System Release 7.17.2

ASTRO® 25

INTEGRATED VOICE AND DATA

# Dynamic System Resilience

# Feature Guide

NOVEMBER 2017

MN004317A01-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 specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

## Trademarks

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

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

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

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

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

This page intentionally left blank.

# Contact Us

## Motorola Solutions Support Center

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

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

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

## North America Parts Organization

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

| For... | Phone |
|---|---|
| Phone Orders | **800-422-4210** (US and Canada Orders)<br>For help identifying an item or part number, select choice 3 from the menu. |
| | **302-444-9842** (International Orders)<br>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 |
|---|---|---|
| MN004317A01-A | Original release of the *Dynamic System Resilience Feature Guide*. | November 2017 |

This page intentionally left blank.

# Contents

This page intentionally left blank.

# List of Figures

This page intentionally left blank.

# List of Tables

This page intentionally left blank.

# List of Processes

This page intentionally left blank.

# List of Procedures

This page intentionally left blank.

# About Dynamic System Resilience Feature Guide

This manual provides information relating to the implementation and management of the Dynamic System Resilience (DSR) feature in an ASTRO® 25 system.

**NOTICE:** The figures in this document are a high-level, conceptual representation for demonstration of the Dynamic System Resilience feature and are not intended to depict exact architectures found in your ASTRO® 25 system. For a detailed description of the zone core architectures, see the *Master Site Infrastructure Setup Guide*.

## What Is Covered In This Manual

This manual contains the following chapters:

- Description contains introductory information on the DSR feature.
- Theory of Operation contains theoretical information on how the DSR feature is implemented and how it operates in the system.
- Installation details installation information relating to the DSR feature.
- Configuration contains configuration information relating to the DSR feature.
- Optimization contains optimization procedures and recommended settings relating to the DSR feature.
- Operation details tasks that you perform once the DSR feature is implemented on your system.
- Maintenance describes periodic maintenance procedures feature to the DSR feature.
- Troubleshooting provides fault management and troubleshooting information relating to the DSR feature.
- FRU/FRE Procedures lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the DSR feature.
- Reference contains reference materials relating to the DSR feature.
- Feature Expansion/Upgrades contains information on DSR feature expansion/upgrade.

## 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

| 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. |

*Table continued…*

| Related Information | Purpose |
|---|---|
| | This manual may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842). |
| *System Overview and Documentation Reference Guide* | 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. |
| *Master Site Infrastructure Setup Guide* | Covers site-level information required to install and maintain equipment at the ASTRO® 25 system master sites. |
| *Authentication Services Feature Guide* | Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems. |
| *Private Network Management Servers Feature Guide* | Provides information on the installation, configuration, and management of the Private Network Management (PNM) servers, namely, Air Traffic Router (ATR), User Configuration Server (UCS), Unified Event Manager (UEM), Zone Database Server (ZDS), System Statistical Server (SSS), and Zone Statistical Server (ZSS). |
| *Unified Network Configurator User Guide* | Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers, and base radios, and is used to set up sites for ASTRO® 25 systems. UNC has two components: VoyenceControl and Unified Network Configurator Wizards (UNCWs). |
| *Network Time Protocol Server Feature Guide* | Provides an introduction to the components that comprise the Network Time Protocol (NTP) server, including detailed procedures for the TRAK 9100 NTP server installation and configuration and for the Field Replaceable Units (FRUs) replacement. |

Chapter 1

# Dynamic System Resilience Description

This chapter provides a high-level description of Dynamic System Resilience (DSR) and the function it serves on your system.

1.1

## Dynamic System Resilience Overview

Dynamic System Resilience (DSR) strengthens ASTRO® 25 voice and data communications networks for greater redundancy to ensure operational continuity if disaster occurs. Each zone in a system with DSR is supported by two cores: a primary core and a geographically separate backup core. The backup core includes all components necessary to provide redundancy for voice, data, network management, network transport, and IP services.

With DSR, system functionality for critical services is maintained automatically. The failure of a DSR-supported element in a primary core causes automatic switchover to the backup core. Some non-critical services require system operator intervention, for example, to bring backup core components into the active state from standby. Operator procedures if a switchover occurs are covered in Dynamic System Resilience Operation on page 89. Manual switchover capability is provided for system testing and maintenance.

Separate site links are created between remote sites and the primary and backup cores for a zone. If the primary core fails completely, the link to the backup core supports wide-area trunked operation. As always, the transport subsystem uses redundant equipment and routes to maintain service automatically during failures. If a zone controller in the primary core is active, and the site link to the primary core fails, traffic may be rerouted to the backup core and then across the InterZone link to the active zone controller in the primary core.

A switchover to the backup core of a zone occurs only if the entire primary core is destroyed or two individual failures of paired equipment occur in the primary core, such as both zone controllers or both gateway routers.

DSR is supported by the following ASTRO® 25 system architectures:

- M1 Architecture – a Single Zone, Non-Redundant Zone Core
- M3 Architecture – a Multizone Capable, Redundant Zone Core

**NOTICE:** DSR is optional on a zone-by-zone basis in an M3 architecture.

DSR is not supported by the following ASTRO® 25 system architectures:

- M2 Architecture – a Single Zone, Redundant Zone Core
- L1 Architecture – a Single Zone, Small Scale Non-Redundant Zone Core
- L2 Architecture – a Single Zone, Small Scale Redundant Zone Core
- K core Architecture – a Conventional Master Site (ASTRO® 25 Conventional & Integrated Data System)

The Edge Availability with Wireline Console feature providing a Trunking subsystem (Tsub) architecture in the ASTRO® 25 system supports DSR. For more information, see the *Edge Availability Feature Guide*.

## 1.2 Dynamic System Resilience Terminology

The Dynamic System Resilience (DSR) feature introduces several new terms into the ASTRO® 25 system terminology.

Table 1: DSR Terms

| Term | Definition | Conditions |
|---|---|---|
| Master Site | A master site is the geographic location of the ASTRO® 25 zone core equipment. A master site location (or master site) can contain zone core equipment supporting a single zone, or zone core equipment supporting two zones. When DSR is implemented, zone core equipment for the primary zone core is at one master site location while its backup zone core equipment is at another geographically separate master site location. Therefore, a master site location might have zone core equipment supporting the Primary Zone Core for Zone 1, and have zone core equipment supporting the Backup Zone Core for Zone 2. | A DSR system can have one to seven master sites as long as at least one of the sites is a Non-DSR site.<br>• If a master site contains a primary core, a second master site must exist as its backup core.<br>• If a master site has two cores, a second master site must exist with the primary/backup core that complements the primary/backup core at the first master site (sometimes referred to as a master site pair.)<br>• If a master site has two cores, one must be a primary core and the other a backup core. The primary and the backup core must belong to different zones.<br>**NOTICE:** DSR is not supported in the Conventional Master Site (K core) of the ASTRO® 25 Conventional and Integrated Data system. |
| Core | A core is the hardware and software necessary to create a zone. The core provides an optimized IP network supporting six service areas: voice, data, connectivity, mobility, operations management, and enterprise IT management. A dual-core master site includes a primary core for one zone and a backup core for another zone. Some equipment is shared between the two cores. | A one-core master site, sometimes called a standalone core, could be a primary core (for one DSR zone), or a backup core (for one DSR zone). The primary core and backup core for a zone must complement each other; they must be identically configured. The Firewall Manager is an exception; it is present only in a primary core for a dual-core zone.<br>**NOTICE:** DSR is not supported in an L Zone Core. |
| InterZone | InterZone is the traffic that flows from one zone core to another and to the physical and logical transport for that traffic. All packets that leave one exit router and arrive at another exit router. The traffic may include: | For a single-zone system with DSR, an InterZone link exists between the primary and backup cores. While the traffic is not actually between two zones, it is between two cores; the term is also used in this case. |

*Table continued…*

| Term | Definition | Conditions |
|---|---|---|
| | • Call control and payload traffic between zones<br>• IP data bearer service control traffic and payload traffic<br>• Network management traffic<br>• High-availability traffic between redundant cores<br>• IP services traffic<br>• Call control traffic and payload traffic between a core and its associated radio sites and dispatch sites (intrazone traffic) | InterZone links in the system must use the same type of physical transport. |
| Radio Site | Part of the radio system architecture, a radio site is a system access point. Sites include IV&D repeater sites, IV&D IP-simulcast subsystems, Site Gateway (Conventional Channel Interface), or High Performance Data (HPD) sites. | For DSR functionality, radio sites must contain G-series site controllers and base radios. The following subsystems do not support DSR functionality but can be part of a DSR system. These subsystems can be controlled only from the primary core. They do not connect to the controllers in the backup core for a zone.<br>• Circuit-based Simulcast RF sites<br>• Repeater sites with PSC 9600 site controllers or QUANTAR/STR 3000 base radios; a DSR repeater site must include G-series site controllers (GCP 8000 Site Controllers) and base radios<br>• SmartX Site Converter<br>• ISSI.1 Network Gateway<br>Repeater sites with a mix of QUANTAR and GTR 8000 Base Radios support DSR when used with a GCP 8000 Site Controller. The GCP 8000 Site Controller establishes a separate physical path to the backup core, and if the entire primary core fails and remains in wide-area trunking mode, a site can switch over. |
| Dispatch Site | A system access point that provides dispatch terminals access to the system.ma | For DSR functionality, a dispatch console site must be IP based. The NEC Console Telephony Gateway and NEC/AudioCodes Console Telephony Media Gateway only support being configured with one Syslog Server. The NEC/AudioCodes Console Telephony Media Gateway only supports |

*Table continued…*

| Term | Definition | Conditions |
|---|---|---|
| | | being configured with one RADIUS Server. |
| Network Management Site | A system access point that provides network management clients access to the system. | |
| Radio or Dispatch Site Link | The physical connection between a radio site or a dispatch site and a core. | Radio or dispatch site links must use one of the following physical transports. The site link type can differ between sites.<br>However, for a single DSR site, the same site link type is required for the site links to the primary core and the backup core.<br>• IPv4 Ethernet without encryption<br>• IPv4 Ethernet with encryption<br>• IPv4 T1/E1 without encryption<br>• IPv4 T1/E1 with encryption<br>• IPv6 Ethernet with encryption |
| Customer Enterprise Network (CEN) Interface | CEN interface is the conduit for IP data bearer traffic to enter and exit the system. An M3 system can support up to eight CENs. An M1 system supports one CEN. | CEN must connect to each primary core of a master site pair.<br>CEN interfaces must use one of the following physical transports:<br>• IPv4 Ethernet without encryption<br>• IPv4 Ethernet with encryption*<br>• IPv4 T1/E1 without encryption<br>• IPv4 T1/E1 with encryption<br>• IPv6 Ethernet with encryption<br>*The physical link between the two endpoints is not encrypted, but the tunnels between them are encrypted. |
| Authentication Center (AuC) Server | AuC is a radio authentication server supported as part of the DSR solution. | Radio authentication session information is not transferred from the Primary Zone Controller (ZC) to the Backup (DSR) ZC. Therefore, ZC configuration information (authentication keys) does not get replicated to DSR ZC like mobility information does.<br>AuC loads the authentication keys only to the active ZC. After Primary to Backup ZC switchover, Backup ZC loads the keys from AuC. Data between Primary and Backup AuC is synchronized automatically. In case of disaster recovery, the Backup AuC should be reinstalled. See "Radio Authentication |

| Term | Definition | Conditions |
|---|---|---|
| | | Disaster Recovery" in the *Radio Authentication Feature Guide*. |

## 1.3 Dynamic System Resilience Repeater Site with GCP 8000 Site Controller

In M1 and M3 Architectures, a mix of QUANTAR and GTR 8000 Base Radios support a Dynamic System Resilience (DSR) repeater site when used with a GCP 8000 Site Controller. The GCP 8000 Site Controller establishes a separate physical path to the backup core, and if the entire primary core fails and remains in wide-area trunked mode, a site can switch over.

GCP 8000 Site Controllers enable Trunked Site Repeater systems to be deployed using standalone GTR 8000 Base Radios.

The GCP 8000 Site Controller supports various system configurations using QUANTAR Base Radios, GTR 8000 Base Radios, and GTR 8000 Expandable Site Subsystems (ESS).

Redundant Network Management Service (Unified Event Manager (UEM)/Unified Network Configurator (UNC) and InfoVista) in the backup core are supported for the repeater site devices (GCP 8000 Site Controller, GTR 8000 ESS, transport devices), except for QUANTAR base radios.

See the *Repeater Site Infrastructure Reference Guide*.

This page intentionally left blank.

Chapter 2

# Theory of Operation for M3 DSR Systems

This chapter explains how Dynamic System Resilience (DSR) works in the context of your M3 system. It covers the architecture of components that provide DSR functionality and how these components interact to provide redundancy in an ASTRO® 25 system.

Included in this chapter are interactive illustrations and animations. If necessary, you can download the latest Flash® Player from http://www.adobe.com/. Click anywhere inside an image to display the interactive content. An option list allows you to select which drawing to view. Depending on the settings of your Adobe® Reader®, a **Manage Trust** dialog may open when you click an image. Select one of the options in the dialog box and click **Play** to view the content.

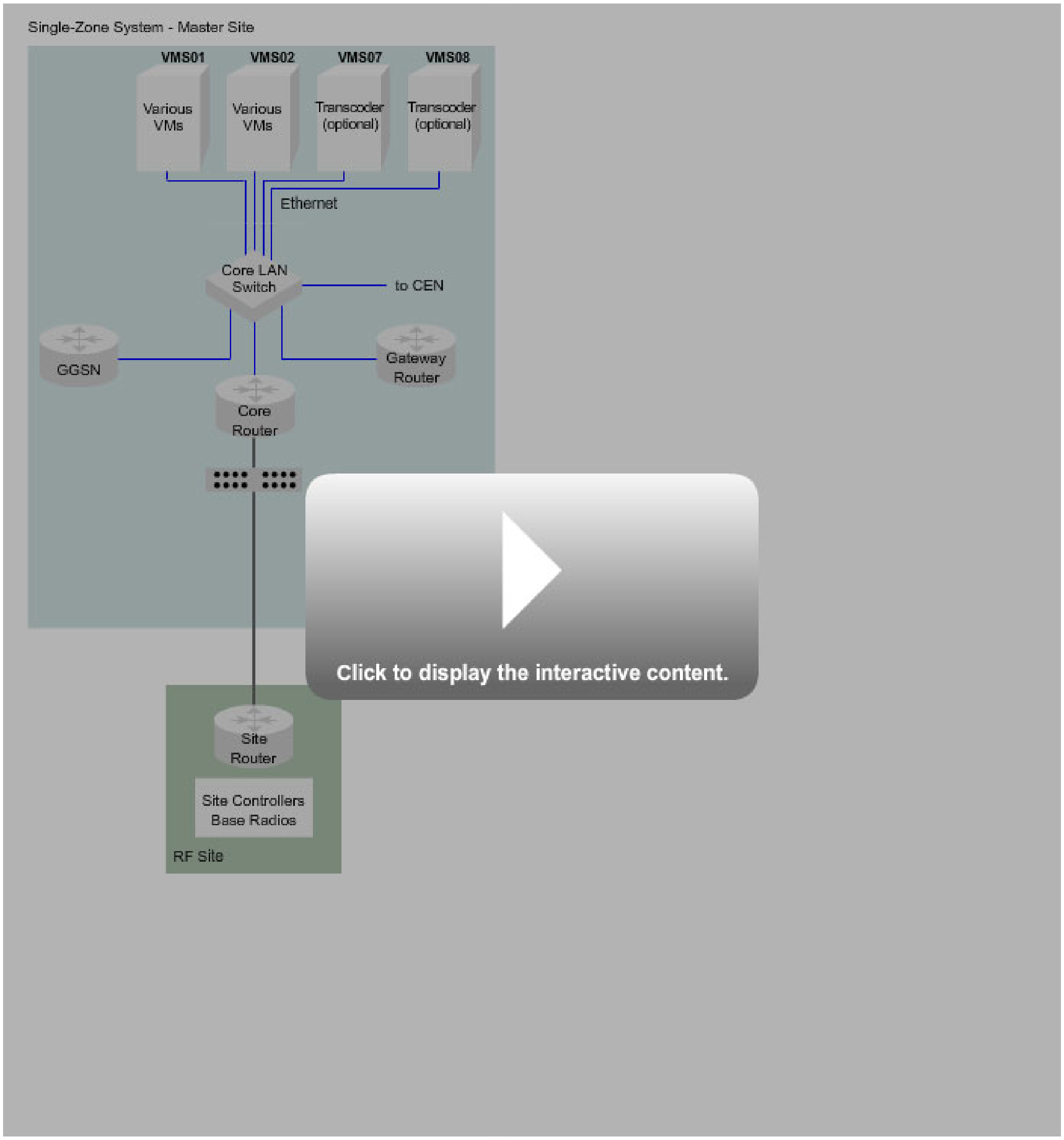
To print an illustration or a single frame of an animation, right-click the image and select **Print...** from the popup menu. In the **Print** dialog box, ensure that **Page Range** is set to **Selection**, then click **Print**.

**IMPORTANT:** Every frame of an animation (in some cases, hundreds) prints if the **Page Range** is set to **All**.

## 2.1 Single-Zone Master Site without DSR

This figure shows a simple, single-zone master site in an M3 system. For example, an M1 system would contain no Zone Controller 2 (ZC2). These drawings are provided to familiarize you with typical master site infrastructure architecture before Dynamic System Resilience (DSR). For simplicity, redundancy of equipment within each core is not shown in the illustrations, but exists as in any ASTRO® 25 master site.

**Figure 1: Single-Zone Master Site without DSR**



**NOTICE:** See the *GGM 8000 System Gateway Feature Guide* for details regarding the implementation of Gateway devices providing an alternative solution for the border gateway.

### Connection to Customer Enterprise Network (CEN)

If the master site connects to a CEN, a firewall, DMZ switch, and peripheral router are required. Tto save space, the additional components to connect to the CEN are shown in this drawing but in other illustrations in this chapter they are implied ("to CEN").

### Connections to Remote Sites

The master site can connect to different types of remote sites, for example, RF, HPD, or MCC 7500 VPM console.

**Zone Core Protection (ZCP)**

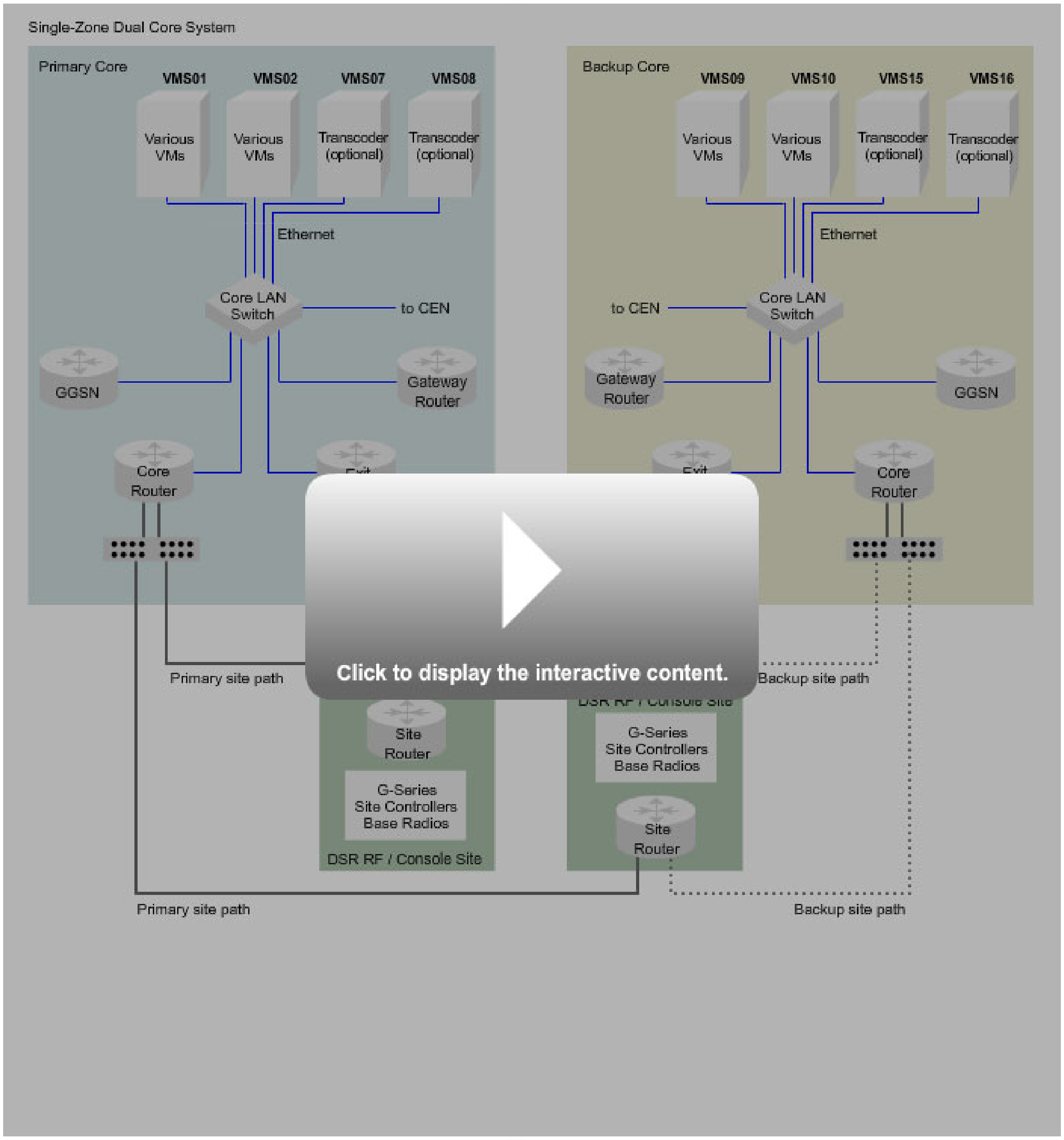
The optional ZCP feature (for M3 systems) requires the addition of a firewall, a Mediation LAN switch, and a Central Event Logging server. The core routers and exit routers connect to Mediation LAN switches. These connections allow traffic from remote sites into the ZCP firewalls at the master site. The firewall monitors traffic and applies policies and rules to determine what traffic is safe to allow into the zone. If a CEN connection is at the master site, an Intrusion Detection System (IDS) switch can be added to monitor traffic from both the Mediation LAN switch and the DMZ switch. Contact Motorola Solutions Support Center (SSC) for configuring ZCP in a system with DSR. ZCP is not supported in M1 systems.

## 2.2 Single-Zone Master Site with DSR

This figure shows a simple single-zone master site with Dynamic System Resilience (DSR) (a single zone/dual core). The backup core (Master Site 2) contains most of the same infrastructure components as the primary core. Exit routers are added to each master site for the InterZone link. The InterZone link can be T1/E1 or Ethernet. It is used for traffic between the primary and backup core, including but not limited to call control traffic, IP data bearer service control traffic, network management traffic, and configuration management synchronization traffic. The core routers at each master site route call control, voice, data payload, and network management traffic. Both the primary core and the backup core have site paths to the remote sites. If a primary core fails, the backup site path is used to continue services to subscriber radios.

For simplicity, redundancy of equipment within each core is not shown in the illustrations, but exists as in any ASTRO® 25 master site.

**Figure 2: Single-Zone Master Site with DSR**



### 2.2.1
## Remote Sites

Remote sites with G-series site controllers and base radios can be configured for Dynamic System Resilience (DSR) or non-DSR. Sites that include PSC 9600 Site Controllers, QUANTAR or STR 3000 Base Radios, circuit-based simulcast, SmartX, or ISSI.1 Network Gateway can be present in a system with DSR, but do not support DSR functionality. Non-DSR sites are linked only to the primary core. On a per-site basis, DSR capability is established by configuring a separate physical path to the backup core. With a path to the backup core, a site can switch over if the entire primary core fails. The backup site path can also be used in the event the primary site path fails. Traffic can be rerouted along the backup site path, through the backup core and over the InterZone link to the primary core without interrupting wide-area trunking.

A mix of QUANTAR and GTR 8000 Base Radios support DSR when used with a GCP 8000 Site Controller. The GCP 8000 Site Controller establishes a separate physical path to the backup core, and if the entire primary core fails and remains in wide-area trunking mode, a site can switch over.

## 2.3 DSR Scalability

In an M3 multi-zone capable system, Dynamic System Resilience (DSR) is optional on a zone-by-zone basis. An M3 multi-zone system with DSR can include up to seven zones, provided that one of the zones is added without DSR. The following sections discuss typical architectures with DSR. M3 Multi-Zone System with DSR on Selected Zones on page 40 describes an M3 multi-zone system with DSR on selected zones.

**NOTICE:** Although the following descriptions and diagrams show co-located primary and backup master sites, systems may be constructed in which the primary and backup cores are not co-located pairs. For example, a two-zone system may have four master sites.

### 2.3.1 Hybrid T1 and Ethernet Links Feature

This feature allows the two redundant connections between a zone core and remote sites to be different types, providing a more available connection scheme using diverse networks and paths. It also provides cost saving over adapting T1/Ethernet connections using third-party devices, which not only adds costs, but also adds complexity and reduced reliability. The third-party devices are also usually not network managed.

This feature is compatible with M3 Dynamic System Resilience (DSR) systems so that now the redundant links between the zone core and the remote sites may be different types.

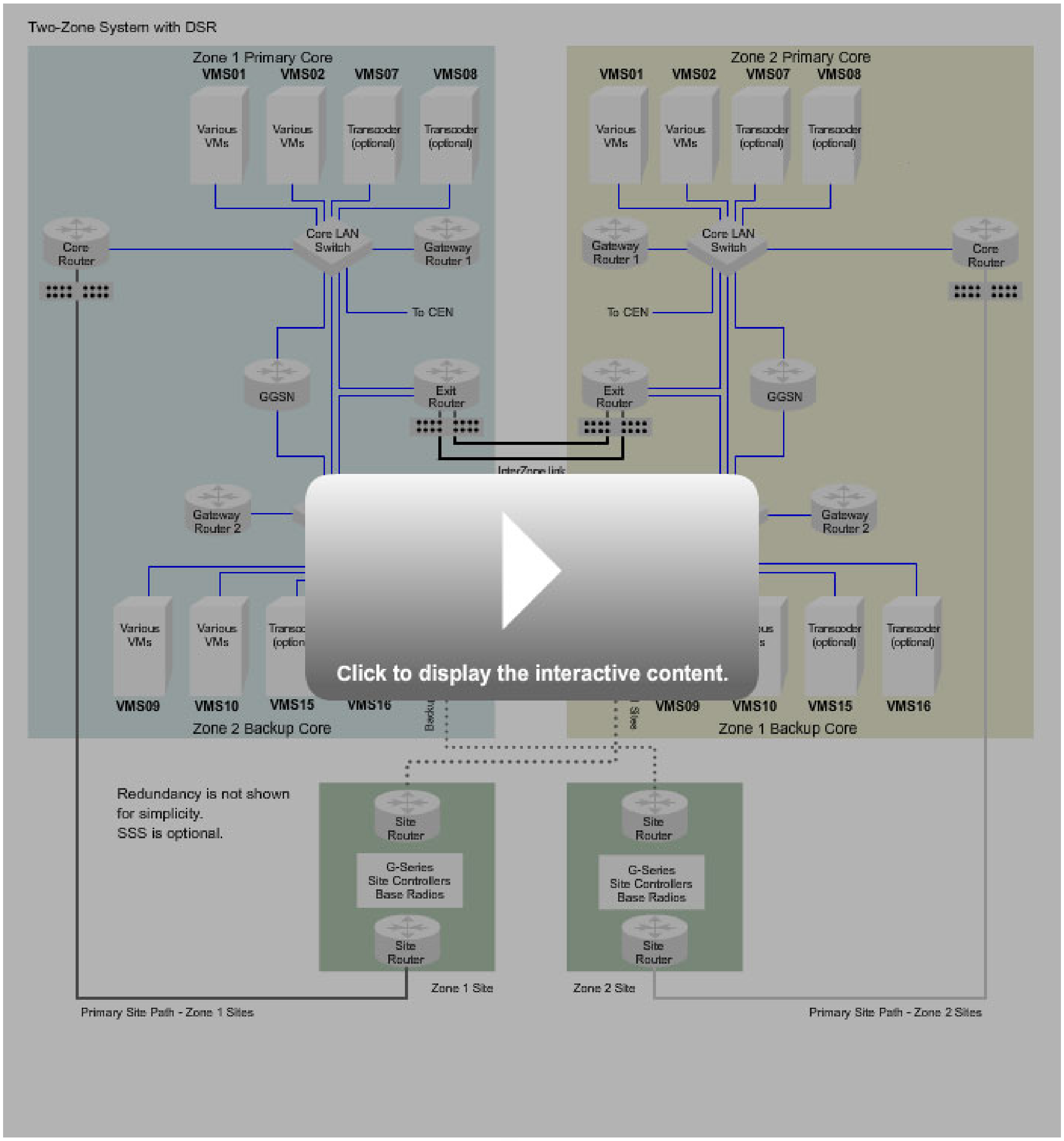
**IMPORTANT:** In a hybrid links configuration, only Motorola Network Resource (MNR) S6000s and GGM 8000s are used as the core routers and site gateways, respectively.

### 2.3.2 Two-Zone System with DSR

In a two-zone system with Dynamic System Resilience (DSR), each of the two master sites contains a primary core for one zone and the backup core for another zone. As shown in this figure, most of the system infrastructure is duplicated when a backup core is added to a site.

Shared transport equipment includes the redundant pair of LAN switches, exit routers, core backhaul switches, and gateway routers that provide transport and rendezvous point functions for both zones. Some systems with DSR may require a third LAN switch to support the extra infrastructure equipment. If a connection to a Customer Enterprise Network (CEN) exists, only one Gateway GPRS Support Node (GGSN) router is required and it is shared between the two cores.

**Figure 3: Two-Zone System with DSR**

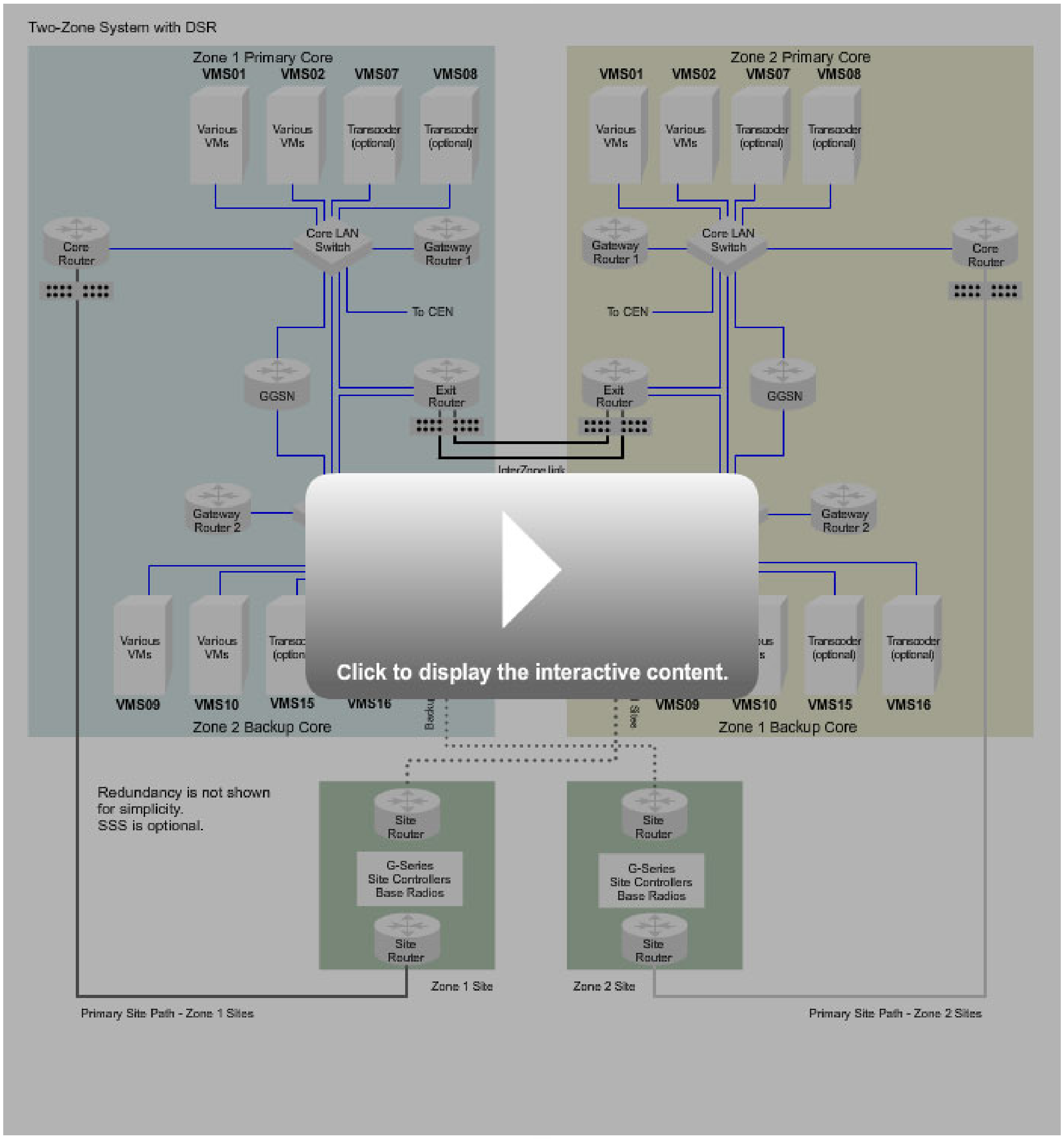


**NOTICE:** See the *GGM 8000 System Gateway Feature Guide* for details regarding implementation of Gateway devices providing an alternative solution for the site gateways.

