System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Master Site with HPD Overlay

NOVEMBER 2016

MN003326A01-A

Copyrights

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

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

Disclaimer

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

Trademarks

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

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

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

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

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

This page intentionally left blank.

Contact Us

Motorola Solution Support Center

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

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

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

North America Parts Organization

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

We welcome your feedback on this and other Motorola manuals. To take a short, confidential survey on Motorola 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
MN003326A01-A	Original release of the *Master Site with HPD Overlay* 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 Master Site with HPD Overlay

This booklet provides information required to install, configure and manage an ASTRO® 25 master site with HPD overlay from the site perspective.

What is Covered In This Manual

This booklet contains the following chapters:

- Master Site with HPD Overlay Description on page 17 provides a high-level overview of master sites equipped with the HPD overlay.
- Master Site with HPD Overlay Technical Overview on page 19 includes a technical overview of the master site equipment and Private Radio Network Management (PRNM) applications. It also describes how these items apply to HPD operation.
- Master Site with HPD Overlay Installation on page 37 describes the installation requirements for HPD overlay equipment at a master site.
- Master Site with HPD Overlay Configuration on page 39 includes the software installation and configuration requirements for HPD overlay on a master site.

Helpful Background Information

Motorola 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 to follow when setting up a Motorola 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	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.

This page intentionally left blank.

Chapter 1

Master Site with HPD Overlay Description

This chapter provides a high-level overview of HPD overlay at a master site.

1.1 Overview

The high performance data (HPD) overlay feature can be added to new or existing integrated voice and data (IV&D) systems. The feature is added to provide 96 kbps wireless data service for mobile subscriber units (MSUs) in the system coverage area. A system may be configured with some zones that provide HPD services and other zones that do not provide HPD services.

Each zone that provides HPD services must include an HPD Packet Data Gateway (PDG) at the master site. When configuring the master site, make additional considerations for adding site links for standalone HPD remote sites or increasing site link bandwidth for remote sites that have HPD overlay equipment.

One master site within the system contains a Gateway GPRS Service Node (GGSN) to provide the inbound/outbound routing of data traffic to the Customer Enterprise Networks. If IV&D packet data services are supported in the system, the HPD PDG and IV&D PDG share the one common GGSN in the system. An additional GGSN is not required or supported.

Additionally, an optional network interface barrier (including a firewall and intrusion detection system sensor) may also be installed at the customer network interface point in the system. If IV&D packet data services are supported in the system, the IV&D and HPD traffic can use the same network interface barrier. An additional network interface barrier is not required for HPD services.

1.2 Dynamic System Resilience Interactions

When the system with Dynamic System Resilience features Master Site with HPD Overlay then the Backup Core also has an HPD Overlay. For more information, see the *Dynamic System Resilience* manual.

This page intentionally left blank.

Chapter 2

Master Site with HPD Overlay Technical Overview

This chapter explains how the master site equipment and Private Radio Network Management (PRNM) applications work with HPD operation in the context of your system.

2.1 Master Site Equipment

The master site includes the core infrastructure for controlling operations, managing the network, and routing traffic within a zone. Each zone includes one master site and some remote sites. In a multizone system, multiple master sites are connected together to form the system.

Each master site with the HPD overlay consists of the equipment shown in the diagrams below.

All of the master site equipment is centrally connected to a common LAN. The master site communicates with its own remote sites and other zones through Cooperative WAN Routing (CWR). In the US, these connections are typically made through T1 links (other locations outside the US may use E1 links). Terminal servers that are connected to the master site equipment provide administrative access to the different devices on the master site network.

The master site can be connected to the peripheral network, which provides the connection to Customer Enterprise Networks (CENs).

Each master site includes the following major subsystems. These subsystems work together to provide the control, routing, management, security, and data services within the zone.

- Resource management subsystem
- Network management subsystem
- Network transport subsystem
- Network security subsystem
- Data subsystem

One master site in the system is designated as the system master site. This system master site contains the System Statistics Server (SSS) application, and the Unified Network Configurator (UNC) server, which are used for system-level configuration and statistics. Only one UCS server application, one SSS server application, and one UNC server are required per system. Each system-level server application runs in its own server environment (or container) on a Virtual Management Server (VMS).

When the HPD overlay option is installed, an HPD PDG is added at the master site to provide routing of HPD user traffic in the zone. The HPD PDG and GGSN are the most critical devices associated with HPD operation within the zone.

NOTICE:
L2, M2, and M3 zone cores can be configured with a vCenter server and redundant PDGs, GGSN routers, and CNI path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers) to support the High Availability for Trunked IV&D and HPD (HA Data) feature. See High Availability for HPD Installation on page 38 for more information.

For more information on the VMS Host architecture, see the *Virtual Management Server Software* manual.

