System Release 7.17
ASTRO® 25

INTEGRATED VOICE AND DATA

Zone Controller

AUGUST 2020

© 2020 Motorola Solutions, Inc. All rights reserved

MN003381A01-C

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.

© 2020 Motorola Solutions, Inc. All Rights Reserved

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

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

Disclaimer

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

Trademarks

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

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

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

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

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

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

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

Document History

Version	Description	Date
MN003381A01-A	Original release of the *Zone Controller* manual.	November 2016
MN003381A01-B	This version includes the following updated process and new procedure: • Deploying the Zone Controller Virtual Machine on page 36 • Applying the Platform Patch on page 50	May 2017
MN003381A01-C	Updated section: • Upgrading Linux-Based Virtual Machines on page 73	August 2020

Contents

List of Figures

List of Tables

List of Procedures

List of Processes

About Zone Controller

This manual provides an introduction to the Zone Controller.

What Is Covered in This Manual?

The following topics are included in this manual:

- Zone Controller Description on page 18 provides a high-level description of the zone controller and how it fits into the system.
- Zone Controller Theory of Operations on page 25 provides details on how the zone controller functions in the system.
- Zone Controller Installation and Configuration on page 36 details installation procedures relating to the zone controller on the ESXi-based platform.
- Zone Controller Installation and Configuration on page 36 details installation procedures relating to the zone controller on the VMS platform.
- Zone Controller Operations on page 56 details tasks that you perform once the zone controller application is installed and operational.
- Zone Controller Maintenance on page 75 provides maintenance information relating to the zone controller.
- Zone Controller Troubleshooting on page 78 provides fault management and troubleshooting information relating to zone controller.
- FRU/FRE Procedures on page 89 lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the zone controller.
- Zone Controller Reference on page 90 contains supplemental reference information relating to the zone controller.
- Zone Controller Disaster Recovery on page 93 provides disaster recovery procedures relating to Zone Controller.
- Centralized Backup and Restore on page 94 provides disaster recovery information for the zone controller when utilizing centralized Backup and Restore (BAR) service.

Helpful Background Information

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

Related Information

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

Related Information	Purpose
Standards and Guidelines for Communication Sites (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. It is also known as R56 manual. This may be purchased on a CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).

Related Information	Purpose
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Authentication Services	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.
Backup and Restore Services	Provides information relating to the implementation and management of centralized backup and restore services for supported devices in ASTRO® 25 systems. This manual addresses server and client functions required for these services.
Dynamic System Resilience Feature Guide	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature that adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Enhanced Telephone Interconnect Feature Guide	Provides information describing the Enhanced Telephone Interconnect solution supporting voice-over-IP (VoIP) to allow individual subscriber units to access the Public Switched Telephone Network (PSTN).
Information Assurance Features Overview	Provides an overview of Information Assurance features for ASTRO® 25 systems, including a description of each feature and their impact on system implementation and management. Additionally, the manual contains details about Motorola Solutions services related to Information Assurance and physical security considerations for ASTRO® 25 systems.
MAC Port Lockdown	Provides information on the implementation and management of MAC Port Lockdown for standard Ethernet ports on Hewlett-Packard (HP) switches and for the internal switch of GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules (RDMs) in ASTRO® 25 systems. Additionally, the document contains instructions for configuring supplemental Ethernet port security, including the implementation of fiber optic ports on HP switches.
Private Network Management Servers	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).
Provisioning Manager	Provides a description of the Provisioning Manager application, including information on how to tailor this application for system use and how to provision ASTRO® 25 systems with various system-level, user-level, and device-level configuration parameters.
Securing Protocols with SSH	Provides information on the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in ASTRO® 25 systems, including configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
SNMPv3	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems.
Trunked Data Services Feature Guide	Describes the implementation and use of data services in ASTRO® 25 systems, specific to the Classic Data (Integrated Voice and Data) and

Related Information	Purpose
	Enhanced Data functionalities, as well as the High Availability for Trunked IV&D and HPD feature.
Unified Event Manager	Covers the use of Unified Event Manager (UEM) that provides reliable fault management services for devices in ASTRO® 25 systems.
Unified Network Configurator	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 the ASTRO® 25 IV&D system. UNC has two components: • VoyenceControl (EMC Smarts™ Network Configuration Manager) • Unified Network Configurator Wizards (UNCW)
Unix Supplemental Configuration	Provides additional procedures for Solaris-based and Linux-based devices, including password management, welcome banners configuration, and general administration.
Virtual Management Server Hardware	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in ASTRO® 25 systems.
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.

Chapter 1

Zone Controller Description

The Zone Controller is a software application that provides centralized control for call processing and mobility management functions in an ASTRO® 25 system. The Zone Controller application is responsible for processing calls, managing audio paths, controlling zone infrastructure, and providing services to subscribers and dispatch consoles.

The Zone Controller can operate in a standalone configuration or a redundant configuration. In a standalone configuration, the Zone Controller communicates with other components in the system through a Local Area Network (LAN) switch installed at the zone core of an ASTRO® 25 system. In a system with redundant Zone Controllers, the LAN switch is used to switch system resources between the Zone Controllers and provide high availability call management within the zone. While both Zone Controllers are powered and enabled at the same time, only one is actively participating in call processing tasks at any one time.

The redundant Zone Controller configuration provides protection against a single point of hardware or software failure that results in the loss of wide area trunking until the Zone Controller is repaired or recovers automatically. The redundant Zone Controller remains in the standby state as long as the active Zone Controller does not report a malfunction that causes a switchover.

Wide area trunking is the normal operating state for each site in the system and provides subscribers with the capability to communicate with members of their talkgroup regardless of site location. The Zone Controller provides control information that allows the system components to set up call processing and audio routing.

1.1 Dynamic System Resilience

Dynamic System Resilience (DSR) allows a system to continue to function without loss of functionality on the failure or destruction of any controlling master site within a single- or multi-zone by providing geographic redundant Fixed Network Equipment. DSR also improves protection for major components by providing redundant components. DSR supports voice traffic for systems that have up to six zones. DSR and non-DSR zones cannot be mixed within the same system. Redundancy is provided using Zone Controllers, Network Management functionality, IP services, network equipment, and optional features, including packet data and information assurance. DSR consists of two geographically separated zone core sites.

If a remote site is unable to establish contact with either the primary or redundant Zone Controller at the primary zone core, the remote site establishes connectivity with a Zone Controller at the backup zone core. If a primary site link is down, a remote site uses the backup site link and traffic is routed to the primary zone core via the backup zone core. Some remote sites can support DSR, whereas other remote sites cannot and switch to site trunking if the primary zone core is unavailable.

If DSR is implemented on your system, see the *Dynamic System Resilience Feature Guide* manual.

1.2 Server Hardware Description

The Zone Controller application resides on the HP DL380 server. On the HP DL380 the ZC runs Red Hat Linux in a VMware ESXi virtual machine.

For the HP DL380 server hardware description, see the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.

1.3 Zone Controllers in the ASTRO 25 System

Zone Controllers are used in various system configurations ranging from standalone single zone systems to multizone DSR systems.

In a standalone configuration, the Zone Core is equipped with a single Virtual Management Server (VMS) that hosts all the Network Management applications and a single non-redundant Zone Controller.

In a redundant configuration, the Zone Core is comprised of two Virtual Management Servers with the Network Management applications split between the two VMS’s and a single Zone Controller residing on each.

In a DSR system, a backup Zone Core provides redundant Network Management and the Zone Controller applications. Both standalone and redundant configurations can be configured with DSR.

In a Trunking Subsystem (Tsub), a Tsub Zone Controller provides dispatch and mobility services within a local area when normal system wide area communication is not possible.

Related Links

Non-Redundant Single Zone Configuration on page 19
Redundant Single Zone Configuration on page 20
Redundant Multi-Zone Configuration on page 22
Zone Controller at a Trunking Subsystem Prime Site on page 23

1.3.1 Non-Redundant Single Zone Configuration

A non-redundant single Zone Controller application is used to manage and support all call processing in the zone. Residing on one server is the Zone Controller application and each of the Network Management applications. Each application on the server is managed by the Virtual Management Server software that assigns and controls access to platform resources.

A non-redundant single zone configuration supports up to 24 sites of any type per zone.

