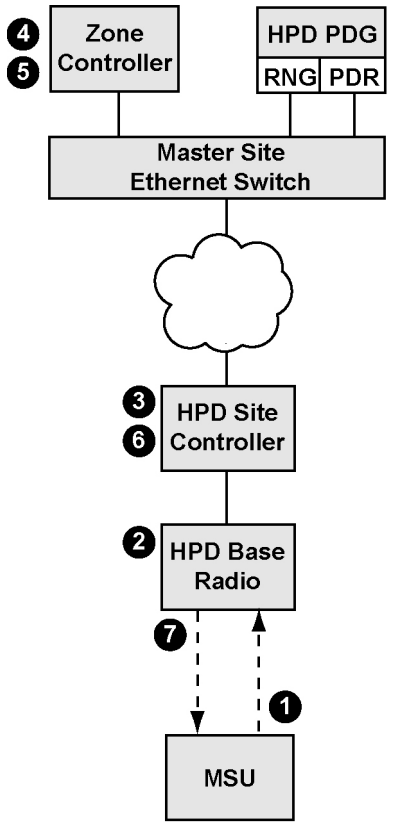
1. After the High Performance Data (HPD) modem is powered up, it begins searching for an available channel from its pre-programmed list of channels.
2. The HPD modem receives a System Identification Broadcast from a channel at the HPD remote site.
3. The HPD modem initiates a MAC open request over the channel.
4. The HPD base radio confirms that the traffic was received, then sends the request to the HPD site controller.
5. The HPD site controller creates a record for the MSU in its database and sends a response to the MSU. Afterwards, the MSU can try to register with the system.

2.4 Unit Registration

When a Mobile Subscriber Unit (MSU) powers up or enters the system coverage area, it performs a channel hunt and attempts to acquire a channel in the system. After successfully acquiring a channel, the MSU initiates a unit registration request.

Figure 4: Unit Registration

The following diagram shows the MSU unit registration request sequence.



HPD_unit_registration

1. The MSU sends a unit registration request over the High Performance Data (HPD) channel. The request includes the Wide Area Communication Network (WACN) ID, System ID, Radio ID, and other information.
2. The HPD base radio acknowledges the air interface reception of the request, then forwards the registration request to the HPD site controller.
3. The HPD SC updates its database and forwards the request to the zone controller.
4. The ZC evaluates the request and determines whether the MSU should be registered with the system (according to the Provisioning Manager configuration records). Then the ZC sends a registration response back to the HPD SC (accepted, refused, or denied).
5. The ZC creates an entry for the MSU in the ZC VLR, then pushes the VLR information to the Radio Network Gateway (RNG) in the zone.
6. The HPD SC updates its database and forwards the response to the HPD BR.
7. The HPD BR sends the response to the MSU. If the MSU registration is accepted, then the MSU initiates a context activation request.

2.4.1
Registration Rejects and Failures

If there are any conflicts between the Mobile Subscriber Unit (MSU) registration request and the system settings, registration requests can be denied or refused.

When a registration is denied, the MSU has sent a request with an incorrect WACN ID or system ID. If it is trying to register at a site that is configured as an invalid site for that MSU, the MSU can also be denied. The MSU searches for another system/site.

When a registration is refused, the MSU sends a request with an invalid radio ID or a radio ID that conflicts with another ID in the system. If the system cannot retrieve a record for the MSU, the registration can also be refused.

A registration timeout occurs when an MSU sends a registration request and does not get a response. It could happen when the MSU is out of range or when a system failure has occurred.

2.4.2
Deregistration

A Mobile Subscriber Unit (MSU) is deregistered from the system when it powers down or roams into another network. The zone controller also maintains an inactivity timer for each MSU. When an inactivity timer expires for an MSU, the zone controller queries the MSU. If the MSU does not respond, it is removed from the system.

2.5
Context Activation

After a Mobile Subscriber Unit (MSU) is successfully registered with the system, it initiates a context activation request. The context activation establishes a tunnel for High Performance Data (HPD) traffic between the MSU and its assigned Customer Enterprise Network (CEN).

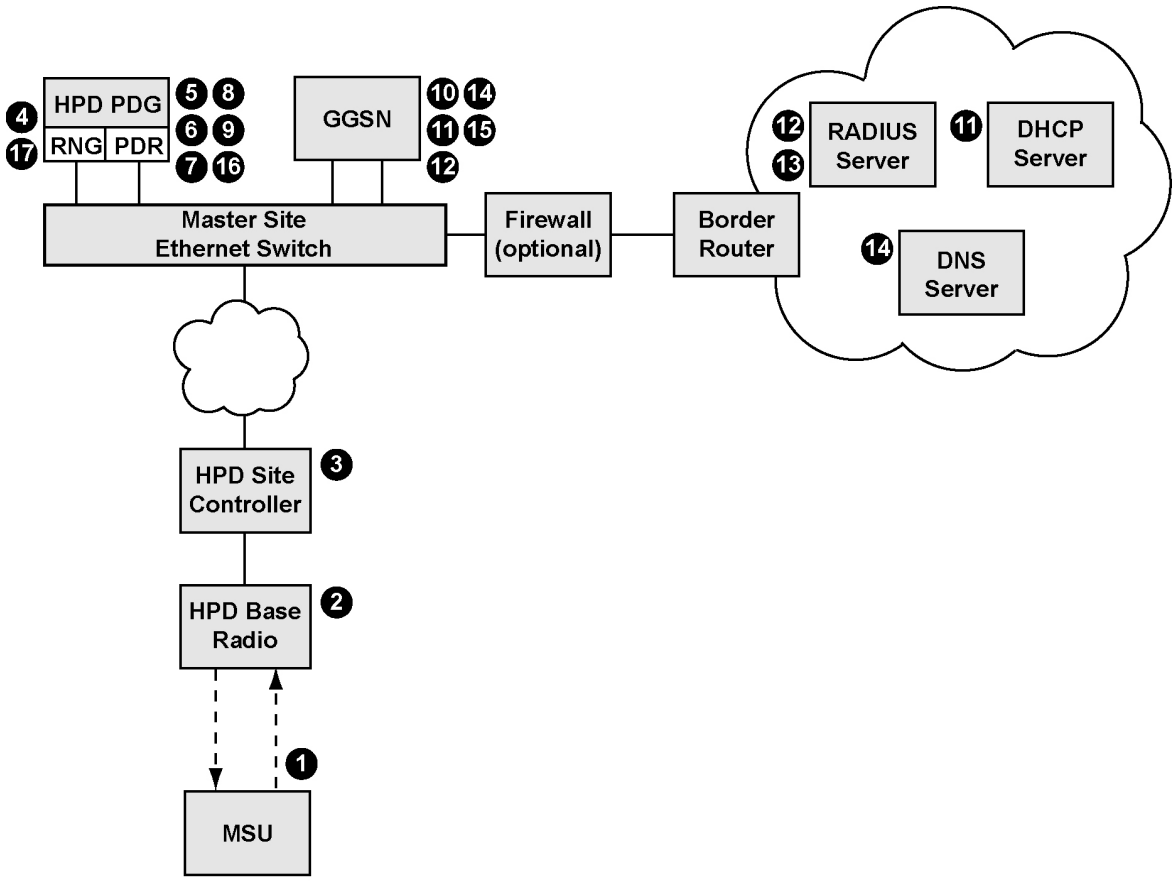
The context activation can be initiated through the Connection Manager on the mobile data device, or by the internal application in the HPD modem. The mobile data device and the internal HPD modem application require separate context activations (they do not share a context).

During the context activation process, the MSU initiates an internal activation wait timer. If the MSU does not receive a response from the system before this timer expires, then the MSU considers that the context activation has failed and retries the request.

Only MSU initiated context activations are supported. Hosts on the CEN cannot initiate a context activation with an MSU.

The diagram and figure show the context activation sequence.

Figure 5: Context Activation



1 After the MSU is successfully registered, it sends a context activation request. The request includes the IP address of the HPD modem (or a null address if the dynamic addressing is used), a flag that indicates whether the static or dynamic addressing is used, user authentication information (username and password), and other information.

2 The HPD BR acknowledges that it has received the request over the air interface, then forwards the request to the HPD SC.

3 The HPD SC forwards the request to the High Performance Data Radio Network Gateway (HPD RNG) in the zone.

4 The HPD RNG creates a temporary record for the MSU and updates its PD-VLR tables.

5 The HPD RNG forwards the context activation request to the High Performance Data Packet Data Router (HPD PDR) that resides in the home zone of the MSU.

6 The HPD PDR validates the MSU information (compared with the provisioned values for the MSU HPD Radio record in Provisioning Manager). If the MSU information is not valid, a reject response is sent to the MSU.

7 The HPD PDR adds an Access Point Name (APN) to the request. This APN identifies the appropriate Customer Enterprise Network (CEN) for the MSUs context activation. The APN for the MSU is defined in an HPD Radio record in Provisioning Manager.

8 If the MSU has requested a dynamic IP address, while the MSU has a static address defined in Provisioning Manager, then the HPD PDR adds the provisioned IP address to the request.

9 The HPD PDR forwards the context activation request to the Gateway GPRS Support Node (GGSN).

10 The GGSN configuration determines the user authentication and dynamic IP addressing requirements for the APN.

11 If the MSU did not provide a static address and the HPD PDR did not assign a provisioned static address from Provisioning Manager, then the GGSN gets an IP address through one of the following methods (according to the GGSN settings for the APN):

GGSN Local Pool
The GGSN provides an address from a local pool of addresses within the GGSN.