## 2.3.3 M3 Two-Zone System with DSR with Zone Core Protection

This figure shows Zone Core Protection (ZCP) added to the Dynamic System Resilience (DSR) master site. Shared equipment in this configuration includes the ZCP firewalls and the mediation LAN switches. A dedicated Centralized Event Logging (CEL) Server (Syslog server) in the Demilitarized Zone (DMZ) is added to the backup core.

**Figure 4: Two-Zone System with DSR with ZCP**



Redundancy is not shown for simplicity.
SSS is optional.

## 2.3.4 M3 Three-Zone System with DSR

A three-zone system with Dynamic System Resilience (DSR) is built with one pair of dual-core master sites and one pair of single-core master sites. It is a two-zone system plus a single-zone system, each with DSR. A three-zone system with DSR could also be created using three pairs of single-zone cores.

## 2.3.5 M3 Four-Zone System with DSR

A four-zone system with Dynamic System Resilience (DSR) is the same as two, two-zone systems.

Regardless of the number of zones, system-wide servers include only two Core Security Management Servers (CSMSs) (for IP services), two System Statistics Servers (SSSs) (for performance management), and two User Configuration Servers (UCS) and Unified Network Configurator (UNC) servers (for configuration management). Each pair of these system-wide servers can be in any master site pair (primary and backup core) in any one zone.

## 2.3.6 M3 Five-Zone System with DSR

A five-zone system with Dynamic System Resilience (DSR) structurally looks like two two-zone systems plus a single-zone system.

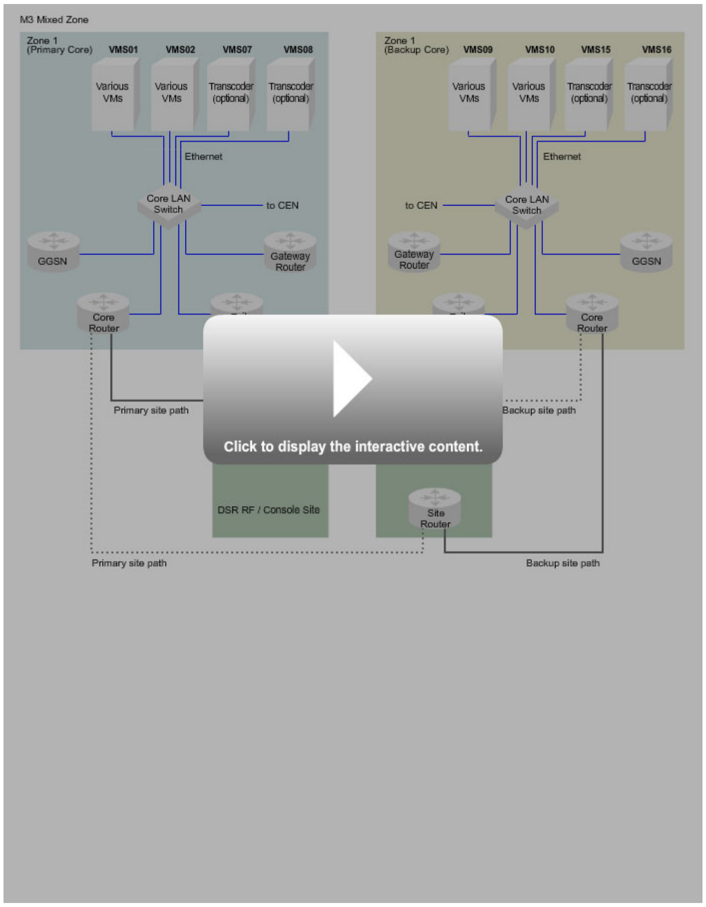
## 2.3.7 M3 Six-Zone System with DSR

A six-zone system with Dynamic System Resilience (DSR) looks like three, two-zone systems.

## 2.3.8 M3 Multi-Zone System with DSR on Selected Zones

An M3 multi-zone system can put Dynamic System Resilience (DSR) on selected zones, as shown in the following figure. In this scenario, a seventh master site can be added if this seventh site is not a DSR site.

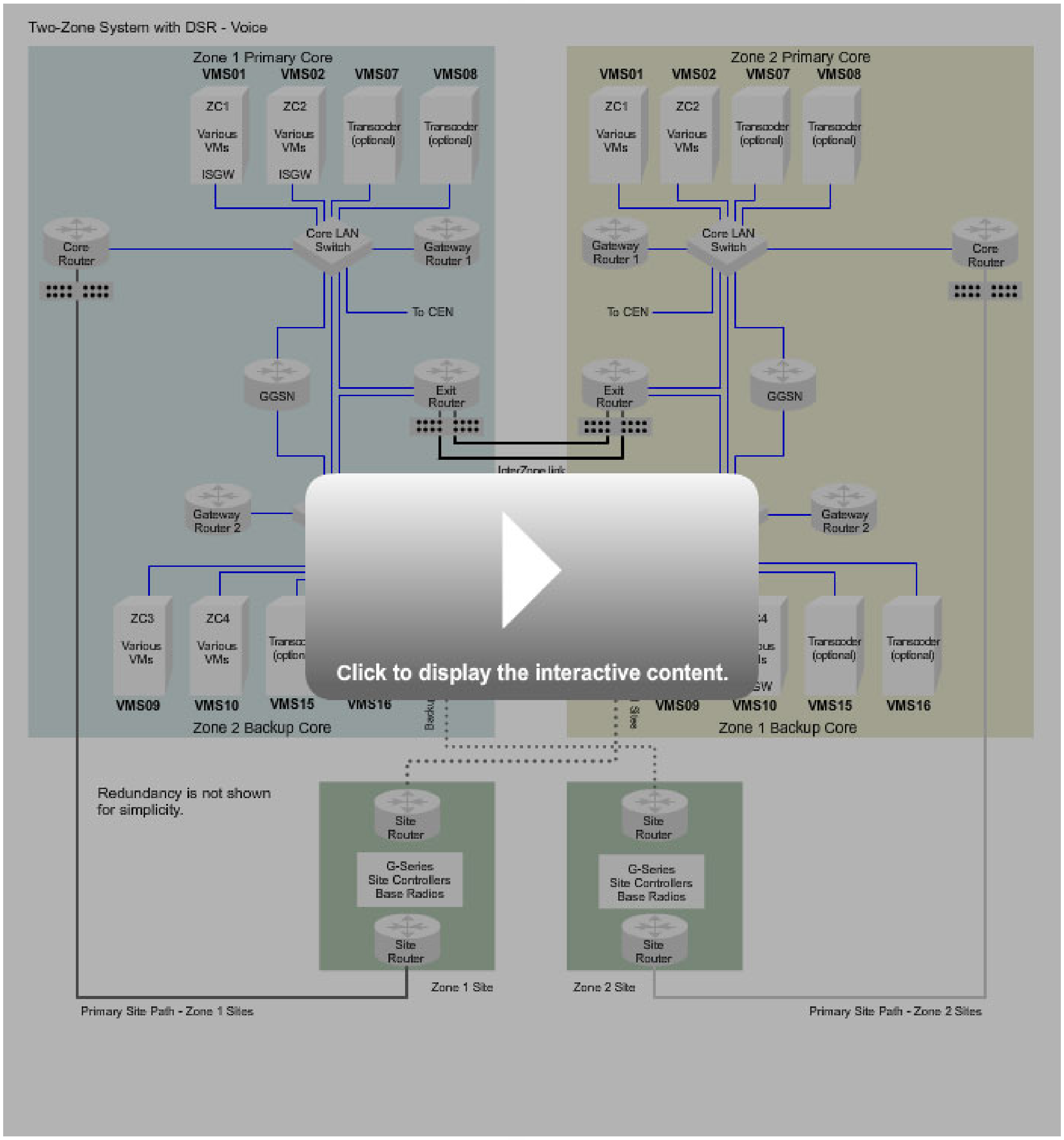
**Figure 5: M3 Mixed-Zone System**



## 2.4 Voice Services

Dynamic System Resilience (DSR) allows a system to continue to function with minimal loss of voice communication due to the failure of any controlling master site. This figure shows voice subsystem components in a two-zone system with DSR with possible failure scenarios. Due to space constraints, other core equipment and redundancy have been left out of the drawings.

**Figure 6: Voice Services Components**



The Zone Controllers (ZCs) are the heart of the voice subsystem. For each zone, two dedicated ZC applications exist in each master site. The four ZCs securely communicate to select one active ZC. The selection algorithm is weighted to give preference to the ZCs in the primary core. The standby ZCs automatically synchronize their subscriber location and talkgroup affiliation databases with the active ZC in real time so that they can immediately host voice calls after a ZC switchover.

Under normal conditions, ZC1 in the primary core is typically in the “Active” state. Assuming no critical failures, the remaining ZC2, ZC3, and ZC4 are either in the "Standby" or "User Requested Standby" state. If no other failures are in the system and the active ZC fails (that is, ZC1), the lowest numbered ZC in the "Standby" state becomes active automatically. The lowest number gives preference to the primary core. If both ZCs in the primary core fail, a ZC in the backup core becomes active.

The three major states that each ZC supports are:

- Standby – in a standby state, the ZC is capable of an automatic switchover. While a ZC is in a standby state, it suspends establishing connection to remote sites and other zones. In this state, the ZC monitors heartbeat messages from the active ZC. If a ZC misses consecutive heartbeats or is informed that the active ZC can no longer remain active, it becomes active.
- Active – in an active state, the ZC is capable of accepting connection requests from the remote sites and other zones, and is capable of establishing call sessions. In each zone, only one ZC is active at a time.
- User Requested Standby – in a user requested standby state, the ZC disables the automatic switchover capability and remains in a User Requested Standby state until a user changes the state to Standby or Active.

When a remote RF site, Site Gateway (Conventional Channel Interface), or MCC 7500 VPM site detects a Site Control Path (SCP) failure, the site attempts to re-establish the link by switching between the primary and backup cores until the active ZC responds.

## 2.4.1 RF Site Switchover

On a per site basis, Dynamic System Resilience (DSR) capability is established by configuring a separate physical path to the backup core. With a path to the backup core, a site can switch over if the entire primary core fails. Without a backup path, a site cannot switch over and goes into site trunked operation.

The backup path also operates as a redundant site path. If the path to the primary core fails, traffic is rerouted over the backup path and then across the InterZone link to the primary core. The rerouting is fast enough to maintain wide-area trunked operation.

As previously described, sites alternate between the primary and backup core to establish a Site Control Path (SCP). At a low level, the sites are configured with two additional broadcast subnet IP addresses for the zone controllers in the backup core. The two broadcast addresses allow the site to establish redundant SCPs to the active zone controller; one to each Network Interface Card (NIC) of the active zone controller. For DSR, after the site establishes one SCP to a core, it does not broadcast requests to the other core. The site persistently tries to establish the redundant SCP to the same core.

## 2.4.2 MCC-Series Dispatch Console and Site Gateway with Conventional Channel Interface Switchover

As with an RF site, an MCC 7500 VPM/MCC 7500E/MCC 7100 Dispatch Console and Site Gateway with Conventional Channel Interface (CCI), is given Dynamic System Resilience (DSR) capability by configuring a separate physical path to the backup core. This backup path also offers redundancy. If the primary path fails, traffic is rerouted through the backup core over the InterZone link to the primary core without interrupting wide-area trunking. Without this backup path, the console site reverts to site conventional mode (site conventional also applies to entire conventional subsystems), if the primary core fails.

For console sites with two or more consoles, a pair of consoles at the console site establishes redundant links (one link per console) to the active zone controller. For DSR, the consoles coordinate their attempts to establish links to the same core. For console sites with one console, the console establishes two links to the active zone controller.

For site link establishment, the Site Gateway (CCI) mimics the RF sites. That is, the Site Gateway (CCI) alternates between the primary and backup cores.

Consoles and Site Gateways (CCI) work independently to establish links to the active zone controller regardless of whether they are colocated.

**NOTICE:** For an alternative implementation of the CCI device, see the *GGM 8000 System Gateway Feature Guide*.

### 2.4.3 MCC 7100/MCC 7500E Dispatch Console and Dynamic System Resilience

A remote MCC 7100/MCC 7500E Dispatch Console registers with the Zone Database Server (ZDS) (Lightweight Directory Access Protocol (LDAP) server). If it loses a connection to the ZDS, it attempts to re-register, but it keeps the link to the Console Proxy intact. During a Dynamic System Resilience (DSR) switchover from the primary zone core to the backup zone core, if concurrent LDAP downloads are taking place by multiple console operator positions (due to the switchover) and the remote MCC 7100/MCC 7500E Dispatch Console has a valid database, the MCC 7100/MCC 7500E Dispatch Console continues to operate while the new database is being downloaded. After initial registration with the ZDS and an LDAP database has been downloaded, the MCC 7100/MCC 7500E Dispatch Console has the option to turn off ZDS downloads to conserve bandwidth.

### 2.4.4 Radio Authentication and Dynamic System Resilience

The Authentication Center (AuC) Server supports radio authentication and is supported as part of the Dynamic System Resilience (DSR) solution.

Radio authentication session information is not transferred from the Primary Zone Controller (ZC) to the Backup (DSR) ZC. Therefore, Zone Controller configuration information (authentication keys) is not replicated to the DSR Zone Controller like mobility information is.

AuC loads the authentication keys only to the active ZC. After Primary to Backup ZC switchover, Backup ZC loads the keys from AuC. Data between Primary and Backup AuC is synchronized automatically. In case of disaster recovery, the Backup AuC should be reinstalled. See "Radio Authentication Disaster Recovery" in the *Radio Authentication Feature Guide*.

## 2.5 Data Services Without High Availability

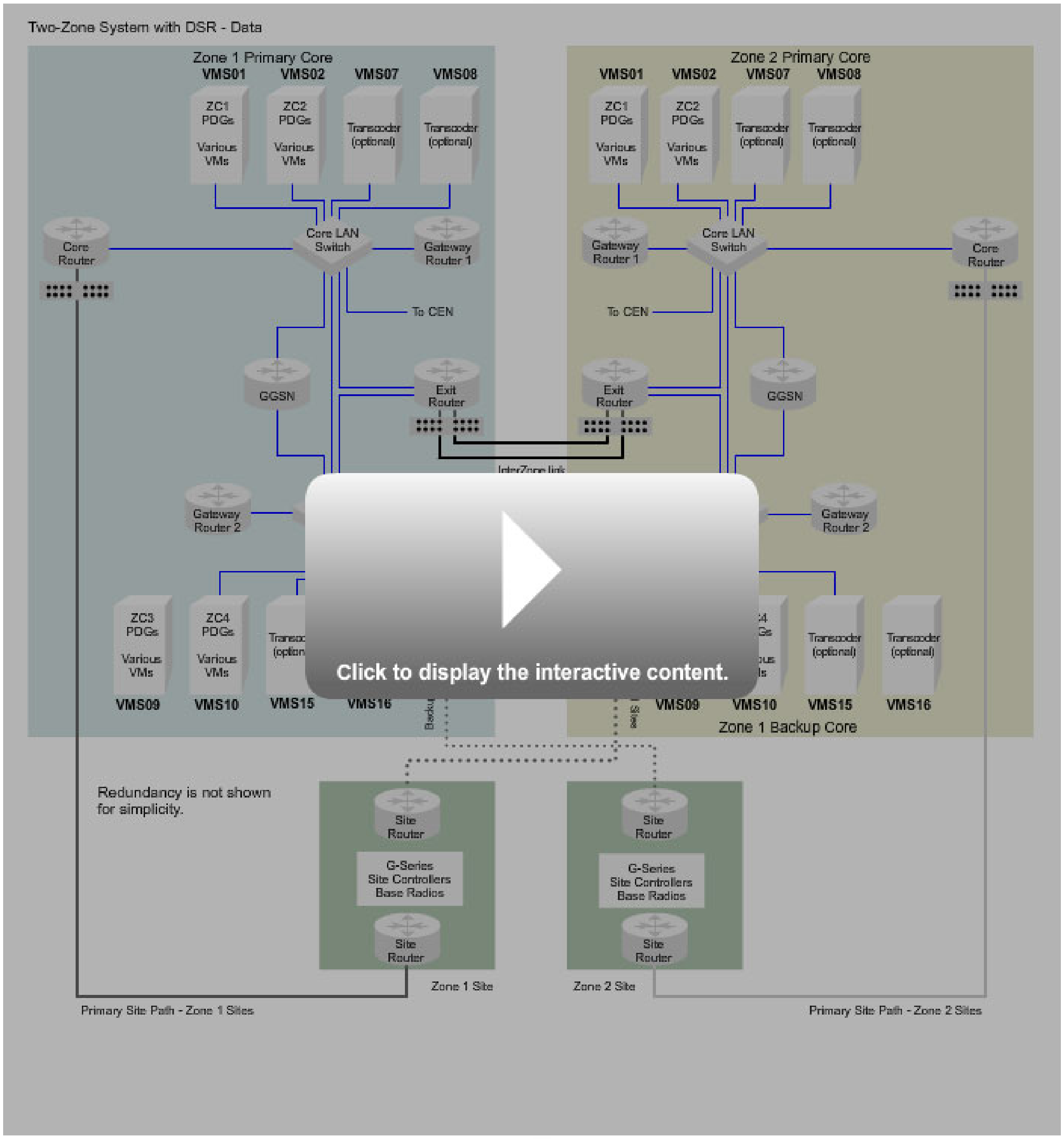
In a system with Dynamic System Resilience (DSR), each zone may have Packet Data Gateways (PDGs) for Trunked Integrated Voice and Data (IV&D), High Performance Data (HPD) service, and Packet Data Gateways (PDGs) for conventional with IV&D. Trunked IV&D and HPD have one PDG in the primary core and one PDG in the backup core.

DSR is also supported for conventional IV&D.

The PDGs securely communicate to automatically select one active PDG. The selection algorithm is weighted to give preference to the PDG serving the most number of sites/channels, or the PDG in the primary core if the number of serving sites is equal. The active PDGs synchronize context databases with the standby PDG. After a switchover, you are not required to context activate with the newly active PDG. In each zone, only one PDG can be active at a time.

This figure shows data subsystem components in a two-zone system with DSR and possible failure scenarios. Due to space constraints, other core equipment and redundancy have been left out of the drawings.

**Figure 7: Data Services Components**



Under normal conditions, the PDG in the primary core is typically in the “Active” state. Assuming no critical failures occur, the PDG in the backup core is in either the "Standby" or "User Requested Standby" redundancy state. If there are no other failures in the system, and the primary core PDG fails, the backup core PDG becomes active automatically. Even if the primary core PDG becomes operable, switchover to the primary core PDG does not happen unless there is a critical failure of the backup core PDG.

The three major states that each PDG supports are:

- Standby – in a Standby state, the PDG is capable of an automatic switchover. While a Packet Data Router (PDR) is in a Standby state, it suspends sending Home Location Register (HLR) queries to the Zone Controller (ZC), and the Radio Network Gateway (RNG) suspends sending Visitor

Location Register (VLR) queries to the ZC. While in a Standby state, the RNG does not accept connection requests from RF sites or remote PDRs in other zones. The Gateway GPRS Support Node (GGSN) can forward data to a PDR without a data session established. The PDR does not process any echo requests or data messages from the GGSN. The PDR sends GTP echo requests and processes the echo responses from the GGSN. The PDR monitors heartbeat messages from the active PDR. If the PDR misses consecutive heartbeats or is informed that the other PDR can no longer remain active, it becomes active.

- Active – in an Active state, the PDR is capable of establishing a data session with remote RNGs, process data messages from the GGSN, and send HLR queries to the ZCs. The RNG in the Active state can accept connection requests from RF sites and a remote PDR in other zones. Upon establishing a data session with the PDR, the GGSN forwards outbound data for the radios currently context activated.
- User Requested Standby – in a User Requested Standby state, the PDG disables the automatic switchover capability and remains in a User Requested Standby state until a user changes the state to Standby or Active.

The user can control a switchover by setting the redundancy states to User Requested Standby or Active in the UNC. The user can also change a PDG redundancy state from User Requested Standby to Standby if the user previously wanted to prevent a PDG from automatically switching to active but now wants the PDG to be able to automatically switch to active as the need arises.

## 2.5.1 PDR to Local RNG Link

Part of the Packet Data Router (PDR) operational health is the ability to talk to the local Radio Network Gateway (RNG). Without that ability, the PDR is in the inoperable operational health state. The PDR always sends periodic loopback messages to the local RNG to verify the communication path exists. Upon transitioning to the active state, the PDR informs the local RNG to go active, which triggers the RNG to accept connection requests from RF sites and remote PDRs.

## 2.5.2 PDR to Remote RNG Link

After a Packet Data Router (PDR) becomes active, the PDR initiates connections with remote Radio Network Gateways (RNGs). For each remote zone, the PDR first makes several attempts to connect with the RNG in the primary core. If those attempts fail, the PDR tries the RNG in the backup core. The PDR alternates between the primary and backup cores until the remote RNG connection is established.

## 2.5.3 Zone Controller to PDG Mobility Updates

The Packet Data Gateway (PDG) gets subscriber mobility updates from the Zone Controller (ZC). Mobility multicast groups hosted by the gateway router are used to push mobility updates from the ZC and to make specific queries from the PDG. Multicast groups efficiently handle redundant ZCs and are used by High Performance Data (HPD) and IV&D PDGs in the same zone. The PDG can get mobility information from any active ZC.

## 2.5.4 Site Controller to RNG Link for HPD and IV&D

The Site Controller (SC) establishes the SC-to-Radio Network Gateway (RNG) link for High Performance Data (HPD) and IV&D. The SC makes multiple attempts to establish a link with the RNG in the primary core. After those attempts fail, the SC gives up and tries the RNG in the backup core. After those attempts fail, the SC goes back to the primary core. While attempting to connect to the

RNG, the SC alternates between the primary core and backup core. This process continues until a connection is established to the active RNG. When established, the link is maintained by exchanging periodic messages between the SC and RNG.

## 2.5.5 Conventional Channel Gateway to RNG Link for Conventional IV&D

The Conventional Channel Gateway (CCGW) establishes the CCGW-to-Radio Network Gateway (RNG) link for Conventional IV&D The CCGW makes multiple attempts to establish a link with the RNG in the primary core. After those attempts fail, the CCGW gives up and tries the RNG in the backup core. After those attempts fail, the CCGW goes back to the primary core. While attempting to connect to the RNG, the CCGW alternates between the primary core and backup core. This process continues until a connection is established to the active RNG. When established, the link is maintained by exchanging periodic messages between the CCGW and RNG.

## 2.5.6 RNG to SC Multicast Link for Broadcast Data

Upon establishing the Site Controller (SC)-to-Radio Network Gateway (RNG) link, the SC joins the multicast/broadcast groups, one for each gateway router in a core. A pair of multicast/broadcast groups is for the primary core and a pair for the backup. The SC joins the multicast/broadcast groups associated with the same core as the established SC-to-RNG Link Access Procedure for D channel (LAPD) link.

The RNG periodically sends a broadcast hello message to the multicast/broadcast group. Your organization broadcasted data traffic is also sent to the multicast/broadcast group.

The SC uses reception of the broadcast hello message or broadcast data traffic on either multicast group as an indication that the multicast/broadcast link with the RNG is up. If the SC receives nothing for a time, the SC leaves and rejoins those multicast/broadcast groups.

## 2.5.7 RNG to CCGW Multicast Link for Broadcast Data

The Conventional Channel Gateway (CCGW) joins the multicast/broadcast groups, one for each gateway router in a core, upon establishing the CCGW-to-Radio Network Gateway (RNG) link. A pair of multicast/broadcast groups is for the primary core and a pair for the backup. The CCGW joins the multicast/broadcast groups associated with the same core as the established CCGW to RNG Link Access Procedure for D channel (LAPD) link.

The RNG periodically sends a broadcast hello message to the multicast/broadcast group. Your organization broadcasted data traffic is also sent to the multicast/broadcast group.

The CCGW uses reception of the broadcast hello message or broadcast data traffic on either multicast group as an indication that the multicast/broadcast link with the RNG is up. If the CCGW receives nothing for a period of time, the CCGW leaves and rejoins those multicast/broadcast groups.

## 2.5.8 Packet Data Router to GGSN Link

In a system with Dynamic System Resilience (DSR), each of the redundant Packet Data Routers (PDRs) is configured to communicate with its local Gateway GPRS Support Node (GGSN). Each PDR can be associated with only one GGSN. Part of the PDR operational health is having a link to the GGSN. Without that link, the PDR cannot be in the operable state. The PDR monitors the health of the GGSN link by sending periodic GPRS Tunneling Protocol (GTP) echo requests with the GGSN. In the Standby or User Requested Standby states, the PDR does not process any echo requests or data messages from the GGSN.

The GGSN is a system-level device because it may support more than one zone. However, it is resident in a zone core. This situation presents implications for the deployment of the GGSN in a system with DSR zones and non DSR zones. A PDG in a non DSR zone can be configured only to communicate with one GGSN. DSR data service is not available to non DSR zones. If the GGSN is in a non DSR zone, PDGs in DSR zones can configure the PDGs in the primary zone to communicate with the GGSN. However, PDGs in the backup cores cannot communicate with the GGSN in the non DSR zone. DSR data service is not available for the entire system in this configuration. DSR for data service is an optional feature. If the DSR data service is not required, the GGSN can be in any zone.

If the DSR data service is required, the GGSN must be in a DSR zone. This location allows DSR data service to be supported for DSR zones in the system. The PDG in a non DSR zone is configured to communicate with the GGSN in the primary core of the DSR zone. Data services in non DSR zones are not capable of DSR service. If a failure causes a switchover to the backup core of the DSR zone containing the GGSN, the PDGs in the non DSR zones cannot communicate with that GGSN. The non DSR zones lose data service until data service is resumed in the primary core. Because DSR does not automatically switch back to the primary core for data service when the primary core is recovered for data service, a manual switchover to the primary core is necessary to recover the data service in the non DSR zones.

Only the active PDR sends context activation requests to its GGSN and establishes tunnels for passing data. After the GGSN has established active tunnels with a PDR, it sends periodic messages to that PDR to maintain the tunnels. If the PDR is still active, it responds and the tunnels are maintained. The GGSN tears down the tunnels if the PDR does not send any messages. To stay in sync with the PDR, if the PDR-to-GGSN link is down for 4 minutes or longer, the GGSN flushes its active contexts. On link recovery, the PDR re-context activates all the active contexts in its database with the GGSN.

When the PDR detects the GGSN link as down, the PDR brings down the local RNG link to force the site links to the RNG to be dropped. After losing the link to the RNG, the sites tries to connect to the backup RNG, and alternates between the primary core and backup core.

## 2.5.9 GGSN to Customer Network Interface Link

In a system with Dynamic System Resilience (DSR), each Customer Enterprise Network (CEN) which requires full data redundancy has two Customer Network Interface (CNI) connections to the system. These connections must be made to a master site pair. For example, if the CEN connects to Master Site 1, which has the primary core for zone 1 and backup core for zone 2, the CEN must also connect to Master Site 2.

For another level of resilience, each Gateway GPRS Support Node (GGSN) in the redundant pair can establish a tunnel through either CNI. The preferred tunnel goes through the CNI equipment in the same core as the serving GGSN.

## 2.5.10 Packet Data Router to Gateway Routers Monitoring

The Packet Data Router (PDR) sends periodic ping requests to monitor that it can reach the gateway routers through both its interfaces. If the PDR cannot reach both gateway routers through one of its interfaces, the PDR transitions into an inoperable operational health state which allows the peer Packet Data Gateway (PDG) to transition to active. Not reaching the gateway routers through one of its interfaces is an indication that the PDR either cannot reach the sites or cannot reach the Gateway GPRS Support Node (GGSN).

## 2.5.11 Data Subsystem Failures and Recovery

The following sections describe data subsystem failures and recovery.

### 2.5.11.1 Complete Data Subsystem Failure in Primary Core

Upon a failure of the primary core, the data subsystem in the backup core becomes active and re-establishes the data bearer service.

The recovery process is driven by the Packet Data Router (PDR), which detects the failure as described in PDR Failure and Recovery on page 49.

### 2.5.11.2 PDR Failure and Recovery

If the active Packet Data Router (PDR) fails, the PDR in the backup core stops receiving heartbeat messages. After a number of consecutive heartbeats are missed, the PDR in the backup core becomes active.

Upon transitioning to the active state, the PDR establishes the link to all remote Radio Network Gateways (RNGs). The PDR also starts processing messages from the GPRS Gateway Support Node (GGSN). The PDR and RNG subscribe to the mobility groups for mobility information from the Zone Controller (ZC).

The newly active RNG accepts a connection from any remote PDR in other zones and from the site controllers in this zone.

If the RNG in the primary core remained alive when the PDR failed, the RF sites would temporarily stay connected to the RNG. After the RNG detects the link to the PDR is down, it drops the links to all RF sites. The RF sites attempt to establish an RNG connection through the site controller to the backup RNG after exhausting all retry attempts with the primary RNG.

### 2.5.11.3 RNG Failure and Recovery

After the Packet Data Router (PDR) determines its local Radio Network Gateway (RNG) has failed, the PDR goes inoperable and informs the standby PDR through the heartbeat that it is no longer operable. The backup PDR becomes active and initiates the data subsystem recovery process. While the PDR is inoperable, when it receives notification through the heartbeat that the peer PDR went active operable, the inoperable PDR transitions to the standby state and resets.

If the standby PDR loses the link to its local RNG, it tries to re-establish that link. The standby PDR cannot go operable without the local RNG.

### 2.5.11.4 PDR to Remote RNG Failure and Recovery

If the Radio Network Gateway (RNG) loses its link to the remote Packet Data Router (PDR), it waits for the PDR to reconnect. If the PDR loses a link to a remote RNG, it attempts to reconnect following the procedure in PDR to Remote RNG Link on page 46.

### 2.5.11.5 PDR to GGSN Link Failure and Recovery

If the active Packet Data Router (PDR) loses the link to its Gateway GPRS Support Node (GGSN), it goes inoperable, drops the local Radio Network Gateway (RNG) link, and informs the standby PDR through the heartbeat. The standby PDR becomes active and re-establishes data services. When notified that standby PDR transitioned to the active state, the inoperable PDR transitions to the standby state and reset.

If the standby PDR loses the link to its GGSN, it tries to re-establish that link. The standby PDR cannot go operable without the GGSN.

### 2.5.11.6 CDEM Failure and Recovery for Conventional Data

The encryption/decryption of secure data packets in a conventional system is handled by the CAI Data Encryption Module (CDEM) devices, connected locally to the Radio Network Gateway (RNG). In a Dynamic System Resilience (DSR) system, a CDEM is connected to each instance of the conventional Packet Data Gateway (PDG) in the zone. If the CDEM connected to the active PDR/RNG fails or the connectivity to the CDEM is lost, the PDR/RNG goes into an active semi-operable state indicating it is only capable of providing clear data services. The semi-operable PDR informs the standby PDR through the heartbeat that it is no longer able to provide secure data services. The standby operable PDR becomes active and initiates data subsystem recovery process. When notification through the heartbeat is received that the peer operable PDR went active operable, the semi-operable PDR transitions to a standby semi-operable state and resets.

If a dual CDEM failure occurs, no repeat switchover occurs, and the PDR operating in a semi-operable state continues to provide data services, albeit clear only.

### 2.5.11.7 ZC to PDG Mobility Failure and Recovery

As indicated in Zone Controller (ZC) to Packet Data Gateway (PDG) mobility updates, the PDG and ZC use multicast groups to transfer mobility information. By using multiple multicast groups, both the Packet Data Router (PDR) and Radio Network Gateway (RNG) within the PDG are resilient to ZC and gateway router failures.

### 2.5.11.8 GGSN-to-CEN Failure and Recovery

The primary Customer Enterprise Network (CEN) interface is a tunnel established between the primary border gateway and the Gateway GPRS Support Node (GGSN) in the primary core. When that tunnel fails, the transport subsystem re-establishes a backup tunnel from the GGSN over the InterZone link to the backup border gateway in the CEN. After this backup tunnel is established, the delivery of CEN traffic is resumed. When the primary CEN interface is restored, the original tunnel is restored and used for packet delivery.

## 2.5.12 Data Subsystem Component Failure and Context Activation

When a data subsystem failure occurs, the data subsystem communication is restored in less than 75 seconds.

If component failure involves the Radio Network Gateway (RNG), Packet Data Router (PDR), Gateway GPRS Support Node (GGSN), or both gateway routers, the subscribers which are home to the zone need not initiate a context activation request with the newly active data subsystem. The failure forces a switchover to the backup data subsystem, which has the replicated context records. Context activation is shared between the two cores.

If the PDR-GGSN link has been down for more than 4 minutes, the GGSN flushes their active contexts. When the GGSN link is re-established, the active PDR sends the context renewal for the active subscriber contexts in its database.

Subscribers that have roamed to a visiting zone have the context renewed re-establishment of the link from the newly active PDR with the remote RNG.

## 2.5.13 IV&D and HPD Subscriber Radios

With Dynamic System Resilience (DSR) failure and recovery resulting in data service restoration in the other core, the subscriber continues to operate with the same IP address as the one before the switchover. The transport routing enables the new routing of the same IP address to the Customer Enterprise Network (CEN). The newly active Packet Data Gateway (PDG) performs a proxy and context renew of the subscriber context with the existing IP address with its Gateway GPRS Support Node (GGSN), thus establishing a valid data path for the subscriber. The DSR switchover of the data subsystem resumes service on a switchover without triggering an application registration for the internal application in the radio such as Over the Air Rekeying (OTAR), Text Messaging, Presence Notifier, Outdoor Location, and so on.

## 2.5.14 Radio Authentication

Radio Authentication ensures that subscriber radios accessing the system are authorized and validated to access the radio communication system. The Authentication Center (AuC) server supports this feature and can be established in the primary and backup zone core. The AuC Server resides with an AuC Client on a Virtual Machine (VM) hosted by the same hardware platform as the virtualized Domain Controller.