Figure 1: Non-Redundant L1 Single Zone Configuration

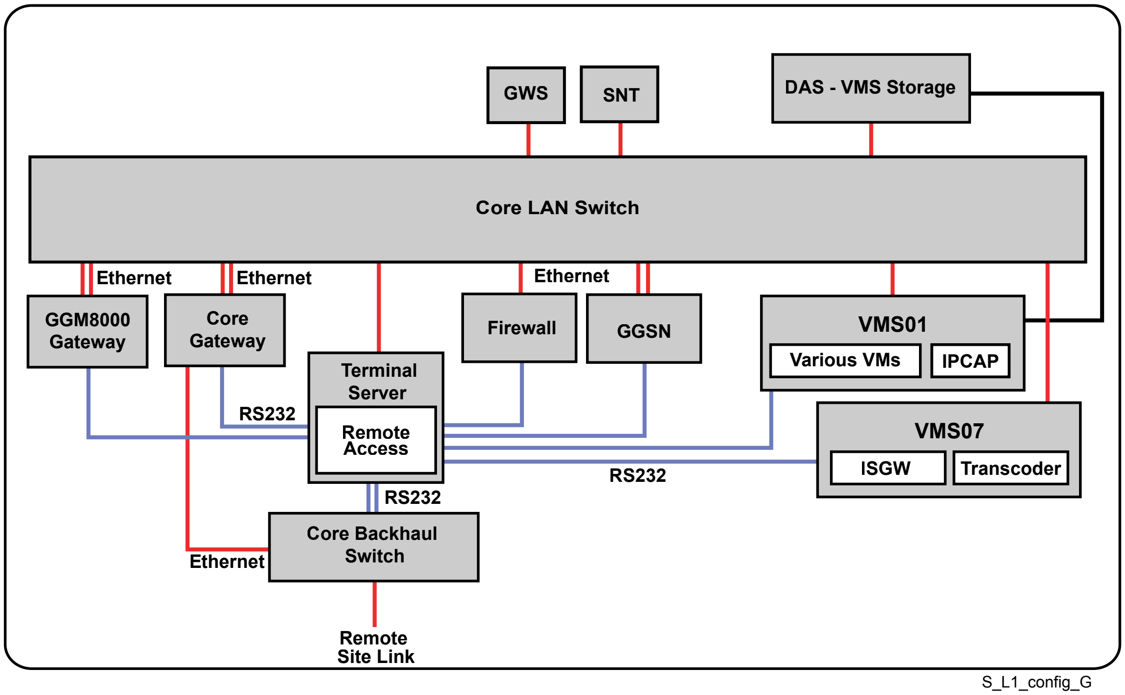
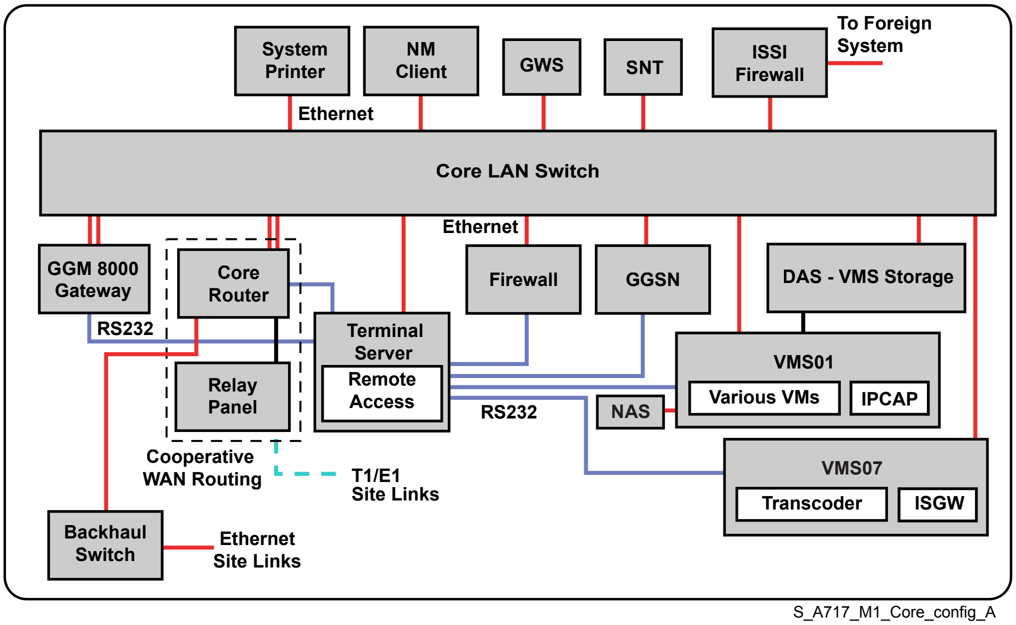


Figure 2: Non-Redundant M1 Single Zone Configuration



Related Links

Zone Controllers in the ASTRO 25 System on page 19

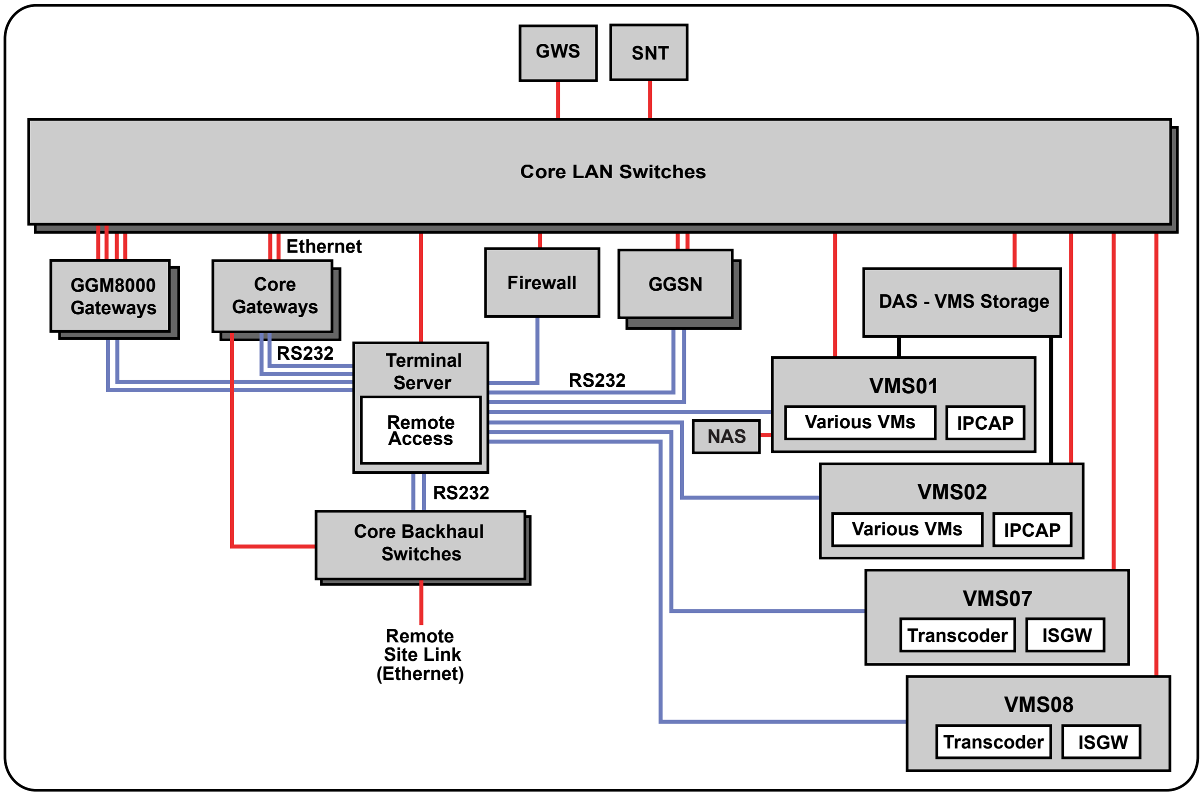
1.3.2 Redundant Single Zone Configuration

The redundant single zone configuration splits the application VMs between two physical servers in the rack. A second, redundant Zone Controller application (zc02) is added to the second server.

Additionally, redundant network transport equipment (LAN switch, and core and gateway routers) is provided with the capability to provide redundant T1 and flexible site links using optional equipment.