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

Figure 1: Master Site with HPD Overlay – Single Zone Non-Redundant Configuration

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

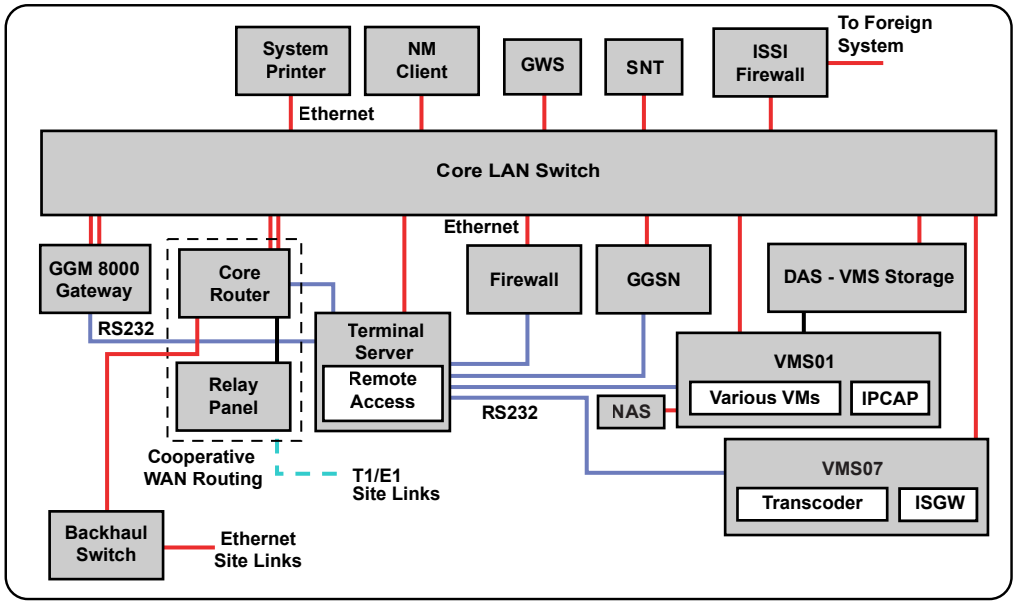


Figure 2: Master Site with HPD Overlay – Single Zone Redundant Configuration

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

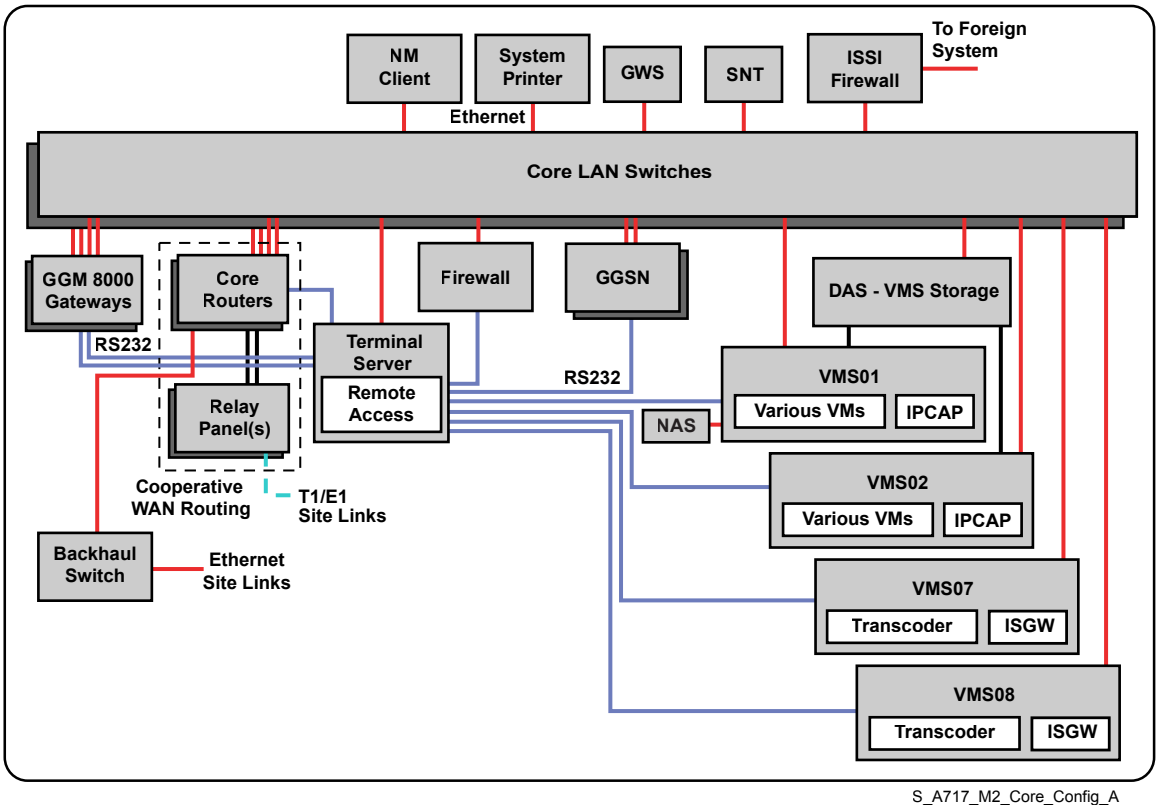
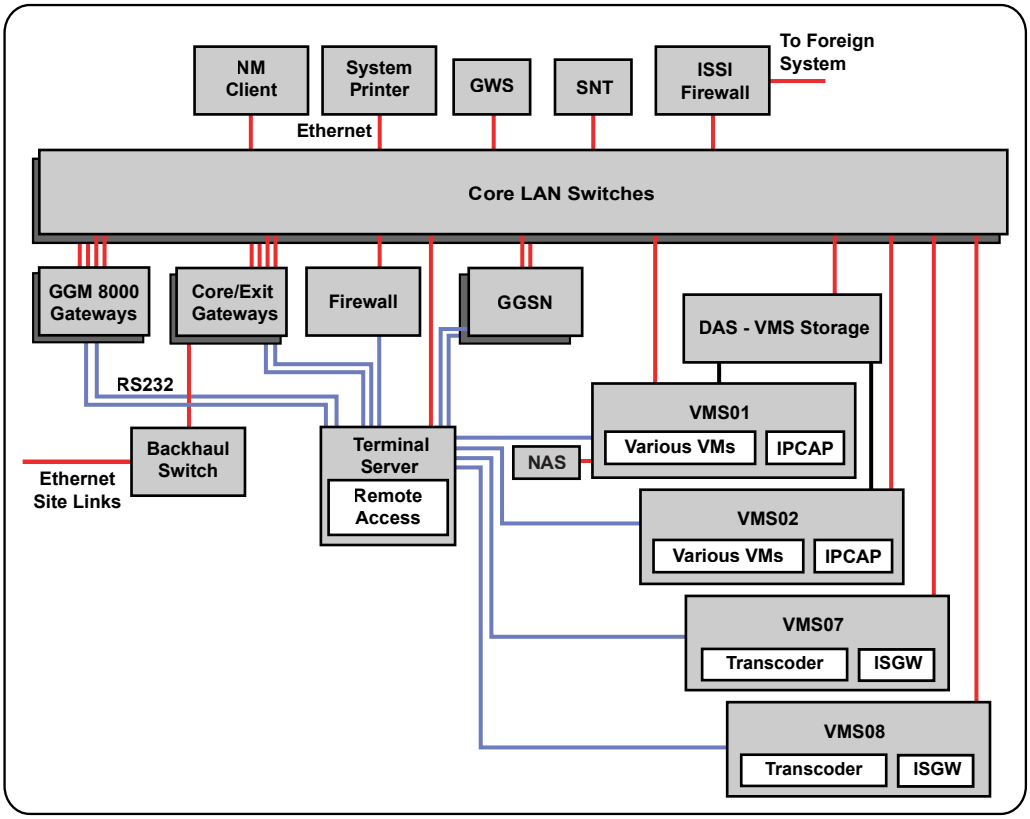


Figure 3: Master Site with HPD Overlay – Multi-Zone Capable Redundant Configuration

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



2.1.1

Resource Management Subsystem

The resource management subsystem consists of the zone controller (ZC) platform. See the zone controllers in the following diagrams showing the available configurations of the resource management subsystem.

Figure 4: Resource Management Subsystem – Single Zone Non-Redundant Configuration