An M3 zone core configuration with DSR has two AuC servers. Procedurally, only one of the two AuCs is enabled at a time. Each AuC has its own IP address and Fully Qualified Domain Name (FQDN) where the AuC is on different physical servers. A common agent runs on both AuCs and the Unified Event Manager (UEM) discovers both; one is enabled and the other disabled. The zone controller tries to connect to the AuC and connects to the first enabled one it finds. If no active AuC can be found, the zone controller considers the failure to be an infrastructure failure. In this case, the zone controller continues to authenticate.

AuC data is replicated to the backup AuC together with additional information, such as passwords and the Master Key synchronization status (the Master Key itself gets synchronized only by setting it manually on the primary and backup AuC server).

See the *Radio Authentication Feature Guide* for details.

# 2.6 Data Services with High Availability

High Availability (HA) Data is an optional feature which introduces redundant Packet Data Gateways (PDGs) and GPRS Gateway Support Node (GGSN) transport devices to support data system availability. While HA Data can be implemented in systems that do not employ Dynamic System Resilience (DSR), the redundancy can also be implemented in systems employing DSR.

**NOTICE:** HA Data is available to L2, M2, and M3 zone core systems employing Common Server Architecture (Virtual Management Server host platforms).

## 2.6.1 HA Data Without DSR Redundancy at a Single Zone Core

High Availability (HA) Data in a single-zone system that does not implement Dynamic System Resilience (DSR) employs two (redundant) HA Packet Data Gateways (PDGs) co-located in a single zone core supported by two GPRS Gateway Support Node (GGSN) transport devices. Conventional HA PDGs co-located in a single zone core use two CAI Data Encryption Module (CDEM) devices.

Zone 1 Master Site location:

- HA PDG1 and HA PDG2

- HA GGSN1 and HA GGSN2
- HA CDEM1, HA CDEM2, with CDEM2 attached to the HA shadow conventional PDG

An HA PDG can be an I&VD PDG, a Conventional PDG, or a High Performance Data (HPD) PDG.

For information regarding CDEM failure and recovery, see CDEM Failure and Recovery for Conventional Data on page 50

## 2.6.2 HA Data With DSR in a Single Zone

High Availability (HA) Data in a single-zone system that implements Dynamic System Resilience (DSR) employs two (redundant) HA Packet Data Gateways (PDGs) co-located at the Primary Zone Core and Backup Zone Core. Two GPRS Gateway Support Node (GGSN) routers are (physically) established at both the primary zone core and backup zone core in a single zone core supported by two GGSN devices. Each HA PDG employs two CAI Data Encryption Modules (CDEMs).

Master Site “A” location:

- Zone 1 Primary Core – Single Zone DSR
  - HA PDG1 and HA PDG2
  - GGSN1 and GGSN2
  - CDEM1, CDEM2, CDEM3, CDEM4

Master Site “B” location:

- Zone 1 Backup Core – Single Zone DSR
  - HA PDG1 and HA PDG2
  - GGSN3 and GGSN4
  - CDEM1, CDEM2, CDEM3, CDEM4

Numbering of the PDG, GGSN, and CDEM devices identifies physical devices. The assumption is that Zone 1 Primary Core equipment is physically at a Master Site “A” location, while Zone 1 Backup Core equipment is physically at a different Master Site “B” location. The GGSN devices may be viewed logically (from an IP plan perspective) as associated with the primary core. See your IP plan for details.

## 2.6.3 HA Data With DSR Dual Zone

High Availability (HA) Data in a dual-zone system that implements Dynamic System Resilience (DSR) employs two (redundant) HA Packet Data Gateways (PDGs) for the Primary Zone Core and two HA PDGs for the Backup Zone Core at a given Master Site location. At a given Master Site location, only two (physical) Gateway GPRS Support Node (GGSN) transport devices routers are (physically) established to support the HA PDGs at a given Master Site location. Each HA PDG employs two CAI Data Encryption Modules (CDEMs). The physical devices for dual-zone system that implements HA Data with DSR are:

Master Site “A” location:

- Zone 1 Primary Core – Dual Zone DSR
  - HA PDG1 and HA PDG2
  - GGSN1 and GGSN2
  - CDEM1, CDEM2, CDEM3, CDEM4
- Zone 2 Backup Core – Dual Zone DSR
  - HA PDG3 and HA PDG4

  - CDEM1, CDEM2, CDEM3, CDEM4

Master Site “B” location:

- Zone 2 Primary Core – Dual Zone DSR
  - HA PDG1 and HA PDG2
  - GGSN3 and GGSN4
  - CDEM1, CDEM2, CDEM3, CDEM4
- Zone 1 Backup Core – Dual Zone DSR
  - HA PDG3 and HA PDG4
  - CDEM1, CDEM2, CDEM3, CDEM4

Numbering of the PDG, GGSN, and CDEM devices identifies physical devices. The assumption is that Zone 1 Primary Core equipment and Zone 2 Backup Core equipment is physically at a Master Site “A” location, while Zone 2 Primary Core and Zone 1 Backup Core equipment is physically at a different Master Site “B” location. Also, the GGSN devices may be viewed logically (from an IP plan perspective) as associated with the primary core, and only one pair of GGSN devices is required to support transport for a master site location. See your IP plan for details.

### 2.6.4 High Availability Data Services and DSR

High Availability (HA) Data switchover is implemented when a failure occurs that prevents the currently active HA element from providing packet data service for its zone. In a system with both HA Data and Dynamic System Resilience (DSR) data redundancy, a DSR switchover occurs if both HA Packet Data Gateways (PDGs) or both HA Gateway GPRS Support Nodes (GGSNs) in the primary DSR core experience a failure that prevents them from providing packet data service. Several conditions trigger a DSR switchover in an HA Data environment.

### 2.6.5 PDG to GGSN Link (GTP Interface) Failure

A Dynamic System Resilience (DSR) switchover between the primary zone core and backup zone core occurs upon a communication failure (GPRS Tunneling Protocol (GTP) interface) between the High Availability (HA) Packet Data Gateway (PDG) pair and the HA Gateway GPRS Support Node (GGSN) pair.

### 2.6.6 Gateway Router Communication Failure

The active High Availability (HA) Packet Data Gateway (PDG) communicates with both gateway routers located in its zone core. In an ASTRO® 25 system providing both HA Data and Dynamic System Resilience (DSR) packet data redundancy, the active DSR PDG in the primary core and the backup DSR PDG in the backup DSR core for a zone both send messages to each of the two gateway routers in the respective zone core.

A DSR switchover occurs if the DSR active HA PDG pair in a zone core experiences timeout of its gateway router pings.

### 2.6.7 PDR Loss of Communication with Remote DSR PDR

Each Packet Data Router (PDR) in a Dynamic System Resilience (DSR) Packet Data Gateway (PDG) group communicates "state status" messages with the other members of the DSR group. If this communication ceases from one PDG in the group, the PDG in the other zone core must become active. If the High Availability (HA) PDG pair in a primary DSR zone core stops sending the "state status" (heartbeat) messages, the HA PDG pair in the backup DSR core assumes it must become active.

Normally, the only cause of the heartbeat messaging to not be received from a PDG is when that PDG detects some failure causing it to become inoperative. However, multiple simultaneous network transport failures could also prevent the heartbeat messages from being exchanged between PDGs.

### 2.6.8 Customer Network Interface HA Data and DSR

For information about Customer Network Interface (CNI) High Availability (HA) Data and Dynamic System Resilience (DSR), see the “HA Data – Failure and Recovery” section in the *Trunked Data Services Feature Guide*.

### 2.6.9 Conventional Data Redundancy HA Data and DSR

This feature provides Dynamic System Resilience (DSR) with a Conventional Data Redundancy High Availability (HA) Data fault-tolerant conventional integrated data service, to remove all single points of failure within a single master site, including connections to and from the Customer Enterprise Network (CEN). It also provides a data service solution for the complete loss of the master site.

Because data is mission critical to operations, Conventional Data Redundancy HA Data eliminates single points of failure from system entry to the RF site by providing redundant devices. Geographically separate redundancy is provided by a redundant master site. Redundant controllers and elements within the master site provide fast recovery times within each master site. The time to switch over to redundant components within the data subsystem at a master site is less than 90 seconds, ensuring a minimum interruption of data capabilities to the conventional data system users.

An HA device has a redundant counterpart, part of an HA pair. In an HA pair, one device is active, providing data service to the master site, and one is inactive, providing redundancy. This feature provides the HA counterparts for the following devices:

- CAI Data Encryption Module (CDEM) (up to four per zone)
- Gateway GPRS Support Node (GGSN) (up to two per zone)
- Customer Network Interface (CNI) Network Transport:
  - Firewall
  - De-Militarized Zone (DMZ) Switch
  - Peripheral Network Router
  - Border Router

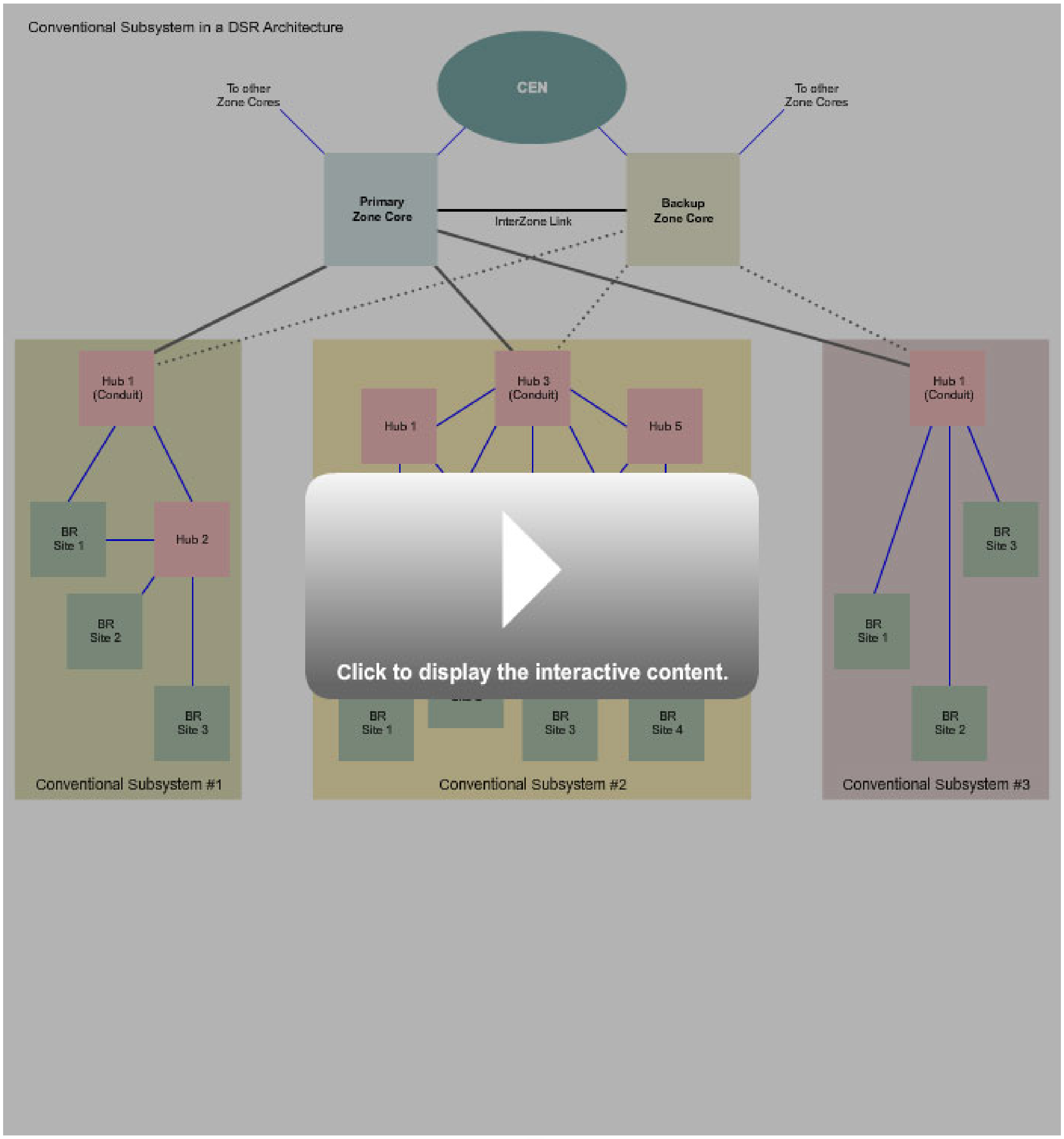
Devices currently deployed in redundant configurations, such as Gateway Routers, Zone Controller, or PDEG, are unchanged.

## 2.7 Conventional Subsystem with DSR

The distributed conventional architecture consists of conventional hub sites and conventional base radio sites in an architecture that allows the collection of consoles, comparators, and repeaters to extensively interconnect for increased availability. The architecture is designed to support conventional audio processing for a conventional subsystem if the conventional subsystem interface to the zone core and backup zone core is lost in case of Dynamic System Resilience (DSR).

Conventional subsystems are supported on DSR and non-DSR zones. The core routers see the conventional subsystem as a single site, but require additional static routes and Access Control List (ACL) modifications to reach all the devices in the subsystem.

**Figure 8: Conventional Subsystem in a DSR Architecture**



Each site within the conventional subsystem uses one (non-redundant) or two (redundant) GGM 8000 Site Gateway devices and one (non-redundant) or two (redundant) site switches. See the *GGM 8000 System Gateway Feature Guide* for details regarding implementation of Site Gateway devices, and the *System LAN Switches Feature Guide* for details regarding implementation of Site Switches.

The GGM 8000 v.24 and 4W modules in the site gateway provide, respectively, a digital or analog conventional channel interface. For the conventional IP channel interface, the Site Gateway is equipped with Ethernet ports in standard. Additional Site Gateway devices can be added as needed.

Each site can support a total of ten conventional channel interfaces (any combination of V.24, 4W, or IP).

The conventional subsystem architecture is only supported on Ethernet site links from one of the conventional hub sites (a “Conduit” Hub Site) to a zone core/master site.

For conventional channel calls in a system where DSR is implemented, if a failure occurs with the active call controller which prohibits voice call processing services at the primary zone core, the system automatically switches to activate the call controller at the backup (DSR) zone core to support voice call processing services for the conventional calls.

If the link between the primary zone core and backup zone core fails and communication paths between the primary and backup zone cores (DSR) are not available, the system continues to provide voice call services between conventional radio users and console operators connected to the same core.

When all the intermaster site links between the primary zone core and backup zone cores fail in a system with no other path, the call controllers at both the primary and backup zone cores can become active if a DSR system employs two master site locations.

In this scenario, the traffic normally routed directly between the primary zone core and backup zone cores should not be rerouted via a remote site.

If the site link between a remote site and primary zone core goes down and the remote site connects to the backup zone core (DSR), even if the site link between the primary zone core and remote site is restored, the remote site remains connected to the backup DSR core. Whenever a site loses all logical connections with an active call controller, it undergoes site mode.

The system provides the capability for the RF sites, console sites (MCC 7500 VPM), and conventional sites to connect to a preferred zone core (DSR) for voice call processing. The preferred zone core concept is used where a call controller is active at both the primary zone core and backup zone core, and when it is desirable for all the remote sites to connect to the same zone core so the radio users and dispatchers can communicate.

The primary zone core is the preferred zone core. When the RF sites and conventional sites do not have a connection with a zone core, they attempt to connect to the preferred DSR core first.

However, if console sites (MCC 7500 VPM) do not have a connection to a zone core, they attempt to connect to both zone cores (instead of the preferred zone core first). However, the sites may not connect to the preferred zone core.

For remote sites that have a physical path to the primary zone core and backup zone core, the preferred zone core is tried first, if possible, but the site may land and stay on the backup zone core. The sites include ASTRO® 25 Repeater Sites, IP simulcast subsystem sites, and conventional only sites, console sites, conventional subsystems.

## 2.8 Network Management Services

An ASTRO® 25 system with Dynamic System Resilience (DSR) includes the following redundant network management services:

- Fault management: Unified Event manager (UEM)
- Configuration management:
  - Provisioning Manager (PM) (running on the User Configuration Server (UCS))
  - Unified Network Configurator (UNC) (running on the UNC server)
  - Zone Database Server (ZDS)
- Performance management:
  - System Statistics Server (SSS)

  - Zone Statistics Server (ZSS)
  - Air Traffic Router (ATR)
- InfoVista (optional feature on a standalone server; redundancy is optional)

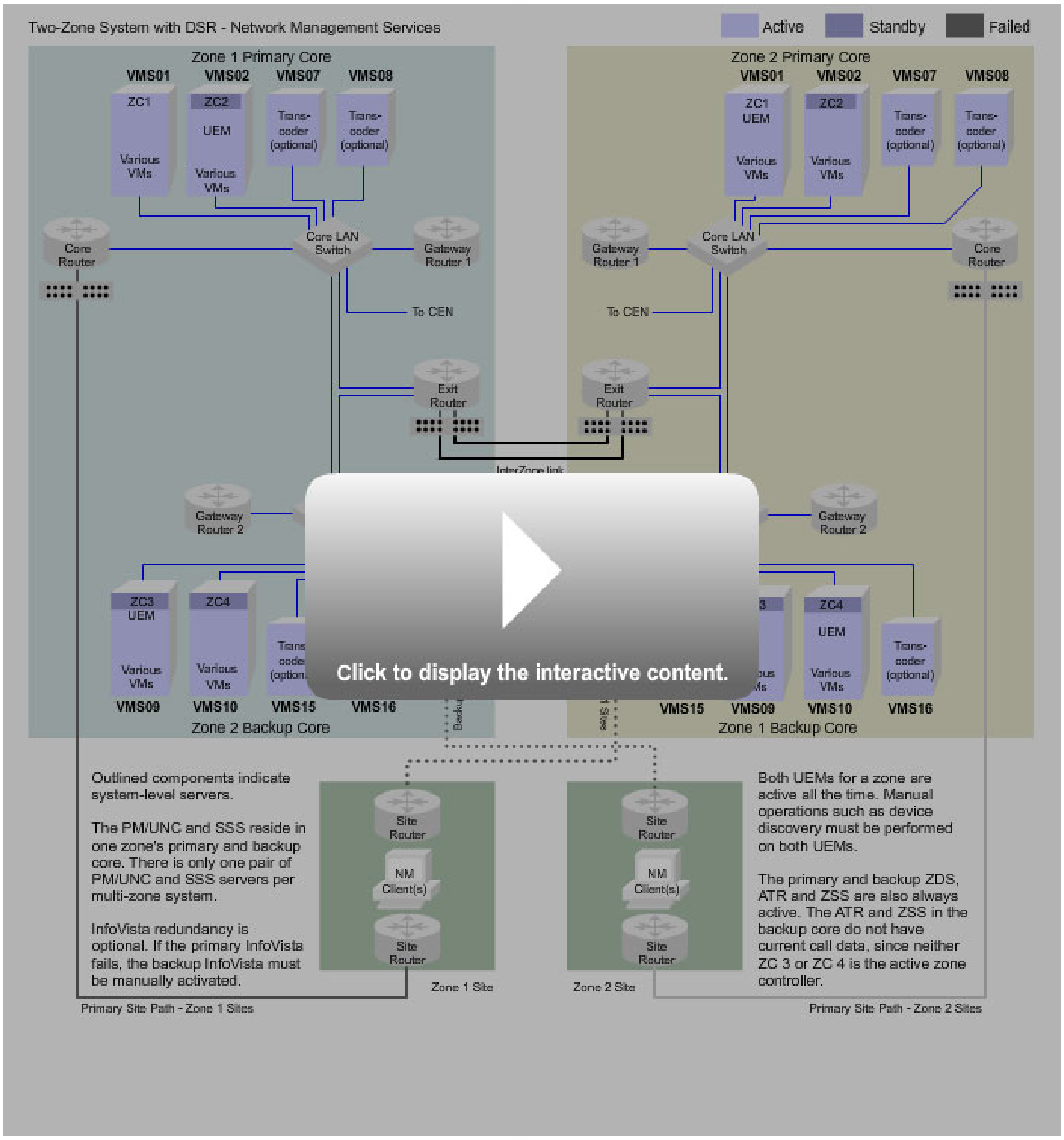
Regardless of the type of remote site, the equipment is managed by the active UNC in the system and visible to the UEM and UNC in both the primary core and the backup core.

Geographic redundancy for the system network management servers (UCS, UNC, SSS) is supported across a non-DSR zone and a DSR zone. In this case, the primary servers may be present in the non-DSR zone and the backup servers may be present in the backup core of a DSR zone. This configuration is useful to address network management service concerns when a deployed system with non-DSR zones expands some zones to DSR or adds a DSR zone because it allows system servers to remain in the currently deployed location. If a system is being modified to add non-DSR zones to a system with DSR zones, or if a system is being initially deployed, this configuration is not needed as the system Network Management (NM) servers can be deployed in DSR zones.

From the transport design, the system NM servers are on the system subnet. This subnet is an address space outside of the zone core that enables elements on the subnet to be physically deployed at any master site in the system. Primary and backup system NM servers may be deployed in different DSR zones. Non-DSR master sites are configured for access to both the system subnet and the DSR system subnet. The system NM servers in the non-DSR zone are configured for DSR.

This figure shows the servers and components related to network management services. Due to space constraints, other core equipment and redundancy have been left out of the drawings.

**Figure 9: Network Management Services Components**


Two-Zone System with DSR - Network Management Services
Active
Standby
Failed
Zone 1 Primary Core
VMS01
VMS02
VMS07
VMS08
ZC1
ZC2
UEM
Trans-coder (optional)
Trans-coder (optional)
Various VMs
Various VMs
Core Router
Core LAN Switch
Gateway Router 1
To CEN
Exit Router
InterZone link
Zone 2 Primary Core
VMS01
VMS02
VMS07
VMS08
ZC1 UEM
ZC2
Trans-coder (optional)
Trans-coder (optional)
Various VMs
Various VMs
Gateway Router 1
Core LAN Switch
Core Router
To CEN
Exit Router
Gateway Router 2
Gateway Router 2
ZC3 UEM
ZC4
Trans-coder (optional)
Various VMs
Various VMs
VMS09
VMS10
VMS15
VMS16
Zone 2 Backup Core
Backup
ZC4
UEM
Trans-coder (optional)
Various VMs
VMS15
VMS09
VMS10
VMS16
Zone 1 Backup Core
Click to display the interactive content.
Outlined components indicate system-level servers.
The PM/UNC and SSS reside in one zone's primary and backup core. There is only one pair of PM/UNC and SSS servers per multi-zone system.
InfoVista redundancy is optional. If the primary InfoVista fails, the backup InfoVista must be manually activated.
Site Router
NM Client(s)
Site Router
Zone 1 Site
Site Router
NM Client(s)
Site Router
Zone 2 Site
Both UEMs for a zone are active all the time. Manual operations such as device discovery must be performed on both UEMs.
The primary and backup ZDS, ATR and ZSS are also always active. The ATR and ZSS in the backup core do not have current call data, since neither ZC 3 or ZC 4 is the active zone controller.
Primary Site Path - Zone 1 Sites
Primary Site Path - Zone 2 Sites

### 2.8.1 Fault Management

To achieve redundancy for fault management information, an additional Unified Event Manager (UEM) is provided in the backup core for each zone. Both UEMs for a zone are active all the time. The manager/user configures each UEM to enable collection of statistics. System managers can then choose to which UEM in a zone they wish to connect for monitoring.

Each manual operation, such as discovery or synchronization, must be performed on both UEMs for a zone. Any manual customizing of views on the user interface must be applied to both UEMs.

Network elements managed by the UEM are in the primary core, backup core, and remote sites. Additional backup core equipment for network management, voice, transport, IP services, and data are fault managed. The UEM in the backup core can fault manage the non-DSR sites through the InterZone links.

If the primary UEM fails, the backup is already active; no switchover is required. If a primary core failure occurs, an operator can monitor recovery (for example, Ethernet site link statistics) from the backup core UEM for the zone.

See the *Fault Management Reference Guide* for information on fault management of Point-To-Point (PTP) Wireless Ethernet Bridge devices and microwave equipment in an ASTRO® 25 system.

**NOTICE:** DSR expansion requires discovery of new devices in the DSR core. UEM users need to be aware that discovery of redundant devices such as Zone Controller or Packet Data Gateway requires the **Network Element View** window to be refreshed. This type of window does not automatically update to reflect the current redundant group device list status.

### 2.8.2 Configuration Management

Configuration management is performed through Provisioning Manager (PM) and Unified Network Configurator (UNC) applications. The conventional and console configuration is performed on the PM and is distributed to agents using the Zone Database Server (ZDS). The Advanced Distribution Service (ADS) server is a part of the ZDS that provides the connection between the PM and several network elements, and is used for radio alias distribution. In a system with Dynamic System Resilience (DSR), a redundant User Configuration Server (UCS) is added to the backup core of the master site that contains the primary UCS. If the system contains more than two master site pairs, the UCS may be at any one zone's primary/backup master sites.

The UCS hosts the PM application and database for subscriber access control records, console profiles, and site gateway (conventional channel interface) conventional channel data, whereas the UNC contains system infrastructure data. The ZDS is a Lightweight Directory Access Protocol (LDAP) server that contains data from the UCS, obtained through database synchronization between the UCS and the ZDS. The distribution of data from the UCS to the ZDS occurs when the PM user executes a Distribute Changes or Force Initialization operation.

Only one PM/UNC can be active at a time, determined by the network manager or operator. Therefore, one PM/UNC is configured to be in the active state and the other in warm standby state. The active PM must be in the same master site core (either primary or backup) as the active UNC. If failure of either one occurs, both applications must switchover to the backup core. Switchover is manual. It requires the PM and the UNC on the backup core to be switched from the warm standby state to active. After a switchover, network management client computers must launch the UCS for the newly active PM and the UNC client for the newly active UNC. See Dynamic System Resilience Operation on page 89 for more information on manual switchover procedures for the PM and UNC. If a switchover is known to be a short-duration event, a user may choose not to bring the backup configuration subsystem on line.

Periodic secure synchronization over the InterZone link from the primary PM and UNC to its corresponding backup ensures that up-to-date configuration data is available in the backup core. Configuration databases are synchronized at configurable intervals, between 30 minutes and 24 hours (the default), in one direction, from active to the standby. Typically, a full configuration baseline is transferred the first time and subsequent transfers include only changed data from the previous transfers. A system operator can perform manual synchronization as well.

A redundant ZDS is installed in the backup core for a zone. Both the primary core ZDS and the backup core ZDS pull data from the active PM database (UCS), so no synchronization between the two ZDS LDAP services is needed. The PM database relies on the ZDS LDAP service in each zone for distributing some configuration data. The ZDS is the low-level LDAP server for the LDAP clients in MCC 7500 VPM/7500E/7100 Dispatch Console sites and site gateway (conventional channel interface). The LDAP server on each ZDS is active at all times, so ZDS LDAP clients can pull configuration data from either ZDS and their affiliated ADS.

The UCS/PM switchover from the primary zone core to the backup zone core causes an automatic LDAP database rebuild and a download of data to all the consoles in the system; the clients are responsible for downloading the data. The time taken for this download depends on the number of records and the number of consoles. MCC 7500 VPM/MCC 7500E/7100 Dispatch Consoles must be restarted for the new database to take effect. The MCC 7100/MCC 7500E Dispatch Consoles may have ZDS download turned off to save bandwidth during a switch-over and in this case they continue to use their existing LDAP until updated. The Site Gateway (CCI) LDAP server IP address must be modified to the backup core ZDS, and then must be reset to complete the switchover. Because the configuration data is unlikely to change, this manual switchover is usually not required.

### 2.8.2.1 Domain Controllers

Any system with the Dynamic System Resilience (DSR) has a virtual server in each backup zone. There, the virtual server hosts a single Domain Controller (DC) along with other services like Baseline Backup and Recovery Server.

In a single zone or multi-zone system, additional DCs are optional for any zone where high availability and performance is desired. If the system is non-redundant (colocated zone), the secondary DC within the zone (or User Configuration Server (UCS) subnet) is deployed on the same virtual server as the primary DC. For a redundant configuration, the two DCs in the subnet are on two separate physical servers in virtual environments. For more information, see the *Authentication Services Feature Guide*.

## 2.8.3 Performance Management

Performance management addresses the collection of features and applications that provides operators with information about radio system use. Performance management data includes real-time information and historical statistics regarding radio call activity and affiliations. Performance management uses both system-level and zone-level servers: the System Statistics Server (SSS), Zone Statistics Server (ZSS), and Air Traffic Router (ATR). Applications include:

- Affiliation Display
- Air Time Information Access (ATIA)
- Computer Aided Dispatch Interface (CADI)
- ZoneWatch
- Radio Control Management (RCM)

The Unified Event Manager (UEM) gathers some performance management statistics (like Ethernet site link statistics). Both UEMs in a zone are continuously active.

In a system with Dynamic System Resilience (DSR), an additional ATR, and ZSS are installed on a zone-level server in the backup core to provide zone-level performance management services while a zone controller in the backup core is active. The additional ZSS pulls data from its colocated ATR. For multi-zone systems, an additional SSS is installed on a system-level server at the same backup core master site as the redundant Unified Network Configurator (UNC) server. Both the primary and backup SSSs pull data from all active ATRs in the system, regardless of location in either a primary or backup core. Only the ATR in the same core as the active zone controller sources information to the SSS.

ATRs in a primary core do not share information with ATRs in the backup core. An ATR in a backup core cannot assume services of an ATR in the primary core. For example, the backup core ATR has no knowledge of RCM commands executed or emergency alarms received at the primary ATR, thus, any pending commands in RCM are lost on switchover if a failure occurs. Performance management services that rely on the primary core ATR are unavailable until that ATR is repaired/replaced or until there is a zone controller switchover to the backup core with a functional ATR. If an ATR application (like CADI, ATIA, or RCM) is critical, the ATR would need immediate repair, or the system should be switched to the backup core with a functional ATR.

Performance management services are available in the event of a total primary core failure. However, not all of them are available when certain individual server failures take place in the primary core. In addition, the redundant servers installed in the backup core do not share any call activity data, statistics, or RCM data with their primary core counterparts. Redundant ZSSs and SSSs do not share or synchronize historical data. When a switchover to a backup core zone controller occurs, performance management is available but requires manual intervention by an operator to retrieve historical statistics and previously issued RCM commands.

## 2.8.3.1 High Availability Performance Management and Radio Control Services

High Availability (HA) Performance Management and Radio Control Services is an optional feature which provides redundant Air Traffic Routers (ATRs). While HA Performance Management and Radio Control Services can be implemented in systems that do not employ Dynamic System Resilience (DSR), the redundancy can also be implemented in systems employing DSR. HA Performance Management and Radio Control Services is available to L2, M2, and M3 zone core systems employing Common Server Architecture (Virtual Management Server host platforms). The following sections summarize the configurations.

### HA Performance Management and Radio Control Services Without DSR Redundancy at a Single Zone Core

HA Performance Management and Radio Control Services in a single-zone system that does not implement DSR employs two (redundant) HA ATRs co-located in a single zone core. Zone 1 Master Site location includes HA ATR1 and HA ATR2 (shadow).

### HA Performance Management and Radio Control Services With DSR at a Single Zone

HA Performance Management and Radio Control Services in a single-zone system that implements DSR employs two (redundant) HA ATRs co-located at the Primary Zone Core and Backup Zone Core.

Master Site “A” location:

- Zone 1 Primary Core – Single Zone DSR
  - HA ATR1 and HA ATR2 (shadow)

  Master Site “B” location:

- Zone 1 Backup Core – Single Zone DSR
  - HA ATR1 and HA ATR2 (shadow)

The numbering of these ATR devices identifies physical devices. The assumption is that Zone 1 Primary Core equipment is physically at a Master Site “A” location, while Zone 1 Backup Core equipment is physically at a different Master Site “B” location.

### HA Performance Management and Radio Control Services With DSR at a Dual Zone

HA Performance Management and Radio Control Services in a dual-zone system that implements DSR employs two (redundant) HA ATRs for the Primary Zone Core and two HA ATRs for the Backup Zone Core at a given Master Site location.

Master Site “A” location:

- Zone 1 Primary Core – Dual Zone DSR

  - HA ATR1 and HA ATR2 (shadow)
- Zone 2 Backup Core – Dual Zone DSR
  - HA ATR3 and HA ATR4 (shadow)

Master Site “B” location:

- Zone 2 Primary Core – Dual Zone DSR
  - HA ATR1 and HA ATR2 (shadow)
- Zone 1 Backup Core – Dual Zone DSR
  - HA ATR3 and HA ATR4

The numbering of these ATR devices identifies physical devices. The assumption is that Zone 1 Primary Core equipment and Zone 2 Backup Core equipment is physically at a Master Site “A” location, while Zone 2 Primary Core and Zone 1 Backup Core equipment is physically at a different Master Site “B” location.

### High Availability Performance Management and Radio Control Services and DSR

An HA pair of ATRs in a primary core does not share information with HA pair of ATRs in the backup core. An ATR in a backup core cannot assume services of an ATR in the primary core. For example, the backup core ATR has no knowledge of Radio Control Manager (RCM) commands executed or emergency alarms received at the primary ATRs. Thus, any pending commands in RCM are lost on zone controller switchover in the event of failure. If a physical ATR fails, HA Performance Management and Radio Control Services prevents loss of data. If the physical ATR fails, the ATR on another Virtual Management Server (VMS) (shadow) becomes active and resumes providing the service within 90 seconds.

When both HA ATRs from the primary core fail, performance management services that rely on the primary core ATR are unavailable until that ATR is repaired/replaced, or until there is a zone controller switchover to the backup core with a functional HA ATR. If an ATR application (like Computer Aided Dispatch Interface (CADI), Air Time Information Access (ATIA), or RCM) is critical, immediately repair the ATR, or switch the system to the backup core with a functional ATR.

### CNI HA Performance Management and Radio Control Services and DSR

For information about Customer Network Interface (CNI), see the “HA Performance Management and Radio Control Services Failure and Recovery” section in the *Private Network Management Servers Feature Guide*.