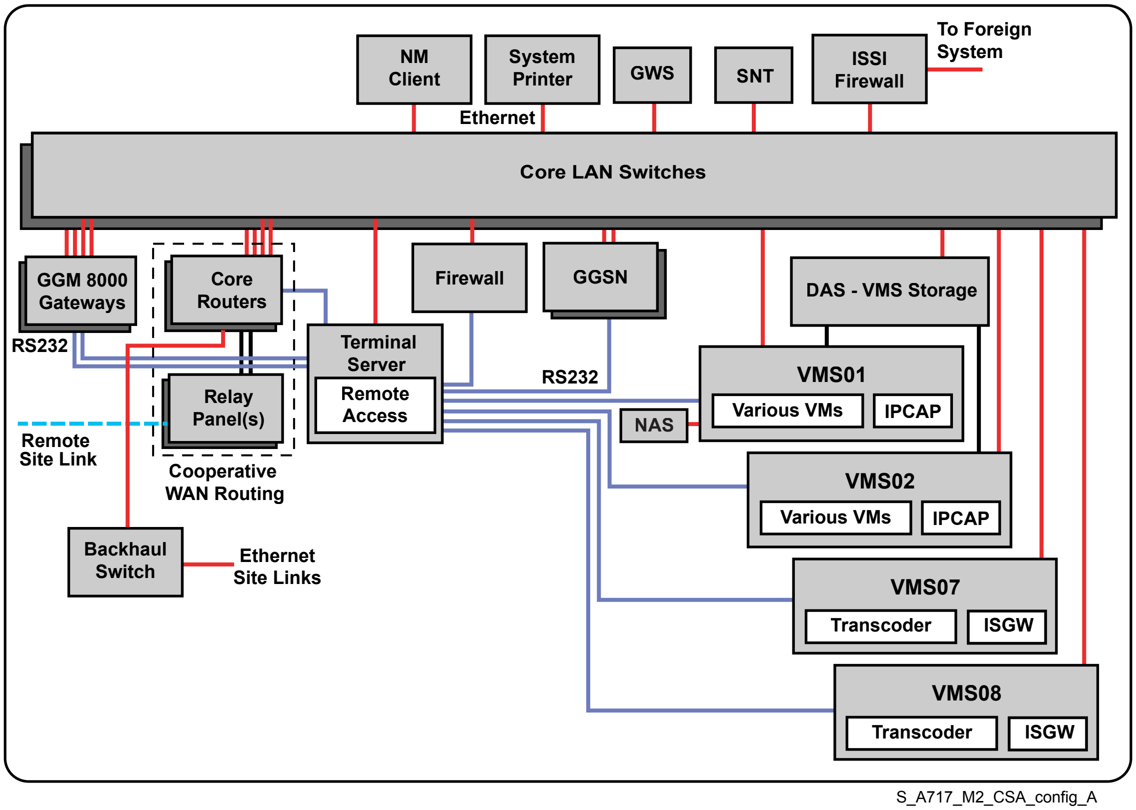
A redundant single zone configuration supports up to 24 sites of any type per zone.

Figure 3: L2 Single Zone Configuration



S_L2_CSA_config_J

Figure 4: Redundant Single Zone Configuration in the Common Server Architecture



Related Links

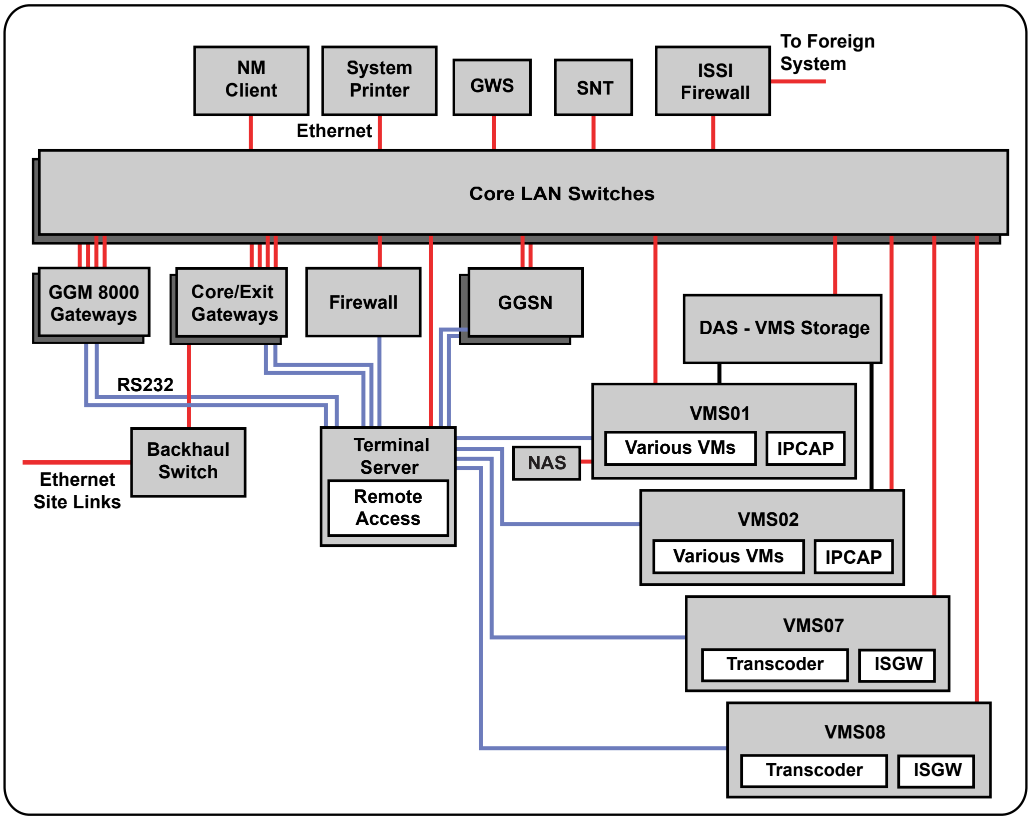
Zone Controllers in the ASTRO 25 System on page 19

1.3.3 Redundant Multi-Zone Configuration

A redundant multi-zone system supports up to seven zones along with all the Network Management applications. Two redundant Zone Controller applications along with the ZDS, ATR, UEM, and ZSS NM applications are used at each zone. The System Statistics Server (SSS) is optional in this configuration. The SSS, UNC, and PM NM applications reside on the same zone level server.

A redundant multi-zone configuration supports 25 or more sites of any type per zone. This configuration can initially be set up as a single zone system and later expanded to a system with up to seven zones.

Figure 5: Redundant Multi-Zone Configuration – Virtual Management Server



S_A717_M3_Primary_System_Zone_Core_Config_A

For information about systems with the Dynamic System Resilience, see the *Dynamic System Resilience Feature Guide* manual.

Related Links

Zone Controllers in the ASTRO 25 System on page 19

1.3.4

Zone Controller at a Trunking Subsystem Prime Site

The zone core is a typical location for the Zone Controller. Additionally, the Zone Controller can be located in a Trunking Subsystem (Tsub).

In the ASTRO® 25 system with the Edge Availability with Wireline Console feature, the Tsub prime site will be equipped with the following devices residing on the same Gen9 Tsub server:

- Tsub Zone Controller (Tsub ZC)
- Domain Controller
- IP Packet Capture
- Dynamic Transcoder (optional)

During Tsub local area operation when connectivity to the zone core is lost, the Tsub ZC provides the call control for voice services, such as group calls and private calls, between radio users and dispatchers located within the Tsub.

The Tsub ZC does not support all features and capabilities normally provided by the zone core ZCs. Any services that require the zone core or access to the Customer Enterprise Network (CEN) via the zone core are lost during Tsub local area operation.

For more information, see the *Edge Availability with Wireline Console Feature Guide for Trunking Subsystems* manual.

Tsub ZC Interface to ADS

The Advanced Distribution Service (ADS) is an alias management solution that resides on the Zone Data Server (ZDS). The Tsub ZC connects to the ADS to receive the subscriber alias records. This interface is the same as the zone core ZC interface to the ADS. However, there is a difference in the way that the Tsub ZC connects to the ADS in a system with Dynamic System Resilience (DSR).

In the zone core, the ZC only connects to the ADS in the same DSR core (for DSR systems). However, since the Tsub ZC is not associated with a particular zone core, it connects to either the primary core or the backup core ADS (for DSR systems). Upon loss of connectivity to the ADS, it will automatically attempt to re-establish a connection to the ADS and if unsuccessful, attempt to connect to the ADS in the other core.

The Tsub ZC reports separate fault instances for the connection to the primary core ADS and for the connection to the backup core ADS. When one link is up, the other link is reported as in standby state. When the active link is lost, links to both ADSs are reported as down until one link is reconnected, at which time the two links are again reported as up and standby.

Related Links

Zone Controllers in the ASTRO 25 System on page 19

Chapter 2

Zone Controller Theory of Operations

This chapter explains how the zone controller works in the context of your system from a system perspective.

2.1 Zone Controller Function

In an ASTRO® 25 system, the Zone Controller is used to process system-wide commands for call processing, mobility management, data transactions, and some network management functions. The Zone Controller communicates with the gateway routers through the zone core LAN switch by establishing an IP session to each router. The gateway router serves as the single access interface for all call control information.

2.2 Redundancy and Switchover Overview

The zone core Zone Controller redundancy and switchover administration activities are conducted either through the Unified Network Configurator (UNC) or locally from the Zone Controller administration menu.

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

ZC switchover can be performed both automatically or manually by forcing a switchover.

ZC redundancy provides protection against a hardware or software failure that may result in the loss of wide-area trunking. In systems with a standby ZC, one ZC actively processes calls and manages ZC resources in the zone, while the other ZC acts as a standby that is brought online when the active ZC is being serviced or has a failure that causes the loss of wide-area trunking capability.

Communication is established between ZCs through the zone core Ethernet LAN switch. Two requirements are satisfied with this hardware configuration:

- Continued functionality in the event of a failure
- Continued functionality in the event of maintenance

ZCs in a redundancy state negotiate with each other through Ethernet LAN links. The Ethernet LAN link is used by the ZCs to exchange operating modes, notify each other of their ability to maintain the zone in wide-area trunking mode, and to negotiate a switchover action if necessary.

System information necessary for call processing is downloaded to the ZCs. The ZCs are provided with server resources for storing data, controlling zone activities, and communicating with other zone resources.