DHCP Server
The GGSN requests an address from the DHCP server at the APN.

RADIUS Server
The RADIUS server provides an address during the user authentication verification process, as explained in the following steps.

12 If the user authentication is required for the APN, then the GGSN sends a request to the RADIUS server at the APN. The request includes the MSU IP address, user name, password (PAP) or challenge/password (CHAP), and other information.

13 The RADIUS server verifies the authentication information and sends a response (accept/reject) to the GGSN. If the MSU IP address in the request is null (0.0.0.0), then the RADIUS server assigns an IP address and includes it in the response.

14 If a Domain Name Server (DNS) is supported at the CEN and if dynamic DNS updates are enabled in the GGSN, then the GGSN forms a Fully Qualified Domain Name (FQDN) for the MSU, and forwards the FQDN in an update to the DNS server at the CEN.

15 The GGSN sends a context activation response to the HPD PDR.

16 The HPD PDR adds the subscriber record to the HPD RNG.

17 The HPD RNG sends the context activation response to the MSU. The response includes the IP address assigned for the MSU, the HPD Standby Timer, and other parameters. At this time, both the HPD RNG and MSU start their own instance of the HPD Standby Timer.

2.5.1
Context Reject Codes

A context activation reject provides a reason for the reject and defines the action that the Mobile Subscriber Unit (MSU) should perform. The table lists the context reject codes and the MSU action that should be performed when receiving the context reject.

Table 1: Context Reject Codes

Reject	Description	MSU Action
Any Reason	The MSU is rejected for some general reason.	Hold-Off
MRC not provisioned for packet data	The MSU is not configured for High Performance Data (HPD) service in Provisioning Manager.	Hold-Off
SNDCP version not supported	The system has determined that the SNDCP version that is used by the MSU is not supported.	Disable
Dynamic address pool empty	The MSU has requested a dynamically assigned IP address, but the DHCP server does not have any available.	Hold-Off

Table continued…

Reject	Description	MSU Action
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.	Hold-Off
Static address not allowed	The MSU has sent a static IP address that is not allowed by the system.	Hold-Off
Temporary Rejection	The system has temporarily rejected the context activation request.	Hold-Off
MRC DSUT not supported	The MSU has provided context activation information for a Data Subscriber Unit Type (DSUT) that is not supported by the system.	Disable
Maximum number of PDP contexts exceeded	The system is servicing the maximum number of contexts.	Hold-Off
User authentication failed	The user authentication has failed. Additional attempts are allowed.	None
Access point name incorrect	The MSU has requested connection with an access point name that does not exist in the system.	Hold-Off

The type of reject indicates the MSU action that should be taken. The MSU responds to the reject in one of the following ways:

Hold-off
Context activation holds off for 5 minutes.

Disable
Context activation is disabled until the MSU is reprogrammed or restarted.

None
The MSU can attempt another context activation request immediately.

2.5.2
Context Renewal

The system can deactivate contexts for Mobile Subscriber Units (MSU) that are no longer operating on the system after a specific time period. The MSU must periodically renew its context to avoid being deactivated from the system.

During the context activation process, the High Performance Data Radio Network Gateway (HPD RNG) sends an HPD Standby Timer value to the MSU. This timer is configured in the Unified Network Configurator (UNC) and can be assigned with a value between 1 hours and 72 hours. Both the MSU and HPD RNG start an instance of this timer during the context activation process. When the timer expires, the system initiates a context deactivation for the MSU.

After an MSU has successfully performed attains an instance of the standby timer, it sends a context activation request before the expiration. When the request is received, the HPD RNG and High Performance Data Packet Data Router (HPD PDR) recognize that the MSU is already context activated. The HPD PDR sends a context activation acceptance back to the MSU along with a refreshed standby timer value. Next, the HPD RNG and MSU restart their standby timers.

If a context renewal request is not received before the standby timer expires, the HPD RNG initiates a context deactivation for the MSU.

2.5.3
Context Deactivation

An existing context between a Mobile Subscriber Unit (MSU) and the Customer Enterprise Network (CEN) can be deactivated due to a normal or failure condition. Some typical causes for a context deactivation or context renewal failure include:

- The MSU is moved out of range and the High Performance Data (HPD) Standby Timer is 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 is lost.
- The HPD modem has performed a graceful shutdown.
- Terminal Data Enabled option is set to Disabled for the MSU.
- The High Performance Data Packet Data Router (HPD PDR) has deactivated its context with the Gateway GPRS Support Node (GGSN) for some reason.
- The connection with the Radio Network Gateway (RNG) is lost.
- Provisioning information for the MSU is changed or deleted.
- The GGSN or home HPD PDR has failed.
- Configuration changes in Provisioning Manager.
- The maximum number of context renewal retries have failed.

2.6
Adjacent Site Scanning

Mobile Subscriber Units (MSU) are given the responsibility for selecting the best site for High Performance Data (HPD) services. To do it, the MSUs occasionally monitor adjacent sites to determine whether a more favorable site is available. The MSUs use an internal adjacent site list, which is built from Adjacent Status Broadcast messages received by the current site. This list consists of the home channel information and status (wide area or local mode) for each adjacent site.

An MSU uses the following criteria when deciding whether to move to a new site:

- Only attempt to change sites if an adjacent site is better, based on Received Signal Strength Indicator (RSSI) and other ranking fields.
- If the current channel fails, attempt to find another channel at this site before attempting to move to another site.
- Attempt to stay in wide area coverage at all times.
- When searching for an adjacent site, first try the adjacent site list, then the pre-programmed scan list. (Full spectrum scan is not supported in this release.)

MSUs perform an adjacent site RSSI sampling occasionally during the broadcast Control Channel time slot. It allows the MSUs to sample signaling at adjacent sites without conflicts with any inbound or outbound traffic that is scheduled for the MSU.

2.6.1
Site Ranking Criteria

The Mobile Subscriber Units (MSU) use the following ranking criteria to determine the most favorable site to be registered with.

- Site Validity (indicated through adjacent site broadcast)
- Network Access (wide area or local area mode)

- Site Preference (MSUs can be programmed to prefer specific sites through CPS)
- Channel Ranking (indication of the rank of the channels at the site)

2.6.2
RSSI Thresholds

Under normal conditions, Mobile Subscriber Unit (MSU) switches to the home channel on the highest ranked site (if the new site has a signal quality that is at least two levels higher than the current channel on the current site).

- Poor
- Acceptable
- Good
- Very Good
- Excellent

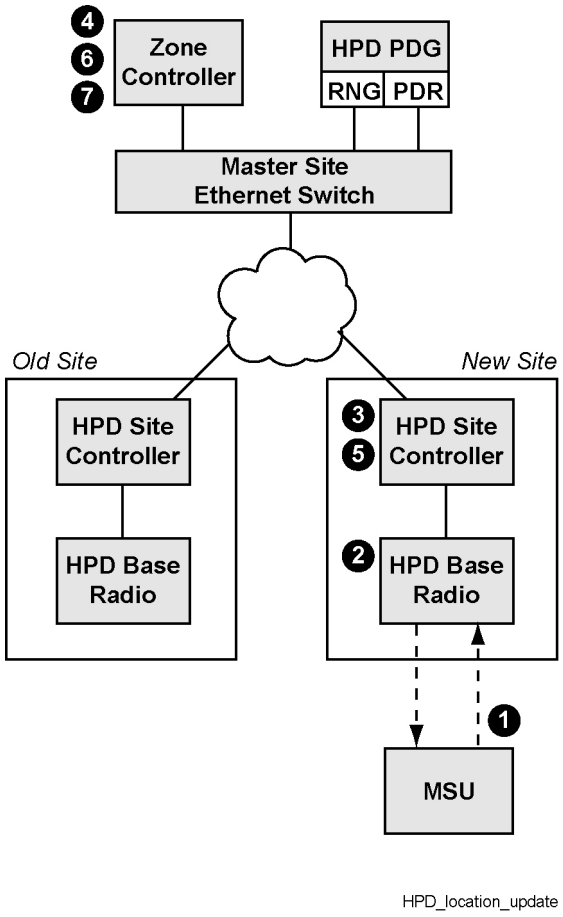
2.7
Location Update

Mobile Subscriber Units (MSU) can maintain continuous access to High Performance Data (HPD) services while roaming throughout the coverage area. When an MSU has determined that a different site has better qualities than its current site (through adjacent site scanning), it can perform a location update to the new site.

The location update does not affect the status of the active context. However, some traffic that is scheduled for the MSU can be affected during the location update.

Figure 6: Location Update

The following diagram shows the location update sequence.



1. When an MSU has found a more favorable site in the system, it sends a location update request to the new site.
2. The HPD BR at the new site sends an air interface confirmation of the received traffic, and sends the information to the HPD SC.
3. The HPD SC updates its database and forwards the request to the zone controller for processing.
4. The zone controller determines whether the location update is valid. The zone controller updates its VLR and sends a location update response to the HPD SC at the new site.
5. The HPD SC updates its database, determines if the MSU should be moved to another channel at the site (for channel loading purposes), and sends the location update response to HPD BR for transmission to the MSU.
6. The zone controller sends a command to the HPD SC at the old site. This command indicates that the MSU should be removed from its database and the connection should be terminated.
7. The zone controller pushes the updated VLR information to the High Performance Data Radio Network Gateway (HPD RNG), allowing the HPD RNG to continue sending outbound traffic for the MSU to the appropriate site.

2.8 Channel Changes Within a Site

Mobile Subscriber Units (MSUs) can change to another channel at a site in the following situations.