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

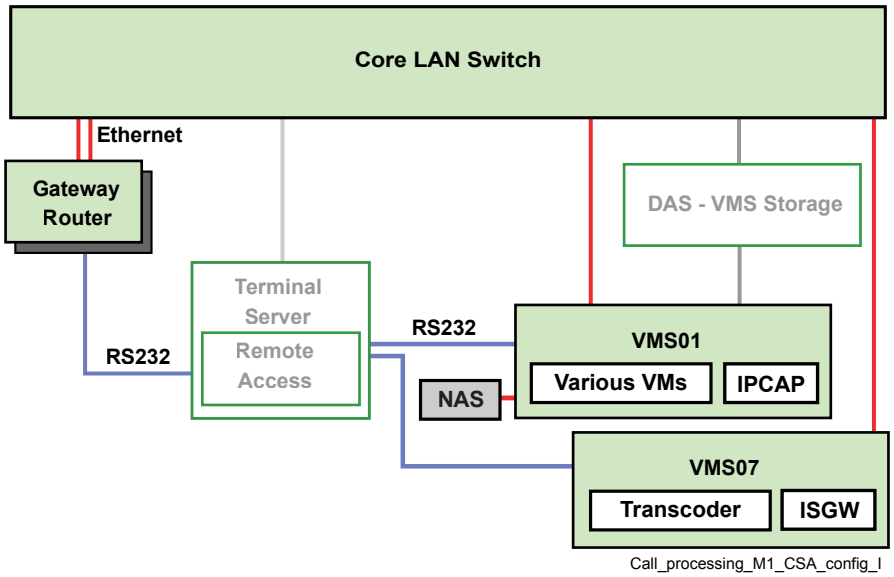


Figure 5: Resource Management Subsystem – Single Zone Redundant Configuration

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

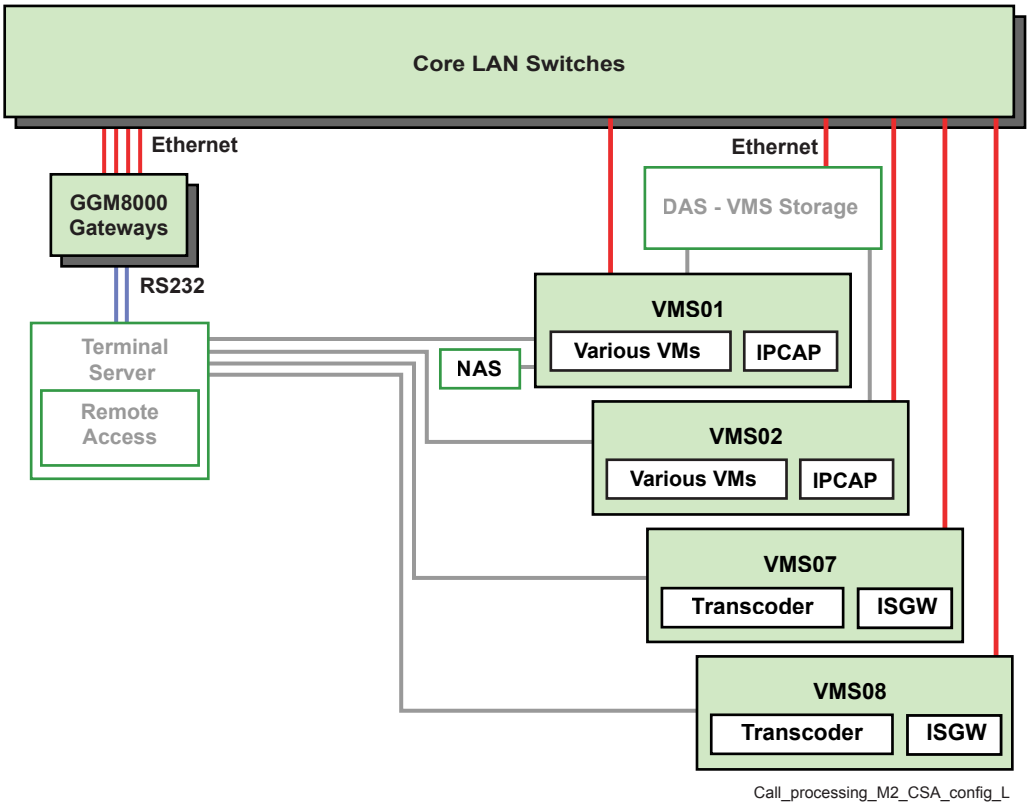
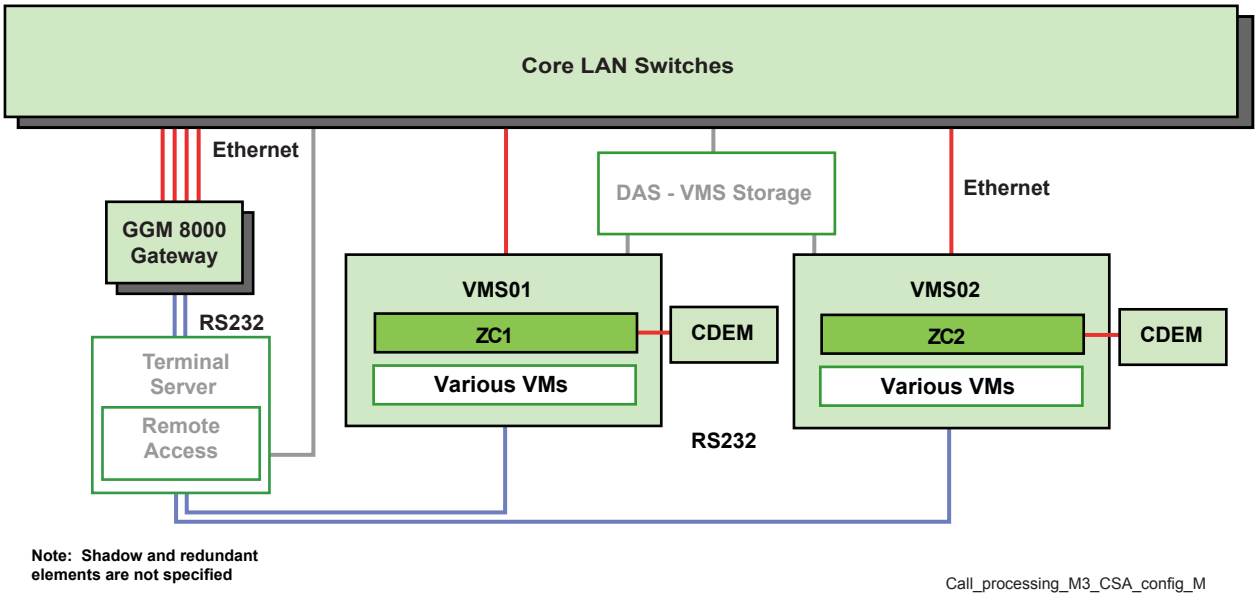


Figure 6: Resource Management Subsystem – Multi-Zone Capable Redundant Configuration

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



The zone controller has many important responsibilities for HPD operation including the following:

- Handles registration and location registration requests for mobile subscriber units (MSUs) in the zone.
- Interacts with the HPD site controllers in the zone during initialization and recovery.
- Dictates the operating mode for each HPD remote site in the zone (wide area mode or local mode).
- Sends updates to HPD remote sites for adjacent site status and other information.
- Selects the home channel for HPD remote sites.
- Maintains configuration records for MSUs in the Home Location Register (HLR).
- Maintains mobility information for MSUs in the zone in the Visitor Location Register (VLR).
- Pushes VLR data to the HPD RNG to keep the PD-VLR updated. Also handles queries from the HPD RNG in the zone.
- Handles queries from the HPD PDR in the zone.

The zone controller maintains control of operations within the zone and manages the zone resources. The zone controller manages the status of all the HPD remote sites within the zone. The zone controller determines whether the sites can be placed in wide area or local modes. The zone controller interacts with remote sites during initialization and recovery events to bring the sites into wide area mode. The zone controller also keeps HPD remote sites up to date with adjacent site status information.

The zone controller maintains several databases including the Visitor Location Register (VLR), Home Location Register (HLR), and infrastructure information. The VLR manages mobility information for all the MSUs that are currently registered in the zone. The HLR manages the configuration settings for all the MSUs that are fleet mapped to the zone (as provisioned through the Provisioning Manager application). The zone controller pushes VLR data to the HPD RNG. The HPD RNG uses the location information to handle routing and administration of HPD traffic flowing through the zone.

At any point in time, one zone controller is active and the other zone controller is in standby mode. The zone controllers monitor one another over a negotiation link. If an active zone controller fails, the standby zone controller takes over operations without affecting services on the network.

The gateway routers support the delivery of all control traffic between the zone controllers and the other devices on the network.

For more information on the VMS Host architecture, see the *Virtual Management Server Software* manual.

For configuration details, see the *Dynamic System Resilience* manual.