For information about UNC commands related to ZC redundancy and switchover, see “Zone Controller Quick Commands” in the *Unified Network Configurator* manual.

Related Links

Zone Controller Redundancy and Switchover on page 51

2.2.1 Zone Controller Redundancy States

The Zone Controllers in the zone core are configured for the following redundancy states:

- Active
- Standby
- User Requested Standby

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

Active State

The Zone Controller in the **Active state** is the ZC that handles call processing for the zone. An automatic switchover to a Standby ZC takes place upon a failure of an Active ZC that causes the loss of wide area trunking capability. The failure event can be either software- or hardware-based.

Standby State

The ZC in a **Standby state** does not handle call processing for the zone, but if something should happen to an Active ZC, a Standby ZC is available to automatically switch over and become the Active ZC.

User Requested Standby State

A ZC in a **User Requested Standby state** does not handle call processing for the zone and, even if something happens to the Active ZC for the zone, a User Requested Standby ZC is NOT available to take over call processing. This state is always set manually, performed for upgrade purposes, and used to prevent any switchovers.

2.3 Zone Controller and Logical Server Interaction

As with many components of the system, the Zone Controllers and logical servers are highly interdependent. They rely heavily on each other to supply critical data in support of their individual functions.

Figure 6: Zone Controller Logical Server Interaction

The following graphic shows a high-level flow of information between the Zone Controller and servers in a system. Each interaction is numbered.

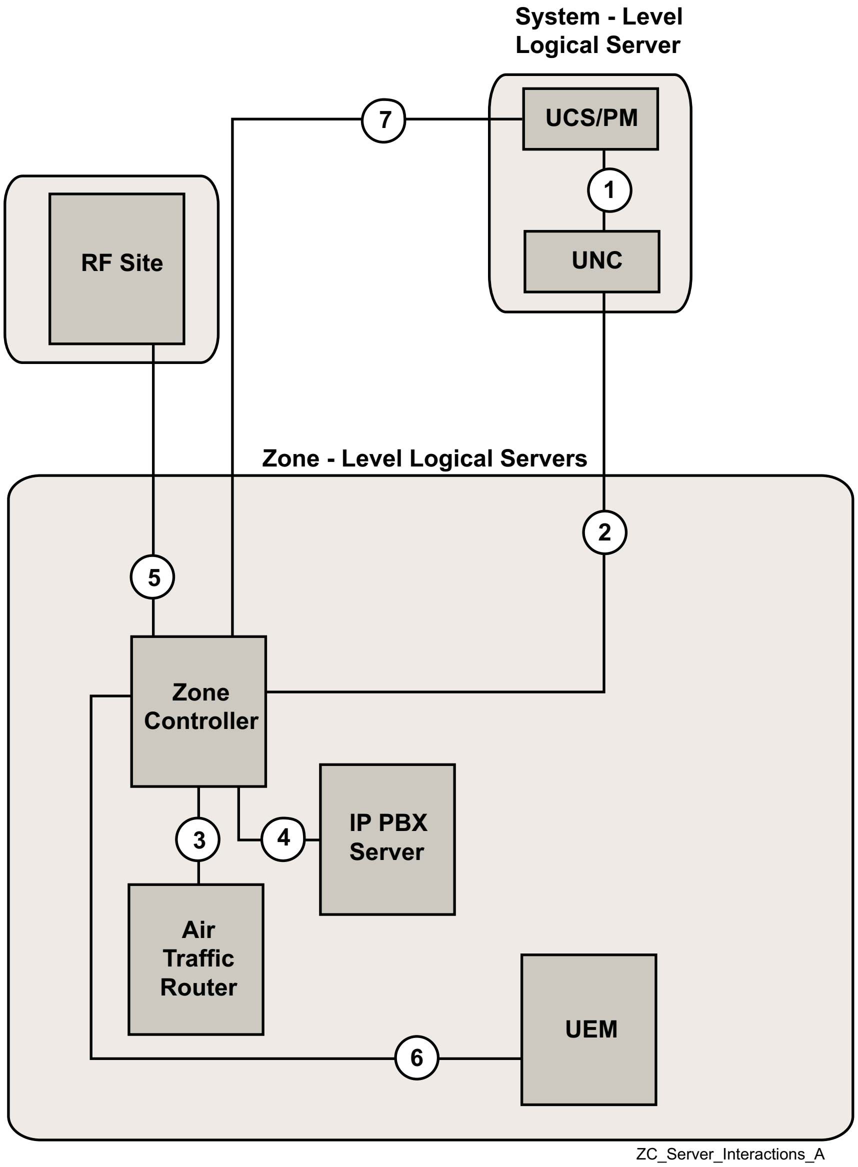


Table 1: Zone Controller Logical Server Interactions

The following table a high-level description of information exchanged between the Zone Controller application and other server applications in the system.

No.	Zone Controller Server Interaction
1	The Provisioning Manager (PM) sends the subscriber database to the Unified Network Configurator (UNC). This process is performed manually from the database administration menus. The Provisioning Manager (PM) is an application that resides on the User Configuration Server (UCS).
2	The Unified Network Configurator (UNC) sends the subscriber and configuration databases to the Zone Controller.

No.	Zone Controller Server Interaction
3	Live call data passes from the Zone Controller to the Air Traffic Router (ATR). Radio user and Radio Control Manager (RCM) commands and information are sent through this link.
4	Call control information is sent from the Zone Controller to the IP PBX server for the Enhanced Telephone Interconnect (ETI) feature. Fault information is passed to the Zone Controller.
5	Call control information is passed between the Zone Controller and the site controller.
6	The Zone Controller is fault managed and sends fault and event notifications to the zone level Unified Event Manager (UEM) after it is discovered in the UEM application.
7	The active Zone Controller sends default subscriber records to the PM.

2.4 Configuration Updates for a Zone Controller

The PM builds the configuration files and sends the files to the UNC. The PM identifies the target devices for each file. When the UNC receives the file, it manages the download of the files to the Zone Controller. The Zone Controller receives this bulk download of configuration data (RF sites, call parameters, and so on), subscriber data, and Home Zone mapping updates from the UNC. The Zone Controller uses this information to populate its Group Home Location Register (GHLR) and Individual Home Location Register (IHLR).

2.5 Persistent Store

The Zone Controller provides a persistent store for all the subscriber data records. This provides faster Zone Controller recovery in a failure and allows the Zone Controller to recover in cases where the UNC is not available.

2.6 Zone Controller and Voice Call Processing

This section explains the Zone Controller databases and voice call processing.

2.6.1 Home Location Register and Zone Controller

A Home Location Register (HLR) is a database maintained by the Zone Controller. Because the home zone is responsible for controlling all voice group calls for a talkgroup, the Zone Controller coordinates the assignment of resources based on the home zone map and the information stored in its HLR and Visitor Location Registers (VLR). An HLR for each zone contains subscriber radio and talkgroup information (home zone information) specifically designated for that zone.

When a system is first installed, home zone subscriber and talkgroup information is entered into the Provisioning Manager (PM). When this data is entered for all the zones in the system, each subscriber radio and talkgroup is assigned a home zone. The home zone information is then downloaded to each Zone Controller.

2.6.2 Visitor Location Register and Zone Controller

The Visitor Location Register (VLR) is a Zone Controller database containing information on all radios currently affiliated to the sites at a zone. The VLR manages a local copy of zone-specific information for individuals and talkgroups. This includes subscriber database information and site location information for both the individual and the talkgroup. Each zone has an Individual VLR (IVLR) and a talkgroup VLR (GVLR).

2.6.3 Default Records

System recognition of a subscriber radio attempting to access the system is achieved after a radio record is configured and established through the PM application. However, default access is a system condition (configured for a zone using PM) that allows subscriber radios being added to the system to access the communication system using a default configuration record (SZ$DEF) when no configuration information is available from the UCS. Under default access, when a subscriber radio attempts to access the system, a default configuration record is automatically assigned to the subscriber radio. This default record provides the subscriber radio with a predefined set of call services and permissions.

2.6.3.1 SZ$DEF Record

The SZ$DEF is a default record that the Zone Controller uses after the UNC database is loaded. The record defines guest privileges and default information for all radios, radio users, and talkgroups attempting to access the system when no provisioned record is available and default access is enabled. This situation could happen for radios added to the UCS database while the link to a zone is down that try to register or affiliate before their data is downloaded to the UNC. New radios or talkgroups created by the Zone Controller are a clone of the SZ$DEF record. This includes the profile settings of this record as well. Changes made to SZ$DEF records are always sent to the Zone Controller (once the UNC database is loaded). Once the Zone Controller receives user-entered records or profiles, those records are used by the Zone Controller instead of the SZ$DEF records.

IMPORTANT: Parameters set in the SZ$DEF record are not forwarded if the radio roams into a new zone. The radio user is controlled by the parameters set in the new zones SZ$DEF record. Site access, Storm plans, and events, such as those monitored by Inbound Event Display, can be severely impacted since the new zone cannot import information from the previous zones SZ $DEF record.