## 2.8.4 InfoVista (Optional)

InfoVista is a tool used to retrieve statistical information from devices such as network products, site devices, and the data subsystem equipment. A redundant InfoVista application is optional in an M3 system with DSR. InfoVista is not available on M1 systems with Dynamic System Resilience (DSR).

On an M3 system, only one InfoVista application can be active at a time and statistics are not shared between the active and inactive InfoVista applications. A system manager or technician must manually switch InfoVista applications by disabling one and enabling the other. If an interzone link failure occurs, InfoVista might not have statistical data from during the time of the failure.

## 2.9 Network Transport Services

In a system with Dynamic System Resilience (DSR), the transport subsystem uses redundant equipment and reroutes to maintain service automatically during failures. If a site link to the primary master site fails, traffic may be rerouted to the backup master site and then across the InterZone link to the active zone controller.

When two cores are supported at a single master site, the following transport equipment is shared:

- Core LAN switches
- Exit routers
- Core backhaul switches
- Gateway routers
- Core terminal server
- Gateway GPRS Support Node (GGSN)
- Customer Network Interface (CNI) equipment
- Solution Support Center (SSC) access
- Data Collection Device (DCD)

**NOTICE:** See the *System LAN Switches Feature Guide* for details regarding implementation of Site Switches in the system.

Transport supports separate site links between remote sites (RF, network manager, and Dispatch) and the cores in the two master sites.

This figure shows transport subsystem components in a two-zone M3 system with DSR, along with possible failure scenarios. Due to space constraints, other core equipment, and redundancy has been left out of the drawings.

**Figure 10: Network Transport Services Components**

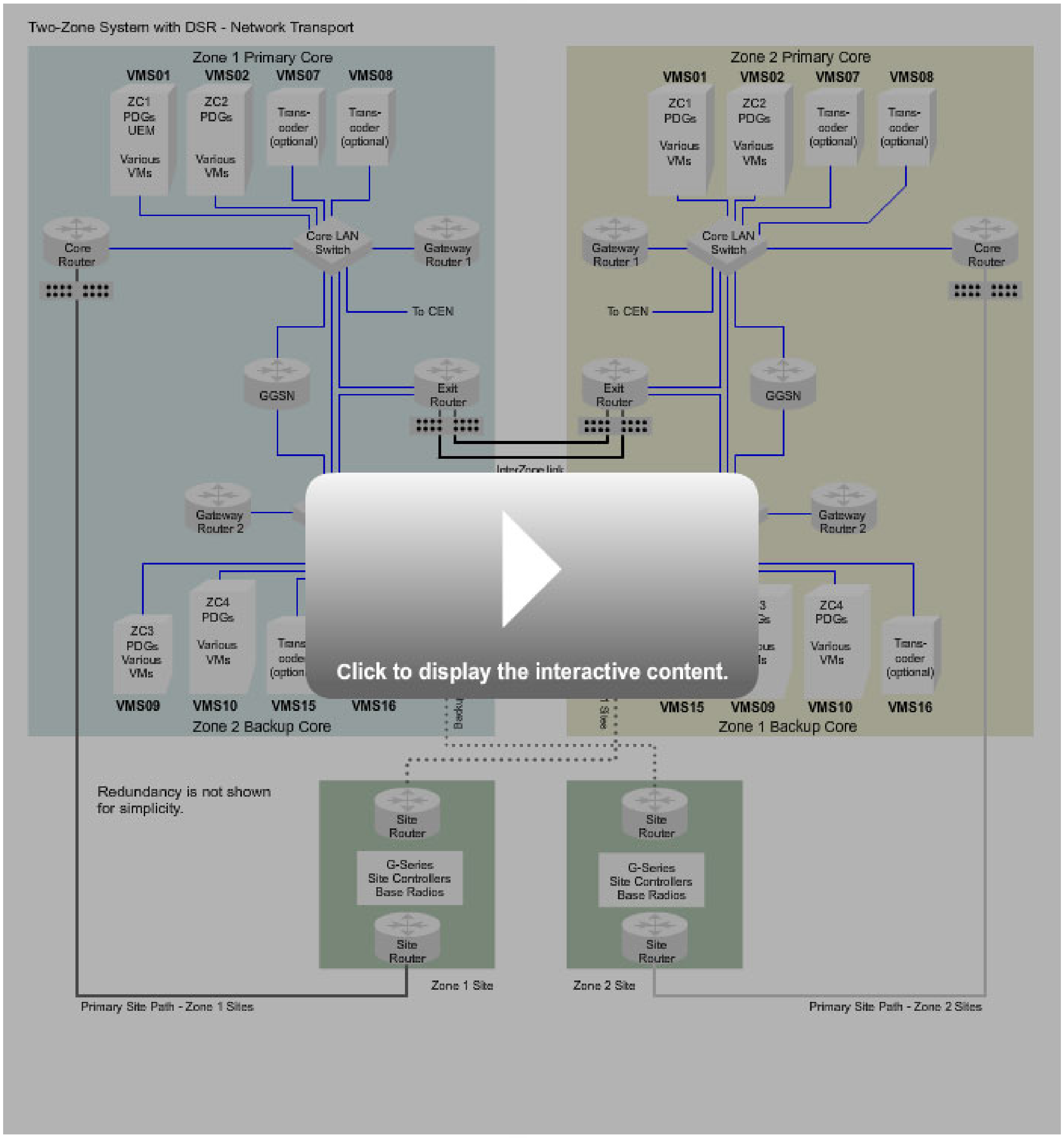
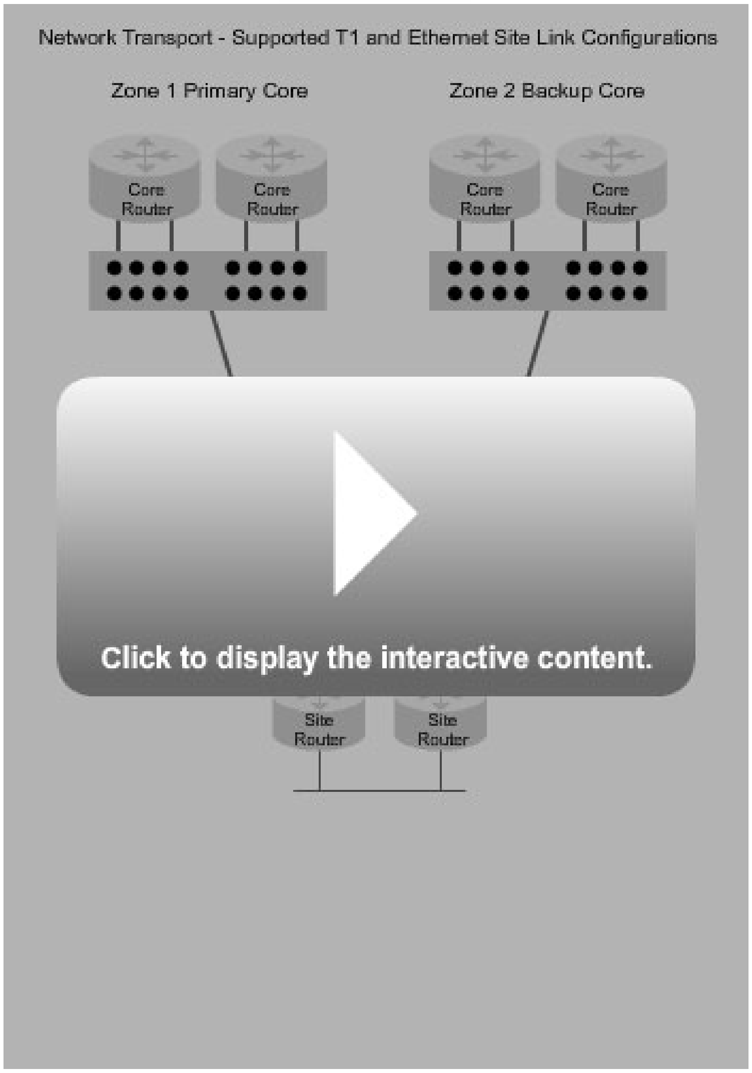


Figure 11: Network Transport Links Configurations on page 65 shows the supported configurations for the physical T1 and Ethernet links between a remote site and the primary and backup cores.

**Figure 11: Network Transport Links Configurations**


Network Transport - Supported T1 and Ethernet Site Link Configurations
Zone 1 Primary Core
Zone 2 Backup Core
Core Router
Core Router
Core Router
Core Router
Click to display the interactive content.
Site Router
Site Router

## 2.9.1 Wide Area Trunking for DSR Voice

If a Dynamic System Resilience (DSR) InterZone link fails and an alternate path through other master sites exists, and no other failures occur, only InterZone calls on the failed link are affected temporarily.

Upon restoration of the failed primary site link, site link packets are rerouted to the primary site link without dropping more than three IP packets.

## 2.9.2 Redundant CEN Interfaces for DSR Data

With a redundant Customer Enterprise Network (CEN) interfaced for Dynamic System Resilience (DSR) data, upon loss of the primary CEN interface between a zone primary core and the CEN, the traffic is rerouted to the backup CEN interface. This loss of primary interface may be caused by any of the components in the Customer Network Interface (CNI), for example, the firewall, peripheral network router, De-militarized Zone (DMZ) switch, and so on.

Upon restoration of the failed primary CEN interface, the traffic is rerouted to the primary CEN interface.

## 2.10 IP Services

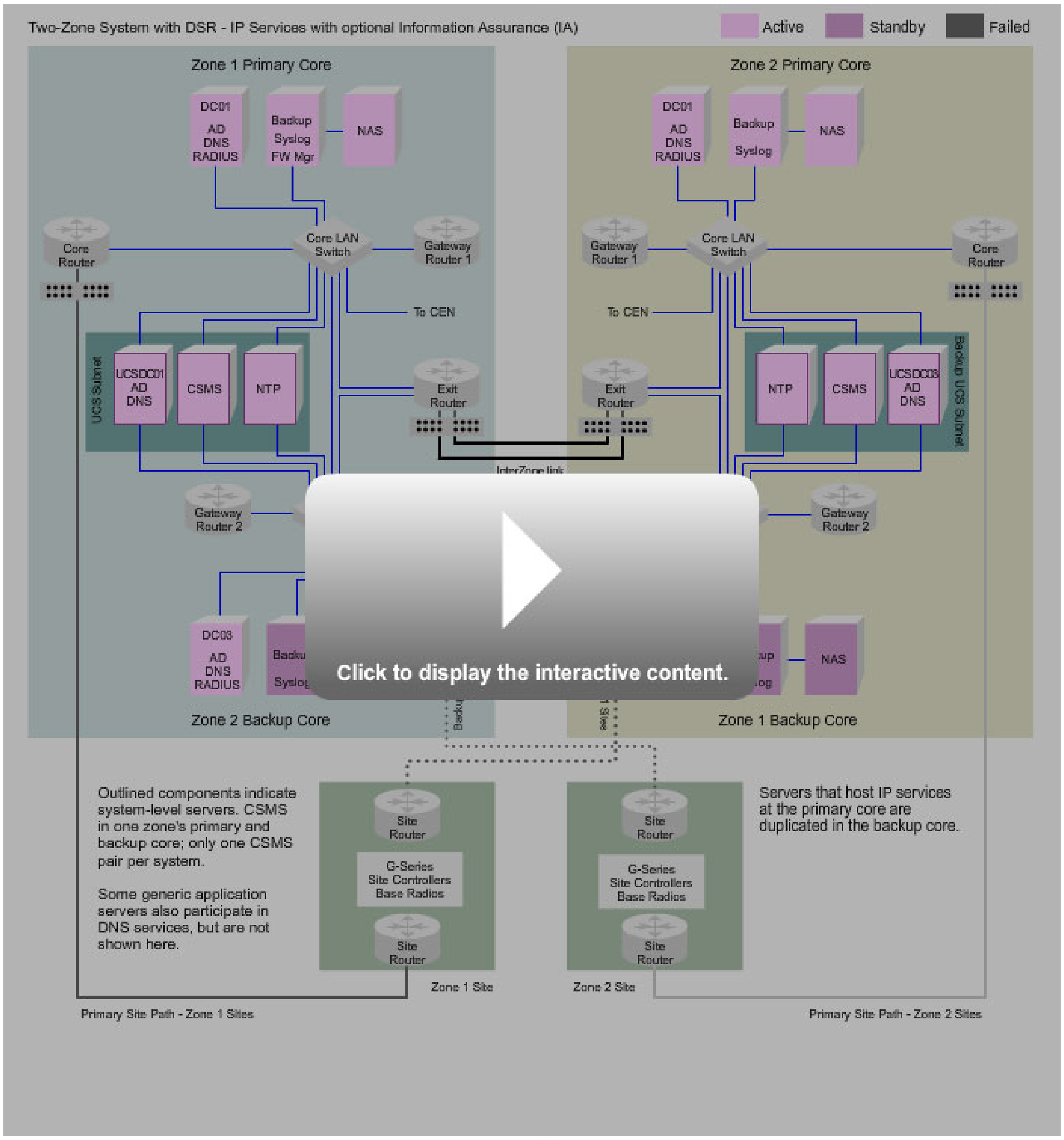
In an ASTRO® 25 system, IP services provide a number of support functions on the network. The following IP services in a system with Dynamic System Resilience (DSR) are:

- Antivirus
- Backup and Restore (BAR)
- Centralized Authentication
- Domain Name Service (DNS)
- Network Time Protocol (NTP)
- Firewall Management
- Centralized Event Logging (optional)

IP services applications are redundant; IP servers at the primary core are duplicated in the backup core, except for the Firewall Management application.

This figure shows the IP services components in a system with DSR. Due to space constraints, other radio network infrastructure components are not shown here. Information Assurance (IA) is an optional feature. As with all other DSR system components, IA servers in the primary core are duplicated in the backup core.

**Figure 12: IP Services Components**


Two-Zone System with DSR - IP Services with optional Information Assurance (IA)
Active
Standby
Failed
Zone 1 Primary Core
DC01
AD
DNS
RADIUS
Backup
Syslog
FW Mgr
NAS
Core Router
Core LAN Switch
Gateway Router 1
To CEN
UCS Subnet
UCSDC01
AD
DNS
CSMS
NTP
Exit Router
InterZone link
Gateway Router 2
DC03
AD
DNS
RADIUS
Backu
Syslog
Zone 2 Backup Core
Zone 2 Primary Core
DC01
AD
DNS
RADIUS
Backup
Syslog
NAS
Gateway Router 1
Core LAN Switch
Core Router
To CEN
Exit Router
NTP
CSMS
UCSDC03
AD
DNS
Backup UCS Subnet
Gateway Router 2
up
og
NAS
Zone 1 Backup Core
Click to display the interactive content.
Outlined components indicate system-level servers. CSMS in one zone's primary and backup core; only one CSMS pair per system.
Some generic application servers also participate in DNS services, but are not shown here.
Site Router
G-Series Site Controllers Base Radios
Site Router
Zone 1 Site
Site Router
G-Series Site Controllers Base Radios
Site Router
Zone 2 Site
Servers that host IP services at the primary core are duplicated in the backup core.
Primary Site Path - Zone 1 Sites
Primary Site Path - Zone 2 Sites

## 2.10.1 Antivirus Service

A system with Dynamic System Resilience (DSR) includes two Core Security Management Server (CSMS) servers that host and manage McAfee ePolicy Orchestrator (ePO) for clients. Each CSMS server is located in one zone in the system. One server is in the primary core and one in the backup core. Only two CSMS servers are in a system, regardless of the number of zones.

If the primary core CSMS fails, new agents must be pushed out manually from the McAfee ePO server on the backup CSMS to the anti-malware clients at the remote sites so that they may be managed. No automatic switchover is available. If the primary CSMS becomes available, the McAfee agents must be pushed from the primary McAfee ePO server to the remote clients.

## 2.10.2 Backup and Restore Service

Backup and Restore (BAR) services in a system with Dynamic System Resilience (DSR) are the same as those in an ASTRO® 25 system without DSR. Each core (primary and backup) has independent backup and restore services for the colocated backup and restore clients.

## 2.10.3 Centralized Authentication

Centralized authentication services are hosted on the Domain Controllers (DCs) and on the Core Security Management Server (CSMS) to protect against any single point of failure.

DCs host Active Directory (AD) and RADIUS services through Microsoft Network Policy Server® (NPS). Two DCs are required for each primary and backup core. DCs are configured to replicate AD information between themselves, regardless of location in the network. This configuration enables transparent switchover of authentication services for clients in the system.

Each DC provides RADIUS service. The RADIUS servers are provisioned individually with the same set of shared secrets. In a system with Dynamic System Resilience (DSR), the additional RADIUS servers in the backup core are provisioned automatically. RADIUS clients, for example network equipment or site equipment like comparators, base radios, or site controllers, are configured with the RADIUS server IP addresses in the primary core and the backup core. Loss of communication with the RADIUS server in the primary core causes transparent automatic switchover to the RADIUS server in the backup core.

## 2.10.4 Domain Name Service

Domain Name Service (DNS) provides name-to-IP address and IP address-to-name resolution. In a system with Dynamic System Resilience (DSR), system-level DNS services are hosted on the system-level Domain Controllers (DCs). At the zone level, DNS services are hosted on the zone level DCs.

In a system with the DSR, clients must be configured with a minimum of two DNS nameservers, and potentially up to four DNS nameservers, depending on the client location.

**NOTICE:** See your System IP Plan for the correct IP addresses of DNS source devices.

Table 2: Recommended DNS Nameserver Configuration Order

This table provides the recommended nameserver order depending on the DNS client location.

| DNS client location | First DNS source | Second DNS source | Third DNS source | Fourth DNS source |
|---|---|---|---|---|
| Primary system level client | Primary system level DC | Primary zone level DC (colocated zone) | N/A | N/A |
| Backup system level client | Backup system level DC | Backup zone level DC (colocated zone) | N/A | N/A |

*Table continued…*

| DNS client location | First DNS source | Second DNS source | Third DNS source | Fourth DNS source |
|---|---|---|---|---|
| Primary zone level client | Primary zone level DC | Primary system level DC | N/A | N/A |
| Backup zone level client | Backup zone level DC | Backup system level DC | N/A | N/A |
| Site level client | Primary zone level DC | Backup zone level DC | Primary system level DC | Backup system level DC |

## 2.10.5 Network Time Protocol

Network Time Protocol (NTP) provides a clock synchronization mechanism for various network devices and computers. NTP is provided through a hierarchical set of time servers, with the most accurate time sources at the top of the hierarchy.

In an M3 system with Dynamic System Resilience (DSR), a TRAK 9100 server in both the primary core and backup core for a zone provides accurate clock and time of day service by using satellite synchronization to a Global Navigation Satellite System (GNSS) receiver. The Virtual Management Servers (VMSs) host servers in both cores receive their NTP times from the colocated TRAK 9100. Domain Controllers and other elements in the zone cores receive their time from the ESXi servers, except for the Windows-based machines joined to Active Directory. Windows-based machines joined to Active Directory receive time using Simple Network Time Protocol (SNTP) from the Domain Controllers.

In an M1 system with DSR, the TRAK 8835 is the default model, but the TRAK 9100 can be used.

With DSR, if a connection to the principal NTP source fails, network devices are configured to automatically switchover to the backup NTP time source. See the *Network Time Protocol Server Feature Guide* for details.

## 2.10.6 Firewall Management

Fortinet FortiManager is a web-based firewall management application hosted as a virtual machine on an ESXi-based virtual server. It is mandatory only in an M3 ASTRO® 25 system configuration with ZCP, otherwise optional in L and M cores and not supported in a K core configuration.

If an FMS fails, firewalls may be individually managed using a Web browser with HTTPS secure protocol. The standard firewall settings allow a Web browser on the Core Security Management Server (CSMS) or Network Management (NM) Client to use the HTTPS management session. Other protocols from other servers must be configured.

For more information about firewall management, see the *Fortinet Firewall Manager User Guide*.

## 2.10.7 Centralized Event Logging (optional)

The optional Centralized Event Logging feature provides a centralized mechanism for collecting audit messages from all devices in the system. It requires the following additional components in both the primary core and the backup core of each zone in a system with Dynamic System Resilience (DSR): parent Centralized Event Logging server, child Centralized Event Logging servers, and Centralized Event Logging clients.

With Centralized Event Logging, both the primary core and backup core for a zone contains a Centralized Event Logging server. In addition, if the optional Zone Core Protection (ZCP) feature is present, an additional Centralized Event Logging server is in the Mediation LAN of the primary and backup cores.

DSR has two parent Centralized Event Logging servers in the system. The zone that hosts the connection to the Motorola Solutions Support Center (SSC) hosts the parent Centralized Event Logging servers, one in the primary core, one in the backup core. Parent Centralized Event Logging servers collect all audit messages for their respective zones as well as audit messages collected by their child Centralized Event Logging servers. In a system without Zone Core Protection (ZCP), one parent Centralized Event Logging server is in a core. With ZCP, the zone core hosts an additional child Centralized Event Logging server in the Mediation LAN.

If child Centralized Event Logging servers exist in a core, messages are not forwarded to other child servers or to the alternate parent Centralized Event Logging server. Child Centralized Event Logging servers associated with a primary core forward messages to the primary parent Centralized Event Logging server. Child Centralized Event Logging servers associated with the backup core forward messages to the backup parent Centralized Event Logging server.

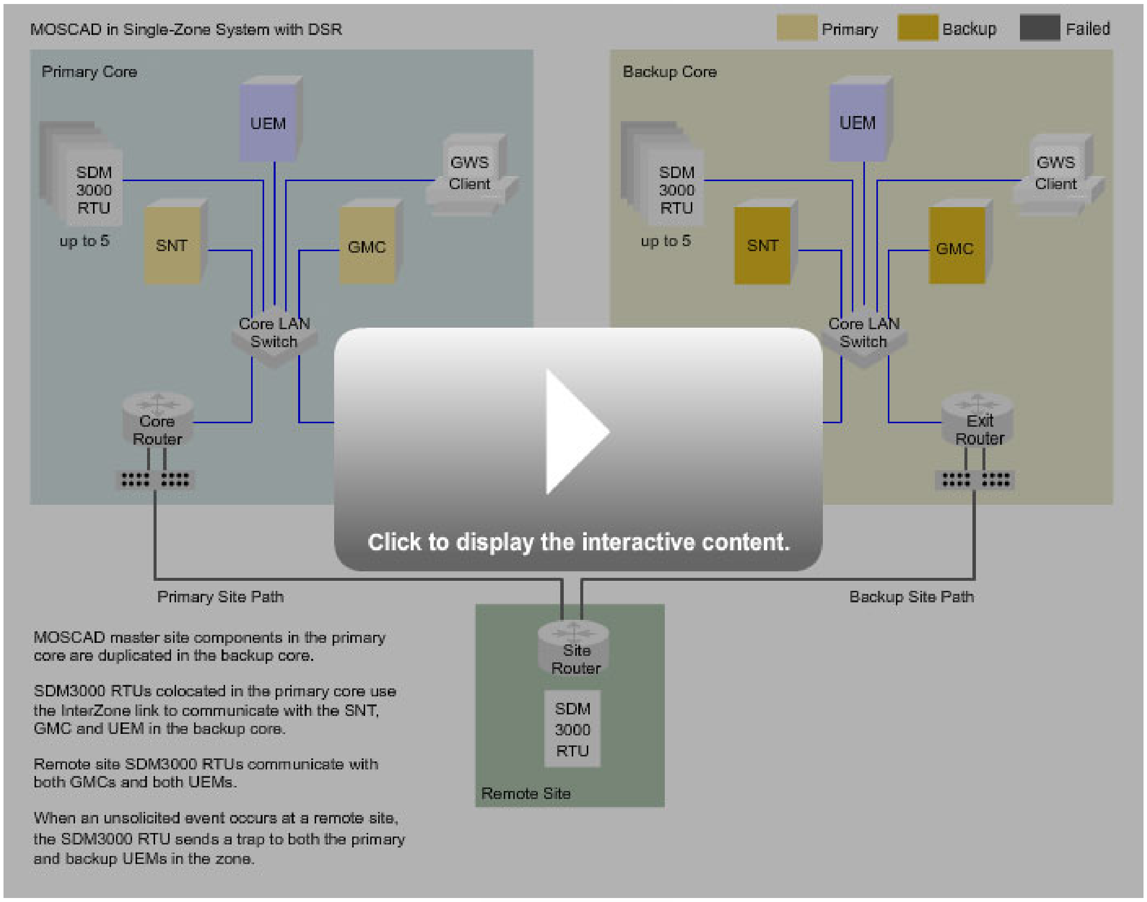
## 2.11 MOSCAD NFM Service (If Required)

In a system with Dynamic System Resilience (DSR), MOSCAD Network Fault Management (NFM) components in a master site primary core are duplicated in the backup core. This duplication includes the SDM3000 Network Translator (SNT) server and the Graphical Master Computer (GMC) server. MOSCAD NFM clients (Graphical Workstations (GWSs) can be in either core. A core can have up to five colocated SDM3000 Remote Terminal Units (RTUs).

**NOTICE:** The MOSCAD IP Gateway is not supported in a system with DSR.

This figure shows the MOSCAD NFM components in a DSR zone. Due to space constraints, other radio network infrastructure components are not shown.

**Figure 13: MOSCAD NFM in Master Sites with DSR**



MOSCAD master site components in the primary core are duplicated in the backup core.

SDM3000 RTUs colocated in the primary core use the InterZone link to communicate with the SNT, GMC and UEM in the backup core.

Remote site SDM3000 RTUs communicate with both GMCs and both UEMs.

When an unsolicited event occurs at a remote site, the SDM3000 RTU sends a trap to both the primary and backup UEMs in the zone.

The SNT and GMC in both the primary core and the backup core are active at all times. A Unified Event Manager (UEM) for network management is in the primary and backup core of each zone. Like SNTs and GMCs, both UEMs are active at all times.

Up to five SDM3000 RTUs can be colocated at each core. SDM3000 RTUs may be used to manage equipment and monitor environmental conditions at a master site location. Colocated SDM3000 RTUs communicate with the SNT and GMC within their zone core and the SNT and GMC in the backup core through the InterZone link. Every SDM3000 RTU in the zone, whether colocated or at a remote site, communicates with primary and backup managers (GMCs and UEMs).

GWS clients and the GMC server interact only with the SNT in the same core to provide management information to operators.

If a master site is shared by two cores (primary core for one zone and backup core for another zone), the SDM3000 RTUs from one zone can be used to manage all the master site equipment. You do not need to add SDM3000 RTUs from both zones.

No synchronization exists between MOSCAD NFM elements (collectively, this refers to all MOSCAD-related equipment) in both DSR cores. For example, an operator performs manual operations, like alarm acknowledgment, separately on the primary core GMC and the backup core GMC. When an unsolicited event occurs in a site, the SDM3000 RTU sends a trap to both primary and backup UEMs and updates both the primary and backup GMCs in the zone.

In a zone with DSR, the MOSCAD NFM components can support up to 100 radio sites, 60 dispatch sites, and two master sites (total of 162). For simulcast prime sites, the maximum number is 64 and for simulcast subsites, the maximum is 15.

## 2.12 ISSI 8000/CSSI 8000 Feature

The Inter-RF Subsystem Interface 8000 (ISSI 8000)/Console Subsystem Interface 8000 (CSSI 8000) feature provides an interconnectivity solution for P25 compatible systems and consoles to interface with an ASTRO® 25 system. The ISSI 8000/CSSI 8000 functionality allows an ASTRO® 25 system to connect up to 24 foreign P25 systems based on the P25 ISSI standard. The other P25 systems are allowed to be ASTRO® 25 systems or third-party systems. The other P25 systems can be trunked radio systems or third-party console subsystems. If the P25 system is a trunked radio system with RF sites, the interface is the ISSI 8000. If the P25 system is a third-party console subsystem, the interface is the CSSI 8000.The other P25 systems can be radio systems or third-party console subsystems. If the P25 system is a radio system with RF sites, the interface is the ISSI 8000. If the P25 system is a third-party console subsystem, the interface is the CSSI 8000.

The ISSI 8000/CSSI 8000 feature is supported on M1, M2, M3, L1, and L2 zone cores. It is not supported on K core systems.

### 2.12.1 ISSI 8000/CSSI 8000 Feature in Systems with DSR

In a Dynamic System Resilience (DSR) system, the ISSI 8000 Inter-system Gateway (ISGW) is optional at the backup site.

In a DSR system, with an ISSI 8000 Gateway in two separate master sites, the ISSI 8000 Gateway in both master sites can connect to the same foreign system interface, or the foreign system can be redundant also. If the foreign system is redundant, both master sites should connect to both foreign system interfaces, because ISSI 8000 Gateway does not switch over upon detecting a failure of the ISSI link, but only based on its own health and its link to the zone controller. Geographically separated redundant foreign interfaces require four physical inter-system links.

A DSR ISSI 8000 system can interface to a non-DSR ISSI 8000 system. In this configuration, the failure of one master site in the DSR system does not cause failure of the inter-system communications, but the failure of the master site containing the ISGWs in the non-DSR system causes failure of the inter-system communications.

If the P25 system is a third-party console subsystem, the interface is the CSSI 8000. In a DSR system, with an ISSI 8000 Gateway in two separate master sites, the ISSI 8000 Gateway in each master site can connect to a separate third-party console interface, or both redundant cores can connect to the same third-party console interface. Both master sites should connect to both third-party console interfaces, because the determination of the active gateway does not take into account the health of the CSSI 8000 link, but only the health of the gateway itself and its link to the zone controller. Geographically separated third-party console interfaces require four physical links.

The ISGW and Transcoders can reside on the same host platform. For supported combinations, see the *Virtual Management Server Software* manual.

Additionally, ISGW can co-reside on the VMS01 in M3 systems, if VMS01 is a HP DL380 Gen9 server.

## 2.13 Dynamic Transcoders

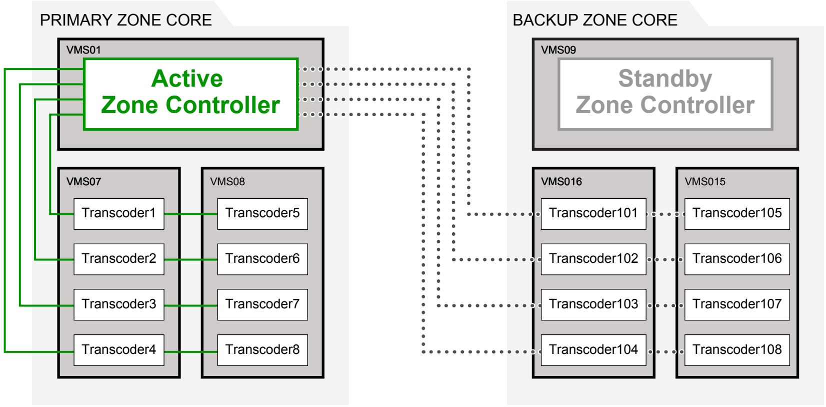
For DSR systems, the dynamic transcoders in both primary and backup zone cores connect to the active Zone Controller. The Zone Controller assigns calls to the available transcoders located in the same zone core. Assuming that the Primary Zone Controller is active, the backup core transcoders are used in the following cases:

- Each of the primary core transcoders is fully utilized with 100 calls in the non-ISGW zone, or 50 calls in the ISGW zone.
- All primary core transcoders are down.
- All primary core transcoders are disabled.

If there are no enabled transcoders in either zone core, the call is granted without a transcoder. If the transcoders in either zone core are enabled, but no transcoders have available capacity, the call is busied until transcoder capacity becomes available in either zone core.

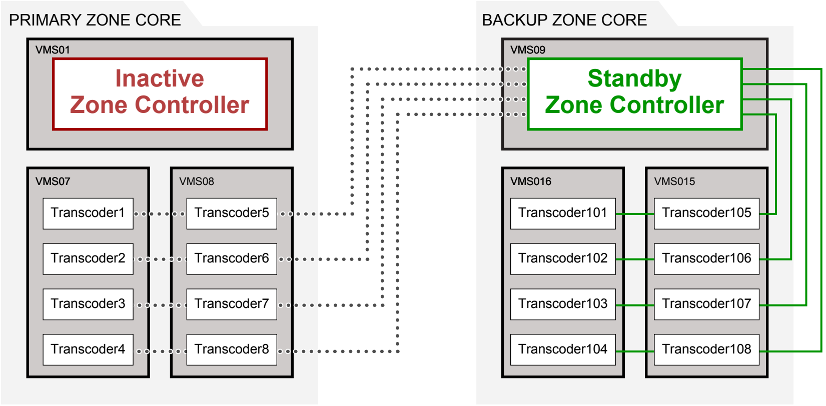
The following diagram illustrates a scenario in which the primary Zone Controller is active and all transcoders in the primary zone core are being assigned calls. The transcoders in the backup zone core are connected to the active Zone Controller, but they do not have any calls assigned.

**Figure 14: Primary Zone Controller with Transcoders in the Primary Zone Core**



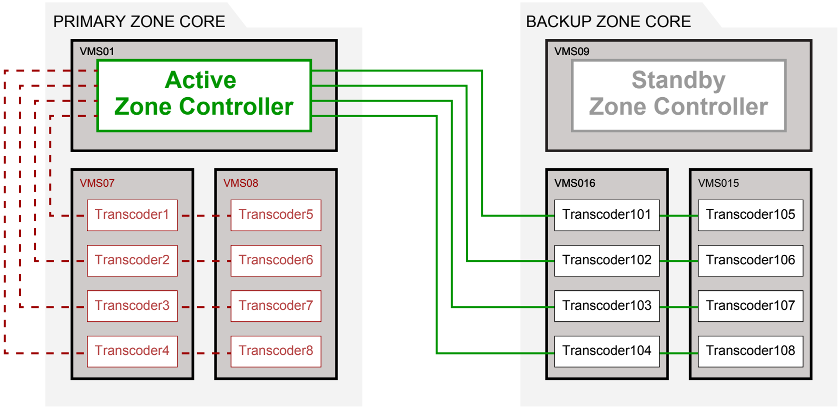
When the Zone Controller in the primary zone core is down, the Zone Controller in the backup zone core becomes active. All calls are then assigned to the transcoders in the backup zone core.