- The MSUs is given a channel loading command from the High Performance Data (HPD) site.
- A channel failure has occurred at the site.

2.8.1
Channel Loading

The High Performance Data (HPD) site controller administers the channel loading of Mobile Subscriber Units (MSU) at the site. MSUs always register with the home channel at a site, and any roaming MSUs also attempts to perform a location update through the home channel. After an MSU successfully performs a unit registration or location update at the site, the HPD SC sends a Channel Command to assign the MSU to the channel that currently has a lower loading. The MSU then remains at the assigned channel until it roams to another site or until the assigned channel fails.

If an MSU attempts to move to an assigned channel but cannot successfully access the channel, the MSU can return to the original channel it was operating on.

Any channel changes are handled locally at the site. A channel change within the same site does not require a new registration or context activation from the MSU.

2.8.2
Channel Change Due to Failure

Each channel at a High Performance Data (HPD) site periodically informs the Mobile Subscriber Unit (MSU) population of additional channels at the site. MSUs maintain this information in an internal list.

If an MSU is operating on a channel that fails, it first attempts to select another channel at the current site before attempting to scan for adjacent sites. If another channel is available at the site, the MSU should be able to change channels successfully.

The channel change is handled locally at the site, and does not require a new registration or context activation from the MSU.

2.9
Data Transmission – IP Bearer Service

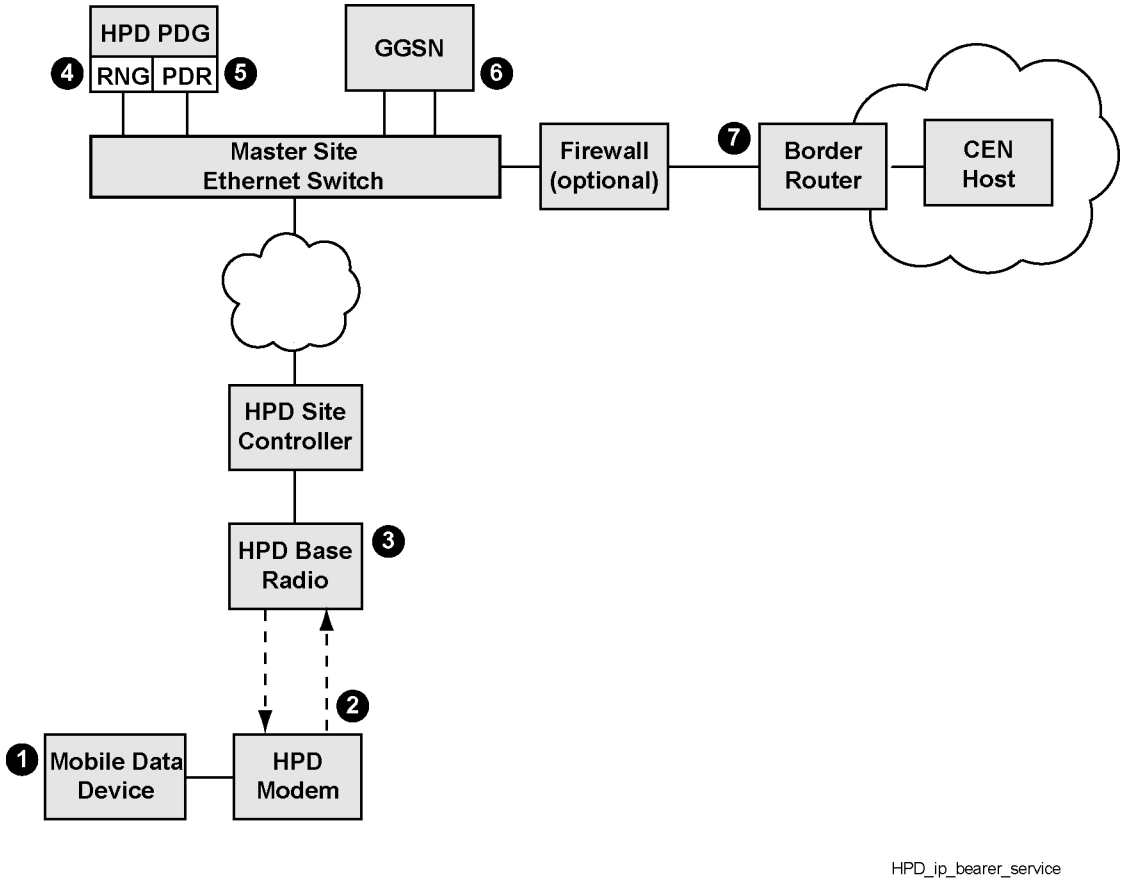
After a Mobile Subscriber Unit (MSU) is successfully registered and context-activated, it sends and receives High Performance Data (HPD) user data through the system. The diagram and process explain the general path of user data through the system.

The Data System record in Unified Network Configurator (UNC) is provisioned with LLC User Plane Response Time, LLC User Plane Number of Confirmed Retries (Inbound/Outbound), and LLC User Plane Window Size parameters.

When the High Performance Data Radio Network Gateway (HPD RNG) or an MSU sends user data through the system, it expects to receive an acknowledgment from the other end of the tunnel. If an acknowledgment is not received before the response time expires, the HPD RNG or MSU can resend the traffic. The HPD RNG or MSU can perform up to the maximum number of retries defined in UNC.

The windowing parameter defines the maximum number of unacknowledged frames that can be sent out by an MSU or HPD RNG. This parameter is used to throttle the transmissions and not overwhelm the receiver of the traffic. The HPD RNGs in the system use the response time, maximum retries, and windowing values and periodically broadcasts to the MSUs.

Figure 7: IP Bearer Service



1 An application on the mobile data device prepares IP datagrams for a host on the Customer Enterprise Network (CEN). The mobile data device sends the datagrams (addressed to the CEN host) to the HPD modem.

2 The HPD modem performs network address translation, as necessary, encapsulates the traffic, and schedules the traffic to be sent over the HPD channel. The HPD modem initiates a response timer for the expected acknowledgment.

3 The HPD BR forwards the traffic to the HPD SC, which then forwards the traffic to the HPD RNG in the zone.

4 The HPD RNG replies with an acknowledgment to the MSU and forwards the inbound traffic to the High Performance Data Packet Data Router (HPD PDR) that is in the home zone of the MSU.

5 The HPD PDR prepares the traffic and sends it through the GTP tunnel to the Gateway GPRS Support Node (GGSN).

6 The GGSN sends the traffic through an IP-IP tunnel to the appropriate Access Point Name (APN)/ Customer Enterprise Network (CEN). The traffic is passed through the firewall (if installed) and routed through the peripheral network to the destination CEN.

7 The border router at the CEN removes the IP-IP encapsulation and routes the traffic to the appropriate host on the CEN.

2.9.1
Inbound IP-IP Routing

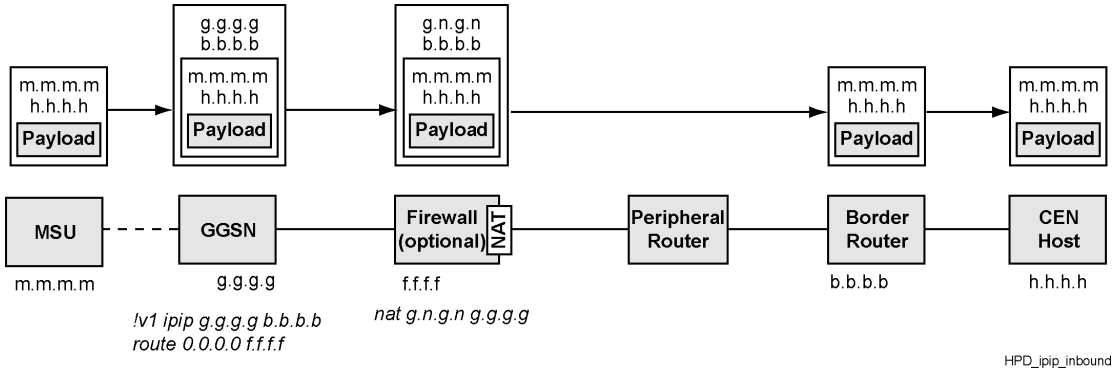
Inbound datagrams are originated by a Mobile Subscriber Unit (MSU) and routed through the network to a destination Customer Enterprise Network (CEN). The Gateway GPRS Support Node (GGSN) is

provisioned with a virtual port and an IP-IP tunnel for each Access Point Name (APN)/Customer Enterprise Network (CEN). The GGSN encapsulates traffic and delivers the traffic over the peripheral network to the appropriate CEN. The destination CEN is determined by the context that is established for the MSU.

If the optional firewall is installed in the system, then the firewall performs network address translation on the GGSN IP address before the traffic is sent over the peripheral network.

The diagram and process gives a basic explanation of the inbound IP-IP routing between the GGSN and border router at the CEN. Some intermediate devices are not shown and generic IP addresses are used.

Figure 8: Inbound IP-IP Routing



1. The MSU (m.m.m.m) sends a datagram addressed to the Customer Enterprise Network (CEN) host (h.h.h.h) through the system. The system routes the datagram to the Gateway GPRS Support Node (GGSN).
2. The GGSN assigns the datagram to a virtual port that is associated with the destination Access Point Name (APN) (!v1). This virtual port has an IP-IP tunnel defined to the border router at that APN (b.b.b.b). The GGSN encapsulates the datagram and addresses the datagram to that border router.
3. The GGSN has a static route defined to the firewall (f.f.f.f). So the datagram is sent to the firewall. If a firewall is not present, then the datagram is sent directly to the peripheral network.
4. The firewall (optional) performs network address translation on the GGSN IP address (translating the GGSN address to g.n.g.n). The firewall then forwards the datagram to the peripheral network.
5. The datagram is sent to the destination border router (d.d.d.d). If the border router is not locally connected on the DMZ switch, then the traffic is routed to the destination through a peripheral network router.
6. The border router receives the datagram, removes the encapsulation, and routes the datagram to the target host (h.h.h.h).