2.1.2
Network Management Subsystem

The network management subsystem includes the zone-level server applications, network transport server applications, and the system-level server applications at the system master site. All these server applications perform diverse functions that are critical to the system.

Figure 7: Network Management Subsystem – Single Zone Non-Redundant Configuration

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

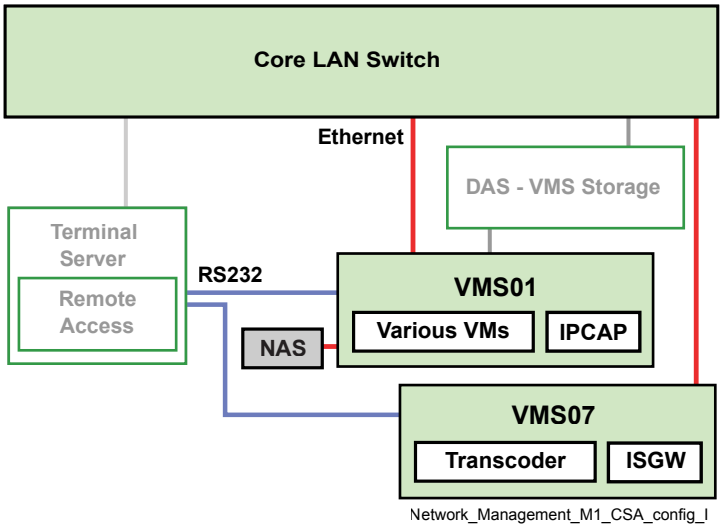


Figure 8: Network Management Subsystem – Single Zone Redundant Configuration

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

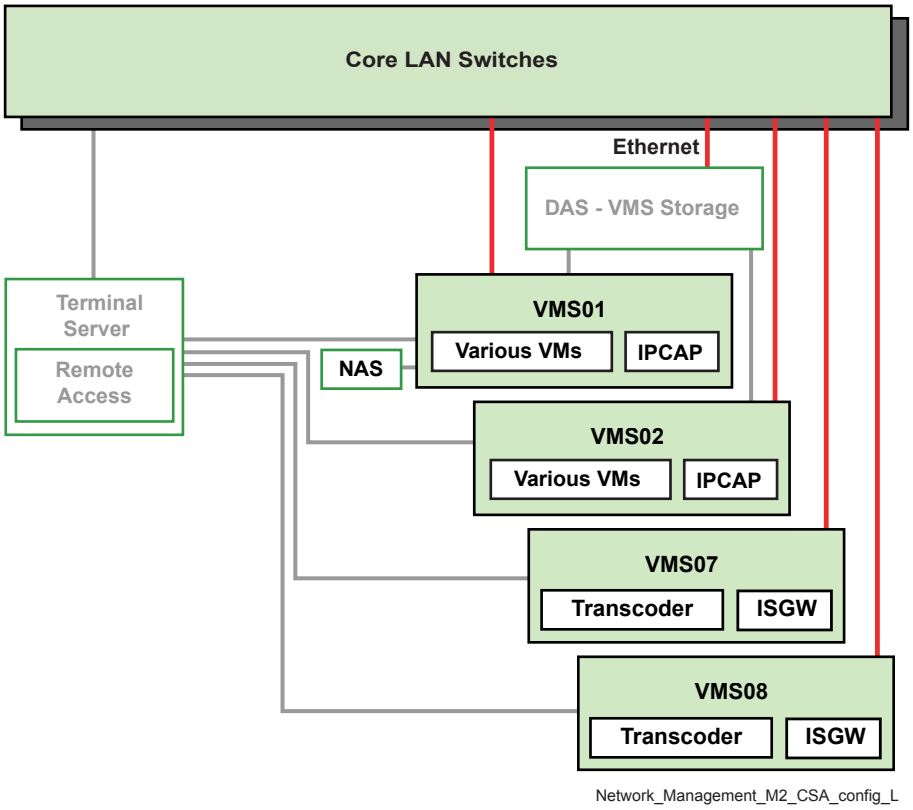
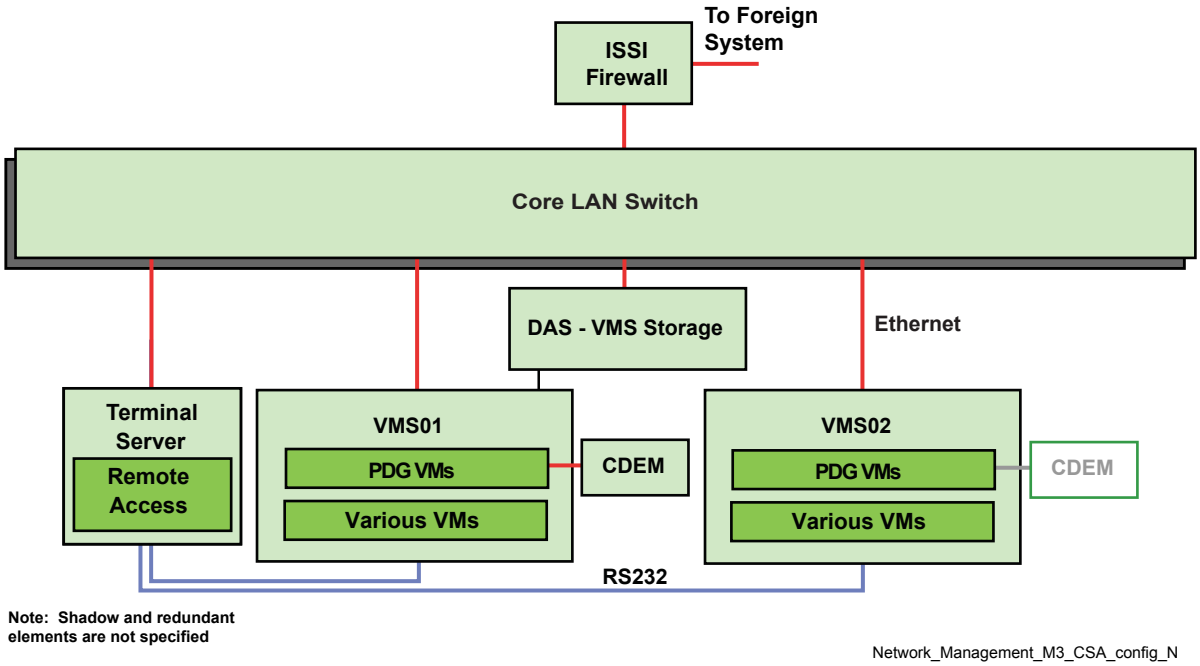


Figure 9: Network Management Subsystem – Multi-Zone Capable Redundant Configuration



For more information on the VMS Host architecture, see the *Virtual Management Server Software* manual.

For configuration details, see the *Dynamic System Resilience* manual.

2.1.2.1
System-Level Server Applications

The system includes the following system-level server applications: Unified Network Configurator (UNC) and System Statistics Server (SSS).

Unified Network Configurator (UNC)
The UNC application maintains a configuration database for equipment in each zone. This database includes information provisioned for both IV&D and HPD infrastructure.

System Statistics Server (SSS)
The SSS application is the central collection server application for system-wide statistics. The SSS server application does not collect statistics for HPD operation in the system.

2.1.2.2
Network Transport Management Server Applications

The system includes two applications that manage the network transport equipment:

- InfoVista
- Unified Network Configurator

The Transport Network Performance Server (TNPS) hosts the InfoVista application. InfoVista may be used to collect and display statistics for the HPD PDR, HPD RNG, and HPD remote site equipment.