**Figure 15: Backup Zone Controller with Transcoders in the Backup Zone Core**



When both VMSs in the primary zone core are down (and thus transcoders residing on those servers are down too), the primary Zone Controller assigns calls to the transcoders residing on servers in the backup zone core.

**Figure 16: Primary Zone Controller with Transcoders in the Backup Zone Core**



For more information, see the “M3 DSR Configurations for Dynamic Transcoder” section in the *Dynamic Transcoder User Guide*.

Chapter 3

# Theory of Operation for M1 DSR Systems

This chapter explains how Dynamic System Resilience (DSR) works in the context of your M1 system. It covers the architecture of components that provide DSR functionality and how these components interact to provide redundancy in an ASTRO® 25 system.

This chapter includes interactive illustrations and animations. If necessary, you can download the latest Flash® Player from http://www.adobe.com/.

Click anywhere inside an image to display the interactive content. An option list allows you to select which drawing to view. Depending on the settings of your Adobe® Reader®, a Manage Trust dialog may open when you click an image. Select one of the radio buttons in the dialog and click the **Play** button to view the content.

To print an illustration or a single frame of an animation, right-click the image and select **Print...** from the popup menu. In the **Print** dialog box, ensure that **Page Range** is set to **Selection**. Click **Print**.

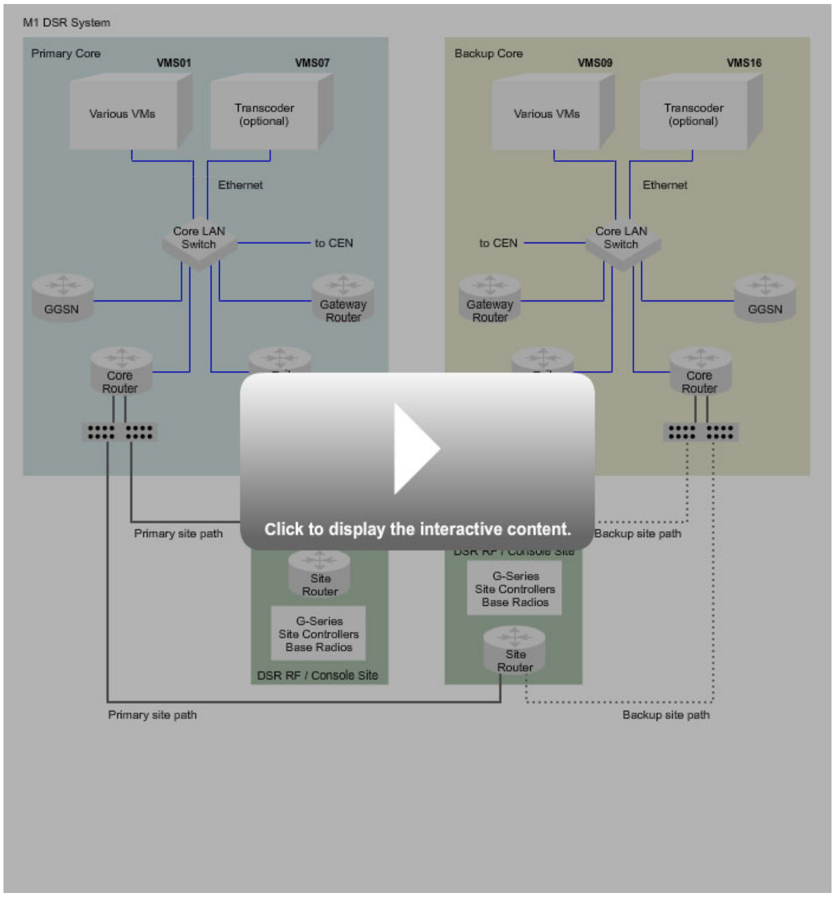
**IMPORTANT:** If the **Page Range** is set to **All**, every frame of an animation (in some cases, hundreds) prints.

## 3.1 M1 Single Zone with DSR

An M1 Dynamic System Resilience (DSR) system consists of a single zone and two master sites. The primary core of the zone is deployed at one master site. The backup core of the zone is deployed at the other master site. An M1 DSR system cannot be used in a multi-zone system.

The subnet configuration for an M1 core is maintained in the primary core and applied in the backup core. The exit router is introduced in the primary and backup cores. The configuration includes two zone controller control subnets and two Transitional Local Area Networks (TLANs). However, one core LAN switch and one gateway router are included to provide the Layer2 path for the subnets and TLANs. An S6000 router or GGM 8000 System Gateway is used for the exit router in an M1 DSR configuration.

**Figure 17: M1 Single Zone with DSR**



3.1.1

## Voice Services for M1 DSR

Dynamic System Resilience (DSR) allows a system to continue to function with minimal loss of voice communication due to the failure of any controlling master site. In an M1 DSR system, one Zone Controller (ZC) application is in the primary core (ZC1) and one in the backup core (ZC2). Under normal conditions, ZC1 is in the active state.

If no other failures occur in the system and ZC1 fails, ZC2 becomes active automatically, assuming it was in the standby state and not user-requested standby state.

3.1.1.1

### RF Site Switchover for M1 DSR

On a per site basis, Dynamic System Resilience (DSR) capability is established by configuring a separate physical path to the backup core. With this path to the backup core, if the entire primary core fails, a site can switch over. The backup site path can also be used if the primary site fails. Traffic is then rerouted along the backup site path, through the backup core, and over the Interzone link to the primary core without interrupting wide-area trunked operation.

An M1 DSR system may support a redundant site gateway for any site configuration supported by M1. For M1 DSR systems with redundant site gateways, one site gateway has a link to the primary core and the other site gateway has a link to the backup core. For M1 DSR systems without redundant site gateways, the site gateway has two links, one to the primary core and one to the backup core.

For an M1 DSR system, the sites are configured with two additional broadcast subnet addresses for the zone controller in the backup core. The two broadcast addresses allow the site to establish redundant Site Control Paths (SCPs) to the active zone controller. For DSR, after the site establishes one SCP to a core, it does not broadcast requests to the other core. The site persistently tries to establish the redundant SCP to the same core.

### 3.1.1.2 MCC-Series Dispatch Console and Site Gateway with Conventional Channel Interface Switchover with an M1 DSR System

A console site with an MCC 7500 VPM/MCC 7500E/MCC 7100 Dispatch Console or Site Gateway (CCI) is given Dynamic System Resilience (DSR) capability by configuring a separate physical path to the backup core. This backup path also offers redundancy. If the primary path fails, traffic is rerouted through the backup core over the interzone link to the primary core without interrupting wide-area trunked operation. However, if an individual console OP (MCC 7500 VPM, MCC 7500E or MCC 7100 Dispatch Console) loses its network, no redundant network is available for the operator to sustain services.

For console sites with two or more consoles, a pair of consoles at the console site establishes redundant links (one link per console) to the active zone controller. For DSR, the consoles coordinate their attempts to establish links to the same core. For console sites with one console, the console establishes two links to the active zone controller.

## 3.1.2 Data Services for M1 DSR

Dynamic System Resilience (DSR) allows an M1 system to provide geographic redundancy for data services. An M1 system offers almost any combination of data services including Trunked Integrated Voice and Data (IV&D), Conventional IV&D, Enhanced Integrated Data (EID), and High Performance Data (HPD). High Availability (HA) Data services are not supported in M1 systems.

An M1 DSR system supporting data services deploys the following elements in the primary and backup cores:

- One Gateway GPRS Support Node (GGSN)
- One Packet Data Gateway (PDG) per data service (IV&D, Conventional IV&D, and HPD)
- One Customer Network Interface (CNI) Path
- One CAI Data Encryption Module (CDEM) for conventional data only

## 3.1.3 ISSI 8000/CSSI 8000 Tiering for M1 Cores

ISSI 8000/CSSI 8000 functionality is available for the following system configurations:

- M1 Non-Redundant Zone Core Configuration
- M1 Dynamic System Resilience (DSR) systems with one Inter-RF System Gateway (ISGW) and one Firewall (FW) in the Primary M1 Core only
- M1 DSR systems with one ISGW and one FW each in the Primary and Backup Core

## 3.1.4 Network Management Services for M1 DSR

An M1 system with Dynamic System Resilience (DSR) includes the following redundant network management services:

- Fault Management - Unified Event Manager (UEM)

- Configuration Management - User Configuration Server (UCS), Provisioning Manager (PM), Unified Network Configurator (UNC), Zone Database Server (ZDS)
- Performance Management - Zone Statistics Server (ZSS), Air Traffic Router (ATR)
- MOSCAD Network Fault Management (NFM) (optional feature)

Regardless of the type of remote site, the equipment is managed by the active UNC in the system and visible to the UEM and UNC in both the primary and backup core.

### 3.1.4.1 Fault Management for M1 DSR

To achieve redundancy for fault management information, an additional Unified Event Manager (UEM) is provided in the backup core. Both UEMs are active at all times. Each UEM is configured to enable collection of statistics. System managers choose which UEM to connect for monitoring.

Each manual operation, such as discovery or synchronization, must be performed on both UEMs. Any manual customizing of views on the user interface must be applied to both UEMs.

Network elements managed by the UEM are in the primary core, backup core, and remote sites. Additional backup core equipment for network management, voice, transport, IP services, and data are fault managed. The UEM in the backup core fault manages the non-Dynamic System Resilience (DSR) sites through the InterZone links.

If the primary core UEM fails, the backup is active and no switchover is required. If a primary core fails, an operator is able to monitor recovery, for example, Ethernet site link statistics, from the backup core UEM.

### 3.1.4.2 Configuration Management for M1 DSR

Configuration management is performed using the Provisioning Manager (PM) and the Unified Network Configurator (UNC) applications and Lightweight Directory Access Protocol (LDAP) services on the Zone Database Server (ZDS). The User Configuration Server (UCS) hosts the PM application and database for subscriber access control records, console profiles, and site gateway (conventional channel interface) conventional channel data, whereas the UNC contains system infrastructure data. The ZDS is an LDAP server that contains data from the UCS, obtained through database synchronization between the UCS and ZDS. The distribution of data from the UCS to the ZDS occurs when the PM user executes a Distribute Changes or Force Initialization operation. The Advanced Distribution Service (ADS) server is a part of the ZDS that provides the connection between the PM and several network elements, and is used for radio alias distribution.

In an M1 system with Dynamic System Resilience (DSR), a redundant UCS (PM), UNC, and ZDS are added to the backup core.

Only one PM/UNC can be active at a time as determined by the network operator. Therefore, one PM/UNC is configured to be in the active state and the other in warm standby state. The active PM must be in the same master site core (either primary or backup) as the active UNC. If either one fails, both applications must switch over to the backup core. Switchover is manual and requires that the PM and UNC on the backup core are switched from the warm standby state to the active state. After a switchover, NM client computers must launch the PM client for the newly active PM as well as the UNC client for the newly active UNC.

Periodic secure synchronization over the InterZone link from the primary PM and UNC to its corresponding backup ensures that up-to-date configuration data is available in the backup core. Additionally, the system operator can manually perform synchronization.

Both the primary core ZDS and the backup core ZDS receive data from the active PM, so no synchronization is required between the two ZDS LDAP services. The PM relies on the ZDS LDAP server for the LDAP clients in MCC-Series console sites and the site gateway (CCI). The LDAP server on each ZDS is active at all times, so ZDS LDAP clients can pull configuration data from either ZDS and their affiliated ADS.

A PM switchover causes an automatic LDAP database rebuild and a download of data to all consoles in the system. The clients are responsible for downloading the data. MCC-Series Dispatch Consoles must be restarted for the new database to take effect. The Site Gateway (CCI) LDAP server IP address must be modified to the backup core ZDS and then must be reset to complete the switchover. Because the configuration data is unlikely to change, manual switchover is not usually required.

### 3.1.4.3 Performance Management for M1 DSR

Performance management consists of the collection of features and applications that provide operators with information about radio system usage. Performance management data includes real-time information and historical statistics regarding radio call activity and affiliation.

Performance management includes the following servers on an M1 Dynamic System Resilience (DSR) system:

- Air Traffic Router (ATR)
- Zone Statistics Server (ZSS)

Performance management applications include:

- Affiliation Display
- Air Time Information Access (ATIA)
- Computer Aided Dispatch Interface (CADI)
- ZoneWatch
- Radio Control Management (RCM)

The ATR receives performance management data when the user invokes the distribute changes operation on the Provisioning Manager (PM). The ATR receives the following data from the PM via the UNC:

- RCM configuration data
- ZoneWatch filters and profiles
- Site and channel information

The UEM also gathers various performance statistics. Both primary and backup UEMs are continuously active.

In an M1 system with DSR, an additional ATR and ZSS are deployed in the backup core to provide zone-level performance management services while a ZC in the backup core is active. The additional ZSS pulls data from its collocated ATR.

An ATR in the primary core does not share information with an ATR in the backup core. An ATR in the backup core cannot assume the services of an ATR in the primary core. Performance management services that rely on the primary core ATR are unavailable until that ATR is repaired or replaced, or until a Zone Controller (ZC) switchover occurs to the backup core with a functional ATR. The ZC-ATR link status is communicated between the primary and backup ATRs so that a fault can be sent to the UEM when no ZC is reachable.

The redundant servers installed in the backup core do not share any call activity data, statistics, or RCM data with their primary core counterparts. Redundant ZSSs do not share or synchronize historical data. When a switchover to a backup ZC occurs, performance management is available but requires manual intervention by an operator to retrieve historical statistics and previously issued RCM commands.

### 3.1.4.4 MOSCAD Network Fault Management for M1 DSR (Optional)

In an M1 system with Dynamic System Resilience (DSR), MOSCAD Network Fault Management (NFM) components in the primary core are duplicated in the backup core. NFM components include the SDM3000 Network Translator (SNT) server and the Graphical Master Computer (GMC) server. MOSCAD NFM clients, Graphical Workstations (GWSs), can be in either core. A core can have up to five collocated SDM3000 Remote Terminal Unit (RTU) servers.

The SNT and GMC in both the primary core and backup core are always active. A Unified Event Manager (UEM) for network management is in both the primary core and backup core and both are always active.

Collocated SDM3000 RTUs communicate with the SNT and GMC within their core and SNT and GMC in the backup core through the InterZone link. Every SDM3000 RTU, whether collocated or at a remote site, communicates with primary and backup managers (GMCs and UEMs).

GWS clients and the GMC server interact only with the SNT in the same core to provide management information to operators.

No synchronization exists between MOSCAD NFM elements in both cores. For example, an operator must perform manual operations, like alarm acknowledgement, separately on the primary GMC and backup GMC. When an unsolicited event occurs in a site, the SDM3000 RTU sends a trap to both primary and backup UEMs and updates both primary and backup GMCs.

### 3.1.4.5 InfoVista for M1 Dynamic System Resilience

InfoVista is not supported on M1 configurations.

## 3.1.5 Radio Authentication for M1 DSR

The Authentication Center (AuC) is a server supporting radio authentication, and is supported for M1 Dynamic System Resilience (DSR) systems.

Radio authentication session information is not transferred from the primary zone controller to the backup zone controller. Therefore, the zone controller must be loaded in the primary core and the backup core with authentication keys.

AuC loads the authentication keys only to the active ZC. After Primary to Backup ZC switchover, Backup ZC loads the keys from AuC. Data between Primary and Backup AuC is synchronized automatically. In case of disaster recovery, the Backup AuC should be reinstalled. See "Radio Authentication Disaster Recovery" in the *Radio Authentication Feature Guide*.

## 3.1.6 IP Services for M1 DSR

In an ASTRO® 25 system, IP services provide a number of support functions on the network including the following IP services in an M1 Dynamic System Resilience (DSR) system:

- Antivirus
- Backup and Restore
- Centralized Authentication
- Domain Name Service
- Network Time Protocol
- Firewall Management

- Centralized Event Logging (optional)

### 3.1.6.1 Antivirus for M1 DSR

Antivirus protection is supported for M1 Dynamic System Resilience (DSR) in both the primary core and backup core.

### 3.1.6.2 Backup and Restore for M1 DSR

The Backup and Restore service is supported in both the primary core and backup core for M1 Dynamic System Resilience (DSR).

### 3.1.6.3 Centralized Authentication for M1 DSR

Centralized Authentication (Active Directory, RADIUS) services are provided for M1 Dynamic System Resilience (DSR). A zone-level and a system-level domain controller reside in both the primary core and backup core for M1 DSR.

### 3.1.6.4 Domain Name Service for M1 DSR

Domain Name Service is supported in both the primary core and the backup core for M1 Dynamic System Resilience (DSR).

### 3.1.6.5 Network Time Protocol for M1 DSR

M1 Dynamic System Resilience (DSR) configurations require a Network Time Protocol (NTP) Stratum 1 device in the primary core and in the backup core. The preferred Stratum 1 device is the TRAK 8835. However, the TRAK 9100 device can be used as the Stratum 1 device.

The CSA server in both the primary core and backup core must be configured as an NTP client and point to the NTP01 server. The service is supported in both the primary core and backup core for M1 DSR.

### 3.1.6.6 Centralized Event Logging for M1 DSR

The Centralized Event Logging (Syslog) service is an optional feature for M1 Dynamic System Resilience (DSR). Centralized Event Logging is supported both in the primary core and the backup core for M1 DSR.

### 3.1.6.7 Firewall Management for M1 DSR

The Firewall Management Server (FMS) is not supported on M1 configurations; it is not available with M1 Dynamic System Resilience (DSR).

## 3.1.7 Dynamic Transcoders in M1 DSR

In M1 DSR system, each zone core has two dynamic transcoders capable of supporting up to 100 simultaneous calls. For more information, see the “M1 DSR Configurations for Dynamic Transcoder” section in the *Dynamic Transcoder User Guide*.

Chapter 4

# Dynamic System Resilience Installation

This chapter details installation procedures relating to the Dynamic System Resilience feature.

## 4.1 DSR Installation

Dynamic System Resilience (DSR) feature installation is a complex process and must be performed by Motorola Solutions. For information on DSR installation, contact the Motorola Solutions Support Center (SSC).

## 4.2 DSR Expansion

Dynamic System Resilience (DSR) feature expansion is a complex process which must be completed by Motorola Solutions. See Dynamic System Resilience Feature Expansion/Upgrades on page 147.

This page intentionally left blank.

Chapter 5

# Dynamic System Resilience Configuration

Initial Dynamic System Resilience (DSR) system configuration is a complex process and must be performed by Motorola Solutions.

For information on initial DSR configuration, contact your Motorola Solutions Support Center (SSC). For detailed information on component configuration, see the appropriate ASTRO® 25 manuals listed in Reference Information for Dynamic System Resilience on page 145.

This page intentionally left blank.

Chapter 6

# Dynamic System Resilience Optimization

No optimization procedures are required for the Dynamic System Resilience (DSR) feature.

This page intentionally left blank.

Chapter 7

# Dynamic System Resilience Operation

This chapter provides the tasks that must be performed after the Dynamic System Resilience feature is installed and operational on your system.

## 7.1 Verifying DSR Operation

This section explains how to verify that all portions of the system are working correctly after Dynamic System Resilience (DSR) has been added and switchovers working as designed. Motorola Solutions conducts initial post-installation verification. However, the system can be verified after each hardware replacement.

⚠ **CAUTION:** Running these verification tests can cause outages including site trunked operation of the system.

**Process:**

1. Verify Zone Controller (ZC) switchover. See Verifying ZC Switchover.
2. Verify all Network Management (NM) services. See Verifying NM Services.
3. Verify transport routes. See Verifying Transport Routers.
4. Verify Archiving Interface Server (AIS) Over-the-Ethernet Keying (OTEK) operation. See Verifying Over-the-Ethernet Keying (OTEK) Operation.
5. Verify Packet Data Gateway (PDG) switchover. See Verifying PDG Switchover.

### 7.1.1 Zone Controller Switchover Verification

This section describes how to verify the status of Zone Controllers (ZCs) in the system. For information on ZC redundancy states, see the “Zone Controller Redundancy States” section in the *Zone Controller Feature Guide*.

For normal operation, only one of the ZCs is in the **Active** state. Assuming no critical failures, the remaining ZCs are in either the **Standby** or **User Requested Standby** state. For instance, if ZC1 was the active ZC and it failed, the redundant ZC2 would take over. Standby ZC3 takes over and becomes active either when both ZC1 and ZC2 fail (for example, because of a master site destruction) or when the InterZone link is down.

#### 7.1.1.1 Verifying Zone Controller Status

Perform this process to verify the status of the Zone Controller (ZC).

**Process:**

1. Log in to the active ZC. See the “Logging On to a Zone Controller Application” section in the *Zone Controller Feature Guide*.
2. Display status information of the active ZC using the **Administration** menu. See the “Display Status” section in the *Zone Controller Feature Guide*.
3. Verify the following:

- **Application Redundancy Object State** of the active ZC is **Active**
- Heartbeat Authentication (HA) Link/Path Info states **LinkUp**

> **NOTICE:** The information is provided for all ZCs. For instance, when logged on ZC1, link and path information with ZC2, ZC3, and ZC4 are present. **LinkUp** is the normal operating state. If the link is **Down**, the cause is stated.

See the “Display Status” section in the *Zone Controller Feature Guide* for information on ZC status.

4 Log off the ZC. See the “Logging Off the Zone Controller Application” section in the *Zone Controller Feature Guide*.

5 Repeat this process for the ZCs in the backup core to verify that its **Application Redundancy Object State** is **Standby**.

### 7.1.1.2 Verifying Zone Controller Switchover

To verify if Zone Controller (ZC) switchover is working as intended, complete a manual ZC switchover. To support Dynamic System Resilience (DSR) operations, the Unified Network Configurator (UNC) provides the capability to manually switch the redundant ZCs and Packet Data Gateways (PDGs) (by setting the redundant state to **Active**). In addition, the UNC supports enabling or disabling the automatic switching by setting the redundant state to **Standby** or **User Requested Standby**, respectively.

**Process:**

1 In the UNC, set the state of ZC3 in the backup core to **Active**. At that point, ZC1 in the primary core should become **Standby** (assuming it was in **Active** state). See Changing the ZC Redundancy State in the UNC.

2 Verify the state of the backup ZC3 in the UNC. It should switch from **Standby** to **Active** state. See Verifying the ZC Status in the UNC.

3 Complete a return switchover back to the primary core. In the UNC, set the state of ZC1 in the primary core back to **Active**. See Changing the ZC Redundancy State in the UNC.

4 Verify the state of ZC1 in the UNC. It should switch to **Active**. See Verifying the ZC Status in the UNC.

## 7.1.2 Network Management Services and Application Verification

This section describes how to verify whether the following Network Management (NM) services and applications in the backup core are operational:

- Dynamic Reports
- ZoneWatch
- Zone Historical Reports
- Provisioning Manager
- System Historical Reports

### 7.1.2.1 Verifying Network Management Services

Follow this process to verify Network Management (NM) services.

**Process:**

1. Follow the “Opening Applications from the Explorer Window” procedure in the *Private Network Management Client Feature Guide*.
2. Verify if the applications work properly. See Verifying the NM Applications.

7.1.2.2
## Opening the PRNM Suite of Applications

Perform this procedure to open Private Radio Network Management (PRNM) applications.

**Prerequisites:** Obtain the following: Network Management (NM) client username and password

**Procedure:**

1. Log in to the Network Management (NM) client.
2. Double-click the **Motorola PRNM Suite** icon on the desktop.

The **Application Launcher** window appears. The window displays accessible **Master Site** (system-level) applications and **Zone Core** (zone-level) applications.

7.1.2.3
## Opening the System-Level Applications from PRNM Suite of Applications

Perform this procedure to open system-level applications from the Private Radio Network Management (PRNM) suite.

**Procedure:**

1. Open the **Application Launcher** explorer window.
2. Select the master site for the application you want to open (primary or backup).
3. Double-click the appropriate icon.

   **IMPORTANT:** The server application you are accessing must be in the appropriate, currently enabled core.

4. If you want to launch different applications, repeat this process for every application to be launched.

The selected application window appears.

7.1.2.4
## Opening the Zone-Level Applications from PRNM Suite of Applications

Perform this procedure to open zone-level applications from the Private Radio Network Management (PRNM) suite.

**Procedure:**

1. Open the **Application Launcher** explorer window.
2. Select the core for the application you want to open (**Primary** or **Backup**).
3. Select the zone for the application you want to open.
4. Double-click the appropriate icon.
5. If you want to launch different applications, repeat the process for every application to be launched.

The selected application window appears.

## 7.1.2.5 Verification of the Network Management Applications

This table contains information on how to verify Network Management (NM) applications.

Table 3: Verify the NM Applications

| Application | Verification |
|---|---|
| Dynamic Reports | See Verifying the Dynamic Reports Application on page 92 |
| ZoneWatch | See Verifying the ZoneWatch Application on page 92 |
| System and zone applications (all) | Verify that application window appears on the desktop. |
| System and zone applications (all) | Verify that names of applications appear in the title bar of the opened Private Radio Network Management (PRNM) Suite Application. |
| Only system applications (all) | Verify that master site information appears in the title bar of the opened PRNM Suite Application (Primary Master Site or Backup Master Site). |
| Only zone applications (all) | Verify that zone core information appears in the title bar of the opened PRNM Suite Application (Primary Core or Backup Core). |
| Only zone applications (all) | Verify that zone ID information appears in title bar of the opened PRNM Suite Application (ZONE00X, where 'X' is number of zones) for which that application was started. |
| Unified Network Configurator (UNC) | The UNC application is launched using a shortcut from the NM client desktop, similar to the Unified Event Manager (UEM). It does not use the application launcher. To verify the backup UNC is operating, follow Verifying the Backup UNC on page 93. |

### 7.1.2.5.1 Verifying the Dynamic Reports Application

Perform this procedure to verify the Network Management (NM) Dynamic Reports application..

**Procedure:**

In the **Security Configuration** window, select security level **NoAuthNoPriv**. Click **OK**.

### 7.1.2.5.2 Verifying the ZoneWatch Application

Perform this procedure to verify the Network Management (NM) ZoneWatch application..

**Procedure:**

In the **Motorola ZoneWatch – Select Watch Profile** window, select **default-profile**. Click **OK**.

## 7.1.2.6 Logging on to Network Management Server Applications with SSH

Follow this procedure to log on to Network Management (NM) server applications with Secure SHell (SSH).

**Prerequisites:** Consult your system administrator or customized system configuration documentation delivered with your system by Motorola Solutions for a list of user names, passwords, IP addresses, and host names.

**Procedure:**

1. Type the appropriate user name in the **User name** field. The default administrative account is `secadm`.
2. Type the appropriate password in the **Password** field. Click **OK**.
3. For additional steps, see the “Logging on to PNM Servers Applications” procedure in the *Private Network Management Servers Feature Guide*.

7.1.2.7

### Logging On to a VMS Host

Perform this procedure to log on to a Virtual Management Server (VMS) host.

**Procedure:**

1. Launch the VMware vSphere Client from the Windows-based device where it resides (a desktop shortcut was created during installation).
2. In the dialog box asking for an IP address, user name, and password, type the IP address for the ESXi-based server.
3. Type `root` in the **User Name** field.
4. In the **User Password** field, type the appropriate password.
5. Click **Login**.

The **vSphere Client Inventory** screen appears.

7.1.2.8

### Verifying the Backup UNC

Perform this procedure to verify operation of the backup Unified Network Configurator (UNC).

**Process:**

1. Restore the backup configuration on the backup UNC. See the “Centralized Backup and Recovery for PNM Server Applications” section in the *Private Network Management Servers Feature Guide*.
2. Enable the backup UNC server application. See Enabling the Standby UNC.
3. Launch the backup core UNC application on the Network Management (NM) client. See the “Accessing UNC Wizards” section in the *Unified Network Configurator User Guide*.
4. Verify that the backup UNC can successfully pull configuration from the backup core devices. See the “Scheduling the Pull of a Device Configuration” section in the *Unified Network Configurator User Guide*.

7.1.3

## Verification of Transport Routes

Verify correct voice traffic routing occurs for all the switchover scenarios executed. To verify transport routes, complete a Zone Controller (ZC) switchover to the backup core, as described in Verifying ZC Switchover. A successful ZC switchover verifies transport routing to the backup core.

To verify correct data traffic routing, check if data applications operate normally after a zone core switchover. For information, see Verifying Over-the-Ethernet Keying (OTEK) Operation.

7.1.4
## Over-the-Ethernet Keying Operation Verification

Set the Over-the-Ethernet Keying (OTEK) inactivity time appropriately based on the Crypto Period established for voice encryption keyset changeover to allow automatic recovery within an acceptable time period. Testing of automatic OTEK recovery for Dynamic System Resilience (DSR) is accomplished by waiting for a time longer than the OTEK inactivity time following DSR Customer Network Interface (CNI) switchover (default 8 hours), and then verifying OTEK communications from the Key Management Facility (KMF) for each OTEK client being tested.

For information on the verification of other data applications, see Customer Enterprise Network Applications Impact After a Switchover.

7.1.5
## PDG Switchover Verification

This section provides the details about verifying the Packet Data Gateway (PDG) switchover.

7.1.5.1
### Verifying the DSR Redundancy State of the PDG

Follow this process to verify the Packet Data Gateway (PDG) redundancy state.

**Process:**

1. In the Unified Network Configurator (UNC), verify that the Dynamic System Resilience (DSR) redundancy state of the PDG in the primary core is **Active**. See Verifying the PDG Redundancy state in the UNC.
2. On the primary Packet Data Router (PDR), verify that the Heartbeat Authentication (HA) Link is up by accessing the **View Redundancy Configuration** menu, and verifying that the HA Link status reads: `HA Link status: Link Up`. See the “Verify HA Link Status on PDR” section in the *Packet Data Gateways Feature Guide*.
3. In the UNC, verify that the PDG in the backup core is in **Standby redundancy** state. See Verifying the PDG Redundancy State in the UNC.

7.1.5.2
### Verifying the PDG Redundancy State in the UNC

Perform this procedure to verify the Packet Data Gateway (PDG) redundancy state in the Unified Network Configurator (UNC).

**Prerequisites:** The Packet Data Router (PDR) must be up and running to complete the procedure. Obtain the UNC username and password from your system administrator.

**Procedure:**

1. Log in to the EMC Smarts™ Network Configuration Manager. See “Logging in to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator User Guide*.
2. In the **Dashboard** navigation pane, select **Networks** → **Astro 25 Radio Network**. Expand **Devices**.
3. Right-click on the selected PDG.
4. From the pop-up menu, select **Quick Commands**.
5. From the sub-menu, select **Get Redundancy State**.

A dialog box appears displaying the redundancy state of the selected PDG.

## 7.2 Primary and Backup Core Status Monitoring

The Unified Event Manager (UEM) application in either core can be used to monitor equipment in the primary or backup core of a given zone. For systems that implement the Motorola Solutions Support Center (SSC) monitoring service, the UEMs in both cores have network connections implemented on the North Bound Interface (NBI) to the SSC. The feeds are correlated for continuous monitoring. If your system does not use this service, it is important to periodically watch for alarms in the backup UEM for potential problems in the primary core and to ensure issues are fixed in a timely manner.

In M3 systems, the UEM displays Zone Controller (ZC) names according to an established numbering scheme with ZC1 and ZC2 tied to the zone number for the ZCs in the primary core, and ZC3 and ZC4 tied to the same number for the ZCs in the backup core. This scheme assists in tracing the source of the fault to the appropriate zone and core. In M1 systems, the UEM displays ZC names according to an established numbering scheme with ZC1 tied to the zone number for the ZC in the primary core and ZC3 tied to the same zone number for the ZC in the backup core.

The Packet Data Gateways (PDGs) have different designators in the primary and backup cores. The IV&D PDGs are numbered odd, and the High Performance Data (HPD) PDGs are numbered even. In the primary core, the PDGs are numbered PDG1 for IV&D and PDG2 for HPD. In the backup core, they are numbered PDG5 for IV&D and PDG6 for High Performance Data (HPD).

For information on using the UEM to monitor alarms, see the *Unified Event Manager User Guide*.

## 7.3 Routine Server Backups

For information on network management server application backups, see the *Private Network Management Servers Feature Guide*. Systems with Dynamic System Resilience (DSR) do not have any specific requirements for performing routine backups.

Always back up the Unified Network Configurator (UNC) after making it active. A backup of a disabled UNC only backs up the platform data, not the UNC data.

## 7.4 Database Synchronization

In a system with Dynamic System Resilience (DSR), most servers hosting applications are duplicated between cores for additional redundancy beyond the standard redundancy in multi-zone ASTRO® 25 systems. Depending on the service they provide or the application they host, it may be necessary to synchronize databases between the two cores. In most cases, this process is automatic. However, a manual option is usually available as well.

This section describes how to synchronize application databases between primary and backup cores. Data synchronization is possible for the following applications:

- Unified Network Configurator (UNC) - automatic and manual
- User Configuration Server (UCS) - automatic and manual
- Zone Database Server (ZDS) - automatic synchronization with the UCS

**IMPORTANT:** Ensure that the UCS and UNC server applications are configured to synchronize in the same time periods.

### 7.4.1 UNC Synchronization

The two Unified Network Configurator (UNC) applications operate as an active and standby pair. Only the active UNC manages the network elements in the system. The operator makes all configuration changes through the active UNC, which periodically synchronizes the changes with the disabled standby UNC. Other information, such as Configuration Change History, is also synchronized. Synchronization prepares the disabled standby UNC for switchover. The **View Synchronization Results** option in the administration menu allows synchronization results (up to the last 400 attempts) to be viewed.

The synchronization process is automatic, but an operator can perform a manual synchronization.

### 7.4.1.1 Synchronizing the Active and Standby UNC Databases

Perform this procedure to manually synchronize the active and standby Unified Network Configurator (UNC) databases.