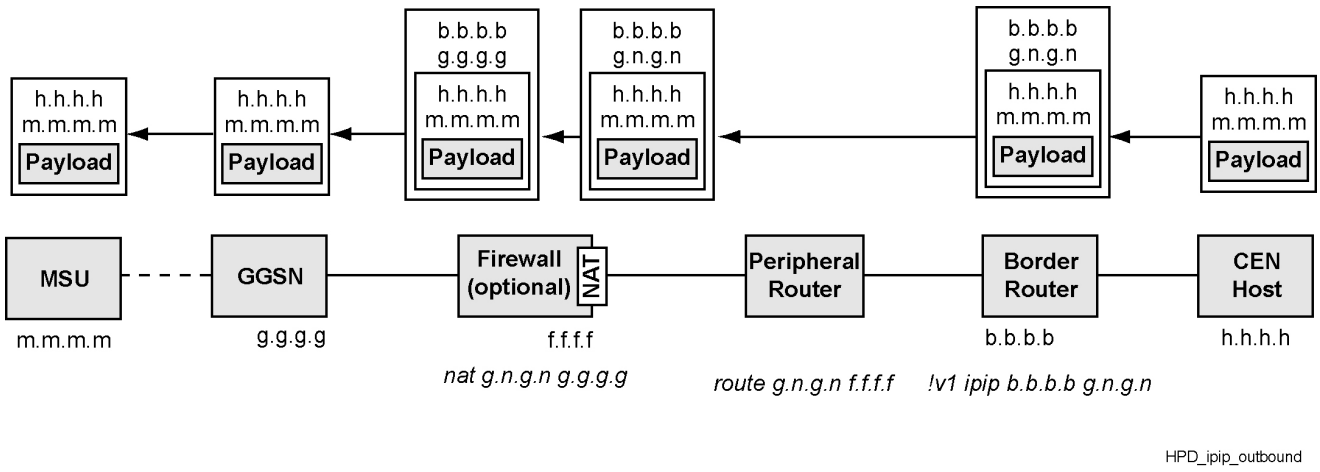
2.9.2
Outbound IP-IP Routing

Outbound traffic is originated from a host on the Customer Enterprise Network (CEN) and routed through the system to a destination Mobile Subscriber Unit (MSU). Each border router must be configured to route traffic intended for MSUs through the Gateway GPRS Support Node (GGSN). When the border router receives a datagram from a host on CEN it encapsulates the datagram and addresses the datagram to the GGSN. If the optional firewall is used in the system, then the border router uses the NAT address of the GGSN as the destination

Border routers can also be provisioned for IP-IP routing to other CENs over the peripheral network. It would require additional virtual ports to be configured to each of the other CENs.

Figure 9: Outbound IP-IP Routing

The following diagram explains the general process for routing outbound traffic from a CEN host to an MSU.



1. The Customer Enterprise Network (CEN) host (h.h.h.h) sends a datagram addressed for the MSU (m.m.m.m).
2. The border router determines that the address is for a node on the radio network (MSU). The border router assigns the datagram to a virtual port that is associated with the Gateway GPRS Support Node (GGSN). The virtual port has an IP-IP tunnel defined between itself and the GGSN. The border router encapsulates the datagram and addresses the datagram using the NAT address for the GGSN (g.n.g.n).
3. If the border router is not locally connected to the DMZ switch at the customer network interface, then the datagram is routed through a peripheral network router. The peripheral router has a route defined for any traffic addressed to the GGSN NAT address. This route definition causes the peripheral router to forward the datagram to the firewall (f.f.f.f).
4. The firewall (optional) translates the GGSN address (g.g.g.g) and forwards the datagram to the GGSN. If a firewall is not installed, then the traffic is received over the DMZ VLAN and address translation is handled by the gateway router.
5. The GGSN removes the IP-IP encapsulation and forwards the datagram through the system. The High Performance Data Packet Data Router (HPD PDR) and High Performance Data Radio Network Gateway (HPD RNG) determine the location of the MSU and route the traffic to the appropriate site.
6. The datagram is delivered to the MSU (HPD modem). The HPD modem can perform NAT translation on the datagram before it is forwarded to the mobile data device.

2.10 Timers and Parameters

The system and Mobile Subscriber Units (MSU) are provisioned with some important timers and time values. These values prevent conflicts in the system, maintain order during failure situations, and cause time-outs and remedial action when expected responses are not received. The diagram and table reflect how some time values and parameters are used within the system for High Performance Data (HPD) operation. The MSU receives many of its parameters through broadcasts from the system. For additional information about the system timers and parameters, see the configuration instructions.

Figure 10: System Timers and Parameters

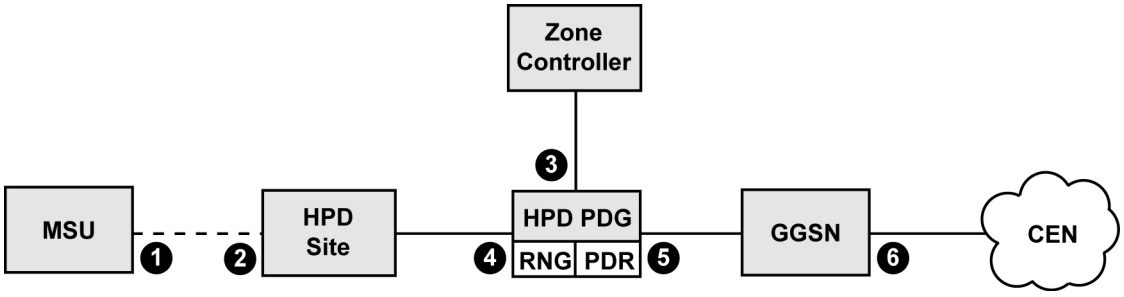


Table 2: Timers and Parameters

Number	Device	Parameters
1	MSU	The MSU is affected by the following system parameters and timers: • HPD Standby Timer • Channel Access Hold-Off Time • Recovery Random Hold-Off Time • Failure Random Hold-Off Time • LLC User Plane Window Size • LLC User Plane Number of Confirmed Retries (Inbound) • LLC User Plane Response Time • Random Access Response Timer • Activation Wait Timer • HPD Advanced Parameters
2	HPD Site	An HPD site uses the following time values: • Context Activation Hold-Off Time • Channel Access Hold-Off Time • Recovery Random Hold-Off Time • Failure Random Hold-Off Time
3	HPD PDG	The following timer is used by the High Performance Data Packet Data Gateway (HPD PDG) for the interface to the ZC: • Mobility Query Timer
4	HPD PDG	The HPD PDG uses the following system parameters and time settings for the interface to the HPD remote sites and MSUs: • SNDCP Queue Dwell Time • LLC User Plane Window Size • LLC User Plane Number of Confirmed Retries (Inbound) • LLC User Plane Response Time
5	HPD PDR	The following system settings are used by the High Performance Data Packet Data Router (HPD PDR) for the interface to the Gateway GPRS Support Node (GGSN):

Table continued...

Number	Device	Parameters
		• GTP T3 Timer • GTP N3 Number of Attempts
6	GGSN	The Gateway GPRS Support Node (GGSN) uses the following system settings and time values for its connection to the CEN equipment: • RADIUS/DHCP Retransmit Time • RADIUS/DHCP Retransmit Count • RADIUS/DHCP Server Switchover

2.10.1
Context Activation Hold-Off Time (CAHT)

Context activation (CA) is the process by which data call registration and service activation is implemented by the ASTRO® 25 system. Context Activation Hold-Off Time (CAHT) is the time a subscriber waits before sending Context Activation/Renew message, when it receives the CA status message. CAHT timer values are in minutes.

2.10.2
Channel Access Hold-Off Time (CAHOT)

When a site is involved with a failure situation, the Mobile Subscriber Units (MSU) hold off from registering with the system or performing any location updates for a random period, up to the Channel Access Hold-Off Time (CAHOT). This parameter is defined for each High Performance Data (HPD) Site record in Unified Network Configurator (UNC).

2.10.3
Recovery Random Hold-Off Time (RRHOT)

When a failed site is restored to normal operation, all Mobile Subscriber Units (MSU) in the coverage area can try to simultaneously flood back to the recovered site, causing collisions and congestion. For this purpose, a Recovery Random Hold-Off Time (RRHOT) is used.

When a site recovery is taking place, the wide area sites that are near the recovered site broadcast the Recovery Hold-Off Time to the MSU population. MSUs are allowed to roam back to a recovered site in a random time period up to a maximum of the RRHOT time. This parameter is defined for each High Performance Data (HPD) Site record in Unified Network Configurator (UNC).

2.10.4
Failure Random Hold-Off Time (FRHOT)

When a site loses wide area connection with the master site, or when the site fails by other means, all Mobile Subscriber Units (MSU) leave the site and attempt to register with other adjacent sites. To prevent all the MSUs from simultaneously shifting from one site to another (causing congestion and collisions), a Failure Random Hold-Off Time (FRHOT) is used.