The Unified Network Configurator server application hosts the UNC software that is used to manage the network transport equipment.

2.1.2.3
Zone-Level Server Applications

Each zone includes the following set of zone-level server applications.

- Zone Database Server (ZDS) application
- Air Traffic Router Server (ATR) application
- Zone Statistics Server (ZSS) application
- Fault Management Application Server

The UNC application maintains a configuration database for equipment within the zone. This database includes information provisioned for both IV&D and HPD infrastructure. Mobile users are configured in the Provisioning Manager application.

The Air Traffic Router Server (ATR) application receives raw processing information from the zone controller. The ATR transforms the raw data into Air Traffic Information Access (ATIA) packets that are used for statistics, ZoneWatch events, and other logging activities. The ATR server application logs the HPD registration events and you can view them through ZoneWatch or ATIA Log Viewer applications.

The Zone Statistics Server (ZSS) application maintains a database of zone-level statistics and provides information for performance reports and historical reports for traffic within the zone. The ZSS server application only maintains statistics for IV&D traffic in the zone and does not collect statistics for HPD service.

The fault management application server hosts the fault management client applications for the zone. The server application manages the alarms and status information for all the devices within the zone, including the HPD PDG, GGSN, and HPD remote site equipment.

2.1.3

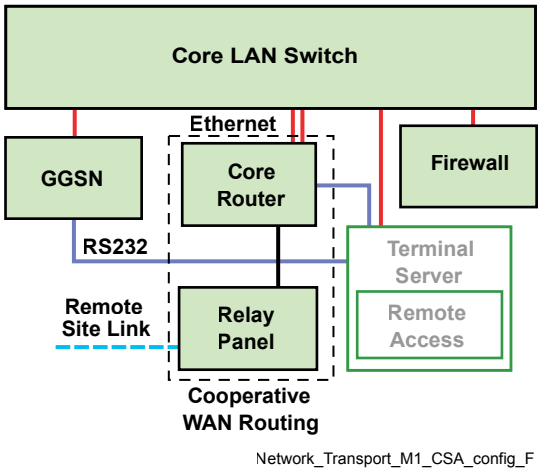
Network Transport Subsystem

The network transport subsystem consists of the routers and switches at the master site that provide routing and network connections between different devices.

Depending on the master site configuration, different equipment can be installed at the site:

- Core LAN switch
- Cooperative WAN routing
- Gateway routers
- Standalone core routers and exit routers or combined core/exit routers

Figure 10: Network Transport Subsystem – Single Zone Non-Redundant Configuration



Core LAN switch

The core LAN switch interconnects all devices at the master site. The switch includes separate virtual LANs (VLANs) that keep traffic isolated from unnecessary devices on the LAN.

Gateway routers

A pair of gateway routers is connected to the core LAN switch to route traffic between different VLANs. HPD registration traffic is routed over the control VLAN to the zone controller. Context activation and HPD user data traffic is routed over the data VLAN to the HPD PDG (PDR/RNG) and GGSN. The gateway routers are also responsible for routing traffic over the DMZ VLAN to the customer network interface or optional firewall.

Core routers and exit routers

Core routers exist at the master site to route traffic between the core infrastructure and remote sites within the zone. The core routers direct inbound HPD traffic to the gateway routers for traffic flow to the data subsystem.

Exit routers exists at the master site to route traffic to other zones or to backup zone cores within the same zone. If either the home PDR for an MSU or the GGSN is located in another zone, HPD traffic may need to cross zones.

Core and exit routers may be deployed as separate standalone routers or combined in a single core/exit router depending on your system configuration. Standalone core and exit routers are used on T1/E1 or Ethernet site links. Combined core/exit routers may only be used with Ethernet site links.

Cooperative WAN Routing

Cooperative WAN Routing provides the physical connection to the remote site links and InterZone links. Inbound/outbound HPD traffic and InterZone routing of HPD traffic pass through CWR. CWR also provides redundant Wide Area Network (WAN) failover capabilities. The CWR solution consists of CWR peers (two S6000 routers with 12-port T1/E1 modules) connected to the relay panel.

Terminal server

The terminal server provides administrative access to the master site components. Client PCs can access local interfaces for the HPD PDR, HPD RNG, and GGSN through the terminal server via a modem or over the network using ssh or sphere client.

NOTICE:
For more information on the VMS Host architecture, see the *Virtual Management Server Software* manual.

For configuration details, see the *Dynamic System Resilience* manual.

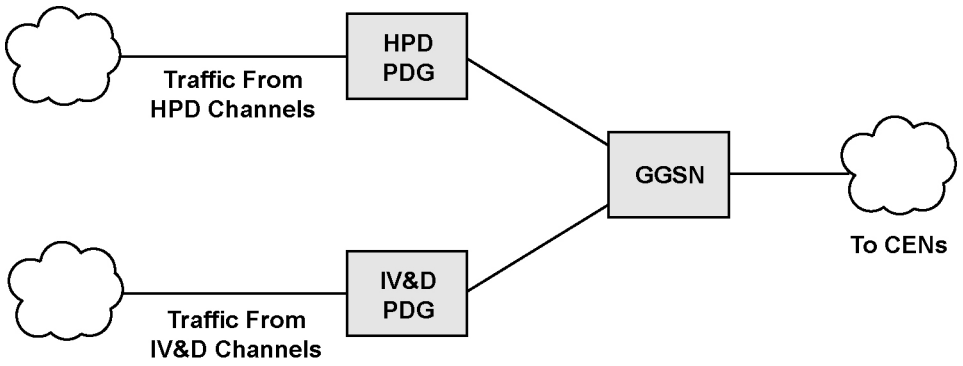
2.1.4 Data Subsystem

The data subsystem is responsible for setting up and tearing down contexts and tunneling traffic between the remote sites and the Customer Enterprise Networks (CENs). In an overlay system, the data subsystem consists of the following devices:

- IV&D Packet Data Gateway
- HPD Packet Data Gateway
- Gateway GPRS Service Node (GGSN)

In an overlay system, an IV&D PDG is used to manage and route 9600 bps data traffic from IV&D data channels. A separate HPD PDG is installed to support HPD services in the zone. All data traffic is routed through the common GGSN. One GGSN is supported per system (see the following diagram).

Figure 11: HPD PDG, IV&D PDG, and GGSN



The HPD PDG includes two modules for handling context activation requests and routing HPD traffic between the sites and customer network. The Radio Network Gateway (RNG) is located in the HPD PDG to handle inbound and outbound traffic routing with the remote HPD sites. The RNG maintains a Visitor Location Register for packet data users that are registered in the zone. The RNG interacts with the zone controller to keep its VLR information updated. HPD traffic from an MSU is routed through the RNG that is in the current zone, even if the MSU is mapped to another home zone. The RNG that is providing the service is referred to as the *serving RNG*.

The HPD Packet Data Router (PDR) in the HPD PDG registers MSUs and routes traffic between the SNDCP tunnel (to the MSUs) and the GTP tunnel (to the GGSN). The HPD PDR maintains a Home Location Register with the system configuration for all HPD users that are fleet mapped to the zone. The HPD PDR is responsible for routing HPD traffic for all users that are mapped to the zone. Each HPD user therefore has a *home PDR* which routes all context requests and HPD user data. Even if the HPD user is in another zone, the home PDR routes the HPD traffic. Notice that the serving RNG and the home PDR may be in different zones, and the HPD traffic may travel through different zones.