**Procedure:**

1. Log in to the active UNC as the administrator. See Logging on to Network Management Server Applications with SSH on page 92.
2. When the command prompt appears, type the corresponding number for **Services Administration**. Press ENTER.
3. From the **Services Administration** submenu, select **Manage System Redundancy and Resilience**.
4. From the **Manage System Redundancy and Resilience** submenu, select **Initiate Synchronization to Standby**. Press ENTER.

   The following message appears: `Synchronization with the Standby UNC has been initiated.`
5. Log out of this UNC.

The synchronization process of the active and standby UNC databases is started.

### 7.4.1.2 Verifying UNC Synchronization

Perform this procedure to verify Unified Network Configurator (UNC) synchronization.

**Procedure:**

1. Log in to the active UNC as the administrator. See Logging on to Network Management Server Applications with SSH on page 92.
2. When the command prompt appears, type the corresponding number for **Services Administration**. Press ENTER.
3. In the **Services Administration** submenu, type the corresponding number for **Manage System Redundancy and Resilience**. Press ENTER.
4. In the **Manage System Redundancy and Resilience** submenu, type the corresponding number for **Display Synchronization Results**. Press ENTER.

   The synchronization results display:

```
Date and Time        | Sync Status          | Failure reason (optional)
                     | M - Manual           |
                     | S - Scheduled        |
===========================================================================
=========
2015-06-17 14:23:59 | (M)Sync succeeded    | OK
2015-06-17 14:23:23 | (M)Sync started      |
Press SPACE to continue or q to quit
```

5. Verify that the last (uppermost) manual synchronization (message marked with `M`) has succeeded. Example of a successful manual synchronization:

   ```
   (M)Sync succeeded   | OK
   (M)Sync started
   ```

   **IMPORTANT:** If the uppermost manual synchronization message is `(M)Sync started`, synchronization is in progress.

6. Press `Q`.

The **Manage System Redundancy and Resilience** submenu appears.

## 7.4.2 UCS Synchronization

The two User Configuration Server (UCS) applications operate as an active and standby pair. Only the active UCS manages configuration data for the system. The operator makes all changes through the active UCS, which periodically synchronizes with the peer disabled standby UCS. Synchronization prepares the standby UCS for switchover.

Although the synchronization process is automatic, a manual synchronization can be performed.

### 7.4.2.1 Synchronizing the Active and Standby UCS Databases

Perform this procedure to manually synchronize the active and standby User Configuration Server (UCS) databases.

**Procedure:**

1. Log in to the active UCS server application as the administrator. Follow Logging on to Network Management Server Applications with SSH on page 92.
2. From the **server** menu, select **Services Administration**. Press ENTER.
3. From the **Services Administration** submenu, select **Manage System Redundancy and Resilience**. Press ENTER.
4. To verify that the server you are logged in to is an active server, from the **Manage System Redundancy and Resilience** submenu, select **Display DSR Status**.

   The following message appears:

   ```
   Display DSR Status  2015-06-17 14:32:41
   ---------------------------------------
   UCS Server State
     LOCAL:  Enabled, Reason: User Requested
     REMOTE: Disabled Standby, Reason: User Requested

   UCS DSR Feature State
     LOCAL:  Enabled
     REMOTE: Enabled

   UCS Synchronization State
     LOCAL:  Data In sync, Reason: Sync Succeeded
     REMOTE: Server capable of being synced by Active, Reason: This
   server is a Standby server

   UCS Last Successful DSR Synchronization Time (outgoing from)
     LOCAL:  2015-06-17 14:23:59
   ```

```
  REMOTE: 2015-06-17 01:37:50

UCS Versions
  LOCAL:  UCS-Astro-07.16.01.26-00
  REMOTE: UCS-Astro-07.16.01.26-00

  LOCAL = ucs-unc01.ucs, REMOTE = ucs-unc02.ucs
```

5 From the **Manage System Redundancy and Resilience** submenu, select **Initiate Synchronization to Standby**. Press ENTER.

   The Dynamic System Resilience (DSR) synchronization process starts in the background. The fact that the menu is displayed does not mean that synchronization is finished. To verify the status of synchronization, use the **View Synchronization Results** menu option.

   **IMPORTANT:** If any other message is displayed on the screen, an error has occurred. See the message text for details.

   The following message appears on the screen and the menu is displayed:`Synchronization with the Standby UCS has been initiated.`

6 Log out of this UCS.

The synchronization process of the active and standby UCS databases is started.

## 7.4.2.2 Verifying UCS Synchronization

Perform this procedure to verify User Configuration Server (UCS) Synchronization.

**Procedure:**

1 Log in to the UCS server application as the administrator. Follow Logging on to Network Management Server Applications with SSH on page 92.

2 When the command prompt appears, type the corresponding number for **Services Administration**. Press ENTER.

3 In the **Services Administration** submenu, type the corresponding number for **Manage System Redundancy and Resilience**. Press ENTER.

4 From the **Manage System Redundancy and Resilience** submenu, select **Display Synchronization Results**. Press ENTER.

   The synchronization results are displayed on the screen:

```


Synchronization results for last 400 attempts:

Date and Time | Sync Status | Failure reason (optional)
       | M - Manual   |
       | S - Scheduled|
===============================

yy-mm-dd hh:mm:ss | (M)Sync succeeded | OK
yy-mm-dd hh:mm:ss | (M)Sync started   |
yy-mm-dd hh:mm:ss | (S)Sync succeeded | OK
yy-mm-dd hh:mm:ss | (S)Sync started   |

Press SPACE to continue or q to quit
```

5 Verify that the last (uppermost) manual synchronization (message marked with `M`) has succeeded. Example of a successful manual synchronization:

```
(M)Sync succeeded | OK
(M)Sync started   |
```

**IMPORTANT:** If the uppermost manual synchronization message is `(M)Sync started`, synchronization is in progress.

**6** Press Q.

The **Manage System Redundancy and Resilience** menu appears.

## 7.4.3 ZDS Synchronization with UCS

The Zone Database Server (ZDS) does not support manual synchronization with other ZDS. The distribution of data from the User Configuration Server (UCS) to the ZDS occurs when the PM user executes a Distribute Changes or Force Initialization operation. See Configuration Management for more information on ZDS synchronization with UCS.

# 7.5 DSR Voice Component Switchover

This section describes the typical switchover and recovery processes of voice-related components in a system with Dynamic System Resilience (DSR).

Table 4: DSR Voice Component Switchover Actions

| Component | Switchover |
|---|---|
| Zone Controller | Automatic – The switchover process is automatic, unless the system is configured otherwise (remaining Zone Controllers (ZCs) set to **User Requested Standby** state).<br>For theoretical information pertaining to voice subsystem switchover, see Voice Services on page 41 and Voice Services for M1 DSR on page 76.<br>For user-initiated switchover procedures, see Changing the ZC Redundancy State in the UNC and Verifying the ZC Redundancy State in the UNC.<br>For further information on ZC switchover and its impact on call processing, see the “Automatic Switchover” and “Manual Switchover” sections in the *Zone Controller Feature Guide*. |
| Transport equipment | Automatic |

## 7.5.1 User-initiated Switchover of the ZC Redundancy State in the UNC

This section provides instructions on how to perform a user-initiated switchover of the Zone Controller (ZC) to the backup core in the Unified Network Configurator (UNC). This option allows you to perform some maintenance tasks and testing.

## 7.5.1.1 Changing the Zone Controller Redundancy State in the UNC

Perform this procedure to change the Zone Controller (ZC) redundancy state in the Unified Network Configurator (UNC).

**Procedure:**

1. From the Network Management (NM) client, double-click the **Unified Network Configurator**.
2. From the logon dialog box, log on to the EMC Smarts™ Network Configuration Manager.

   See “Logging in to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator User Guide*.

   Contact your system administrator for the appropriate username and password.
3. From the **Dashboard** window, in the **navigation** pane, select **Networks** → **Astro 25 Radio Network**.
4. From the list of available options, expand **Devices**.
5. Right-click on the selected zone controller.

   **Step example:** To set the state of ZC1 in zone 1, select **zc01.zone1**.
6. From the menu, select **Quick Commands**.
7. From the sub-menu, select **Set Redundancy State**.

   | If… | Then… |
   |---|---|
   | **If you want to set the redundancy state to Active,** | perform the following actions:<br>**a** Enter `1` in the text field.<br>**b** Click **OK**.<br>⚠ **CAUTION:** Transition to **Active** causes the currently active zone controller to reset and sites to lose wide-area trunked operation. |
   | **If you want to set the redundancy state to Standby,** | perform the following actions:<br>**a** Enter `2` in the text field.<br>**b** Click **OK**. |
   | **If you want to set the redundancy state to User Requested Standby,** | perform the following actions:<br>**a** Enter `3` in the text field.<br>**b** Click **OK**.<br>⚠ **CAUTION:** Transition to **User Requested Standby** causes the active ZC to reset and another ZC in the Standby state to take over. Sites lose wide-area trunking. |

   A **Device Command Parameters** dialog box appears.
8. Verify the switchover was successful.

   See Verifying the ZC Status in the UNC on page 101.

### 7.5.1.2 Verifying the ZC Status in the UNC

Perform this procedure to verify the Zone Controller (ZC) status in the Unified Network Configurator (UNC).

**Procedure:**

1. From the Network Management (NM) client, double-click the **Unified Network Configurator**.
2. From the logon dialog box, log on to the EMC Smarts™ Network Configuration Manager. Follow procedure "Logging in to the EMC Smarts Network Configuration Manager" in the *Unified Network Configurator User Guide*.

   Contact your system administrator for the appropriate username and password.
3. From the **Dashboard** window, in the navigation pane, select **Networks**. Then expand **Astro 25 Radio Network**.
4. From the list of available options, expand **Devices**.
5. Right-click on the selected zone controller. For example, to see the redundancy state of ZC1 in zone 1, select **zc01.zone1**.
6. From the pop-up menu, select **Quick Commands**.
7. From the sub-menu, select **Get Redundancy State**.
8. From the **Device Command Parameters** dialog box, select the desired zone controller under **Devices** and read its **Requested HA State** under **Results**.

## 7.5.2 Voice Dual-Active Condition Recovery

A voice dual-active condition occurs when the InterZone links between the primary and backup cores are broken. This break occurs when Zone Controller 3 (ZC3) is activated due to missed heartbeat messages from ZC1, assuming ZC1 was the active ZC, and now two ZCs are active in two cores. Recovering from a Voice Dual-Active Condition shows the sequence of events to recover from the voice dual-active condition.

**IMPORTANT:** The voice subsystem recovers from dual-active scenarios automatically. However, the system should not remain in this condition. If possible, restore the InterZone link. If restoration is not feasible, and the preference is that sites enter site trunked operation rather than be controlled by a second active ZC in the backup core if the primary site link fails, set the backup core ZCs to **User Requested Standby** to ensure that all the sites in wide-area trunked operation are connected to the same ZC. See Changing the ZC Redundancy State in the UNC.

### 7.5.2.1 Recovering from a Voice Dual-Active Condition

Perform the following procedure to recover from a condition of voice dual active.

**Process:**

1. Decide whether to manually resolve the dual-active condition, or wait until it can be resolved automatically. If you decide to manually resolve the dual-active condition, proceed to step 2. Otherwise, proceed to step 3.
2. If links cannot be easily fixed, and it is your organizational preference that sites enter site trunked operation rather than be controlled by a second active Zone Controller (ZC), set the ZCs in one of the cores to **User Requested Standby** to ensure that all the sites in wide-area trunked operation are connected to the same ZC. Follow Changing the ZC Redundancy State in the UNC to set the ZCs in one core to **User Requested Standby** state.

**IMPORTANT:** Change the state of the ZC which is not active in the pair first. Then, change the state of the active ZC in the pair.

3 Restore connections between the primary and backup core. The ZC with the higher number of active channels remains active while the other ZC goes into the **Standby** state. For more information on resolving link failures, see InterZone Link Failure.

If any ZCs were set to the **User Requested Standby** state per Step 2, switch them to **Standby** after resolving the link failures. Follow Changing the ZC Redundancy State in the UNC to set the ZCs to **Standby**.

## 7.6 Data Switchover

This section describes the typical switchover and recovery processes of data-related components in a system with Dynamic System Resilience (DSR).

Table 5: Data Component Switchover Actions

| Component | Switchover |
|---|---|
| Packet Data Gateway (PDG) | Automatic – The switchover is automatic, unless configured otherwise (PDG set to **User Requested Standby** state). For details on user-initiated switchover, see Changing the PDG Redundancy State in the UNC. |

### 7.6.1 PDG Switchover

This section describes the switchover of Packet Data Gateways (PDGs) in a system with Dynamic System Resilience (DSR). For more detailed information on PDG switchover, see the “Rebooting the PDR” section of the *Packet Data Gateways Feature Guide*.

#### 7.6.1.1 Changing the PDG Redundancy State in the UNC

Perform this procedure to change the Packet Data Gateway (PDG) redundancy state in the Unified Network Configurator (UNC). A user-initiated switchover to the backup PDG is possible for maintenance or testing purposes.

**Prerequisites:** Follow Unified Event Manager (UEM) procedures to check the availability of the Packet Data Gateway before performing this procedure. Data Services may experience additional downtime post switchover if the Packet Data Gateway is in an Inoperable state before the switchover.

**Procedure:**

1 From the Network Management (NM) client, double-click the **Unified Network Configurator** icon on the desktop.

2 From the logon dialog box, log on to the EMC Smarts™ Network Configuration Manager.

See “Logging in to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator User Guide* manual.

Contact your system administrator for the appropriate username and password.

3 In the **Dashboard** window, in the navigation pane, select **Networks** → **Astro 25 Radio Network**.

4 From the list of available devices displayed, select **Devices**.

5 Right-click on the selected PDG.

6 From pop-up the menu, select **Quick Commands**.

7 From the submenu, select **Set Redundancy State**.

8 From the **Device Command Parameters** dialog box, select the appropriate option:

> **CAUTION:**
> Transition to Active causes the currently active PDG to reset.
>
> Transition to **User Requested Standby** causes the currently active PDG to reset and another PDG in the **Standby** state to take over.

| If… | Then… |
|---|---|
| **If you want to set the PDG redundancy state to Active,** | perform the following actions:<br>**a** Enter `1` in the text field.<br>**b** Click **OK**. |
| **If you want to set the PDG redundancy state to Standby,** | perform the following actions:<br>**a** Enter `2` in the text field.<br>**b** Click **OK**. |
| **If you want to set the PDG redundancy state to User Requested Standby,** | perform the following actions:<br>**a** Enter `3` in the text field.<br>**b** Click **OK**. |

9 Verify if the switchover was successful.

See Verifying the PDG Redundancy State in the UNC on page 94.

**Postrequisites:** For procedures on setting the PDG redundancy states through the PDG administration menu, see the following sections in the *Packet Data Gateways Feature Guide*:

- “Setting PDG to Active State”
- “Setting PDG to Standby State”
- “Setting PDG to User Requested Standby (URS) State”

## 7.6.2 PDG Dual-Active Condition Recovery

A Packet Data Gateway (PDG) dual-active condition occurs when two PDGs (one in the primary core and the other in the backup core) are active at the same time. If links between the primary and backup core have failed, the Packet Data Router (PDR) in the backup core stops receiving heartbeat messages. The Packet Data Router (PDR) in the backup core becomes active, while the PDG in the primary core remains active.

When the links are re-established, the active PDG is determined based on the number of sites connected to the PDG. The preferred active PDG is the one in the primary core. In a dual-active condition, the PDG counts the number of connected RF sites and the PDG with the highest number of RF sites remains active. If the number of sites is the same between the two PDGs, the lower numbered element remains active.

> **IMPORTANT:** The data subsystem recovers from dual-active scenarios automatically when the Heartbeat Authentication (HA) link is re-established between the primary and backup PDGs.

### 7.6.2.1 Recovering from a PDG Dual-Active Condition

This process describes the steps that occur when recovering from a Packet Data Gateway (PDG) dual-active condition.

**Process:**

1. Links between the primary and the backup core fail. The PDG in the primary core remains active.
2. After the Packet Data Router (PDR) in the backup core stops receiving heartbeat messages, it becomes active and activates the PDG in the backup core. Both PDGs are active simultaneously.
3. Links between the primary and the backup core are restored.
4. The PDG with the higher number of connected RF sites stays active, while the other PDG goes into Standby state. In case of a draw, the lower numbered element remains active.

## 7.7 Network Management Switchover

This section describes the typical switchover and recovery processes of network management components in a system with Dynamic System Resilience (DSR). Unlike the zone controllers and the Packet Data Gateways (PDGs), the network management servers, although redundant, do not fully support automatic switchovers. Network management failures and switchover do not affect voice operations.

Table 6: Network Management Component Switchover Actions

| Component | Switchover |
|---|---|
| Unified Network Configurator (UNC) | Manual – see Unified Network Configurator and User Configuration Server Switchover. |
| User Configuration Server (UCS) | Manual – see UCS Switchover. |
| Air Traffic Router (ATR) | Automatic – one ATR server application active in each core. |
| Zone Database Server (ZDS) | Automatic – see Zone Database Server Switchover on page 112. |
| System Statistics Server (SSS) | Automatic – both SSS applications are active by default. In case a user-initiated activation is necessary, see Enabling the SSS Server Application. |
| Unified Event Manager (UEM) | N/A – both UEMs monitor cores independently. |
| MOSCAD Network Fault Management (NFM) | N/A – both cores monitored independently. |
| Network Management (NM) applications | Manual – see Switching Over Network Management on page 104. |

### 7.7.1 Switching Over Network Management

Follow this process to restore network management services after a zone core failure.

**Prerequisites:**

1 The primary zone core has undergone a catastrophic failure.

2 The Unified Event Manager (UEM) in the backup core has reported communication alarms for servers in the primary core.

3 No connectivity exists for the Unified Network Configurator (UNC) pair and the User Configuration Server (UCS) pair to perform data synchronization.

4 The Zone Database Server (ZDS) in the backup core has lost its connectivity with the primary UCS.

**Process:**

1 Switch the backup UCS and UNC to the **Active** state. See:

- Switching Over the UCS
- Switching Over the UNC and the UCS

The backup ZDS connects to the newly active UCS. The backup Air Traffic Router (ATR) connects to the newly active UCS. The newly active System Statistics Server (SSS) connects to the newly active UCS.

**NOTICE:** If the backup SSS is not active all the time, manually enable it. See Enabling the SSS Server Application.

2 Launch the NM applications. See Restoring the NM Applications After a ZC Switchover on page 121.

The backup UEM reports site link failures and sites in site trunking. MOSCAD Graphical Master Computer (GMC) in the backup core reports communication alarms for all SDM3000 Remote Terminal Units (RTUs) and SDM3000 Network Translators (SNTs) in primary core.

**NOTICE:** An exception is SmartX and Legacy 9600 sites, that do not go into wide-area trunked operation with the backup core. Also Legacy 9600 sites do not go into wide-area trunked operation with the PDGs in the backup core.

3 Switch Zone Controller 3 (ZC3) to the **Active** state.

The links cycle from down to up and also remote site statuses change from site trunked operation to wide-area trunked operation. A typical switchover flooding of alarms occurs on the UEM.

4 Switch the backup PDG to the **Active** state.

Data services are restored. A typical switchover flooding of alarms occurs on the UEM.

## 7.7.2 Network Management Switchover User Impact

This table lists time and history loss associated with a switchover.

Table 7: Network Management Restore Time and History Loss

| Service | Allowed Maximum Outage | History Loss |
|---|---|---|
| Frequency Modulation (FM) Reporting | 5 minutes or less for Unified Event Manager (UEM). No restoration time if Network Manage- | None; redundant UEM has latest active alarm status and event history. |

*Table continued…*

| Service | Allowed Maximum Outage | History Loss |
|---|---|---|
| | ment (NM) client was connected to the redundant UEM. | |
| | None for MOSCAD Network Fault Management (NFM). | No loss for MOSCAD NFM. No synchronization between the Graphical Master Computers (GMCs) in the primary and backup core. |
| Infrastructure Control Manager (CM) | 60 minutes, from enabling the Unified Network Configurator (UNC) to the time that the administrator can make configuration changes and view configuration change history. | Based on the synchronization schedule configured for the system (30 minutes to 24 hours). No loss if no changes have been made or if the synchronization between the UNCs has been completed. |
| Subscriber CM | 60 minutes, from enabling the User Configuration Server (UCS) to the time that the administrator can make configuration changes and view configuration change history. | Based on the synchronization schedule configured for the system (30 minutes to 24 hours). No loss if no changes have been made or if the synchronization between the UCSs has been completed. |
| Performance Management | Up to 15 minutes for the Zone Statistics Server (ZSS). Up to 60 minutes for the System Statistics Server (SSS). The redundant SSS must be enabled and it may take up to 60 minutes before the SSS has collected records from all Air Traffic Routers (ATRs). | Your organization must back up statistics records; data lost depends on when the last backup occurred. |
| Lightweight Directory Access Protocol (LDAP) Database | Up to 4 hours, depending on the size of the LDAP database. One to two days to synchronize all consoles and Site Gateways (Conventional Channel Interface) with the LDAP database. See Impact to Console and Site Gateway (Conventional Channel Interface) for more details. | No loss. |

## 7.7.3 UNC and UCS Switchover

The Unified Network Configurator (UNC) and User Configuration Server (UCS) switchover is always user-initiated. The operator commands the active UNC and the active UCS to become disabled standby (now two standby UNCs and two standby UCSs are in the system) and then commands the UNC and UCS in other zone core to become active. If UNC and UCS in the primary core fail, the user activates the UNC and UCS in the backup core. Only one UNC and one UCS can be active at a time. UNC and UCS do not change to the active state when they detect another active UNC and UCS. After a switchover, the newly active UNC and UCS take over periodic polling of the network elements for the latest configuration data.

### 7.7.3.1 Switching Over the UNC and the UCS

Perform the switchover of the Unified Network Configurator (UNC) and the User Configuration Server (UCS) only if the zone that fails has collocated UNC and UCS.

**NOTICE:** A dependency exists between the UNC and the UCS. The UNC in a zone core works only with the UCS in the same core and both must be active. Failure of the UNC, the UCS, or both, requires a switchover to recover both services.

**Process:**

1. Back up the active UNC critical data. See “Centralized Backup and Recovery for PNM Server Applications” in the *Private Network Management Servers Feature Guide* for more details.
2. Synchronize active UCS and active UNC with their standby instances. See:
   - Synchronizing the Active and Standby UCS Databases on page 97
   - Synchronizing the Active and Standby UNC Databases on page 96
3. If possible, disable the currently active UNC and UCS server applications. See:
   - Disabling the Active UNC
   - Disabling the UCS
4. Enable the UNC and UCS server applications in the other zone core. See:
   - Enabling the Standby UNC
   - Enabling the Backup UCS
5. Back up the newly active UNC. See “Backing up and Restoring the UNC Database” in the *Private Network Management Servers Feature Guide*.

### 7.7.3.2 Disabling the Active UNC

Perform this procedure to disable the active Unified Network Configurator (UNC). This procedure applies to all switchover scenarios except for a complete UNC server failure. If logging in to the active UNC server is not possible, see Enabling the Standby UNC.

**Prerequisites:** In a system with Dynamic System Resilience (DSR), the proper state of operation of system-level network management peer servers is one server in the **Enabled** state and one server in the **Disabled Standby** state. Before you proceed, ensure that enabling one of the servers is intended.

**Procedure:**

1. Log on to the **UNC administration** menu of the currently active UNC. Follow procedure Logging on to Network Management Server Applications with SSH on page 92.
2. From the **Unified Network Configurator Administration** menu, select **Service Administration**.
3. From the **Service Administration** submenu, under **Unix Administration**, select **Manage System Redundancy and Resilience**.
4. From the **Manage System Redundancy and Resilience** submenu, select **Display DSR Status**.

   The DSR status is displayed.

   ```
   Display DSR Status  yyyy-mm-dd hh:mm:ss
   ---------------------------------------
   UNC Server State
     LOCAL:  Enabled, Reason: User Requested
     REMOTE: Disabled Standby, Reason: User Requested
   ```

```
UNC DSR Feature State
  LOCAL:  Enabled
  REMOTE: Enabled

UNC Synchronization State
  LOCAL:  Data In sync, Reason: Sync Succeeded
  REMOTE: Server capable of being synced by Active, Reason: This
server is a Standby server

UNC Last Successful DSR Synchronization Time (outgoing from)
  LOCAL:  2015-06-17 14:23:59
  REMOTE: 2015-06-17 01:37:50

UNC Versions
  LOCAL:  UNC-Astro-07.16.01.26-00
  REMOTE: UNC-Astro-07.16.01.26-00

  LOCAL = ucs-unc01.ucs, REMOTE = ucs-unc02.ucs
```

**5** Check the DSR Status message:

- Verify that an Active and Disabled-Standby UNC pair is on the system.
- Verify the Active and Disabled-Standby UNCs have a communication path and have the same secure keys (server state must not be Unknown).
- Verify the last successful synchronization time on both UNCs is satisfactory; they should be recent and must not be NEVER.

**IMPORTANT:** If the last successful synchronization time is NEVER, the configuration data on the active UNC has never been synchronized with the standby UNC. If you proceed and make the disabled standby UNC an active UNC, the configuration data on the currently active UNC is lost.

**6** Type `b` and press ENTER twice.

**7** From the **Unified Network Configurator Administration** menu, select **Application Administration**.

**8** From the **Application Administration** submenu, select **Manage Application Status**.

**9** In the **Manage Application Status** submenu, enter `Disable Application`. Press ENTER to disable the UNC application.

A message appears:

```
 The application will be disabled.
 Do you wish to continue? (y,n,?) [n]
```

**10** Enter `y` to continue.

The following messages appear informing about the progress:

```
Executing pre disable scripts
The application state is: Disabling
Executing post disable scripts
The application state is: Disabled Standby
```

**11** When the **Manage Application Status** menu appears, type `q` and press ENTER to close the menu.

**12** Type `exit`. Press **ENTER** to log out.

### 7.7.3.3 Disabling the Active UCS

Perform this procedure to disable the User Configuration Server (UCS). This procedure applies to all switchover scenarios except for a complete UCS server failure. If logging in to the active UCS server is not possible, go to Enabling the Backup UCS.

**Procedure:**

1. Log on to the UCS application as the administrator. Follow procedure Logging on to Network Management Server Applications with SSH on page 92.

   The **User Configuration Server Administration** menu appears.

2. On the UCS, verify that at least one successful Dynamic System Resilience (DSR) synchronization occurs.

   Perform procedure Verifying UCS Synchronization on page 98

3. If no DSR synchronization occurs on the UCS, invoke manual synchronization of UCS databases on the active UCS before disabling the UCS.

   Perform Synchronizing the Active and Standby UCS Databases on page 97

   **NOTICE:**
   If manual DSR synchronization operation fails to complete, continue with next step.

   If at least one successful DSR synchronization entry exists, continue with next step.

4. Select **Application Administration**. Press ENTER.
5. From the **Application Administration** menu, select **Manage Application Status**. Press ENTER.
6. From the **Manage Applications Status** menu, select **Disable Application**. Press ENTER.

   A message appears:

   ```
   The application will be disabled.
   Do you wish to continue? (y,n,?) [n]
   ```

7. Type `y`. Press ENTER.

   The following messages appear informing about the progress:

   ```
   Executing pre disable scripts
   The application state is: Disabling
   Executing post disable scripts
   The application state is: Disabled Standby
   ```

8. When the **Manage Application Status** menu appears, type `q` and press ENTER to close the menu.
9. Type `exit`. Press **ENTER** to log out.

### 7.7.3.4 Enabling the Standby UNC

Perform this procedure to enable the standby Unified Network Configurator (UNC).

**Prerequisites:** In a system with Dynamic System Resilience (DSR), the proper state of operation of system-level network management peer servers is one in the **Enabled** state and one in the **Disabled Standby** state. Before you proceed, ensure that enabling one of the servers is intended.

**Procedure:**

1 Log on to the UNC administration menu of the UNC that you want to make the new active UNC. Follow Logging on to Network Management Server Applications with SSH on page 92.

2 When the command prompt appears, type the corresponding number for **Application Administration**. Press ENTER.

3 In the **Application Administration** submenu, type the corresponding number for **Manage Application Status**. Press ENTER.

4 In the **Manage Application Status** submenu, type the corresponding number for **Enable Application**. Press ENTER to enable the UNC application.

**NOTICE:** Any error message means that the server was not enabled properly. You may also be asked to confirm enabling the standby UNC.

A list of started services appears, followed by a message:

```
The application state is: Enabled
```

5 Type the corresponding number for **Services Administration**. Press ENTER.

6 In the **Services Administration** menu, type the corresponding number for **Manage System Redundancy and Resilience**. Press ENTER.

7 In the **Manage System Redundancy and Resilience** menu, type the corresponding number for **Display DSR Status**. Press ENTER.

**IMPORTANT:** Verify that this UNC is active and the remote UNC is disabled.

A message appears:

```
Display DSR Status  yyyy-mm-dd hh:mm:ss
---------------------------------------
UNC Server State
  LOCAL:  Enabled, Reason: User Requested
  REMOTE: Disabled Standby, Reason: User Requested

UNC DSR Feature State
  LOCAL:  Enabled
  REMOTE: Enabled

UNC Synchronization State
  LOCAL:  Data In sync, Reason: Sync Succeeded
  REMOTE: Server capable of being synced by Active, Reason: This
server is a Standby server

UNC Last Successful DSR Synchronization Time (outgoing from)
  LOCAL:  2015-06-17 14:23:59
  REMOTE: 2015-06-17 01:37:50

UNC Versions
  LOCAL:  UNC-Astro-07.16.01.26-00
  REMOTE: UNC-Astro-07.16.01.26-00

  LOCAL = ucs-unc02.ucs, REMOTE = ucs-unc01.ucs
```

8 Press B twice to return to the Unified Network Configurator Administration menu.

9 If possible, synchronize the newly active UNC with the standby UNC. See Manual Synchronization of Active and Standby UNC Databases for details.

**10** Log out of this UNC.

The UNC is enabled. You can view the Configuration Change History and apply Infrastructure Configuration Changes within 60 minutes of the switchover. The newly active UNC uses the data from the last successful synchronization. For more information, see the *Unified Network Configurator User Guide*.

**Postrequisites:** Back up the newly active UNC. For details, see the “Backing up and Restoring the UNC Database” section of the *Private Network Management Servers Feature Guide*.

### 7.7.3.5 Enabling the Standby UCS

Perform this procedure to enable the backup User Configuration Server (UCS). When no active UCS is in the system, the disabled standby UCS is set to active. Only one UCS can be active at a time; a standby UCS does not change to the active state if it detects another active UCS. The newly active UCS uses the data from the last successful synchronization.

**Prerequisites:** In a system with Dynamic System Resilience (DSR), the proper state of operation of system-level network management peer servers is one in the **Enabled** state and one in the **Disabled Standby** state. Ensure that enabling one of the servers is intended.

**Procedure:**

1. Log in to the UCS server application as the administrator. Follow Logging on to Network Management Server Applications with SSH on page 92.
2. From the **User Configuration Server Administration** menu, select **Application Administration**. Press ENTER.
3. From the **Application Administration** menu, select **Manage Application Status**. Press ENTER.
4. From the **Manage Application Status** menu, select **Enable Application**. Press ENTER.

   **IMPORTANT:** Complete this step only if the other UCS is not available.

   An SA message may appear:

   ```
   Can not determine status of UCS in peer core.
   Do you wish to continue? (y,n,?) [n]
   ```

5. If an SA message appears, type `Y`. Press ENTER.
6. When the **Manage Application Status** menu appears, type `q` to close the menu.
7. Type `exit`. Press ENTER to log out.

The backup UCS is enabled. The logon prompt appears.

**Postrequisites:** After a switchover, users of Network Management (NM) client computers must launch the Provisioning Manager (PM) client for the newly active UCS. Also, the newly active UCS ensures the Unified Network Configurator (UNC) and Lightweight Directory Access Protocol (LDAP) services have the latest configuration data. The new UCS is active within 60 minutes of the switchover.

### 7.7.3.6 Impact to Console and Site Gateway with Conventional Channel Interface

Upon a User Configuration Server (UCS) switchover, the Lightweight Directory Access Protocol (LDAP) server is automatically rebuilt. Rebuilding the LDAP server causes the LDAP database to be downloaded to the LDAP clients, the MCC 7500 VPM Dispatch Consoles and Site Gateways

(Conventional Channel Interface). During the database rebuilding and downloading process, the user cannot change configuration data; for example, talkgroups, subscribers, or channels. The time required to complete this process depends on the number of records and the number of consoles, and can take many hours for a large system.

After a UCS switchover, restart the dispatch console. When a user logs on for the first time after the UCS switchover and before the download is complete, they may not be able to make calls to all the radios in the zone.

## 7.7.4 Zone Database Server Switchover

After the User Configuration Server (UCS) switchover to the other core, the Zone Database Server (ZDS) automatically switches over to the active UCS. No user-initiated switchover for the ZDS is necessary.

⚠ **CAUTION:** Synchronization time for consoles after a UCS switchover depends on the number of console sites in the system.

For more information, see the *Private Network Management Servers Feature Guide*.

## 7.7.5 System Statistics Server Switchover

Depending on user needs, either one or both System Statistics Server (SSS) applications can be active in the system. If only one SSS application is active, the second SSS must be enabled manually.

### 7.7.5.1 Enabling the System Statistics Server Application

Perform this procedure to enable the System Statistics Server (SSS) application.

**Procedure:**

1. Log in to the SSS server application as the administrator.

   See Logging on to Network Management Server Applications with SSH on page 92.
2. At the command prompt, enter: `admin_menu`
3. In the **System Statistics Server Administration** menu, enter the corresponding number for **Application Administration**.
4. From the **Application Administration** menu, enter the corresponding number for **Manage Application Status**.
5. From the **Manage Application Status** submenu, enter the corresponding number for **Enable Application**.

   A message about the state of the peer server is displayed.
6. When the **Manage Application Status** menu appears, type `q` to close the menu.
7. To log out, enter: `exit`

The SSS server application is enabled and the logon prompt appears again.