When a site failure occurs, all the wide area sites that are near the failed site broadcast the FRHOT. An MSU must wait a random time period up to a maximum of the broadcasts FRHOT time before it registers to the sites in wide area mode. This parameter is defined for each High Performance Data (HPD) Site record in Unified Network Configurator (UNC).

2.10.5
Activation Wait Timer

The Activation Wait Timer is programmed into the Mobile Subscriber Unit (MSU) to handle conditions where a context activation response is not received from the system. The MSU considers the context activation has failed, if it sends a context activation request and does not receive any response from the system before the Activation Wait Timer expires. The MSU does not automatically retry the context activation. The Activation Wait Timer is provisioned in the High Performance Data (HPD) modem through CPS.

2.10.6
Random Access Response Timer

The Random Access Response Timer value is provisioned in the High Performance Data (HPD) base radios, and is periodically broadcasts to the Mobile Subscriber Units (MSU). MSUs run the response timer when sending information over a random access subslot. If the system does not respond before this timer expires, the MSU runs its backoff algorithm and retries its random access transmission. After the maximum number of retries, the MSU considers that the channel is unavailable and can seek another channel.

The Random Access Response Timer and other related parameters are configured in the HPD BRs through the Configuration/Service Software (CSS) application.

2.10.7
HPD Standby Timer

The High Performance Data (HPD) Standby Timer is used to delete aged contexts. During context activation, the Mobile Subscriber Unit (MSU) receives a standby timer value from the system and initiates the timer. A standby timer for the MSU is also maintained in the Radio Network Gateway (RNG). The MSU must renew its context before the standby timer expires. Otherwise, the system deactivates the context. The HPD Standby Timer value is defined in the Data System record in Unified Network Configurator (UNC).

2.10.8
InterZone Debounce Timer

The Mobile Subscriber Unit (MSU) utilizes an InterZone debouncing function to prevent potential problems that could occur when an MSU roams quickly back and forth between zones. The MSU starts the debounce timer upon completion of the unit registration or location registration procedure in a new zone.

If the MSU wishes to select a new channel in another zone while the debounce timer is still running, the MSU waits for the debounce timer to expire before initiating the unit registration or location registration procedure. It prevents the MSU from bouncing between zones and potentially creating race conditions in the radio network. If other failure or recovery timers are running during an InterZone handoff event, the debounce timer and all failure and recovery timers must expire before the MSU initiates the unit registration or location registration procedure.

The value for the InterZone debounce timer is defined in the System record in Unified Network Configurator (UNC).

2.10.9
Mobility Query Timer

The High Performance Data Packet Data Router (HPD PDR) and High Performance Data Radio Network Gateway (HPD RNG) use the mobility query timer when requesting mobility information from

the zone controller. This timer is used along with an Outstanding Queries parameter to keep mobility queries from flooding the ZC. This value is defined in Unified Network Configurator (UNC).

2.10.10
SNDCP Queue Dwell Time

The High Performance Data Packet Data Router (HPD PDR) maintains a buffer, called the SNDCP queue, which stores outbound datagrams until they are ready to be sent over the wireless interface. The HPD FNE SNDCP Queue Dwell Time indicates the maximum amount of time a datagram can be retained in the SNDCP queue before it is discarded. This time value is configured in Unified Network Configurator (UNC).

2.10.11
LLC User Plane Parameters

The High Performance Data Radio Network Gateway (HPD RNG) and by Mobile Subscriber Units (MSU) in the system use the LLC User Plane Response Time to determine the amount of time to wait for an acknowledgment of traffic. After this time expires, the HPD RNG or MSU that sent the traffic can retransmit. This time value is used with the LLC User Plane Window Size and LLC User Plane Number of Confirmed Retries parameters.

The LLC User Plane Window Size determines the maximum number of unacknowledged packets that are sent to a destination, and is used to throttle the data flow over the network to the destination device.

The Radio Network Gateway (RNG) uses the LLC User Plane Number of Confirmed Retries (Outbound) parameter to determine the maximum number of retries for outbound user data that can be made to a particular MSU over the air interface.

Inbound and outbound values for LLC User Plane Number of Confirmed Retries are defined in Unified Network Configurator (UNC). The HPD RNG uses the outbound value to determine the maximum number of retries that is used for outbound user data to a particular MSU over the air interface. The MSUs use the inbound value is broadcast to MSUs on the system to determine the maximum number of retries that is made on inbound user data over the air interface.

All the LLC User Plane parameters are defined in UNC.

2.10.12
GTP Parameters

The High Performance Data Packet Data Router (HPD PDR) uses the GTP T3 Timer to determine the maximum amount of time that an HPD PDR should wait for a context activation response from the Gateway GPRS Support Node (GGSN). When this timer expires, the HPD PDR can retry the context activation request until the GTP N3 Number of Attempts parameter is exceeded. Both of these parameters are defined in Unified Network Configurator (UNC).

2.10.13
RADIUS/DHCP Parameters

The Gateway GPRS Support Node (GGSN) is provisioned with Retransmit Time, Retransmit Count, and Switchover Count values for the RADIUS or DHCP server on each defined Access Point Name (APN)/Customer Enterprise Network (CEN). These parameters define how the GGSN manages the interface to the RADIUS or DHCP server.

The Retransmit Time value defines the amount of time that the GGSN uses between retransmissions to a RADIUS or DHCP server on the CEN It is used to ensure that retransmissions do not occur too quickly or too slowly. The Retransmit Count value identifies the total number of retries that the GGSN attempts to a RADIUS or DHCP server before considering that the service has failed. The Switchover

Count value identifies the maximum number of tries that the GGSN attempts before trying a secondary RADIUS or DHCP server.

The GGSN parameters are configured using the Unified Network Configurator (UNC).

2.11 HPD Broadcast Data

The High Performance Data (HPD) Broadcast Data feature builds on the precedent HPD architecture by introducing broadcast data capability. 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 users, each of which are part of a Broadcast Agency Group. Text messages, text alerts, small images such as AMBER alert photos, and the GNSS coordinates of all fleet members are examples of the types of messages to be sent.

Subscriber initiated broadcast message is not supported. Subscriber supports of dynamic or static IP on the precedent HPD architecture is unaffected by this feature.

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 is regardless of whether there are subscribers on the sites. A site upon receiving a broadcast data message replicates the broadcast message for transmission over each HPD data channel ensuring that all modems have the opportunity to receive the message.

The HPD Broadcast feature heavily leverages the approach and implementation of the Data Broadcast solution architecture for the IVD Broadcast Data feature. A Broadcast Data Agency is configured as a radio user with an assigned IP address, much like the configuration of a subscriber. The transmission of broadcast data is outbound only. The transmission of HPD Broadcast Data operates much the same as outbound unicast data up to the Packet Data Router (PDR). The PDR then recognizes the outbound data as broadcast from the destination IP address and relay them to the Radio Network Gateway (RNG) for fragmentation and broadcast to the sites over the HPD Broadcast Multicast IP group. Fragmentation by the RNG involves formatting the outbound data into message blocks compatible for over-the-air transfer by the sites. The outbound data received by the subscribers is then reassembled and forward to the data application running in the mobile computer connected to the subscriber.

The Broadcast Data multicast tree formed between the RNG and the SCs (Site Controllers) is used exclusively for the transmission of Broadcast Data. The transmission only happens from the RNG to the SCs, no messages are sent from any of the SCs back to the RNG to control or shape the Broadcast Data traffic.

2.11.1 HPD Broadcast Data Capabilities and Constraints

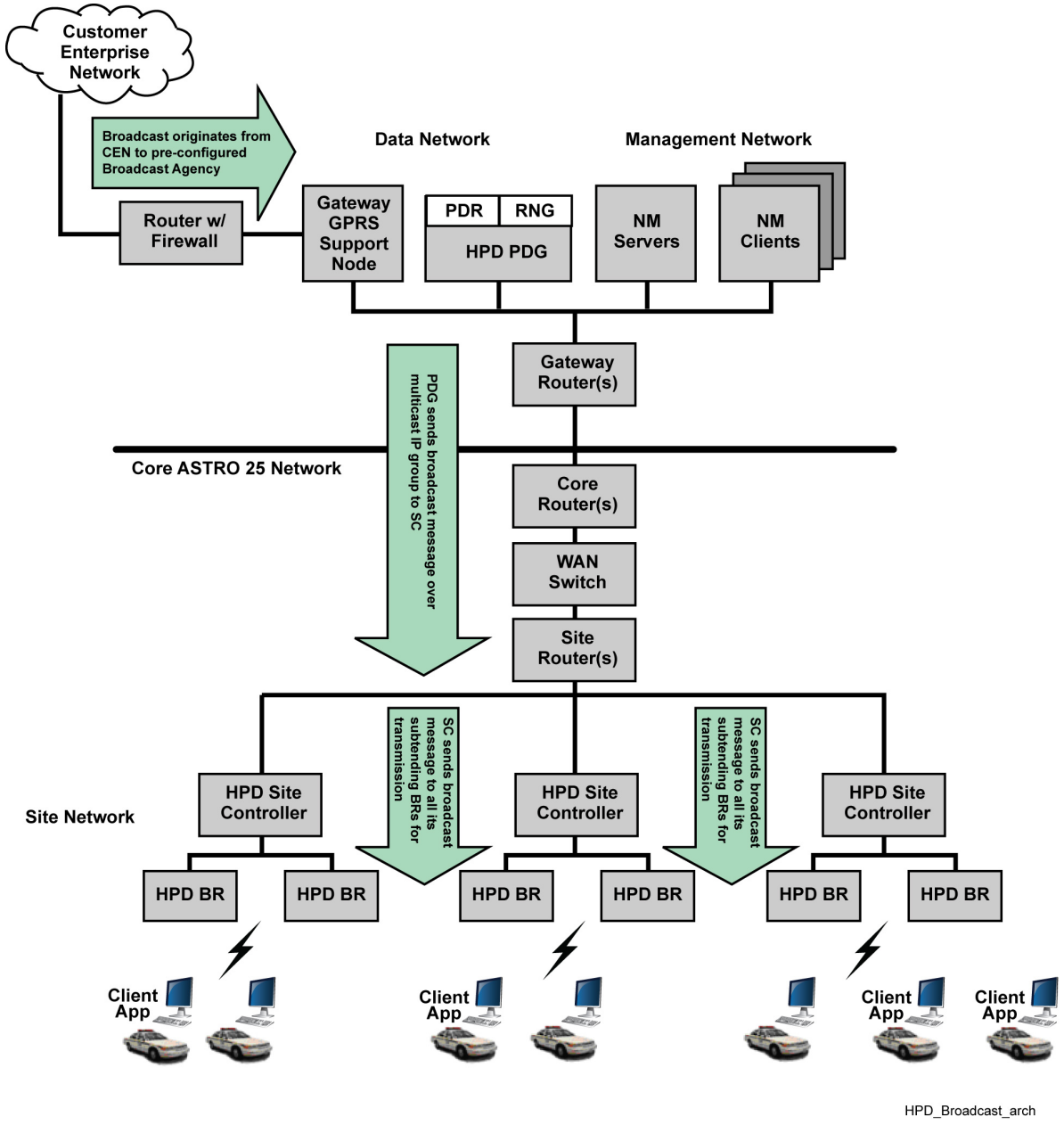
The following capabilities and constraints characterize the High Performance Data (HPD) Broadcast Data functionality.