The PDR interacts with the zone controller to keep its information updated. When an HPD data user attempts to register with the system, the PDR that is in the home zone checks the registration request against the data that is provisioned for the MSU in the Provisioning Manager settings. If successful, the PDR accepts the registration. If there are any discrepancies, the PDR may issue a reject or denial to the MSU.

The GGSN establishes contexts with the appropriate customer networks as requested by MSUs and provides IP-IP tunneling to the customer networks. Additionally, the GGSN can be configured with a pool of addresses for dynamic (DHCP) addressing of MSUs. The GGSN may also forward dynamic address requests or authentication requests to the proper DHCP or RADIUS server located on the customer network.

The following diagrams show the data subsystem in the available configurations.

Figure 12: Data Subsystem – Single Zone Non-Redundant Configuration

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

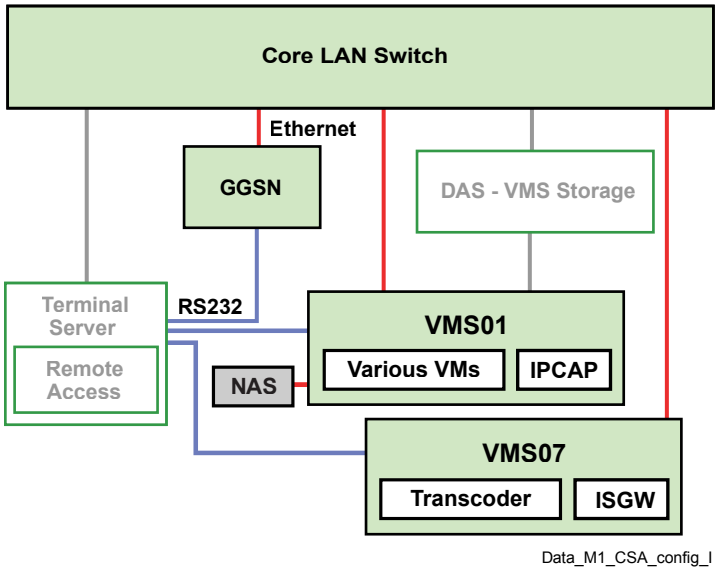


Figure 13: Data Subsystem – Single Zone Redundant Configuration

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

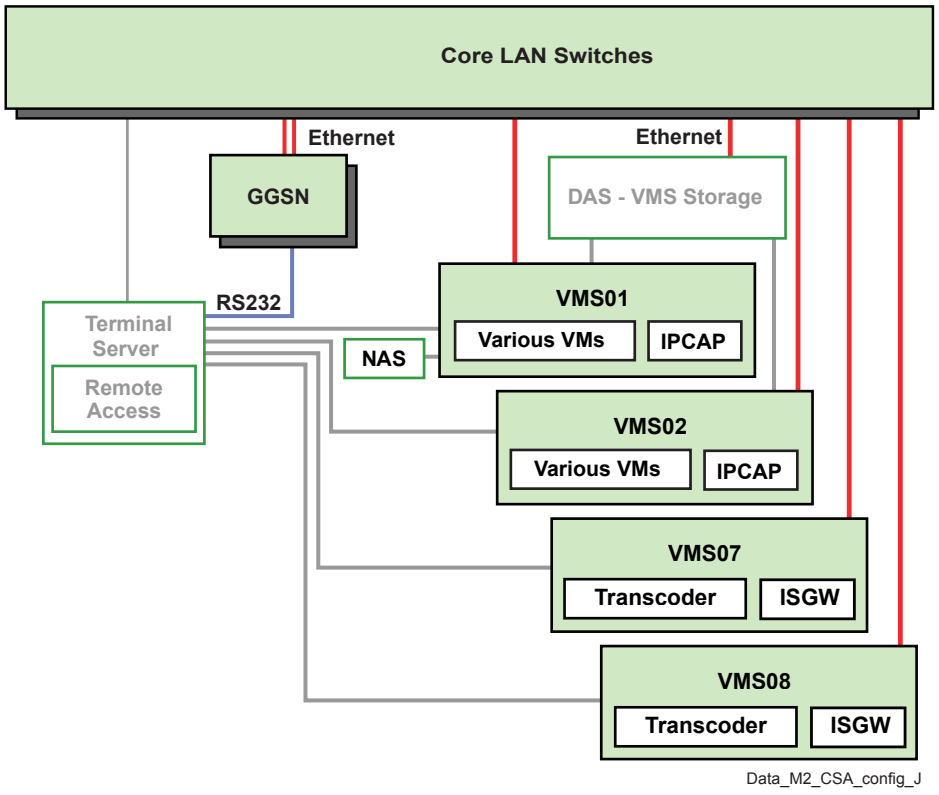
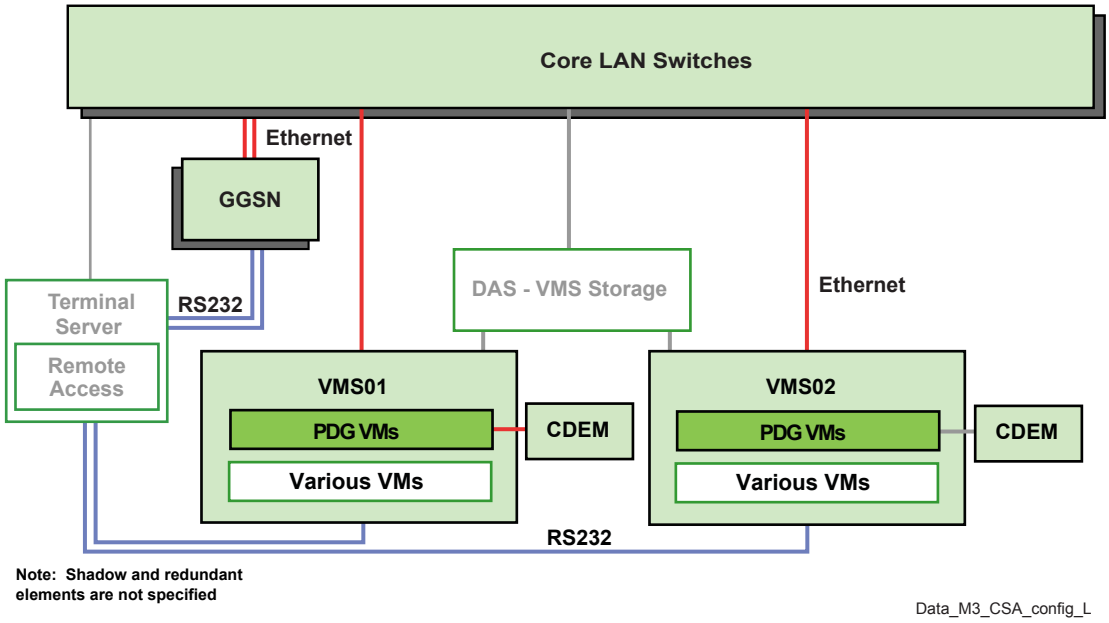


Figure 14: Data Subsystem – Multi-Zone Capable Redundant Configuration



NOTICE:
L2, M2, and M3 zone cores can be configured with a vCenter server and redundant PDGs, GGSN routers, and CNI path equipment (RNI-DMZ Firewall, DMZ Switch, Peripheral Network Routers, Border Routers) to support the High Availability for IV&D and HPD (HA Data) feature. See High Availability for HPD Installation on page 38 for more information.