The SZ$DEF records are customized to control services to the radios until their provisioned record is available. For example, private call is disallowed by the SZ$DEF record. Once the manager provisioned records are available, the feature can be controlled for each individual user.

2.6.4 Radio User and Talkgroup Record Download

After the configuration database is downloaded and the channel capabilities are verified, the UNC loads subscriber and talkgroup records to the Zone Controller. The time required for this download varies depending on the number of subscribers and talkgroups in the system.

Any radio, radio user, and talkgroup record added to the PM database remains in the database until it is distributed from the PM. The Zone Controller replaces the default records with the permanent records as it receives them from the UCS through the UNC.

2.6.5 Zone Controller and Dynamic Transcoding

The Dynamic Transcoding feature allows FDMA-only subscriber radios on a talkgroup to communicate with TDMA radios on a 700 MHz site while preserving the FDMA and TDMA modes of operation at each respective site.

This solution applies only to Dynamic Talkgroups, which enable FDMA and TDMA radios to communicate in a call. A Dynamic Transcoder device running as a virtual machine on a Virtual Management Server (VMS) in each zone is required to support this feature. The Transcoder dynamically converts the audio in a call from full-rate to half-rate or from half-rate to full-rate as instructed by the Zone Controller.

Interoperability Between Sites

Dynamic Transcoding ensures interoperability between radios operating at the following site types:

- FDMA-only sites and TDMA-only sites
- Mixed FDMA/TDMA sites and TDMA-only sites

NOTICE:
Dynamic Transcoding is not necessary to provide interoperability between radios operating at mixed FDMA/TDMA sites. In this scenario, the Dynamic Talkgroup feature ensures interoperability.

However, while not necessary, Dynamic Transcoding can be more efficient in providing interoperability between two dynamic sites.

Example: An FDMA-only radio is at one dynamic site in a call, and only TDMA-capable radios are at another dynamic site in the call. With Dynamic Talkgroups, both sites are granted as FDMA. With Dynamic Transcoding, the site with the FDMA-only radio is granted as FDMA. The site with only TDMA-capable radios is granted as TDMA, which leaves the other TDMA slot on the channel available for another call.

How the Zone Controller Supports Dynamic Transcoding

The Zone Controller performs several functions to support transcoded calls, including Dynamic Transcoder assignments and fault reporting, and FDMA/TDMA site allocation.

Configuration parameters

The Zone Controller accepts configuration parameters related to Dynamic Transcoding and uses these parameters to:

- Enable transcoding in the system.
- Enable transcoding on a foreign talkgroup.
- Identify each Dynamic Transcoder in a zone or in a Trunking Subsystem (Tsub) with a unique ID.

  NOTICE: A Dynamic Transcoder in a Tsub establishes a link with the Tsub ZC only and is not utilized by the zone core ZC. Similarly, the zone core Dynamic Transcoders are not utilized by the Tsub ZC even if the transport network is available during Tsub local area operation.

- Define the Jitter Buffer for calculating the Dekey Delay.

Dynamic Transcoders

The Zone Controller performs the following tasks related to Dynamic Transcoders:

- The Zone Controller receives a list of Dynamic Transcoders in its zone.
- The active Zone Controller accepts connections from the configured Dynamic Transcoders from both the primary and backup core.

- The Zone Controller reports the link status and fault states of the assigned Dynamic Transcoder.
- When assigning Dynamic Transcoders for group and private calls, the Zone Controller prefers Dynamic Transcoders located in the same Dynamic System Resilience (DSR) zone core over the Dynamic Transcoders in the opposite zone core.

Call support

The Zone Controller supports transcoded private calls and group calls, including all the call features available for regular calls.

NOTICE: A zone core Dynamic Transcoder can utilize two transcoder resources per call. This is needed when the zone core Dynamic Transcoder resides in an Intersystem Gateway (ISGW) equipped zone. A Tsub Dynamic Transcoder always uses one transcoder resource per group call. For private calls, two transcoder resources are required.

Site allocation

When Dynamic Transcoding is on, the Zone Controller allocates a dynamic site as FDMA or TDMA according to the resource allocation rules.

Dynamic Dual Mode (DDM)

When no Dynamic Transcoders are connected in a zone, the Zone Controller provides a Dynamic Dual Mode (DDM) fallback mode.

2.7 Zone Controller and Data

Data consists of those elements necessary to provide data services in the following functions:

- Integrated Voice and Data (IV&D)
- Air Traffic Information Access Data
- Transit25 Data

2.7.1 Zone Controller and Integrated Voice and Data

The Zone Controller supports and manages channel resource allocation for both voice and data. From the data services perspective, the Zone Controller provides the following functions:

- Responds to the Home Location Register (HLR) query by sending the Packet Data Router (PDR) to obtain zone affiliation information (subscriber location) and subscriber status information.
- Responds to Visitor Location Register (VLR) of the Radio Network Gateway (RNG) module to obtain site affiliation information. In addition, registration, de-registration, site roaming, and zone roaming information is communicated from the Zone Controller to the RNG for processing data service requests.
- Tracks the number of active data channels at a site.
- Manages and enforces channel preemption rules.
- Maintains data channel lease with the site controllers.
- Provides mobility management functions for each Mobile Subscriber Unit (MSU).
- Allocates and manages radio channel resources and determines which channels are used as the Packet Data Channel (PDCH).
- Determines PDCH preemption based on preemption rules. If the system-wide Data Channel Preemption parameter is set, the TG preempts data parameters.
- Maintains Busy Queue for data channel requests from the sites. PDCH requests follow the existing priority levels for call processing.

- Supports Inter-System Service Data (that is, roaming to / from a foreign system with the assistance of the ISSI 8000/CSSI 8000 gateway device)

A data channel is busy when any one of the following occurs:

- All voice channels are in use.
- The maximum number of data channels at the site has been reached.
- None of the available channels are sub-band restricted.

2.7.2 Zone Controller and Air Traffic Information Access Data

The Zone Controller provides information on the traffic and call information in the system to the Air Traffic Router (ATR) server application.

The data can be obtained from the ATR in the following formats:

- Raw data: Air Traffic Information Access (ATIA) data stream
- Processed data: dynamic reports, historical reports

The data call information includes the following records:

Start of the data call
Data channel request granted

Data call reject
Data channel request rejected

Data call busy
Data channel request busied

End of data call
Data channel de-assigned

Cancel of data channel request
Data channel request canceled

Renew data channel request
Data channel request renewed

2.7.3 Zone Controller and Transit 25 Data

In systems implementing the Transit25 feature, the Zone Controller receives Controlled Channel Access (CCA) packet data channel requests from the active site controller at a site. CCA PDCHs are used for scheduled data transmissions with a subscriber unit assigned a specific slot to transmit on the packet data channel. In contrast, classic PDCHs are granted for unscheduled transmissions.

For detailed information about the role of the Zone Controller in supporting the Transit 25 data application, see the *Trunked Data Services Feature Guide*.

2.7.4 Zone Controller and Foreign System Interface

The Zone Controller receives foreign system configuration and provisioning from the UNC and PM applications. Individual Short Subscriber Identity (ISSI 8000/CCSI 8000) is an optional feature supported by ISGW (ISSI 8000/CCSI 8000). Zone Controller connected to ISGW supports radios from a foreign system registering to the ASTRO® system and roaming of the system radios to a foreign system.

2.8 Zone Controller Relationship to Telephone Interconnect Equipment

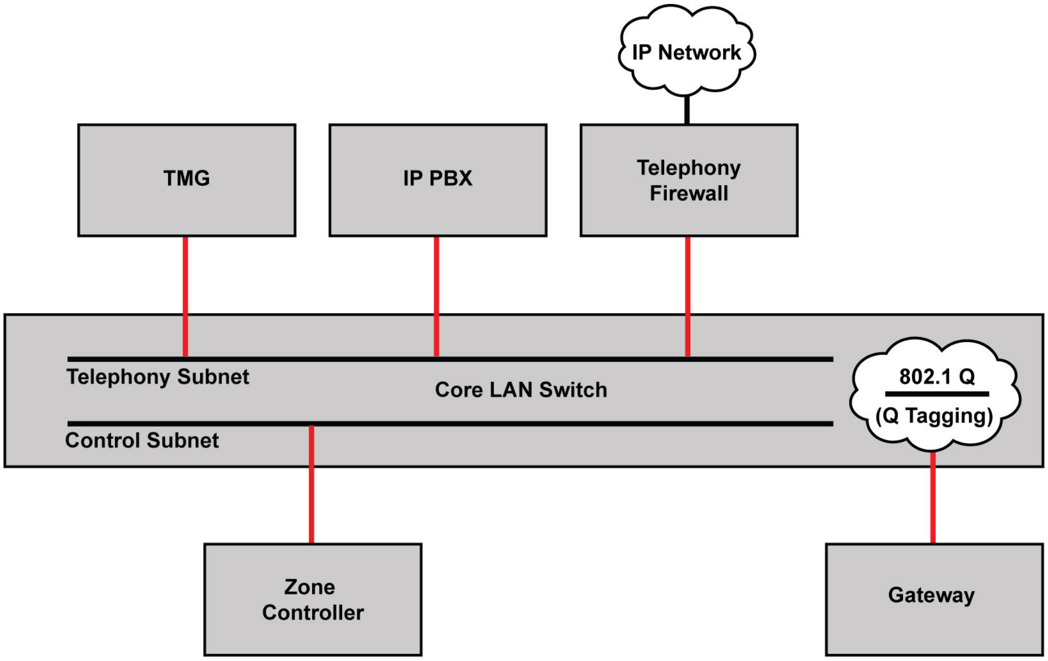
The Zone Controller uses the Telephone Media Gateway (TMG) so that telephone interconnect calls can be made from radios to the Public Switched Telephone Network (PSTN), and from the PSTN to individual radios. The TMG is considered part of the interconnect subsystem along with the UNIVERGE 3C Administrator application and any optional media gateways. The TMG converts G.711 encoded Real-time Transport Protocol (RTP) audio streams into Xzone Infrastructure Signaling protocol (XIS) audio used by the radio infrastructure and XIS audio back to G.711 encoded RTP audio streams.