- Operation in the 700 MHz and 800 MHz frequency bands at 32 kbps non-configurable raw bit rate. The 32 kbps raw bit rate is the upper limit of 25 kHz bandwidth at 4-QAM, 1/2 rate to maintain an acceptable probability of successful broadcast message delivery to the Subscribers.
- Operation in up to seven zones.
- Up to 20,000 active High Performance Data (HPD) data subscribers.
- With inter-mixed of outbound unicast and broadcast messages, up to 300 broadcast messages per hour per zone, each of size up to 1500 bytes in length. Only one broadcast message in flight at a time per zone.
- Mission critical broadcast is outside the HPD Broadcast Data scope. HPD Broadcast Data feature uses best effort delivery using over-the-air unconfirmed data over UDP traffic at the transport layer,

using the reliable modulation type and coding rate of 4-QAM and 1/2 rate respectively, with four times repeated transmission.

- HPD Broadcast Data is intended for relatively small data messages, such as text messages, text alerts, small images such as photos, and GNSS coordinates. Since delivery of the broadcast data is best effort, smaller application messages (files) have a greater probability of being received correctly in their entirety.
- HPD Broadcast Data does not support over the air encryption. It reuses what is already in place in the precedent HPD system and IA features. While the encryption is not supported over the air, overall security threats can be mitigated by supporting security at the higher layers (IP layer and application layer security). Security at the higher layers is not part of the HPD Broadcast Data scope.
- Developments of applications that leverage the HPD Broadcast Data are outside the scope of this feature. Interface to HPD Broadcast Data can be found in the HPD Application Design Guide.
- In order to support system-wide broadcast, each Zone must be configured with the desired Broadcast Groups. A Zone that is configured to support that Broadcast Group forward the message to the appropriate sites within their respective zone. To accomplish a broadcast message to a Broadcast Data Agency over a multi-zone system, the same broadcast message must be sent to the Broadcast Data Agency configured with a unique IP address in each zone of the multi-zone system.

Figure 11: HPD Broadcast Architecture



2.11.2

HPD Broadcast Data and Network Management

The Unified Network Communicator (UNC) communicates the High Performance Data (HPD) Broadcast Data Capability, Maximum Utilization for HPD Broadcast parameters, and any configured Broadcast Data Agency IDs to the Packet Data Router (PDR).

The NM also communicates the HPD Broadcast Data Capability and HPD Broadcast Data Multicast IP Address parameters to the SCs.

2.11.3
HPD Broadcast Data and PDR/RNG

The Packet Data Router (PDR) communicates the Maximum Utilization for High Performance Data (HPD) Broadcast parameters and the Broadcast Data Agency IDs it received from UNC to the local Radio Network Gateway (RNG). The PDR resolves the HPD Broadcast Data Multicast IP Address from DNS and communicates them to the local RNG. The local RNG relays the Broadcast Data Agency IDs it received from the PDR to the SCs. The RNG begins transmitting HELLO messages over the HPD Broadcast Data Multicast IP Address it received from the PDR.

The PDR is also responsible for maintaining Context Activations for the configured Broadcast Data Agencies with the Gateway GPRS Support Node (GGSN). For the multi-zone system deployments, each PDR independently maintains Context Activations for their Broadcast Data Agencies with the GGSN. Maintaining Context Activations for the configured Broadcast Data Agencies includes re-establishing them should the GGSN -> PDR link re-initialize. The Context Activations for the configured Broadcast Data Agencies with the GGSN here do not involve over-the-air transactions with the subscribers.

2.11.4
HPD Broadcast Data and Site Controller

If the HPD Broadcast Data Capability parameter is enabled, the Site Controller joins the HPD Broadcast Data Multicast Group using the HPD Broadcast Data Multicast IP Address. The Site Controller receives the Broadcast Data Capability parameter and the HPD Broadcast Data Multicast IP Address from the Unified Network Configurator (UNC).

The SC reserves the highest 20 Subscriber Access Codes (SACs) in the range of 4092 – 4073. It then maps them to the corresponding Broadcast Data Agency IDs it received from the Radio Network Gateway (RNG) via the indexes (in the range of 1 – 20) associated with each of the Broadcast Data Agency IDs.

2.11.5
HPD Broadcast Data and Subscriber Context Activation

Each broadcast data enabled subscriber is provisioned with the system-wide all-call Broadcast Data Agency ID (0xFFFFFB) by default. This allows for the configuration of up to seven other Broadcast Data Agency IDs, thus the maximum of eight Broadcast IDs per subscriber.

Subscriber context activation occurs when a Subscriber application needs to use the Subscriber-to-FNE connection for data communications. On successful context activation, the subscriber receives the Broadcast Data Agency ID -> SAC mapping pairs from the BR. The Subscriber retains the SACs that match its Broadcast Data Agency IDs configured via CPS. The Subscriber then uses the retained SACs to identify the outbound Broadcast data from the FNE for the duration of its context activation session.

2.11.6
Broadcast Data Service

The transmission of High Performance Data (HPD) Broadcast data started at the fixed host sending IP datagrams with the destination address of the configured IP address of the Broadcast Data Agency in each zone. The Gateway GPRS Support Node (GGSN) forwards the outbound IP datagram to the Packet Data Router (PDR) through the GTP tunnel established for the Broadcast Data Agency.

The PDR replaces the destination address with the broadcast IP address of 255.255.255.255 and forwards the IP datagram in an Outbound Data Request to the Radio Network Gateway (RNG), with the Broadcast Data Agency ID of the Broadcast Data Agency that corresponds to the original destination IP address of the datagram. The RNG fragments the received outbound data into Logical

Link Control (LLC) segments compatible for over-the-air transfer and broadcast them to the SCs over the HPD Broadcast Multicast IP address.

The SCs receiving the LLC segments over the HPD Broadcast Multicast IP address, performs L2_ID to SAC mapping for the appropriate Broadcast Data Agency, and forward the LLC segments to their subtending Base Radios (BRs). Each BR then transmits the LLC segments over the air using unconfirmed service with 4-QAM, ½ rate, and 4 repeats. The repeats are accomplished by sending all the LLC segments sequentially one time, then repeating all the segments again until the required number of repeat transmissions has occurred. The number of repeats is not configurable.

The Subscriber listening to the outbound channel receives the unconfirmed LLC segments. It buffers the data if the SAC of the received LLC segments matches any of the SACs (in the Broadcast Data Agency ID -> SAC mapping pairs) it received and retained during context activation. Upon successfully receiving all the LLC segments, the Subscriber passes the assembled segments up to the attached mobile computer. The Subscriber also performs duplicate reduction on the LLC segments. This is because the LLC segments are transmitted by the BR with repeats. The Subscriber discards LLC segments with SACs that do not match any of the SACs it received during context activation.