### 7.7.5.2 Disabling the System Statistics Server Application

Perform this procedure to disable the System Statistics Server (SSS) application.

**Procedure:**

1. Log in to the SSS application as the administrator.

   See Logging on to Network Management Server Applications with SSH on page 92.
2. At the command prompt, enter the corresponding number for **Application Administration**.
3. From the **Application Administration** menu, enter the corresponding number for **Manage Application Status**.
4. From the **Manage Application Status** submenu, enter the corresponding number for **Disable Application**.

   A `Do you wish to continue?` message about the state of the peer server is displayed.
5. Enter: `y`

   Progress messages appear.
6. When the **Manage Application Status** menu appears, type `q` to close the menu.
7. To log out, enter: `exit`

The SSS server application is disabled and the logon prompt appears again.

## 7.7.6 Enabling the DSR Feature on the Network Management Server Applications

Perform this procedure to enable the Dynamic System Resilience (DSR) feature on the network management server applications. By default, the DSR feature is disabled on all Network Management (NM) applications.

**IMPORTANT:** If necessary (for example, because of hardware replacement), this procedure should be performed only on disabled system-level NM server applications: Unified Network Configurator (UNC), User Configuration Server (UCS), System Statistics Server (SSS).

**Procedure:**

1. Log in to the server application as administrator. Follow procedure Logging on to Network Management Server Applications with SSH on page 92.
2. In the command prompt, type the corresponding number for **Services Administration**. Press ENTER.
3. From the **Services Administration** menu, select **Manage System Redundancy and Resilience**. Press ENTER.
4. From the**Manage System Redundancy and Resilience** submenu, select **Enable DSR Feature**. Press ENTER.

   The following message is displayed:

   ```
   The DSR feature has been enabled on this server.
   ```
5. Type `q` to close the menu.
6. Type `exit`. Press ENTER to log out.

   The login prompt appears.

## 7.7.7 Network Management Dual-Active Condition Recovery Process

When links between the primary and the backup core fail, the backup Zone Core (ZC) and Packet Data Gateway (PDG) become active automatically. During this condition, do not make any configuration changes.

In certain cases, configuration changes to sites or devices not connected to the active core may be necessary. During a dual-active scenario, an active Unified Network Configurator (UNC) might not be able to access the remote sites. If the UNC is not able to access the remote site, either activate the standby UNC to make configuration changes or wait for the dual-active scenario to end.

If the operator inadvertently enters dual-active condition, configuration management is impaired.

Table 8: Dual-Active Impact per NM Server Application

This table provides information on dual-active condition on the Network Management (NM) server applications.

| | Server | Impact |
|---|---|---|
| Zone-level | Air Traffic Router (ATR) | No impact |
| | Zone Database Server (ZDS) | No impact |
| | Zone Statistics Server (ZSS) | No impact |
| | Unified Event Manager (UEM) | No impact |
| System-level | UNC | In dual-active condition, the system can be configured through the UCS and UNC. However, changes can be lost if the server where configuration was done is disabled and subsequent synchronization is performed. |
| | User Configuration Server (UCS) | |
| | System Statistics Server (SSS) | No impact, if active in both cores (depends on configuration). During dual-active condition, SSS might not be able to access all necessary devices to provide a complete report. |
| | InfoVista | No impact, if active in both cores (depends on configuration). During dual-active condition, InfoVista might not be able to access all necessary devices to provide a complete report. |

### 7.7.7.1 Resolving the Network Management Dual-Active Condition

Perform this process to enable the backup User Configuration Server (UCS)/Unified Network Configurator (UNC). Perform manual resolution only if configuration changes to the core without an active UCS/UNC must be made. Before manually switching the Network Management (NM) servers, try to resolve the link failure. After the changes are made in the backup core, the backup UCS/UNC pair should remain active until the links are resolved.

**Prerequisites:** For this process to be necessary, the following conditions have occurred:

- Connections between the primary and backup core failed. Both Unified Event Managers (UEMs) report communication failures of the servers in the other core. Additionally, the primary UEM reports data synchronization failure.

- Zone Controller 3 (ZC3) and the Packet Data Gateway (PDG) in the backup core become active. ZC and PDG dual-active scenarios occur.

**Process:**

1. If you expect the link failure to take an extended time to resolve and configuration changes are required in the backup core, disable the primary UCS and UNC.

   See “Disabling PNM Server Applications” in the *Private Network Management Servers Feature Guide*.

2. Enable the backup UCS and UNC.

   See “Enabling PNM Server Applications” in the *Private Network Management Servers Feature Guide*.

   The backup UEM reports alarms on data synchronization. The backup Zone Database Server (ZDS) now connects to the newly active UCS. The backup UEM shows sites in site trunked operation in the ZC view, but in wide-area trunked operation in the site view. The primary UEM shows sites in wide-area in both views.

### 7.7.7.2
## Recovering from Network Management Dual-Active Condition

Perform this procedure to recover from a network management dual-active condition. After communication is restored, perform data synchronization so that both cores are updated. This synchronization overwrites configuration data on the inactive User Configuration Server (UCS)/Unified Network Configurator (UNC) pair. Afterwards, decide if you want the currently active pair to remains active. Follow this process after unintentionally enabling two UCS/UNC pairs in the system.

**Prerequisites:** Connections between the zone cores are restored. Both Unified Event Managers (UEMs) report communication alarms, which are then cleared.

**Process:**

1. Because both UNCs are active, back up both UNCs.

   See “Backing up and Restoring the UNC Database” in the *Unified Network Configurator User Guide*.

2. Determine whether you want the UNC/UCS pair in the primary or the backup core to be active. After performing the data synchronization, configuration data on the inactive UCS/UNC pair is overwritten.

   When deciding which pair to keep active, consider which pair of servers has the most relevant data that should be kept.

3. Disable the UNC and UCS which become the backup UNC/UCS. If both UNC/UCS pairs have been disabled, enable the servers that become the active servers. See:

   - Disabling the Active UCS on page 109
   - Disabling the Active UNC on page 107
   - Enabling the Standby UCS on page 111
   - Enabling the Standby UNC on page 109

4. Disable then enable the Dynamic System Resilience (DSR) feature on the inactive UNC.

   See Enabling the DSR Feature on the Network Management Server Applications on page 113.

5. Perform data synchronization from the active UNC/UCS pair to the newly inactive pair. See:

   - UNC Synchronization on page 95
   - UCS Synchronization on page 97

Because the DSR feature was disabled then re-enabled on the inactive UNC, full synchronization is triggered on the UNC. To verify this synchronization, perform Verify the UNC Synchronization.

Full data synchronization occurs on the newly active UCS/UNC pair in the primary core to the disabled standby pair in the backup core.

6. Check the configuration data on the active UNC/UCS pair and trigger synchronization on the fixed network equipment data needed.
7. The Zone Database Server (ZDS) automatically connects to the active UCS.
8. The Air Traffic Router (ATR) administrator can trigger synchronization for subscriber aliases and talkgroup data.

## 7.8 IP Services Switchover

This section describes typical failure scenarios for IP service-related components and how the system recovers from these failures.

Table 9: IP Services Recovery Method

| Service | Recovery Method |
|---|---|
| Antivirus | Automatic – Clients check periodically for the nearest available server; when one server is unreachable, they connect to the other. |
| Active Directory | Automatic – A transparent switchover to the redundant domain controller; no interruption in authentication and identity management services for Active Directory and RADIUS clients. |
| Centralized Event Logging | N/A – Both servers are independent; clients can reconnect to the working server. |
| RADIUS authentication | Network Policy Server (NPS) RADIUS – A transparent switchover to the RADIUS service on the backup domain controller. |
| Backup and Restore | N/A – Both servers are independent; clients can reconnect to the working server. |
| Firewall Management | N/A – No switchover; the application can be reinstalled on another server. |
| Network Time Protocol | Devices in the backup core continue to use backup core Network Time Protocol (NTP) sources.<br>Site-levels clients with a primary NTP server in a failed primary core reconnect to the secondary NTP server in the backup core. During a prolonged outage, manual reconfiguration may be desired to restore NTP redundancy. |
| InfoVista | Manual – The operator must switch over to the backup InfoVista. See Primary and Backup InfoVista Server Settings. |
| Mobile Computer Applications | N/A – Session lost; session re-establishment is necessary. See Mobile Computer Application. |

## 7.8.1 Switching over IP Services

Use this process to perform IP services switchover. The IP services switchover process is not fully automatic and requires user intervention.

**Process:**

1. Switch over to the backup InfoVista server, see procedure Promoting the Backup InfoVista Server to Primary.
2. During a prolonged outage, reconfiguration of Network Time Protocol (NTP) clients may be necessary. See procedure Network Time Protocol Post-Switchover Reconfiguration.

## 7.8.2 InfoVista Switchover

InfoVista provides statistics information for site, network, and data subsystem equipment. The optional, redundant InfoVista server is not always active due to the nature of the statistics it collects. Manual intervention is required to complete a switchover. During a primary core failure, the backup InfoVista server in the backup core must be manually set to Primary status.

### 7.8.2.1 Primary and Backup InfoVista Servers Settings

Assigning the Primary and Backup Roles to the InfoVista Servers provides instructions on how to distribute the primary and backup roles between the InfoVista servers on the systems with the Dynamic System Resilience (DSR) feature.

**NOTICE:** This functionality is not supported on M1 DSR systems.

Contact Motorola Solutions Support Center (SSC) to restore the database when the primary InfoVista server comes back online. See the “Disaster Recovery” section in the "InfoVista Troubleshooting" chapter of the *InfoVista User Guide*.

#### 7.8.2.1.1 Assigning the Primary and Backup Roles to the InfoVista Servers

Perform this procedure to assign primary and backup roles to InfoVista servers.

**Process:**

1. Follow the steps in “Running the Discovery Script Manually” in the *InfoVista User Guide* to run the InfoVista discovery script.

   **IMPORTANT:** Perform the discovery tasks in clear mode. Remove any security setting on the SNMPv3 interface for the discovery script to create an instance of that device (must be running in clear mode).

2. Follow the desired option:
   - If you want to activate the InfoVista services on the primary server, see Promoting the Backup InfoVista Server to Primary on page 118.
   - If you want to step the InfoVista services on the primary server and activate them on the backup server, see Changing the Primary InfoVista Server to the Backup on page 118.

### 7.8.2.1.2 Promoting the Backup InfoVista Server to Primary

Perform this procedure on the InfoVista server that originally was the backup InfoVista server to promote it to being the primary InfoVista server.

**IMPORTANT:** This procedure applies only to M3 Dynamic System Resilience (DSR) systems. It does not apply to M1 DSR systems.

**Procedure:**

1. Perform all the installation steps to configure the InfoVista software.

   **IMPORTANT:** Do not run discovery scripts until the server configuration is complete.

2. From **Start**, open **Control Panel**.
3. In the **Control Panel** window, double-click **Services**.
4. In the **Services** window, right-click the status field of the following services. Select **Start** for:
   - **InfoVista Database Server**
   - **InfoVista Server iv1**
   - **InfoVista VistaCockpit Management Agent**
   - **InfoVista Port Mapper**
5. From **Start**, open **Command Prompt**.
6. At the prompt, navigate to: `D:\IV-Customizations\Discovery`
7. Enter: `ivcmd ivdisc-`***<XX>***`.ivc`

   where ***<XX>*** stands for the day of the month you execute the script; the allowed range is 01 to 31.
8. At the prompt, enter an administrator username and the respective password.

   Ignore the `The system cannot find the file specified` message.

The prompt returns. The Backup InfoVista Server is now activated to become Primary.

### 7.8.2.1.3 Changing the Primary InfoVista Server to the Backup

Perform this procedure to change the primary InfoVista server to be the backup server and only if the current primary InfoVista server was previously the backup server.

**Procedure:**

1. Open **Services**:
   - **a** From **Start**, click **Search**.
   - **b** In the search field, type in `administrative`
   - **c** Click **Administrative Tools**.
   - **d** In the **Administrative Tools** window, double-click **Services**.
2. In the **Services** window, right-click the status field for each of the following InfoVista services. Select **Stop** for each service:
   - **InfoVista Database Server**
   - **InfoVista Server iv1**

- **InfoVista VistaCockpit Management Agent**
- **InfoVista Port Mapper**

3 Ensure that the status fields of the services listed in step 2 are blank.

The server returns to the original backup mode.

4 From the **Start** menu, select **Settings** → **Control Panel**. Double-click **Scheduled Tasks**.

5 In the **Scheduled Tasks** folder, right-click **Auto-Discovery**.Select **Delete** to delete the scheduled auto-discovery tasks on the backup InfoVista server.

The backup InfoVista server stops performing the auto-discovery jobs not to create unnecessary traffic on the network.

## 7.8.3 Mobile Computer Applications

Mobile computer applications normally establish a session with a Customer Enterprise Network (CEN) server application by either logging on or using some other transaction that associates the mobile computer application with its IP address and some other identifier like a user name or ID. This technique may or may not include a password. Because the IP address of the radio must change following Customer Network Interface (CNI) switchover, the session IP address association is no longer valid. Therefore, mobile applications must establish a new session with the new IP address. Mobile applications can detect the need to establish a new session by registering with the radio to receive a Simple Network Management Protocol (SNMP) trap that indicates when CNI switchover has occurred.

## 7.9 Completing a Primary Core Switchover

Follow this process to recover from a primary core switchover.

This process lists the actions that occur automatically during a primary core switchover as prerequisites to the steps that require manual intervention. The process itself contains the manual steps which must be followed to successfully complete the primary core switchover along with references to the process to be followed for each.

Depending on the site type, the automated events that occur during this process can occur at different times. This automation does not affect the manual steps that must be performed.

**Prerequisites:** The following events must have occurred as part of the primary core switchover before any user intervention is required:

1 The Unified Event Manager (UEM) in the backup core reports communication alarms for servers in the primary core.

2 In an M3 Dynamic System Resilience (DSR) system, site controllers detect the link failure and send link requests to both Zone Controller 1 (ZC1) and ZC2 in the primary core. In an M1 DSR system, site controllers detect the link failure and send link requests to ZC1 only. The ZCs in the backup core become active.

3 The backup core ZC performs the Heartbeat Authentication (HA) algorithm to determine the new active ZC.

4 The backup core Packet Data Router (PDR) fails to detect heartbeat messages from the PDR in the failed primary core, and the backup Packet Data Gateway (PDG) becomes active.

5 The InterZone link is re-established. Other zones establish communication with the active ZC in the backup core of the zone with the primary core failure.

6 In the case of an M3 DSR system, the Console Site and Site Gateway (Conventional Channel Interface) clients send link requests to ZC3 and ZC4 and establish links with the newly active ZC3. ZC3 receives mobility data from the remote sites and replicates the data to the standby ZC4.

**Process:**

1. Switch the backup User Configuration Server (UCS) to active state. See User Configuration Server Switchover.

   The backup Zone Database Server (ZDS) connects to the new active UCS.

2. Switch the backup Unified Network Configurator (UNC) to active state. See Unified Network Configurator and User Configuration Server Switchover.
3. If the Private Radio Network Management (PRNM) Suite was connected to the primary core, log out then log on using the backup Air Traffic Router (ATR) IP. See Opening the PRNM Suite of Applications.

   The backup ATR connects to the newly active UCS.

4. Manually launch the Network Management (NM) applications. See Restoring NM Applications After a ZC Switchover.
5. If the backup System Statistics Server (SSS) is not active, enable it. See Enabling the Standby UCS on page 111.

   The backup SSS connects to the newly active UCS. The backup UEM reports site link failures and sites in site trunked operation. The Graphical Master Computer (GMC) in the backup core reports communication alarms for SDM3000 Remote Terminal Units (RTUs) and SDM3000 Network Translators (SNTs) in the primary core. Links cycle from down to back up, and wide-area trunked operation is restored.

6. Enable the backup InfoVista. See InfoVista Switchover.

## 7.10 Link Failures and Recovery

This section describes typical link failure scenarios and how the system recovers from these failures. This operation is normal Dynamic System Resilience (DSR) in a situation when links have failed.

**IMPORTANT:** Link failures affect other services and can lead to a dual-active condition. Restoring the failed links should always be the top priority.

### 7.10.1 Dual-Active Condition

For information on dual-active condition recovery of Dynamic System Resilience (DSR) subsystems, see the following:

- Voice Dual-Active Condition Recovery Process
- PDG Dual-Active Condition Recovery Process
- Network Management Dual-Active Condition Recovery Process

#### 7.10.1.1 Dual-Active Condition and Other Zones

The Zone 1 active Zone Controller (ZC) (Z1 ZC1) is in the primary core. A failure of both exit routers in the Zone 1 primary core or Zone 1 backup core occurs. If the Zone 2 active ZC (Z2 ZC1) is in the same master site as Zone 1 backup core, Zone 2 loses connection with the active Z1 ZC1. This exit router failure causes a dual-active condition where Z1 ZC3 becomes active, while Z1 ZC1 is also active.

After Z1 ZC3 becomes active, the active Z2 ZC1 establishes a link with it. When the dual-active condition is resolved and Z1 ZC3 becomes standby again, the active Z2 ZC1 determines its logical link to Z1 ZC3 is down, and sends link re-establishment requests to all the ZCs in Zone 1. Because Z1 ZC1 is active, Z2 ZC1 automatically establishes connection with it.

### 7.10.2 Remote and InterZone Site Link Failure and Recovery

Due to a single point of failure, both the remote site link and InterZone link can fail simultaneously. The remote site detects the logical link failure and sends link requests to the same Zone Controller (ZC) broadcast IP addresses in the current (primary) master site. An RF site probably detects link failure before transport reroutes the traffic.

The routers detect the failed path and route the link requests through other InterZone paths on the WAN. The logical link (active and inactive connections) goes through the InterZone path.

Transport can route automatically. However, site trunked operation probably occurs, especially for RF sites.

The same steps apply to link failure of all three types of remote sites: RF site, console site, and Site Gateway (Conventional Channel Interface).

## 7.11 Post-Switchover Clean-up

This section contains procedures to complete after a core switchover has occurred.

### 7.11.1 Restoring the NM Applications After a ZC Switchover

Follow this process to restore Network Management (NM) applications after a Zone Controller (ZC) switchover.

If both ZCs (primary and redundant) fail in the primary core, an automatic switchover to the backup core occurs. Call processing failure impairs the operation of the following applications in the failed core:

- ZoneWatch
- Air Traffic Information Access (ATIA) Log Viewer
- Dynamic Reports
- Historical Reports

The User Configuration Server (UCS), Unified Event Manager (UEM), Unified Network Configurator (UNC), Zone Database Server (ZDS) applications remain fully operational after the call processing switchover and do not require enabling on the backup core.

**Process:**

1. Enable the ZoneWatch application in the backup core. See the “Starting ZoneWatch Application” in the *ZoneWatch User Guide*.
2. Enable the ATIA Log Viewer application in the backup core. See “Viewing ATIA Logs” in the *ATIA Log Viewer User Guide*.
3. Enable the Dynamic Reports application in the backup core. See “Starting the Dynamic Reports Application” in the *Dynamic Reports User Guide*.

4 Enable the Historical Reports application in the backup core. See “Starting, Selecting, and Outputting Historical Reports” in the *Historical Reports User Guide*.

## 7.11.2 Cleaning up Air Traffic Router Databases

Both Air Traffic Router (ATR) server applications are always active. However, only the ATR in the core with the active Zone Controller (ZC) receives call activity information. The ATR in one core does not receive updated information from the ATR in the other core. As a result, the ATR in the core without the active ZC contains outdated information regarding events such as radio affiliations and Radio Control Management (RCM) commands.

**IMPORTANT:** When a double switchover of the ZCs occurs (from primary core to backup, and back to primary), the affiliation display associated with the primary core shows old affiliation data and the RCM contains history of unsuccessful commands. This stale information may cause confusion. To eliminate the problem, the ATR database can be manually cleared. After a ZC switchover occurs, and the active ZC is now at the alternate core, clear the database of the ATR connected to the previously active ZC.

**Prerequisites:** Ensure that the ATR is disabled. See "Viewing the PNM Server Status" in the *Private Network Management Servers Feature Guide* and, if needed, perform "Disabling PNM Servers Applications" in the *Private Network Management Servers Feature Guide*.

**Procedure:**

1 Log in to the ATR server application.

   See Logging on to Network Management Server Applications with SSH on page 92.

2 When the command prompt appears, type the corresponding number for **Services Administration**. Press **ENTER**.

3 From the **Services Administration** submenu, select **Manage System Redundancy and Resilience**. Press **ENTER**.

4 From the **Manage System Redundancy and Resilience** submenu, select **Pending ATR Data Cleanup**. Press **ENTER**.

The database is cleaned up and a message is displayed indicating that the status of the server is disabled and the cleanup has completed.

## 7.11.3 Network Time Protocol Post-Switchover Reconfiguration

Because it is a complicated process, perform Network Time Protocol (NTP) switchover only if the primary core is not available for an extended time. If a primary core fails, the devices in the backup core continue to use backup core NTP sources. Site-level clients with a primary NTP server in a failed primary core reconnect to the secondary NTP server in the backup core. If a prolonged core failure occurs, manual reconfiguration may be necessary for restoring NTP redundancy.

**IMPORTANT:** If a prolonged primary core outage occurs, re-configure NTP only if you have a clear understanding of the implications and effort involved. If you need assistance, contact the Motorola Solutions Support Center (SSC).

Table 10: Post-Switchover NTP Reconfiguration

This table contains a list of devices and their respective reconfiguration methods.

| NTP Element | Reconfiguration Method |
|---|---|
| Firewall | See "Configuring NTP on the Fortinet Firewall Manager" in the *Fortintet Firewall Manager User Guide*. |
| Zone Core Protection (ZCP) Firewall | |
| Terminal Server | Configuration/Service Software (CSS), see NTP Reconfiguration of Site Devices with the CSS on page 123. |
| MCC 7500 VPM Dispatch Console | |
| Border Gateway, Peripheral Router, Demilitarized Zone (DMZ)/SAA Ethernet Switch | |
| Conventional GCP 8000 Site Controller (CSC) | |
| Site Controller (excluding HPDSC which has its own GNSS module) | |
| Border Gateway | |
| Site Devices: Routers (Non-Simulcast: Site, Network Management (NM), NM Dispatch, Console, Control Room, Site Gateway (Conventional Channel Interface)) | |
| Site Comparator | |
| Simulcast Devices: Prime Site Gateway, SubSite Gateway, SubSite Switch | |

### 7.11.3.1 NTP Reconfiguration of Site Devices with the CSS

If the primary core is unavailable for an extended time, Network Time Protocol (NTP) redundancy is lost (although site devices still point to the local TRAK colocated at the RF site). RF site equipment that references NTP servers in two cores, Virtual Management Servers (VMSs), requires reconfiguration if an extended core failure occurs to restore redundancy.

To restore NTP redundancy, replace the hostname of an NTP source from the primary core with an NTP source hosted on one of the VMS machines in the backup core. See “NTP Servers and Their Time Sources” in the Appendix of the *Network Time Protocol Server Feature Guide*. For a detailed reconfiguration procedure, see “NTP Server Settings” in the *CSS Core Online Help*.

Alternately, RF site equipment that references only other RF site equipment, or references only the RF site TRAK servers, do not require reconfiguration.

## 7.11.4 Synchronizing Configuration Changes

Synchronize all configuration changes between the primary and backup cores. After a switchover and before switching back from the backup core to the primary core (when restored), any configuration changes made in the backup core during the primary core outage must be synchronized with the primary core. If no configuration changes were made in the backup core equipment during the primary core outage, no synchronization is necessary.

Table 11: Post-Switchover Configuration Synchronization

This table lists the components that require synchronization.

| Component | Synchronization |
|---|---|
| Network equipment | Any changes made to network equipment using the backup Unified Network Configurator (UNC) must be transferred to the primary UNC as well. See the *Unified Network Configurator User Guide*. |
| Network Management (NM) Server Applications | If some changes were made in the backup UNC/User Configuration Server (UCS), perform data synchronization from backup to primary. See:<br>• UNC Synchronization on page 95<br>• UCS Synchronization on page 97 |

## 7.11.5 Customer Enterprise Network Applications Impact After a Switchover

The Customer Enterprise Network (CEN) applications use the primary Customer Network Interface (CNI) to communicate with the Radio Network Infrastructure (RNI). CNI traffic is rerouted due to failures of any CNI component. Also, CNI traffic is routed back to the original path when the failures are repaired. Some of these applications use a connection-oriented session, Transmission Control Protocol (TCP), while others use a connectionless session, User Datagram Protocol (UDP). The CNI firewall handles these sessions differently.

The CNI firewall is a stateful firewall that passes TCP messages only if the firewall created an internal, monitoring, state machine when the TCP session was established. When a CNI switchover occurs and the TCP session is routed through the alternate firewall, that firewall has no knowledge of the TCP session and must drop the messages. Because UDP is connectionless, the alternative firewall is allowed to pass these messages after a CNI switchover.

Because subscriber radios receive a different IP address after a CNI switchover, mobile computer applications that require session establishment with a CEN application server lose this session following a CNI switchover. Mobile computer applications must detect CNI switchover by registering for a Simple Network Management Protocol (SNMP) trap from the radio and take appropriate action to re-establish the session following CNI switchover. See the *Motorola ASTRO Trunked Integrated Voice and Data Communication System Application Design Guide* and *Motorola ASTRO High Performance Data Communication System Application Design Guide*.

### 7.11.5.1 CEN Switchover Impact on Your Organization

This table lists switchover impact for the Customer Enterprise Network (CEN) applications.

Table 12: Customer Enterprise Network Switchover Impact

| Component | Impact |
|---|---|
| Computer Aided Dispatch Interface (CADI) | CADI session lost, events dropped by the firewall until the session is re-established. |

*Table continued…*

| Component | Impact |
|---|---|
| Air Traffic Information Access (ATIA) | No effect. |
| Over-the-Ethernet-Keying (OTEK)/Key Management Facility (KMF) | OTEK session lost; automatic recovery in 1 to 8 hours (depending on Inactivity Timer settings). |
| Text Messaging Service (TMS) | Console cohabited Fixed Text Messaging client service lost; manual re-logon necessary. |
| Unified Event Manager (UEM) Digital Notification | Messages dropped. |
| UEM North Bound Interface (NBI) | No effect. |

### 7.11.5.2 CADI/ATIA

Because Computer Aided Dispatch Interface (CADI) uses the Transmission Control Protocol (TCP), after a Customer Network Interface (CNI) switchover occurs, the session is lost. The CADI client in Customer Enterprise Network (CEN) can detect the need to log on again (which re-establishes the session) when commands to the CADI server fail. Additionally, the *Computer-Aided Dispatch Interface (CADI) API Programmer Guide* explains how to detect the CADI session has been lost, without waiting for commands to fail. Until the CADI session is re-established, the firewall drops CADI events from the server.

The Air Traffic Information Access (ATIA) application uses User Datagram Protocol (UDP) protocol and is not impacted.

### 7.11.5.3 OTEK/KMF

Since Over-the-Ethernet-Keying (OTEK) uses the Transmission Control Protocol (TCP), the session between the Key Management Facility (KMF) and the MCC 7500 VPM Dispatch Console is lost when the Customer Network Interface (CNI) switch occurs. For automatic recovery in an acceptable time, adjust the OTEK Inactivity Timer based on the Crypto Period for voice encryption keyset changeover.

The default OTEK Inactivity Timer is 8 hours, but can be set as short as 1 hour. OTEK capability for a console can be manually recovered by logging on/off the console (with temporary loss of console functions). When the primary CNI is restored, the Dynamic System Resilience (DSR) transport switches back and the recovery procedures must be performed again.

### 7.11.5.4 Text Messaging Service

The Text Messaging Service (TMS) uses the Transmission Control Protocol (TCP) protocol. When the Customer Network Interface (CNI) is switched over, the Fixed Text Messaging client on a dispatch console loses its session with the TMS server in the Customer Enterprise Network (CEN). To restore text messaging service, users must log off then log on. When the primary CNI is restored, the transport switches back and users must log off then log on again.

### 7.11.5.5 UEM Digital Notification

Digital Notification uses Transmission Control Protocol (TCP). The Unified Event Manager (UEM) is configured to send e-mail notifications using SMTP protocol through the Customer Network Interface

(CNI) firewall to your organization mail server in the Customer Enterprise Network (CEN). When the CNI is switched over, the session is lost. In this case, the UEM may get a time-out on the current e-mail message, which is logged internally for service technicians. The dropped e-mail messages are not sent again. Subsequent e-mail requests are sent through the backup CNI firewall.

### 7.11.5.6 UEM Northbound Interface

Northbound Interface (NBI) uses the User Datagram Protocol (UDP). The NBI from Unified Event Manager (UEM) to your organization third-party Manager of Manager (MoM) is not affected by a Customer Network Interface (CNI) switchover.

## 7.11.6 MCC 7500 VPM Dispatch Console Switchover

After a Dynamic System Resilience (DSR) Zone Controller (ZC) switchover from one core to another (that is, from the primary core to the backup core or the backup core to the primary core), an MCC 7500 VPM Dispatch Console user can make trunked calls to the majority of radios in the zone within 35 seconds of the switchover. However, to make these calls, the old standby ZC (the new active ZC) must have been in **Standby** state for at least 90 minutes before the switchover, and the console is in a ready condition (the console talkgroups have all been affiliated, which is indicated by the absence of red Xs).

If the new active ZC had been in **Standby** state for less than 90 minutes before the switchover, and the Unified Event Manager (UEM) indicates that data replication to the new active ZC is incomplete, console site re-affiliation and RF site mobility upload may have to occur before a dispatch console user can talk to the majority of radios in the zone. Depending on how incomplete the ZC-to-ZC replication was before the switchover, a dispatch console user may have to wait up to 7.2 minutes after a ZC switchover (for a zone with 64,000 radios) before they can talk to majority of radios in the zone. Because the zone is designed to function with one ZC in **Active** state and three ZCs in **Standby** state, this latter scenario is unlikely to occur.

### 7.11.6.1 Site Gateway (Conventional Channel Interface) Switchover

After a Dynamic System Resilience (DSR) Zone Controller (ZC) switchover from one zone core to another (that is, from the primary core to the backup core or the backup core to the primary core), a Site Gateway (Conventional Channel Interface) is ready for conventional calls to the majority of channels in the zone within 35 seconds of the switchover. This timing is possible only if the old standby ZC (the new active ZC) had been in **Standby** state for at least 90 minutes before the switchover, and the Unified Event Manager (UEM) indicates that the Site Gateway (CCI)-ZC communication link is up.

If the new active ZC had been in **Standby** state for less than 90 minutes before the switchover, and the UEM indicates that data replication to the new active ZC is incomplete, RF site mobility upload may have to occur before a conventional call can be made to the majority of radios in the zone. Depending on how incomplete the ZC-to-ZC replication was before the switchover, a user may have to wait up to 7.2 minutes after a ZC switchover (for a zone with 64,000 radios) before they can make a conventional call to majority of radios in the zone.

Because the zone is designed to function with one ZC in **Active** state and three ZCs in **Standby** state, this latter scenario is unlikely to occur.

Chapter 8

# Dynamic System Resilience Maintenance

This chapter details periodic maintenance procedures relating to the Dynamic System Resilience feature.

## 8.1 Performance Monitoring for DSR Systems

This section describes Dynamic System Resilience (DSR) system performance monitoring methodology and tools. In a system with DSR, a backup server is provided for the Unified Network Configurator (UNC) and User Configuration Server (UCS) system-level applications. If the system contains more than two master sites, the UNC/UCS servers may be at any master site.

### 8.1.1 Historical Statistics Data Recovery

Your organization must protect itself against loss of historical statistics data with a plan in place to back up this data and to store it off-site. If a Zone Statistics Server (ZSS) or System Statistics Server (SSS) fails, the data can be retrieved from the off-site storage and restored to the repaired server.

The redundant ZSS and SSS servers do not share the historical statistics data collected. When a switchover occurs, the data is split between each of the ZSSs and the user must access both servers to get a complete picture of the reports. This situation also applies to the reports from the SSS.

If an interzone link fails, an SSS might not have historical statistics data from during the time of the failure.

### 8.1.2 ASTRO Inbound RF Quality Metrics Collection

Astro Inbound RF Statistics files generated by Site Controllers are collected by Zone Statistical Servers (ZSSes) in both primary and backup cores, and distributed between them. There are no strict distribution rules. However, if system is operating normally, the ZSS in a primary core gets the majority of this data. In case one ZSS falls into malfunction state, the redundant one takes over the responsibility of collecting all statistic files.

### 8.1.3 ZoneWatch Application

The ZoneWatch application uses call activity information forwarded by the Air Traffic Router (ATR). To view call activity, the user must launch ZoneWatch against the ATR located in the core with the active Zone Controller (ZC). The ZoneWatch application launched against the ATR in the inactive core shows no call activity. See ATR Database Clean-up.

### 8.1.4 Affiliation Display

The Affiliation Display application uses radio affiliation information forwarded by the Air Traffic Router (ATR). To view affiliation data, the user launches the Affiliation Display application against the ATR in the core with the active zone controller. The Affiliation Display in the active core does not present affiliation information from the inactive core. See ATR Database Clean-up.

## 8.1.5 CADI/ATIA Applications

The Computer Aided Dispatch Interface (CADI) and Air Traffic Information Access (ATIA) interface provides a means to connect third-party computers that use the radio system call activity information for billing, or as a way to connect third-party dispatch console equipment.

The CADI and ATIA interface is provided by the Air Traffic Router (ATR) server. In a zone configured for Dynamic System Resilience (DSR), one ATR is in the primary core and one in the backup core. Each ATR has its own CADI and ATIA interface resulting in two CADI and two ATIA interfaces. Only the CADI and ATIA interface on the ATR connected to the active zone controller has data reflecting call activity.

The third-party equipment can be designed to connect to the CADI or ATIA interface and resolve the fact that only one has actual call activity data. Alternately, if a zone controller switchover occurs to the other core a procedure can be in place to manually switch the CADI or ATIA connection.