In addition to audio, the telephone interconnect system supports the generation of various tones. For example, media gateway is responsible for Dual Tone Multi-Frequency (DTMF) signaling while TMG generates DTMF overdialing (touch-tone), subscriber dekey, momentary ring back, and other messaging tones (end-of-call warning). This is a necessary feature since digital radios cannot generate their own overdial tones (touch-tones). This capability is essential for accessing automated voice mail systems or other types of automated resources.

The difference between DTMF overdialing and DTMF signaling is overdialing occurs after the call is established. Signaling occurs when the media gateway outpulses dialed number information to the serving switch to initially establish a call (comparable to lifting a handset and pressing DTMF buttons is response to dial tone to initiate a call).

Figure 7: Enhanced Telephone Interconnect Subsystem with Telephony Firewall

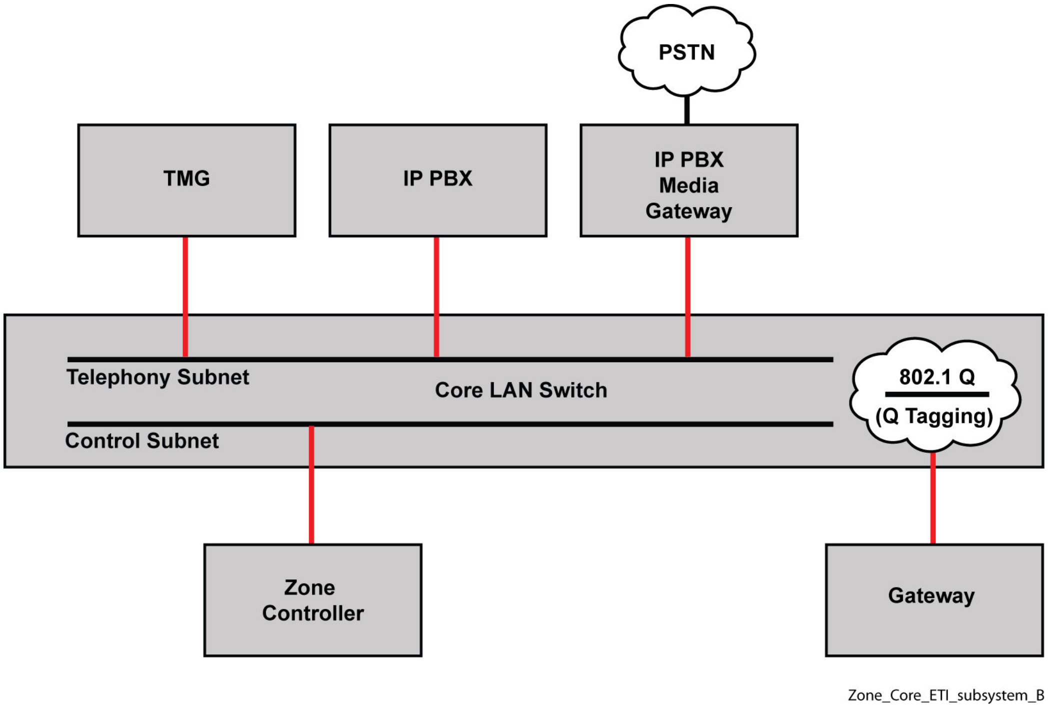
The following figure shows the ETI subsystem with the telephony firewall, which is used for IP connectivity. A firewall is required only when a non-UNIVERGE media gateway (COHub or Branch Hub) is used or when no media gateway is used at all (Session Initiation Protocol (SIP) connection to a 3rd party switch).



Zone_Core_ETI_subsystem_w_telephony_firewall_B

Figure 8: Enhanced Telephone Interconnect Subsystem without Telephony Firewall

The following figure illustrates the ETI subsystem with the IP PBX media gateway, which is used in place of the telephony firewall and provides EI, T1, and analog connectivity to the Public Switched Telephone Network (PSTN).



For more information, see the *Enhanced Telephone Interconnect Feature Guide*.

2.8.1 Exclusion Class and Dialing Restrictions

Dialing restrictions on a subscriber basis may be configured in a system and screened by the Zone Controller by using exclusion classes. For more information, see the *Enhanced Telephone Interconnect Feature Guide*.

2.9 Zone Controller Menu Functions

You can perform the following tasks through the Zone Controller administration menus.

Software Administration menu for the Zone Controller
This menu allows you to display software versions, eject the CD/DVD drive, and reboot the server.

OS Administration menu for the Zone Controller
This menu contains options related to SNMPv3 administration, SSH key administration, and log file access. You can use this menu to display platform resource and configuration information and reboot or shut down the server.

Services Administration menu for the Zone Controller
This menu contains the options for joining a domain, managing the centralized logging and backup client configurations, and managing the NTP Client configuration.

Backup and Restore Administration menu for the Zone Controller
This menu contains backup and restore services.

Application Administration for the Zone Controller menu

This menu contains options for setting InterZone capabilities, isolating zones, checking call processing status, resetting the application, and managing system redundancy.

2.10 Network Time Protocol Services

The Zone Controller uses the Network Time Protocol (NTP) to synchronize its internal clock to an external time source. See the *Network Time Protocol Server* manual.

2.11 Dynamic System Resilience and Call Processing

For systems utilizing the Dynamic System Resilience feature and for the call processing scenarios specific to that feature in the event of a system failure, see “Theory of Operation” in the *Dynamic System Resilience Feature Guide*.

Chapter 3

Zone Controller Installation and Configuration

This chapter details the installation procedures related to the Zone Controller on a VMS Host in an ASTRO® 25 system master site.

For information on installing the hardware and making the physical connections for installing these components, see the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.

3.1 Deploying the Zone Controller Virtual Machine

The Zone Controller application resides as virtual machine on an ESXi platform which has its own installation and configuration process.

For information about the installation, security settings, and other details, see the *Virtual Management Server Software* manual.

Prerequisites: Review the entire software installation process and each supporting procedure. Some procedures in this process can be implemented as standalone procedures or as part of this process.

Process:

1. Satisfy all appropriate requirements and review all appropriate installation considerations before installing a virtual machine on the Virtual Management Server (VMS) host.
2. Log on to the VMS.

   See Logging On to the VMS Host of the Zone Controller Virtual Machine on page 37.
3. Import the virtual machine.

   See Importing the Virtual Machine on page 37.
4. **Only for systems with vCenter installed:** Configure VMware vCenter for the Zone Controller virtual machine.

   See Configuring the vCenter for the Newly Deployed VM on page 40.
5. Set the correct start up/shut down order.

   See Setting the Virtual Machine Startup and Shutdown Order on page 41.
6. Configure CPU and memory settings.

   See Configuring CPU Memory Settings for the Zone Controller on page 43.
7. Configure the Zone Controller security settings.

   See Applying Supplemental Configuration to Virtual Machines on page 44.
8. Connect and power on a new Zone Controller Virtual Machine application.

   See Connecting and Powering On the Zone Controller on page 46.
9. Configure the time zone.

   First set the time zone, then set the identity. If time zone is set after identity, an additional reset is required.

See Configuring the Time Zone on Linux Servers on page 46.

10 Set the identity for the Zone Controller virtual machine.

See Establishing the Zone Controller Identity on page 47.

11 Join the Zone Controller virtual machine to the domain.

See Joining a Domain for Centralized Authentication on page 49.

12 Apply the platform patch to the Zone Controller virtual machine.

See Applying the Platform Patch on page 50.

Related Links

Recovering the Zone Controller on page 93

3.1.1 Logging On to the VMS Host of the Zone Controller Virtual Machine

The Zone Controller virtual machine is installed on a Virtual Management Server (VMS) with the ESXi operating system. You can log on to the VMS from the VMware vSphere Client.