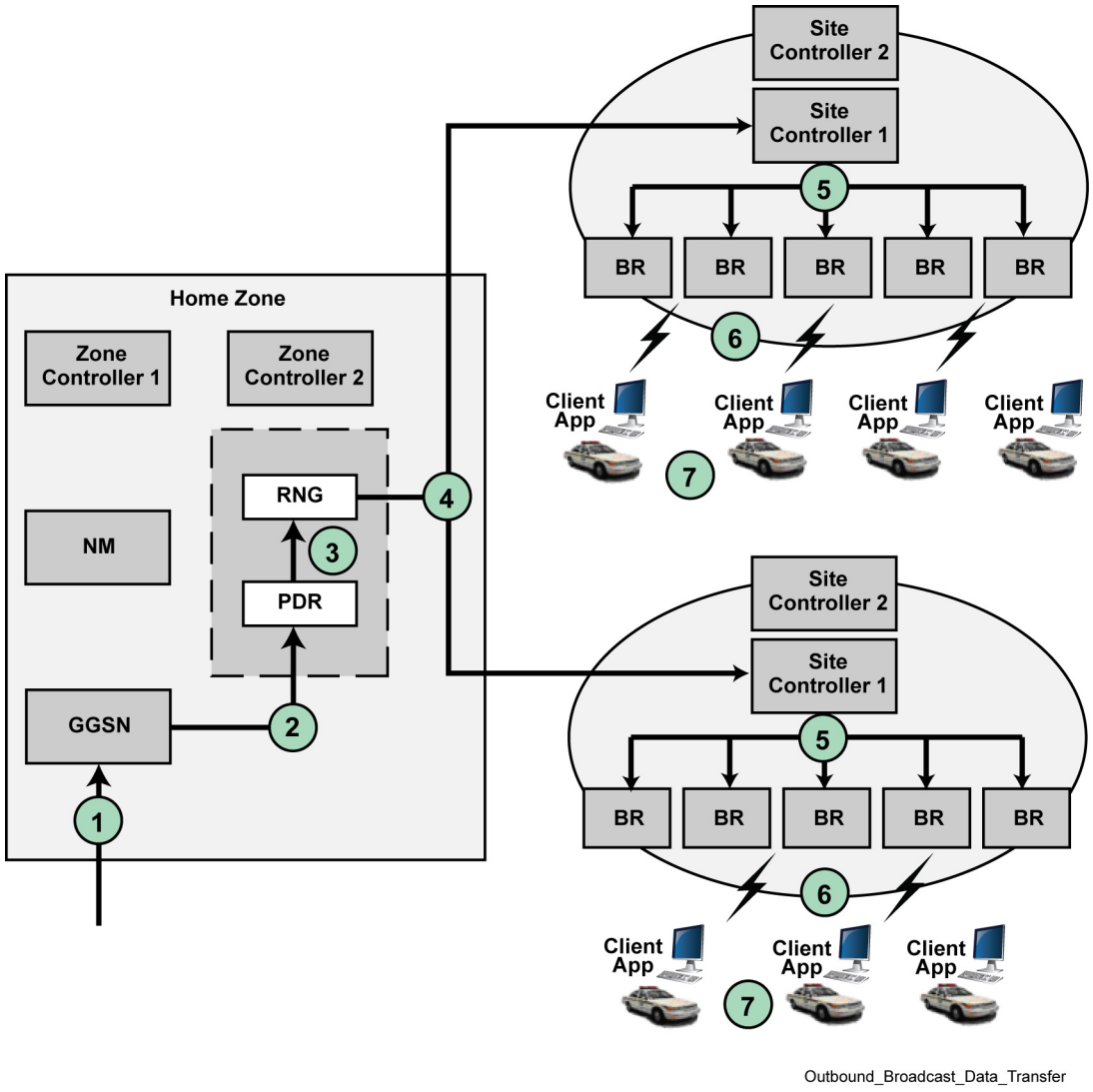
2.11.6.1
Broadcast Data Pacing

The transmission of broadcast data has priority over unicast data. The Maximum Utilization for the High Performance Data (HPD) broadcast parameter is used to mitigate broadcast data from taking over full control of the outbound channel. The pacing of broadcast data by the Radio Network Gateway (RNG) based on the configuration value of Maximum Utilization for HPD broadcast and the broadcast message size, ensuring outbound opportunities for unicast data. The pacing of Broadcast Data by the RNG also ensures inbound unicast opportunities for half-duplex subscribers.

2.11.6.2
Outbound Broadcast Data Transfer

The following diagram and process flow show an example of an broadcast data transfer

Figure 12: HPD Outbound Broadcast Data Transfer



1 GGSN
The Gateway GPRS Support Node (GGSN) receives a datagram destined for Broadcast delivery identified by the Destination IP Address of the message.

2 GGSN to PDR
The GGSN forwards the message to the Packet Data Router (PDR) associated with the Destination IP address in the received message.

3 PDR to RNG
The PDR replaces the Destination IP Address with 255.255.255.255 and forward message to the Radio Network Gateway (RNG).

4 RNG to Site Controller
The RNG broadcasts the received message with the Destination IP Address of 255.255.255.255 to the Site Controller over the Multicast IP Address

5 Site Controller to BRs
The Site Controller sends the received message with the Destination IP Address of 255.255.255.255 to all its subtending BRs.

6 **BR**
The BR transmits the received message with Destination IP Address of 255.255.255.255 over-the-air using 4-QAM, 1/2 rate with four repeats.

7 **Subscriber**
The Subscriber forwards the received message with Destination IP Address of 255.255.255.255 to the Mobile Computer.

2.11.7
Broadcast Data Agency Configuration

The Packet Data Router (PDR) continues to maintain the broadcast data paths it established for the Broadcast Data Agencies with the Gateway GPRS Support Node (GGSN). This task includes activations and deactivations for new and deleted Broadcast Data Agencies at the Provisioning Manager during runtime. The PDR also continues to send any Broadcast Data Agency updates to the Site Controllers. The system does not force the subscribers in Context Activate state to Context Activate again just because Broadcast Data Agency has changed. This is because updates to the Broadcast Data Agencies are expected to be infrequent occurrence, and any new agencies have to be configured on all subscribers associated with the new Agencies.

2.11.8
Capacity Planning

During broadcast data transmission, the system blocks/queues all other outbound messages until the Broadcast data transmission is completed. Also during broadcast data transmission, a half-duplex subscriber blocks/queues all its inbound messages until the Broadcast data transmission is completed.

2.12
Other Planning Considerations

This section covers considerations relating to the commissioning and ongoing maintenance of the High Performance Data (HPD) Broadcast Data feature.

2.12.1
Installation

If you are interested in High Performance Data (HPD) Broadcast Data, profile the application before adding Broadcast data to their HPD systems. For information on application profiling techniques, contact your field system engineering organization.

2.12.1.1
Installation Tools

The High Performance Data (HPD) Broadcast Data feature does not require any new installation of tools beyond items required to install and troubleshoot general network equipment.

2.12.1.2
Hardware Installation Considerations

The High Performance Data (HPD) Broadcast Data feature does not introduce any new hardware platforms to the system.

2.12.1.3

Software Installation Considerations

Software required for the High Performance Data (HPD) Broadcast Data feature is included with the system. A separate install for the HPD Broadcast Data feature is not required.

2.12.2

Configuration

The High Performance Data (HPD) Broadcast Data feature is Enabled or Disabled system wide by the UNC. Up to 20 Broadcast Data Agencies can be configured in the system with the Provisioning Manager using reserved IP addresses. A standalone IVD or HPD system can support up to 20 Broadcast Data Agencies. An IVD and HPD overlay system can support up to 20 Broadcast Data Agencies combined. In an overlay system, a specific Broadcast Data Agency can only be used for IVD 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 the Enabling and Disabling of HPD Broadcast Data in a subscriber is performed by the CPS.

The same Broadcast ID within an Access Point Name (APN) has associated different IP addresses between zone cores. The IP addresses are unique within a system for a given APN. For information about the mapping between Broadcast ID, APN, and the configuration of IP addresses per zone core, see your IP plan or contact your system administrator. At most, there can be 20 associations per zone core (one per Broadcast ID).

The Broadcast Data Agency Parameters tables include parameters for IVD and HPD Broadcast Data configurable by the Provisioning Manager.

Table 3: Broadcast Data Agency Parameters – Identity

Field	Default	Allowed Values	Description
Radio ID	N/A	1 to 16,777,211 10,000,000 to 16,777,211	Enter a number that refers to a specific radio on the system. This ID is unique within the system. **IMPORTANT:** Do not exceed the total number of individual IDs. This can overload the resources in your system. You can enter up to 64,000 total radios into the system. The total range of individual identification numbers used by the system is 16,777,217. The IDs are distributed as follows: • 1 to 16,777,211 are available for assignment to radios and console resources • 16,777,212 to 16,777,217 are reserved for system use
Broadcast Data Agency Alias	N/A	1 to 16 characters. Use the following characters: A to Z, a to z, 0 to 9, space ! #	Enter a unique name.

Table continued…

Field	Default	Allowed Values	Description
		$ ( ) * + . / ; : - > ? [\ ] ^ ` ~ (No leading and trailing spaces)	
Broadcast Data Agency Data Type	IVD	• IVD • HPD	Select the type of data service that is available to this Broadcast Data Agency.
Subscriber Type	IVD Radio	• Broadcast Data Agency • IVD Radio • HPD Radio • Console Platform	Select the appropriate value.

Table 4: Broadcast Data Agency Parameters – Security Group

Field	Default	Allowed Values	Description
Identity			
Security Group Alias	N/A	1 to 16 characters. Use the following characters: A to Z, a to z, 0 to 9, space ! # $ ( ) * + . / ; : - > ? [\ ] ^ ` ~ (No leading and trailing spaces)	Enter a unique name that identifies an individual security group.
Notes			
Notes	N/A	0 to 255 characters. No character choice restrictions.	Enter the text that provides relevant description and information about the record.
Change Audit			
Date Modified	N/A	N/A	(Read only) The information about the time of last modification.
Record Identifier			
Record Identifier	N/A	1 to 2,000	(Read only) A number that identifies a record in the set of records of a given object type.

Table 5: Broadcast Data Agency Parameters – IP Identity

Field	Default	Allowed Values	Description
Record Identifier	N/A	0 to 2,147,483,647	(Read only) A number that identifies a record in the set of records of a given object type.
IP Address	N/A	7 to 15 characters. Use the following characters: A to Z, a to z, 0 to 9, . - (No leading and trailing spaces)	An IP address for the object.