For more information on the VMS Host architecture, see the *Virtual Management Server Software* manual.

For configuration details, see the *Dynamic System Resilience* manual.

2.2 HPD Packet Data Gateway

An HPD Packet Data Gateway (PDG) is added to each zone that requires HPD coverage. Zones that do not require HPD coverage do not have an HPD PDG installed. The HPD PDG application is critical to context activation, IP bearer services, and mobility management of Mobile Subscriber Units (MSUs) within the zone. An HPD PDG is hosted as a virtual machine on a Virtual Management Server (VMS).

For a detailed description of the VMS platform, see the *Virtual Management Server Hardware* manual.

Figure 15: Virtual Management Server HP DL380 Gen9

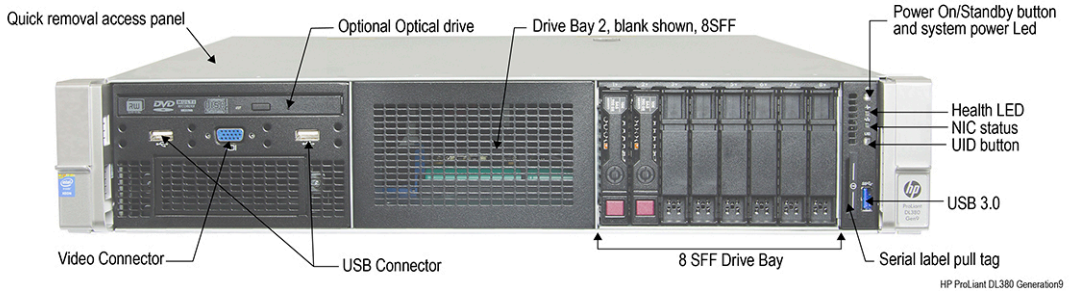
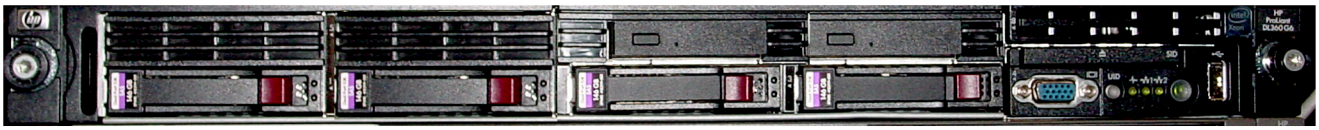


Figure 16: Virtual Management Server HP DL360 G6



HP_DL360_G6_front

2.2.1 HPD Packet Data Router

The HPD Packet Data Router performs activities for context activation and routing of HPD traffic between the HPD RNGs and GGSN.

The HPD PDR:

- Manages context activation and deactivation
- Approves/denies context activation of MSUs based on provisioning in Provisioning Manager
- Contains a database of provisioned information for MSUs and Broadcast Data Agencies mapped to the zone
- Routes HPD traffic between the HPD RNG and GGSN
- Originates/terminates the SNDCP and GTP tunnels

- Buffers outbound messages
- Provides a network management interface for HPD RNG
- Generates ICMP error notifications for failed delivery of HPD traffic

MSUs perform context activation with their home HPD PDR. The home HPD PDR is located in the zone where the MSU is home zone mapped. When a context activation request is received from an MSU, the HPD PDR determines whether the context activation is granted or rejected. This decision is made by checking the request information against the information provisioned in the system for the MSU. If the request and the provisioned information for the MSU are mutually acceptable, the HPD PDR requests that the GGSN establish a context to the requested CEN. This request occurs when the network conditions permit.

The HPD PDR maintains a local database, called the Packet Data Home Location Register (PD-HLR). The PD-HLR contains the Provisioning Manager record settings for MSUs mapped to the zone. The HPD PDR may also query the zone controller for zone location information.

After an MSU is context activated, all inbound or outbound traffic associated with the MSU is routed through its home HPD PDR. For inbound traffic, the HPD PDR receives the traffic from the serving HPD RNG in the zone where the MSU is located. The HPD PDR forwards the inbound traffic to the GGSN. The GGSN delivers the traffic to the appropriate CEN. The HPD PDR terminates the SNDCP tunnel from the HPD RNG and originates the GTP tunnel to the GGSN.

Outbound traffic takes place in the reverse direction. The GGSN sends traffic to the HPD PDR. The HPD PDR forwards the traffic to the serving HPD RNG that is in the zone where the MSU is currently registered.

The HPD PDR buffers outbound traffic. If the delivery fails due to a timeout of buffered datagrams, connection loss, or unexpected context deactivation, the HPD PDR sends an ICMP error notification to the traffic originator.

The HPD PDR may deactivate a context for an MSU under any of the following conditions:

- The context has been deactivated with the GGSN.
- The HPD PDR is unable to contact the HPD RNG.
- MSU provisioning information has changed or been deleted.

The HPD PDR monitors its links to the GGSN, zone controller, and local RNG. The HPD PDR performs services for the local HPD RNG. If the HPD PDR fails, the HPD RNG within the chassis also fails.

2.2.2
HPD Radio Network Gateway

The HPD RNG is responsible for routing traffic between HPD PDRs and the HPD remote sites within the zone. MSUs may be assigned to HPD PDRs in different zones, and MSUs may be roaming to different sites. Thus the HPD RNG must maintain the site location and home HPD PDR assignments for MSUs in the zone.

The HPD RNG tracks the active context state for each MSU in the zone and determines how to route the messages to the appropriate home HPD PDR. For this purpose, the HPD RNG maintains a database of MSUs that are currently registered in the zone. This database is called the Packet Data Visitor Location Register (PD-VLR). The PD-VLR is pushed to the HPD RNG from the zone controller. The HPD RNG may also query the zone controller for PD-VLR information.

When inbound traffic is received, the HPD RNG forwards the traffic to the home HPD PDR that is associated with the MSU sending the traffic. When outbound traffic is received from an HPD PDR, the HPD RNG sends the traffic to the appropriate site for the target MSU.

The HPD RNG tracks the current SNDCP Standby Timer status for each MSU. The SNDCP Standby Timer determines how long the MSU may remain context activated without receiving a renewal before

it is removed from the system. The System record in Unified Network Configurator (UNC) contains provisioning information for the SNDCP Standby Timer.

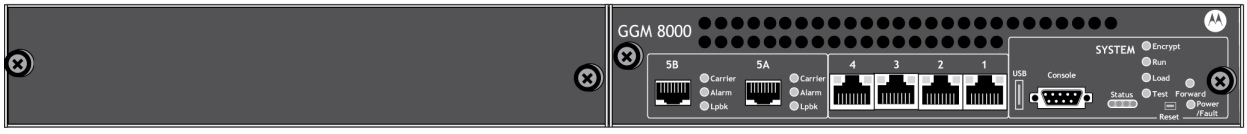
2.3 GGSN

The GGSN acts as a gateway for all IV&D and HPD traffic in and out of the system. It connects with the data subsystem through a GTP tunnel and connects with the CENs through an IP-IP tunnel.