NOTICE: If a vCenter Server manages the ESXi hosts in the system, the Zone Controller must be deployed and installed from the vCenter Server. Otherwise, the Zone Controller will be deployed and installed on the appropriate ESXi host. If an ESXi host is being managed by a vCenter Server, then a message indicating this will be displayed when the vSphere client is connected to the ESXi host. A Zone Controller cannot be deployed from an ESXi host managed by a vCenter Server.

Prerequisites: Obtain the following information:

- IP address of the VMS hosting the Zone Controller virtual machine.
- Password for the root user account

Procedure:

1 From a Windows-based device, launch the **VMware vSphere Client**.

2 Log on to the VMS as the root user:

   a In the **IP address / Name** field, enter the IP address of the VMS.

   b In the **User name** field, enter: `root`

   c In the **Password** field, enter the password for the root user account.

   The **vSphere Client Inventory** window appears.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.2 Importing the Virtual Machine

Importing a virtual machine may take approximately an hour, depending on network traffic and disk usage.

Prerequisites: Obtain the following media and information:

- *Zone Controller DVD*
- IP address of the ESXi-based server (Virtual Management Server host)
- ESXi-based server root account password

- Hostname for the device that you are importing
- Zone network for the virtual machine

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.

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

2. Log on to the server by entering the IP address of the ESXi server, `root` in the user name field, and the appropriate password in the password field.
3. In the **vSphere Client Inventory** window, perform one of the following actions:
   - If you are installing from the DVD, insert the media listed in the prerequisites in the DVD drive of the device where the vSphere Client resides.
   - If you are not installing from the DVD, determine the location of the following file: ***<Zone_Controller.ovf>***
4. Select **File → Deploy OVF Template**.
5. In the **Deploy OVF Template – Source** window, click **Browse**.

   A window displays file directories.

6. Perform the following actions:

   a Navigate to the file location.

   b Select the file:

   <Zone Controller.ovf>

   c Open the file.

   The `.ovf` file has the following format: `ZC-Astro-`***<VERSION_NUMBER>***`.ovf`

   d Click **Next**.

7. In the **Deploy OVF Template – OVF Template Details** window, click **Next**.
8. In the **Deploy OVF Template – Name and Location** window, perform the following actions:

   a In the **Name** field, enter the appropriate host name.

   - For a Zone Controller at a zone core, enter: `zc0`***<Y>***`.zone`***<X>***
   - For a Zone Controller at a Tsub prime site, enter: `z00`***<X>***`s`***<PPP>***`tzc01.site`***<P>***`.zone`***<X>***

   where:

   <X> is the number of the zone in which the VMS hosting the Zone Controller is located. The possible values are: 1–7.
   <Y> is the Zone Controller instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.
   <PPP> is the 3-digit zero-padded number of the Tsub prime site in which the Zone Controller is located. The possible values are: 001-064.
   <P> is the number of the Tsub prime site. The possible values are: 1-64.

NOTICE: The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

b Click **Next**.

9 Optional: If the **Resource Pool** window appears, click on the IP address of the server. Click **Next**.

10 **If you are deploying the Zone Controller from the vCenter Server:** In the **Host / Cluster** window, perform the following actions:

a Select **Cluster** under **Datacenter**.

b Click **Next**.

c Select the host on which you want to deploy the Zone Controller. See the *System IP Plan*.

d Click **Next**.

11 If the **Deploy OVF Template – Storage** window appears, perform the following actions:

a Select a datastore to install the virtual machine upon.

- For the Zone Controller in an L1 or M1 core, outside a Trunking Subsystem (Tsub), select: **z00*<X>*das*<YY>*_datastore1**
- For the Zone Controller in an L2, M2, or M3 core, outside a Trunking Subsystem (Tsub), select: **z00*<X>*vms*<VV>*_datastore1**
- For the Zone Controller in a K core, select **z00*<X>*vms01_datastore1**
- For the Zone Controller at a Trunking Subsystem (Tsub) prime site, select: **z00*<X>*s*<PPP>*vms01_datastore1**

where:

<X> is the zone number. The possible values are: 1-7.
<YY> is the instance of the Direct Attached Storage (DAS).
<VV> is the number of the Virtual Management Server (VMS) on which the Zone Controller virtual machine is hosted.
<PPP> is the 3-digit zero-padded number of the prime site in which the Zone Controller virtual machine is located. The possible values are: 001-064.

b Click **Next**.

12 In the **Deploy OVF Template – Disk Format** window, perform one of the following actions:

- If the **Thick Provision Eager Zeroed** format is an available option, select it.
- If that option is not available, select **Thick Provision**.

13 Click **Next**.

14 In the **Deploy OVF Template – Network Mapping** window, select the appropriate **Destination Network** for each **Network Source**.

- For **znm0**, select **Zone Network Management**.
- For **cp1**, select **Call Processing Site Link 1**.
- For **cp2**, select **Call Processing Site Link 2**.

15 Click **Next**.

16 In the **Deploy OVF Template – Ready to Complete** window, verify the deployment settings. Click **Finish**.

NOTICE: Ensure that the **Power on after deployment** check box is cleared. Modifications done after deployment require the virtual machine to be powered off.

The import starts.

17 When the process is completed successfully, verify that the left pane of the **vSphere Client** main window displays the application virtual machine name. You may need to expand the list in the left pane to locate the virtual machine name.

18 In the **Deployment Completed Successful** window, click **Close**.

19 Optional: If you used the DVD, remove it from the DVD drive.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.3 Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default HA cluster settings and modify the restart priority for the new VMs. After a host failure, the VMs are restarted in the relative order determined by their restart priority.

When and where to use:

- This procedure applies only to systems where vCenter is installed.
- Run this procedure only if a VM OVF was deployed after the vCenter was originally configured.

Procedure:

1 Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.

   - Connect to: `https://`***`<vCenterIP>`***`/vsphere-client`
   - Ignore or accept any warnings about the connection security or self-signed certificates.

2 In the dialog box, perform the following actions:

   a Type in the user name `administrator@z00`***`<Z>`***`vcs`***`<H>`***`.zone`***`<Z>`***

   where ***<Z>*** is the zone number and ***<H>*** is the vCenter instance number

   b Type in the administrator user password.

   c Click **Login**.

   The vSphere Web Client homepage appears.

3 In the left pane, click **Hosts and Clusters**.

4 Expand the tree and right-click the **Zone*<X>*** HA cluster

   where ***<X>*** is the zone number.

5 Select **Settings**.

6 In the **Settings** window, click **VM Overrides**.

7 Click **Add**.

8 Click the **+** button.

9 Select the check box for the VM you are configuring. Click **OK**.

10 Depending on the VM you are configuring, perform the following actions:

- For the vCenter VM, change the **VM Restart Priority** to **Medium**.
- For the VMs that are monitored under Fault Tolerance, change the **VM Restart Priority** to **High**.
- For the VMs that are not monitored under Fault Tolerance/HA, change the **VM Restart Priority** to **Disabled**.

11 Click **OK**.

12 **Perform the following actions only if you are recovering the VM after a failure and the VM is not monitored under Fault Tolerance:**

  a In the **Settings** window, click **VM/Host Groups**.

  b Select the group for the Virtual Management Server (VMS) on which the VM resides and click **Edit**.

  c Click **Add**.

  d Select the check box next to the VM and click **OK**.

  For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.

  e Click **OK**.

The restart priority setting for the newly deployed virtual machine is configured.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.4

Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

A desktop shortcut was created during installation.

2 Log on to the server as a user with root privileges.

3 On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.

4 On the right side of the window, select the **Configuration** tab.

The window displays information about the configuration of the ESXi server.

5 In the **Software** section, select **Virtual Machine Startup/Shutdown**.

6 On the right side of the main window, select **Properties**.

7 In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.

8 In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.

9 In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.

10 Put the virtual machines hosted on the ESXi server in the correct boot order:

   a In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

   b By using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

   NOTICE:
   Zone Core Virtual Machine Boot Order on page 42 outlines the boot order for the virtual machines that can reside on an ESXi-based Zone Core Virtual Management Server (VMS).

   To determine the correct ordered slot for each virtual machine hosted on the ESXi server that you are configuring, see the boot order table.

   c Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.

11 Click **OK**.

The **Properties** window closes.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.4.1 Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the GMC can be on the server.

If UNCDS is present, three instances of the UNCDS are on the server.