Table continued…

Field	Default	Allowed Values	Description
Core ID	Primary	• Primary • Backup	Select the type of the core configured to broadcast data for Broadcast Data Agency. **NOTICE:** Core ID must be unique within a zone.

Table 6: Broadcast Data Agency Parameters – Change Audit

Field	Default	Allowed Values	Description
Date Modified	N/A	N/A	(Read only) The information about the time of last modification.

Table 7: Broadcast Data Agency Parameters – Record Identifier

Field	Default	Allowed Values	Description
Record Identifier	N/A	0 to 2,147,483,647	(Read only) A number that identifies a record in the set of records of a given object type.

2.12.3
Optimization

No optimization or optimization tools are needed for the High Performance Data (HPD) Broadcast Data feature.

2.12.4
Operation

See Outbound Broadcast Data Transfer on page 46 for the operation steps from the startup to the broadcast of messages.

2.12.4.1
Reliability, Redundancy, and Failover Scenarios

The High Performance Data (HPD) Broadcast Data solution is based on best effort delivery using unconfirmed data. Mission critical transmission for HPD Broadcast Data is outside the scope of this feature. Its implementation on an HPD system is not considered mission critical.

For a system with Dynamic System Resilience (DSR), see the *Dynamic System Resilience* manual.

For a system without DSR, follow the precedent High Performance Data (HPD) system.

2.12.5
Troubleshooting

The Base Radio reports overflow condition to the Unified Event Manager (UEM) (through the SC) when it receives a Broadcast message and there is already a previous Broadcast message buffered. If the outbound buffer allocated for the Broadcast Agency involved is full, the Packet Data Router (PDR) reports overflow condition to the UEM. The PDR allocates outbound buffer on a per Subscriber basis. For Broadcast data, it is on a per Broadcast Agency basis.

The PDR sends an ICMP message notifying the application initiating the Broadcast message of non-delivery. If the PDR was unable to send the Broadcast message to the Radio Network Gateway (RNG),

or if the PDR received a negative acknowledgment for a Broadcast message the PDR sent to the RNG.

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 BR or PDR to the UEM.

Chapter 3

High Availability for HPD

This chapter explains how the High Availability for HPD (HA Data) feature works in the context of your system.

3.1
High Availability for HPD Description

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

HA Data is available for:

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

Components needed for HA Data include:

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

HA Data provides:

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

Relation to Dynamic System Resilience (DSR):

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

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

PDG Redundancy

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

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

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

GGSN and CNI Path Equipment Redundancy

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

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

3.2 High Availability for HPD Theory of Operation

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

The following components support HA Data:

- Redundant HPD PDG virtual machines
- Redundant GPRS Gateway Support Node (GGSN) routers
- Redundant Customer Network Interface (CNI) path equipment, including the RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers

Redundant HPD PDG Virtual Machines

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

The components supporting PDG redundancy include:

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

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

Redundant GGSN Routers

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

Redundant CNI Path Equipment

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

Data Subsystem with HA Data

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

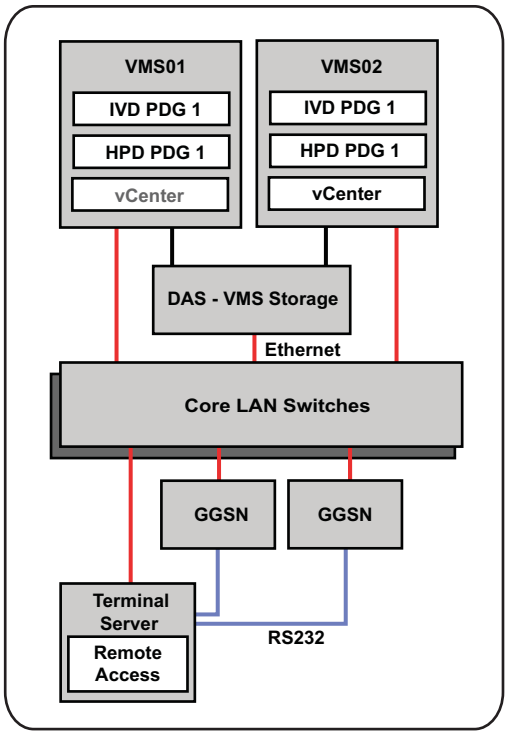
The following diagrams show the data subsystem in an HA Data configuration with redundant PDG and GGSN devices. The diagrams do not show other virtual machines which may reside on the VMS hosts in CSA systems.

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

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

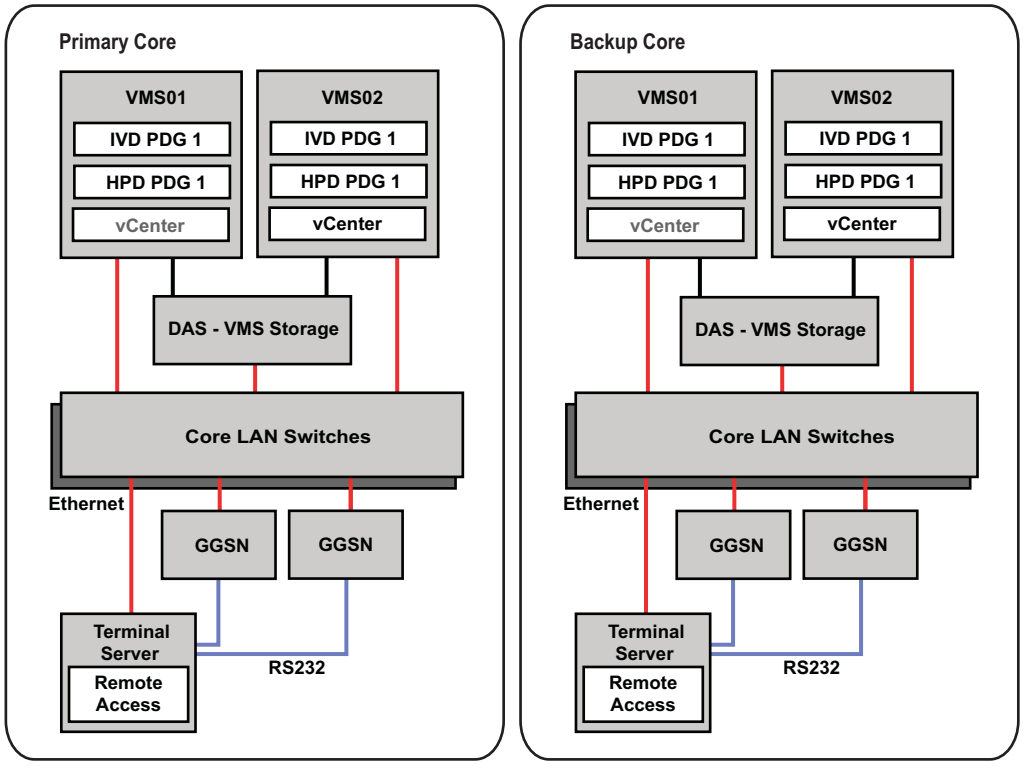
In the case of High Availability for vCenter, there is only one vCenter VM that is instantiated on one server. If that server fails, the vCenter VM moves to the secondary server. To show that the potential for this vCenter VM to reside on the secondary server exists if the primary server fails, one vCenter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

Figure 13: Data Subsystem in an HA Data Configuration without DSR



High_Avail_Data_Option_NonDSR_B

Figure 14: Data Subsystem in an HA Data Configuration with DSR



High_Avail_Data_Option_DSR_B

3.2.1

HA Data – Application Experience

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

Data Bearer Service Applications

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

Non-Data Bearer Service Applications

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

3.2.2

HA Data – Failure and Recovery

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

Virtual Management Server (VMS)

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

VMS Network Interfaces

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

GPRS Gateway Support Node (GGSN)

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

Customer Network Interface (CNI)

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

HA Data without DSR

Two CNI paths exist per Master Site:

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

HA Data with DSR

Four CNI paths exist per Master Site:

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

HA Data with Encrypted CEN links

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

- RNI Server IP Address – The IP address used by a client in the CEN to connect to a server in the RNI changes when there is a CNI path switchover. When there is a switchover of the HA CNI path, new connections from the CEN client to the RNI server need to use an alternate RNI server IP address. It is recommended that the application develop a procedure to monitor the connection between the CEN client and the RNI server. When a broken connection is detected, the alternate RNI server IP address should be used. During a prolonged condition where the CEN client is unable to communicate with the RNI server, the CEN client will need to alternate between the two RNI server IP addresses until the connection is re-established. In a system with both HA Data and DSR, this procedure needs to execute in both the primary and backup zone cores.
- RNI Client IP Address – The IP address of a client in the RNI changes when there is a CNI path switchover. It is expected that servers in the CEN are able to recover from a change in the IP address of an RNI client.

Solution Support Center (SSC) Connections

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

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.

3.4 High Availability for HPD Operation

In case of a hardware failure, the High Availability for HPD (HA Data) feature provides automatic switchover to a redundant peer device. A switchover can also be initiated manually on a PDG and GGSN.

Manual PDG switchover
Performed with Unified Event Manager (UEM). The procedure is described in Performing a Manual Switchover between High Availability PDGs on page 59.

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

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

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

3.4.1 Performing a Manual Switchover between High Availability PDGs

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

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

Procedure:

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

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

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

The **Command** window appears.

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

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

This page intentionally left blank.