The GGSN performs the following specific functions:

- Forwards outbound traffic to the appropriate home HPD PDRs
- Sends inbound traffic through VPN tunnels to the appropriate CEN
- Originates/terminates the GTP tunnels to the HPD PDRs and the IP-IP tunnels to the CENs
- Sends dynamic updates to the DNS server on the CEN for MSUs after context activation (if configured)
- Queries the RADIUS or DHCP server on the CEN for authentication or dynamic addressing (if configured)
- Provides local dynamic addressing for MSUs (if configured)

Figure 17: GGSN – GGM 8000



GGM_8000_base_no_callouts

Figure 18: GGSN – S6000

S6000_router_front

The GGSN originates IP-IP tunneling to the CENs. These IP-IP tunnels provide secure data delivery traffic to the CENs over the peripheral network. The IP-IP tunneling also provides IP isolation between the system and the CENs to prevent IP addressing conflicts.

The GGSN is configured with an Access Point Number (APN) for each CEN using Unified Network Configurator (UNC). This APN is mapped to the physical/virtual ports assigned for each of the CEN border routers. Each MSU is assigned to a particular CEN/APN using Provisioning Manager. When the GGSN receives inbound traffic, it forwards the traffic to the appropriate CEN according to the APN.

The GGSN may be provisioned to interact with a RADIUS server, DHCP server, and DNS server on each CEN. The GGSN can query a RADIUS server on the CEN with authentication credentials received from a context activating MSU. It permits mobile users to authenticate with the CEN during the context activation process.

Depending on the MSU and system configuration, the GGSN may also query a DHCP server on the CEN to receive dynamic addresses for context activating MSUs. If a RADIUS server is used at the CEN, it may operate as both an authentication server and DHCP server. Otherwise, the GGSN may be configured with its own pool of IP addresses to locally provide dynamic addresses to context activating MSUs.

The GGSN may also be configured to supply dynamic updates to a Domain Name Server (DNS) on the CEN. These dynamic updates would provide fully qualified domain name (FQDN) bindings for each context activating MSU (for example, c620100000e0df659f.hpd.cen20). This FQDN consists of a host name plus the domain name for the MSU.

2.4 Private Radio Network Management (PRNM) Applications

The following Private Radio Network Management (PRNM) applications relate to High Performance Data (HPD) operation or configuration.

Affiliation Display
Affiliation Display can be configured to display the site location and registration status of MSUs within a zone.

ATIA Log Viewer
ATIA Log Viewer can be configured to archive daily logs of system activity. The daily logs include the same information that is displayed in the ZoneWatch raw display window. Logging on the ATR must be turned on if archives should be collected for this application.

Dynamic Reports
The Dynamic Reports application does not generate any reports that apply to HPD operation. Instead, use InfoVista to generate reports for the HPD PDG, GGSN, or HPD remote site equipment.

Historical Reports
The Historical Reports application does not generate any reports that apply to HPD operation. Instead, use InfoVista to generate reports for the HPD PDG, GGSN, or HPD remote site equipment.

Provisioning Manager
Provisioning Manager must be used to provision the HPD Radio record (for each HPD modem and mobile user).

Radio Control Manager (RCM)
RCM only applies to IV&D operation. RCM commands, such as lock, inhibit, or other status/ command features do not apply to HPD modems.

ZoneWatch
ZoneWatch can be configured through Provisioning Manager to show a raw data display, site display, and channel grid. The raw display and site displays can show HPD-related events taking place in the zone (such as registration events from the HPD MSUs). The channel grid shows the channels at the sites in the zone, along with the status and home channel information. HPD activities (such as MSUs sending traffic) are not shown on the channel grid. ZoneWatch filters can be configured in Provisioning Manager to define the types of mobile subscribers that are logged in the raw display window (HPD, IV&D, or All).

2.5 HPD Licenses

The License Manager Web-based user interface allows you to load, view, and manage the active licenses for High Performance Data (HPD) and other features.

The ASTRO® 25 system requires one License Manager server per zone to store and manage licenses for the zone. Additionally, one of these servers is designated as the system-level License Manager server for managing system-level licenses.

The following licenses are required for HPD:

HPD Radio User
Order the appropriate number of licenses based on the number of HPD equipped radios in the system. Load these licenses to the system-level License Manager server.

HPD Site

Order the appropriate number of licenses based on the number of HPD sites in the zone. Load these licenses to the License Manager server for the zone.

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

This page intentionally left blank.

Chapter 3

Master Site with HPD Overlay Installation

This chapter details installation procedures relating to HPD overlay equipment at a master site.

3.1 Installing HPD Overlay Hardware

The following process lists the components that you must install at the master site for HPD operation.

Process:

1. The network interface barrier components should have been installed during the system installation or upgrade. Verify that the hardware is installed.
2. Install the GGSN in the appropriate zone (if not already installed in the system). The GGSN platform must be the S6000 router. Other routers cannot be used with HPD.

   See “GGSN Router – Installation and Configuration” in the *S6000 and S2500 Routers* manual.
3. Install the HPD PDG as a virtual appliance on the VMware ESXi-based Virtual Management Server (VMS).

   For information on HPD PDG installation, see the *Packet Data Gateways* manual.

3.2 HPD Packet Data Gateway

Table 1: HPD Packet Data Gateway Connections

The following table shows the master site connections to the HPD PDG.

Device	Port / Type	Device	Port / Type	Notes
HPD PDR module	10/100 BaseT, RJ45	Master Site LAN Switch #2	RJ45	HPD PDR connection to the master site LAN.
HPD RNG module	10/100 BaseT, RJ45	Master Site LAN Switch #2	RJ45	HPD RNG connection to the master site LAN.

3.3 GGSN

Table 2: GGSN Connections

The following table shows the master site connections to the GGSN.

Device	Port / Type	Device	Port / Type	Notes
GGSN	RJ45	Master Site LAN Switch #1	RJ45	GGSN connection to the ZNM on the master site LAN switch.
GGSN	RJ45	Master Site LAN Switch #2	RJ45	GGSN connection to Data on the master site LAN switch.
GGSN	RJ45	Master Site LAN Switch #2	RJ45	GGSN connection to DMZ on the master site LAN switch.

3.4 Ethernet Connections

Table 3: Master Site LAN Switch Connections to HPD PDR and HPD RNG

The following table shows the additional connections for the master site Core LAN switch when the IV&D system includes an HPD Overlay.

Port	Destination	Type of port
Assignable	HPD RNG	RJ45
Assignable	HPD PDR	RJ45

3.5 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.

Chapter 4

Master Site with HPD Overlay Configuration

This chapter details configuration procedures relating to HPD overlay on a master site.

4.1 Installing and Configuring HPD Overlay Software at a Master Site

The following process explains the general steps for adding HPD overlay to a master site.

Process:

1. The software installation and configuration of the network interface barrier (NIB) components (firewall and intrusion detection sensor) should be one of the first steps during the installation or upgrade of the system. Install software and configure the network interface barrier components if these components have not already been configured in the system. If the NIB components have already been installed and configured, then no special settings or further configuration changes are required for the NIB to work with HPD services.
2. Configure any additional parameters in the GGSN as necessary. Define any Customer Enterprise Networks (CENs) that must be added to the GGSN configuration through Unified Network Configurator (UNC). See the *Unified Network Configurator* manual.
3. Install and configure the HPD PDG software. See the *Packet Data Gateways* manual.
4. Make any necessary configuration changes to data parameters in UNC and Provisioning Manager. See the *Provisioning Manager* and *Unified Network Configurator* manuals.

This page intentionally left blank.