The CADI or ATIA interface provides an indication for the CADI or third-party billing equipment that a zone controller switchover has occurred. This indication helps determine which CADI or ATIA interface has the actual call activity data.

## 8.1.6 Radio Control Manager

The Radio Control Manager (RCM) application has a number of functions useful in monitoring or controlling radios. Inbound events such as Emergency Alarm Display can be viewed on the RCM display. Outbound events such as Dynamic Regrouping and Radio Inhibit can be used to control radios using the system. The RCM functionality is provided by the Air Traffic Router (ATR). If the ATR connected to the active zone controller fails, RCM functionality is lost until either the failed ATR is repaired or a zone controller switchover occurs to the alternative core with a working ATR.

If a zone controller switches over to the alternative core, RCM functionality is provided by the ATR in the alternative core. The previous RCM display indicates the ATR hosting the session is no longer connected to the active zone controller. The RCM user must launch the RCM application against the ATR connected to the active zone controller.

The ATRs in the primary and backup cores do not share information. Therefore, the backup core ATR has no knowledge about RCM commands executed or emergency alarms received by the primary core ATR. Pending commands (for example, a Dynamic Regrouping command that has not yet been acknowledged by the radio) are lost after a switchover. A user can launch the RCM application against the ATR no longer connected to the active zone controller to retrieve this type of information and run reports if necessary.

# 8.2 Periodic Maintenance Switchover

To ensure the system with Dynamic System Resilience (DSR) can handle a catastrophic failure, use a periodic switchover test to verify that DSR and system backup functions are working as expected. Several layers of switchover testing are possible. For example, perform a switchover of the Zone Controller (ZC) and Packet Data Gateway (PDG) to ensure recovery at the application level. Configuration management can be switched over for separate testing of that aspect.

Perform a periodic manual switchover to test if the DSR feature is working properly. Perform a switchover test in the middle of the night or when traffic is low to minimize impact to radio users. Frequency depends on your organizational needs, but intervals of 6 or 12 months are advised.

Each subsystem can be switched over independently or a complete switchover to the backup core can be performed.

**IMPORTANT:** All switchovers, automatic and manual, implicate impact to user services (ranging from minor to major). See Dynamic System Resilience Operation on page 89 for more details on switchover procedures and how they affect the system.

Table 13: User-Initiated Switchover by Subsystem

This table lists the manual switchover procedures.

| Subsystem | Section |
|---|---|
| Full Switchover (all subsystems) | User-Initiated Switchover to the Inactive Core |
| DSR Voice | User-Initiated Voice Switchover to the Backup Core |
| DSR Data | User-Initiated Data Switchover to the Backup Core |
| Network Management | User-Initiated NM Switchover to the Backup Core |

8.2.1

## Performing a Switchover to the Inactive Core

Follow this process to perform a manual switchover to the inactive core. This process may be useful in the following cases:

- When the primary core recovers after a failure, you can switch over from the backup core to the primary.
- For maintenance, testing, or hardware replacement purposes, you can switch over from the primary core to the backup core and, if needed, back again.

**Process:**

1. Switch the zone controller in the backup core to the **Active** state. See Changing the ZC Redundancy State in the UNC.

   The currently active zone controller resets and enters **Standby** state.

2. Switch the Packet Data Gateway (PDG) in the backup core to the **Active** state. See Changing the PDG Redundancy State in the UNC.

   The currently active PDG resets and enters **Standby** state.

3. The Air Traffic Router (ATR) automatically receives call data from the active zone controller in the same core.
4. Launch Network Management (NM) applications in the core with the newly active zone controller. See Restoring the NM Application After a ZC Switchover.
5. Synchronize active UCS and active UNC with their standby instances. See:
   - Synchronizing the Active and Standby UCS Databases on page 97
   - Synchronizing the Active and Standby UNC Databases on page 96
6. Disable the currently active User Configuration Server (UCS) and Unified Network Configurator (UNC) server applications. See:
   - Disabling the UCS to disable the UCS.
   - Disabling the Active UNC to disable the UNC.

7. Enable the UCS and UNC server applications in the core with the newly active zone controller. See:
   - Enabling the Backup UCS to enable the UCS.
   - Enabling the Standby UNC to enable the UNC.

   **NOTICE:** Force initialization of all devices is a required step after the switchover. For details, see “Restoring Force Initialize Ability After a DSR Switchover” in the *Provisioning Manager User Guide*.
8. The Backup System Statistics Server (SSS) connects to the newly active UCS.

   **NOTICE:** If the backup SSS is not active, it must be enabled. See Enabling the Backup SSS Server Application.
9. Clean up the previously active Air Traffic Router (ATR) database. See ATR Database Cleanup.

## 8.2.2 Performing a Voice Switchover to the Backup Core

Follow this process to perform a manual call processing subsystem switchover to the backup core. Voice switchover in a system with Dynamic System Resilience (DSR Network Management (NM) services and data subsystem remains unaffected during zone controller switchover.) tests the backup core Zone Controllers (ZCs).

**Process:**

1. Change the backup ZC3 to the **Active** state. See Changing the ZC Redundancy State in the UNC.
2. When the backup ZC3 becomes active, the primary ZC1 switches to **Standby** state automatically.
3. Monitor the Unified Event Manager (UEM).

   If sites establish link with the newly active ZC3 in the backup core, they remain in wide-area trunking.

## 8.2.3 Performing a Data Switchover to the Backup Core

Follow this process to perform a user-initiated data subsystem switchover to the backup core. A data switchover in a system with Dynamic System Resilience (DSR) tests the backup Packet Data Gateway (PDG).
Voice call processing and Network Management (NM) services remain unaffected during data subsystem switchover.

**Process:**

1. Change the backup PDG to the `Active` state. See Changing the PDG Redundancy State in the UNC.
2. Once the backup PDG becomes active, the primary PDG resets and goes into `Standby` state.
3. Check the Unified Event Manager (UEM) for any data-related alarms. Verify the status of the backup PDG. See Verifying the PDG Redundancy State in the UNC.

8.2.4

## Performing a Switchover of the NM Subsystem to the Backup Core

Follow this process to perform a manual switchover of the Network Management (NM) subsystem to the backup core. An NM subsystem switchover tests the proper operation of backup NM server applications.
Voice call processing and data services remain unaffected during NM switchover.

**Process:**

1. Synchronize active UCS and active UNC with their standby instances. See:
   - Synchronizing the Active and Standby UCS Databases on page 97
   - Synchronizing the Active and Standby UNC Databases on page 96
2. Disable the currently active User Configuration Server (UCS) and Unified Network Configurator (UNC) server applications. See:
   - Disabling the UCS to disable UCS.
   - Disabling the Active UNC to disable UNC.
3. Enable the UCS and UNC server applications in the core with the newly active Zone Controller (ZC). See:
   - Enabling the Backup UCS to enable UCS.
   - Enabling the Standby UNC to enable UNC.
4. Shared core components include the redundant pair of LAN switches, exit routers, core backhaul switches, and gateway routers that provide transport and rendezvous point functions for both zones.
5. Back up the newly active UNC after switchover. See “Back Up a PNM Server Application to the Backup and Restore Application” in the *Private Network Management Servers Feature Guide*.
6. Enable the System Statistics Server (SSS) in the newly active core. See Enabling the SSS Server Application.

   Complete this step only if both SSS applications were not active in the system.
7. Launch the System Historical Reports application to verify that the data is being stored on the SSS.
8. Clean up the previously active Air Traffic Router (ATR) database. See ATR Database Clean-up.

This page intentionally left blank.

Chapter 9

# Dynamic System Resilience Troubleshooting

This chapter provides fault management and troubleshooting information relating to the Dynamic System Resilience feature.

## 9.1 DSR Troubleshooting Methodology

Dynamic System Resilience (DSR) fault management is handled at the zone level. This section contains a list of tools helpful in diagnosing and fixing the problem.

### 9.1.1 Network Troubleshooting Commands

Many device and network commands can be used to determine the status of different ports, links, routes, and devices in the network. See “Troubleshooting with Network Commands” in the *Master Site Infrastructure Reference Guide*.

### 9.1.2 Alarm Logs

Many of the devices in the radio network maintain local alarm logs. See “Local Logs and Administration Menus” in the *Master Site Infrastructure Reference Guide*.

### 9.1.3 Suggested System Monitoring

Table 14: System Monitoring

| Action to take | Frequency |
|---|---|
| Review critical system functions using the Unified Event Managers (UEMs) in both cores. Verify the following:<br>• All sites are in wide-area mode<br>• All zones are in InterZone trunking<br>• A control path exists between the zone controller and sites<br>• A control path exists between zone controllers (in multi-zone systems)<br>• A control path exists between the primary and backup zone core<br>See the *Unified Event Manager User Guide* for more information. | • At the beginning of your shift<br>• Periodically throughout your shift |

*Table continued…*

| Action to take | Frequency |
|---|---|
| Review logged alarms for both cores in the UEM. See the *Unified Event Manager User Guide* for more information. | |
| Monitor activities within each zone through the Dynamic Reports application. Check for high reject counts or other unusual site activity statistics. | Daily |
| Monitor system-wide statistics through the Historical Reports application. Check for any anomalies including high busy counts, unusually high or low volumes of certain calls or services, and surges of traffic within particular talkgroups. | Monthly, or as needed |
| Monitor the performance of network transport equipment by generating reports through InfoVista, if available. Check for prolonged overloading of critical network transport equipment. | Daily |
| Monitor the general status and activities for all sites through the ZoneWatch application. Verify that radio users are using the sites, check for any site or channel failures, and observe any unusual raw Air Traffic Information Access (ATIA) messages. | • At the beginning of your shift<br>• Periodically throughout your shift |

## 9.2 DSR Failure Troubleshooting

This section covers the symptoms, diagnosis, and corrective action for each major type/point of failure if the Dynamic System Resilience (DSR) feature in the system is not working as intended.

### 9.2.1 Loss of Voice Communication

This section describes what to do if voice communication is lost in a system with Dynamic System Resilience (DSR). The failure of any of the following hardware components may result in loss of voice communication:

- Both gateway routers (in the case of an M3 system) or the gateway router (in the case of an M1 system)
- Both core switches (in the case of an M3 system) or the core switch (in the case of an M1 system)

If a switchover does not occur, the zone controllers might have been changed to the **User Requested Standby** state. In that case, the zone controllers would not switch to **Active**, even if there is a failure of their peers. They must be activated manually.

#### 9.2.1.1 Recovering from a Voice Loss

Follow this process to recover from a voice loss.

**Process:**

1. Check both primary and backup Unified Event Managers (UEMs) for a list of voice-related alarms. See the *Unified Event Manager* online help.
2. Check the status of peer Zone Controllers (ZCs) and the link/path status. Ensure the ZCs are not in **User Requested Standby** state. If necessary, change the state of one of the ZCs to **Active**. See Verifying ZC Status.

3. If the UEM or the ZCs report link failures, see Heartbeat Authentication Link is Down on page 135.
4. A hardware failure of any of the components mentioned in this section might be the cause of the problem. If this failure occurs, replace the failed hardware. See Dynamic System Resilience FRU/FRE Procedures on page 143 for replacement information and references.

   For detailed troubleshooting information (diagnostic tests, and so on.), see voice-related troubleshooting sections in the following manuals:

   - *Zone Controller Feature Guide*
   - *Call Processing and Mobility Management Feature Guide*
   - *Master Site Infrastructure Reference Guide*

### 9.2.1.2 Heartbeat Authentication Link is Down

Heartbeat Authentication (HA) Link failure between the zone controllers causes loss of communication. See the following sections to troubleshoot logical and physical link failures.

#### 9.2.1.2.1 Troubleshooting Logical Link Failures

Follow this process to troubleshoot logical link failures.

**Process:**

1. Check the Unified Event Manager (UEM) for critical alarms on link and Zone Controller (ZC) failures. See the *Unified Event Manager* online help.
2. Verify in the UEM that the ZCs reporting link failures are enabled. See the *Unified Event Manager* online help.
3. Verify that Heartbeat Authentication (HA) keys are correctly provisioned. See “Setting the Heartbeat Key” in the *Zone Controller Feature Guide*.
4. If the problem remains, proceed to Troubleshooting Physical Path Failures on page 135.

#### 9.2.1.2.2 Troubleshooting Physical Path Failures

Follow this process to troubleshoot physical path failures.

**Process:**

1. Check the Unified Event Manager (UEM) for alarms on path failure. See the *Unified Event Manager* online help.
2. From the Network Management (NM) client, execute the following command: `ping zc0`***<X>***`.zone1`, where ***<X>*** is the number of the Zone Controller (ZC) which failed. If the command times out, investigate network connectivity problems. If it succeeds, proceed to step 3.
3. If the link to `zc0`***<X>***`.zoneZ` failed (where ***<X>*** is the number of the ZC which failed), log in to the ZC reporting the link failure as root and enter the following commands to ping the zc0X:

   Depending on which path failed, a different command is used.

   - For path 1, `ping zc0`***<X>***`.zoneZ`.
   - For path 2, `ping -g zcYcp1.zoneZ zc`***<X>***`cp1.zoneZ`
   - For path 3, `ping -g zcYcp2.zoneZ zc`***<X>***`cp2.zoneZ`

Where ***<X>*** is the number of the ZC which failed.

4. Repeat step 3 for every other ZC reporting a link failure. If ping requests a time out, investigate network connectivity problems.

9.2.2
## Loss of Data Delivery

This section describes what to do if a loss of data delivery occurs in a system with Dynamic System Resilience (DSR). A failure of the following components may result in a data delivery loss:

- Packet Data Gateway
- Packet Data Router
- Radio Network Gateway
- Gateway GPRS Support Node (GGSN)
- Both gateway routers (in the case of an M3 system) or the gateway router (in the case of an M1 system)
- CAI Data Encryption Module (CDEM)

Normally, any of the listed failures would result in a geographic switchover to the standby Packet Data Group in the backup core. If a switchover does not occur, see Recovering from a Data Delivery Loss.

9.2.2.1
### Recovering from a Data Delivery Loss

Follow this process to recover from a data delivery loss.

**Process:**

1. Check both the primary and the backup Unified Event Managers (UEMs) for a list of data-related alarms. See the *Unified Event Manager* online help.
2. Check the status of the primary and backup Packet Data Gateways (PDGs) and confirm that at least one of the PDGs is in the **Active** state. See Verifying the PDG Redundancy State in the UNC.
3. On the active PDG, perform the following actions:
   a. Check if the PDG has an established communication path to the local Radio Network Gateway (RNG). Use the **RNG Configuration** option from the **PDG Local Configuration** menu.
   b. Check if the PDG has an established communication path to at least one gateway router. Use the **View Gateway Router Configuration** option from the **PDG Local Configuration** menu.
   c. Check if the PDG has an established connection path with at least one Gateway GPRS Support Node (GGSN). Use the **View System Parameters** option from the **PDG Local Configuration** menu.

   See the *Packet Data Gateways Feature Guide*.
4. Check the Heartbeat Authentication (HA) link status. See “Verify HA Link Status on PDR” in the *Packet Data Gateways Feature Guide*.
5. If the links are down, see:
   - Recovering Heartbeat Authentication Link on page 137
   - Recovering InterZone RNG Link on page 137

6 Look for communication alarms in the active UEM. See the *Unified Event Manager* online help for details.

7 Manually switch over to the standby PDG in the backup core. See Changing the PDG Redundancy State in the PDG.

For detailed troubleshooting information (diagnostic tests, and so on), see the following data-related manuals:

- *Packet Data Gateways Feature Guide*
- *Trunked Data Services Feature Guide*
- *S6000 and S2500 Routers Feature Guide*
- *GGM 8000 System Gateway Feature Guide*

9.2.2.2

## Recovering Heartbeat Authentication Link

Perform this procedure if the Heartbeat Authentication (HA) link is down.

**Process:**

1 Set the same Heartbeat Key on both Packet Data Gateways (PDGs). See “Setting Heartbeat Key on PDG” in the *Packet Data Gateways Feature Guide*.

2 Ping the peer PDG. If it does not work, see “Pinging a Peer Device” in the *Packet Data Gateways Feature Guide*.

3 Check the Packet Data Router (PDR) cabling.

9.2.2.3

## Recovering InterZone RNG Link

Perform this procedure if the InterZone Radio Network Gateway (RNG) link is down.

**Process:**

1 Ping the RNG. If it does not work, see “Pinging a Peer Device” in the *Packet Data Gateways Feature Guide*.

2 Check if Packet Data Gateway (PDG) is in the **Active** state. See Verifying the PDG Redundancy State in the UNC.

9.2.2.4

## Packet Data Gateway Network Interface Card Failure

A Network Interface Card (NIC) failure on the active Packet Data Gateway (PDG) results in an automatic switchover to the other PDG.

9.2.2.5

## Component Failures in Dynamic System Resilience Enabled Systems

If a Dynamic System Resilience (DSR) component failure involves the Radio Network Gateway (RNG), Packet Data Router (PDR), or Gateway GPRS Support Node (GGSN), the subscribers do not need to initiate a context activation request. The failure forces a switchover to the backup data subsystem, which has the replicated context records. Context activation is shared between the two cores.

Upon a PDG or GGSN failure and switchover, data subscribers whose home zone is served by the switched PDG experience a data service downtime during the switchover, and are able to resume data services without having to re-context activate with the newly active PDG to receive data services.

See Data Subsystem Failures and Recovery on page 48.

9.2.3

## InterZone Link Failure

This section describes what should be done if a link fails in a system with Dynamic System Resilience (DSR). A failure of the following components may result in a link failure:

- Both exit routers (for M3 system) or single exit router (for M1 system)
- Both core switches (for M3 system) or single core switch (for M1 system)
- Core backhaul switches (for M3 system) or single backhaul switch (for M1 system)

An InterZone link failure causes voice and data subsystems to enter a dual-active scenario (unless the zone controllers and the Packet Data Group in the inactive core are in **User Requested Standby**). Do not leave the system in this condition. Fixing the broken link is a priority, but also consider alleviating the dual-active condition in the interim. Depending on the severity of the link failure and expected time until it is restored, you can take different actions. The InterZone Link Failure Recovery Scenarios section lists possible resolution scenarios and their consequences.

9.2.3.1

### InterZone Link Failure Recovery Scenarios

⚠ **CAUTION:** Do not change the state of the Zone Controllers (ZCs) if you do not have a clear understanding of the implications. For assistance, contact the Motorola Solutions Support Center (SSC).

Table 15: InterZone Link Failure Recovery Scenarios

| Scenario | Consequences | Advantages |
|---|---|---|
| Change the ZCs/Packet Data Gateway (PDG) in the backup core to **User Requested Standby** state. | Sites connected to the affected core lose wide-area trunking. Subscribers connected to the affected core must context activate with the active core. When the transport equipment is fixed and the links are restored, switch the **User Requested Standby** ZCs/PDG back to **Standby** state. | The system avoids dual-active condition and splitting sites between the two cores. The choice which core should be forced into **User Requested Standby** depends on the number of connected sites and their priority (limiting the impact to data and voice services). |
| Change the ZCs/PDG in the primary core to **User Requested Standby** state. | | |
| Do not change the states of the ZCs/PDG. Focus on resolving the transport issue (while maintaining dual-active condition). | Two ZCs and two PDGs continue to be active in the system, until the InterZone link is restored. This activity can potentially cause sites to become isolated from the rest of the system, members of one talkgroup can be connected to different sites, and so on. (See Isolated Site Scenario). | Sites remain in wide-area trunking. Apart from fixing the InterZone link (which must be done in all cases), this scenario does not require any action by the user. |

9.2.3.2

### Recovering from a Link Failure

Follow this process to recover from a link failure.

**Process:**

1. Check both primary and backup Unified Event Managers (UEMs) for a list of communication-related alarms. See the *Unified Event Manager* online help.
2. Follow Changing the ZC Redundancy State in the UNC to force the desired zone controller pair into **User Requested Standby**, or (in case of a minor link failure) wait until the dual-active condition is resolved automatically.

   **IMPORTANT:** If changing the zone controller states, change the state of the zone controller which is not active in the pair first. Then, change the state of the active zone controller in the pair.
3. After the InterZone link is fixed, and if you are switching one pair of zone controllers to **User Requested Standby**, switch the **User Requested Standby** zone controllers back to **Standby** state.

   For additional troubleshooting information, see “InterZone Communications Problems” in the *Zone Controller Feature Guide*.

9.2.3.3
## Resolving an Isolated Site Scenario

Follow this process to recover from an isolated site scenario by forcing a site reconnect. During a dual-active scenario, a site (or sites) may connect to the backup core and be isolated from the rest of the system because site links to the primary core fail when both cores are active. When the site links are fixed, the site remains connected to the backup core, remaining an isolated site.
Options for resolving an isolated site scenario exist. For example, one option is to wait until the InterZone link is restored (ending the dual-active condition). Another option is to switch the backup zone controllers and Packet Data Gateway (PDG) to **User Requested Standby** to force the site to connect to the primary core. The choice depends on the number of isolated sites and their priority.

**Process:**

1. Change the state of the zone controllers in the core to which the isolated site is connected to the **User Requested Standby** state. See procedure Changing the ZC Redundancy State in the UNC.
2. Set the PDG in the core to which the isolated site is connected to the **User Requested Standby** state. See procedure Changing the PDG Redundancy State in the PDG.
3. After the InterZone link is restored, change the zone controllers and PDG in the **User Requested Standby** state back to **Standby** state. See procedure Changing the ZC Redundancy State in the UNC and procedure Changing the PDG Redundancy State in the PDG.

9.2.4
## Specific Failure Scenarios

This section describes specific failure scenarios not automatically resolved by the system.

9.2.4.1
### Voice Logging for Colocated Console Sites

If a console site providing voice logging capability is colocated with a primary core, it is lost if a catastrophic failure occurs. Add another colocated console site with voice logging capability to the backup core. This backup console site must have the same talkgroup information as the primary site.

### 9.2.4.2 Context Activation

Subscriber radios do not automatically context-activate following a switchover. Ensure that the subscribers are configured for SNDCPv3 operation. Internal applications, such as Over-the-Air-Rekeying (OTAR), Text Messaging, Presence Notifier, Outdoor Location, and Over-The-Air-Programming (OTAP), register automatically. Check the application design guide for registration recommendations for external third-party applications. Manual registration may be required.

### 9.2.4.3 Pre-Existing Subscriber Recovery from Dual-Active

If both Packet Data Gateways (PDGs) are active as a result of a dual-active condition, pre-existing subscriber radios may roam across sites that may be split across the dual active PDGs. Depending on which PDG remains active after a dual-active resolution, some subscribers may not be able to receive data due to the PDG not correctly updated with the latest location of the Subscriber. This limitation is due to units roaming to a site connected with another PDG during dual-active condition and returning to the initial site after the condition is resolved. You may experience no outbound data though they are context activated. The PDG sends data to the wrong location. In this case, turn off and then turn on the subscriber unit or send an inbound data request which results in the correction of the subscriber location information on the PDG.

### 9.2.4.4 Network Management NIC Failure and Recovery

If the Network Management (NM) Network Interface Card (NIC) fails, mobility information cannot be replicated to the standby Zone Controllers (ZCs). The longer the active ZC is allowed to operate with a failed NM NIC, the more out of date the mobility information becomes. In addition, fault and configuration management traffic to and from the ZC is lost. Therefore, if an NM NIC fails, the operator should manually switch to a different ZC as soon as it is operationally convenient for the system.

If an NM NIC fails and wants to have another ZC active, log on to the ZC you want to make active and change that controller to the **Active** state. This action causes the ZC with the failed NIC to transition to **Standby** state. Follow Changing the ZC Redundancy State in the UNC to set the ZC to **Active** through the Unified Network Configurator (UNC).

### 9.2.4.5 Data Services for HPD Subscribers with CHAP User Authentication on DSR Switchovers

High-Performance Data (HPD) radio user Challenge Handshake Authentication Protocol (CHAP) user authentication information is not replicated with the HPD active contexts across Dynamic System Resilience (DSR) cores because it is sensitive information. The HPD Packet Data Gateway (PDG) fails to refresh the preserved context on a DSR switchover without the user authentication information. The HPD PDG de-registers the radio user at the ASTRO core. The radio user has no knowledge that the deregistration has occurred. The context activation failure events are sent on the network fault manager. The technician must trigger subscriber re-registration using the **admin** menu option at the HPD PDG local configure interface. Subscribers that are SNDCPv3 capable detect the need to register with this action and send re-registration requests to the HPD PDG. Radio users must turn off and turn on the SNDCPv1 subscriber units.

## 9.3 Motorola Solutions Support Center

The Motorola Solutions Support Center (SSC) is available for support for an ASTRO® 25 system with Dynamic System Resilience (DSR). As communication systems are evolving and expanding to enable greater capabilities such as what DSR offers, the need for a technical system resource to assist with the operational aspects of the feature increases. Motorola Solutions system managers are dedicated resources who coordinate all aspects related to the support, monitoring, and maintenance of your network. A system manager is effective in planning and managing the complex tasks associated with addressing DSR events when they happen. Because it is imperative for DSR to operate as intended when a site fails, the system manager can drive the necessary steps to periodically test the various steps and expected behaviors before an actual DSR event.

## 9.3.1 Obtaining Support

The hardware and software that make up the system are complex. Therefore, coordinate any repair action through the Motorola Solutions Support Center (SSC).

Consulting the Motorola SSC helps ensure that the problem is rectified in a timely fashion and that all warranty requirements are met.

Check your contract for specific warranty information. Your contract may also provide for extended warranty or service by Motorola Solutions personnel or service centers.

Motorola Solutions provides technical support services throughout the lifecycle of a system.

### 9.3.1.1 Necessary Background Information

Collect the following information before you call the Motorola Solutions support staff:

- System ID number (each ASTRO® 25 system has a unique system ID number)
- Location of the system
- Symptom/observation of the problem:
  - When did it first appear?
  - Can it be reproduced?
  - What is the step-by-step procedure to cause it?
  - Do other circumstances contribute to the problem? For example, changes in weather or other conditions.
- Maintenance action preceding problem:
  - Upgrade of software or equipment
  - Changed hardware and/or software configuration
  - Reloaded software from backup or from CD/DVD, and the version and date

### 9.3.1.2 Motorola Solutions Service Requests and Support

Motorola Solutions offers the following support centers to help with problems or to assist with obtaining a Return Material Authorization (RMA) number for faulty Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs):

- North America: visit http://www.motorolasolutions.com/en_us/support.html or call 1.888.325.9336
- International: visit http://www.motorolasolutions.com/en_xu/support.html or call +44 (0) 203 0277 499

9.3.1.3
## North America Parts Organization

The Radio Products and Services Division is your source for manuals, replacement parts, and assemblies.

The address for the United States, Canada, Central America, and South America is:

Motorola Solutions, Inc. Radio Products and Services Division

2200 Galvin Drive

Elgin, IL 60123, USA

The telephone numbers for ordering are:

- US and Canada orders: (800) 422-4210
- International orders: (302) 444-9842

The Fax numbers are:

- US and Canada orders: (800) 622-6210

The number for help identifying an item or part number is:

(800) 422-4210; press **3** to follow the menu prompt.

In addition, see Contact Us on page 5 at the front of this manual.

9.3.1.4
## Motorola Solutions Radio Rental

The Motorola Solutions Radio Rental group rents Motorola Solutions radios, mobiles, base stations, repeaters, and accessories.

The address for the United States, Canada, Central America, and South America is:

Motorola Solutions Radio Rental

1307 E. Algonquin Road

Schaumburg, IL 60196, USA

The telephone numbers are:

- Domestic: (888) 736-8567
- Canada only: (800) 268-3395

For more information, visit http://www.motorolasolutions.com/en_us/services/rental.html.

9.3.1.5
## Motorola Test Equipment Service Center

The Motorola Test Equipment Service Center provides your organization with test equipment support, technical support, repair services, software support and upgrades, module exchange program, pre-scheduled calibrations, reconditioned equipment sales, and equipment rentals.

The Service Center telephone numbers are:

- Phone: (800) 323-6967
- Fax: (847) 783-2800

Chapter 10

# Dynamic System Resilience FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the Dynamic System Resilience (DSR) feature.

## 10.1 Ordering Information and Part Numbers

Field Replaceable Unit/Field Replaceable Entity (FRU/FRE) information for the various components is included in their respective individual manuals. See Related Information on page 25.

## 10.2 Hardware Replacement Guidelines

This section describes how to plan for downtime when a component is being replaced. It also explains the activities which should be performed after the replacement is completed.

Replacing hardware elements in a system with Dynamic System Resilience (DSR) is generally no different than replacing hardware in a non-DSR system. For detailed replacement procedures, see the *Master Site Infrastructure Reference Guide*. The only differences are the switchover implications.

### 10.2.1 Transport Equipment Replacement

Replacing transport equipment in a system with Dynamic System Resilience (DSR) is no different from replacing it in a non-DSR system. Because only multi-zone systems support DSR, wide-area voice traffic and networking services is not affected, but the traffic capacity that can be handled may be reduced until the transport component is brought back into service.

#### 10.2.1.1 Shared Transport Equipment

Core LAN switches are shared devices in a system with Dynamic System Resilience (DSR), meaning that they are IP addressed for the master site where they reside. However, they potentially have twice as many hosts terminated on them. Other shared devices within a DSR master site include: gateway routers, exit routers, terminal servers (two are possible), Gateway GPRS Support Nodes (GGSNs), and backhaul switches. Core routers are dedicated to a single zone.

Single-core master sites do not share any equipment with another zone. However, the gateway routers, exit routers, core LAN switches, and terminal servers in the master site containing only a backup core have IP addresses configured for a second zone (usable by the backup devices of the first zone).

**IMPORTANT:** A failure of both switches and/or core routers in a system with DSR affects both zone cores in a master site. Replacing the switches and routers also affects the links to the remote sites and interzone links to the backup core. If the interzone link is down during replacement of the routers (for example, core routers), the Zone Controllers (ZCs) in the backup core become active. This active state means that two ZCs in a zone are active (dual-active scenario) for both zones. To avoid a dual-active condition, manually set the backup core ZCs to the **User Requested Standby** state.

This page intentionally left blank.

Chapter 11

# Reference Information for Dynamic System Resilience

This chapter contains supplemental reference information relating to the Dynamic System Resilience feature.

11.1

## DSR Reconfiguration Procedures

This table provides manuals and sections required to configure the Dynamic System Resilience (DSR) components.

Table 16: Component Configuration for DSR

| Subsystem | Device | Manual | Section(s) |
|---|---|---|---|
| DSR Data | Packet Data Gateway/ Packet Data Router (PDG/ PDR) | *Packet Data Gateways Feature Guide* | “Dynamic System Resilience Configuration”:<br>• “Setting Heartbeat Key on the Trunked PDG”<br>• “Verifying the HA Link Status on the PDR”<br>• “Trunked PDG Redundancy Configuration”<br>• “Checking the Trunked PDG Redundancy State (DSR)” |
| DSR Voice | Zone Controller (ZC) | *Zone Controller Feature Guide* | • “Setting the Zone Controller to User Requested Standby”<br>• “Zone Controller Display Status”<br>• “Setting the Heartbeat Key” |
| IP services | Core Security Management Server (CSMS) | *Core Security Management Server Feature Guide* | "Recovering CSMS" |
|  | Centralized Event Logging | *Centralized Event Logging Feature Guide* | “Recovery Sequence for a Centralized Event Logging Server” |
| Network Management (NM) | NM Server Applications | *Private Network Management Servers Feature Guide* | “Dynamic System Resilience Feature Administration” |
|  | DSR | *Dynamic System Resilience Feature Guide* | Enabling the Dynamic System Resilience Feature on the Network Management Server Applications |
|  | InfoVista | *InfoVista User Guide* | “Primary/Backup InfoVista Server Configuration” |

*Table continued…*

| Subsystem | Device | Manual | Section(s) |
|---|---|---|---|
| MOSCAD Network Fault Management (NFM) | | *MOSCAD Network Fault Management Feature Guide* | “Dynamic System Resilience Configuration” |

Chapter 12

# Dynamic System Resilience Feature Expansion/Upgrades

This chapter includes information pertaining to expansions and upgrades of the Dynamic System Resilience feature.

## 12.1 Expansion Paths

Zones in a system with Dynamic System Resilience (DSR) are configured for DSR on a zone-by-zone basis. A mixed system with DSR and non-DSR zones is supported. The maximum number of zones in an M3 DSR system is seven, but of these seven zones, at most six can be configured for DSR.

**IMPORTANT:** DSR system expansion is a complex process and can be performed only by Motorola Solutions. For information on DSR expansion, contact your Motorola Solutions representative.

Following are expansion paths for when a new zone is added to the system as a non DSR zone in a zone expansion, and then that zone is expanded to a DSR zone:

- Adding a third or fifth DSR zone to a two- or four-zone system with DSR.
- Adding a fourth or sixth DSR zone to a three- or five-zone system with DSR.

Additional DSR licenses must be purchased when expanding the DSR system.

### 12.1.1 DSR Service Outage Time

This table lists site trunking time for various M1 system Dynamic System Resilience (DSR) expansion scenarios in case of a switchover.

Table 17: M1 System DSR Service Outage Time

| Expansion Scenario | Number of Site Trunking Events | Site Trunking Time (sec) |
|---|---|---|
| 1 | 3 | 120-450 |
| 2 | 6 (3 per zone) | 240-900 |

This table lists site trunking time for various M3 system DSR expansion scenarios in case of a switchover.

Table 18: M3 System DSR Service Outage Time

| Expansion Scenario | Number of Site Trunking Events | Site Trunking Time (sec) |
|---|---|---|
| 1 | 3 | 120-450 |
| 2a | 6 (3 per zone) | 240-900 |
| 2b | 9 (3 per zone) | 360-1350 |
| 3 | 3 | 120-450 |

*Table continued…*

| Expansion Scenario | Number of Site Trunking Events | Site Trunking Time (sec) |
|---|---|---|
| 4 | 6 (3 per zone) | 240-900 |