Table 2: Zone Core Virtual Machine Boot Order

Order		Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup						
	1	ZC	Enabled	Use Default	Use Default	Use Default
	2	Transcoder	Enabled	Use Default	Use Default	Use Default
	3	ISGW	Enabled	Use Default	Use Default	Use Default
	4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
	5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
	6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
	7	License Manager	Enabled	Use Default	Use Default	Use Default
	8	ATR	Enabled	Use Default	Use Default	Use Default
	9	DC-System	Enabled	Use Default	Use Default	Use Default
	10	DC-Zone	Enabled	Use Default	Use Default	Use Default
	11	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order		AuC	Enabled	Use Default	Use Default	Use Default
		BAR	Enabled	Use Default	Use Default	Use Default

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
	CSMS	Enabled	Use Default	Use Default	Use Default
	InfoVista	Enabled	Use Default	Use Default	Use Default
	FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
	GDG	Enabled	Use Default	Use Default	Use Default
	GMC	Enabled	Use Default	Use Default	Use Default
	NM Client	Enabled	Use Default	Use Default	Use Default
	UCS	Enabled	Use Default	Use Default	Use Default
	SSS	Enabled	Use Default	Use Default	Use Default
	Syslog	Enabled	Use Default	Use Default	Use Default
	UEM	Enabled	Use Default	Use Default	Use Default
	UNC	Enabled	Use Default	Use Default	Use Default
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.5

Configuring CPU Memory Settings for the Zone Controller

Procedure:

1. From a Windows-based device, launch the **VMware vSphere Client**.

   A desktop shortcut was created during installation.

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

2. Log on to the ESXi server as the root user. In the appropriate fields, enter the IP address of the server, the `root` user name, and the root password.

   The **vSphere Client Inventory** screen appears.

3. In the pane on the left, verify the state of the Zone Controller virtual machine that you want to configure. If the virtual machine is powered on, power it off by right-clicking the virtual machine and selecting **Power** → **Power Off**.
4. Right-click the virtual machine and click **Edit Settings**.
5. In the **Virtual Machine Properties** window, perform the following actions:
   - a In the **Hardware** column on the left, select **Memory**.
   - b In the **Memory Configuration** section on the right, set the **Memory Size** to **2304 MB**.
   - c In the **Hardware** column on the left, select **CPUs**.
   - d In the section on the right, set the **Number of virtual sockets** to **2**.

- **e** Click the **Resources** tab.
- **f** In the **Settings** column on the left, select **CPU**.
- **g** In the **Resource Allocation** section on the right, set the **Reservation value**:
  - For the Zone Controller installed on an HP ProLiant DL380 Gen8 server, set the **Reservation value** to **2593 MHz**.
  - For the Zone Controller installed on an HP ProLiant DL380 Gen9 server, set the **Reservation value** to **2497 MHz**.
- **h** In the bottom right corner, click **OK**.

  The changes are saved and the **Virtual Machine Properties** window is closed.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.6 Applying Supplemental Configuration to Virtual Machines

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) require supplemental configuration to improve their security settings. You apply the supplemental configuration by running a script stored on the *VMware vSphere Configuration Media* disc.

Prerequisites:

- Obtain the *VMware vSphere Configuration Media* disc.
- Install VMware PowerCLI on the Windows-based device. See "Installing VMware PowerCLI" in the *Virtual Management Server Software* manual.

When and where to use: To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, Dispatch Console, or service computer/laptop.

Procedure:

1. Insert the *VMware vSphere Configuration Media* disc into the optical drive of the Windows-based device.
2. Open the PowerShell command prompt as administrator, using the actions that apply to the Windows operating system version present on the device.

If…	Then…
For Windows 7 or Windows Server 2008,	perform the following actions: **a** From **Start**, in the **Search programs and files** field, enter: `Command Prompt` **b** Right-click **Command Prompt** and select **Run as administrator**. **c** If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see. **d** If you are not logged on with an administrative account, enter the domain admin credentials. **e** At the command prompt, enter: `powershell`
For Windows 10 or Windows	perform the following actions: **a** From **Start**, click **Search**.

If…	Then…
Server 2012,	**b** In the search field, type in `powershell` **c** Right-click **Windows PowerShell**, and select **Run as administrator**. • If the **User Account Control** window appears, click **Yes**. • If you are not logged on with an administrative account, enter the domain admin credentials.

3. At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* disc followed by a colon.

   Step example: `E:`
   The directory is changed to the root directory of the *VMware vSphere Configuration Media* disc.

4. At the PowerShell prompt, enter: `cd common\bin`

   The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media* disc.

5. At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`
6. At the ESXi host IP prompt, enter the IP address of the ESXi host.
7. At the user name prompt, enter the ESXi host user name for an administrative account.
8. At the password prompt, enter the ESXi host password for an administrative account.
9. At the PowerShell, prompt, enter the name of the virtual machine for which you want to update the configuration.

   NOTICE: Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the ESXi host.

   - For a zone core Zone Controller virtual machine, the name is: `zc0`***<Y>***`.zone`***<X>***
   - For a Tsub Zone Controller virtual machine, the name is: `z00`***<X>***`s`***<PPP>***`tzc01.site`***<P>***`.zone`***<X>***

   where:

   <X> is the number of the zone in which the VMS hosting the Zone Controller is located. The possible values are: 1–7.
   <Y> is the Zone Controller instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.
   <PPP> is the 3-digit zero-padded number of the prime site in which the Zone Controller is located. The possible values are: 001-064.
   <P> is the number of the Tsub prime site. The possible values are: 1-64.

   The virtual machines supplemental configuration is applied.

10. Verify that there are no messages stating `[FAILED]` in the output of the script.
11. At the PowerShell prompt, enter: `exit`
12. At the Windows command prompt, enter: `exit`

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.7 Connecting and Powering On the Zone Controller

Prerequisites: Obtain the name of the appropriate zone network for the server you are setting up as a virtual machine from your system administrator.

When and where to use: After all virtual machines applications are installed, run the Zone Controller application as the first one in the boot sequence order.

Procedure:

1. To edit the configuration settings for the virtual machine you imported, in the navigation pane, right-click the virtual machine that you imported.

   A pop-up menu appears.

2. Select **Edit Settings** from the menu.

   A dialog box appears.

3. Select the first network adapter.
4. Select the **Connect at power on** check box.
5. Ensure that the correct zone network connection displays for **Network label**.
6. Select the second network adapter.
7. Select the **Connect at power on** check box.
8. Ensure that the correct zone network connection displays for **Network label**.
9. Select the third network adapter.
10. Select the **Connect at power on** check box.
11. Ensure that the correct zone network connection displays for **Network label**.
12. Click **OK**.
13. In the navigation pane, perform the following actions:
    - a Right-click the Zone Controller virtual machine.
    - b Select **Power** → **Power On**.

    The selected virtual machine powers on.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.8 Configuring the Time Zone on Linux Servers

As a part of the installation, ensure that the virtual machine is set to the correct time zone.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.

2. Log on to the ESXi server hosting the virtual machine as root by entering the IP address of the server and the root credentials.

3 In the **vSphere Client Inventory** window, verify that the virtual machine is powered on. If the virtual machine is powered off, power it on by right-clicking the virtual machine in the navigation pane and selecting **Power** → **Power On**.

4 From the navigation pane on the left, select the virtual machine. Click the **Console** tab for this virtual machine.

5 Wait until a prompt to log on console appears.

6 Click in the **Console** window and log on to the virtual machine as root.

7 At the prompt, enter: `admin_menu`

8 In the main administration menu, enter the number for the **OS Administration** option.

9 In the **OS Administration** menu, enter the corresponding number for **Manage Platform Configuration**.

10 In the **Manage Platform Configuration** menu, enter the corresponding number for **Set Time Zone**.

A menu displays numbered options to the change time zone.

11 The **Set Time Zone** option starts by prompting you for the region of the world.

You can choose to specify the time zone using the **Posix TZ format**. Continue responding to the prompts until you see a message regarding `/usr/bin/tzselect`. Ignore the message.

12 Press `q` to quit the menu.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.9

Establishing the Zone Controller Identity

Configure the identity parameters of the Zone Controller virtual machine.

The identity configuration allows other network elements to locate the Zone Controller virtual machine in the system. The identity parameters include the zone core or Tsub location, DSR configuration, zone ID, application ID, and optionally, a list of Centralized Logging Servers.

Procedure:

1 From a Windows-based device, launch the **VMware vSphere Client**.

A desktop shortcut was created during installation.

2 Log on to the ESXi server hosting the Zone Controller virtual machine as root by entering the IP address of the server and the root credentials.

The **vSphere Client Inventory** window appears.

3 In the navigation pane on the left, select the Zone Controller virtual machine. Click the **Console** tab.

4 In the **Console** tab, log on to the Zone Controller virtual machine as root.

5 At the command prompt, enter: `admin_menu`

6 In the **Main Menu**, enter the number corresponding to the **OS Administration** option.

7 In the **OS Administration** menu, enter the number corresponding to the **Manage Platform Configuration** option.

8 In the **Manage Platform Configuration** menu, enter the number corresponding to the **Set Identity** option.

9. At the location type prompt, enter the number corresponding to the zone core or the Trunking Subsystem (Tsub) in which the Zone Controller virtual machine is located.
10. **Zone Controller at a Tsub prime site:** At the Tsub ID prompt, enter the number corresponding to the Prime Site in which the Zone Controller virtual machine is located.
11. At the Dynamic System Resilience (DSR) prompt, perform one of the following actions:
    - If the system is configured for DSR, enter: `y`
    - Otherwise, enter: `n`
12. **DSR systems only:** At the DSR core type prompt, enter the number corresponding to the DSR core type that this virtual machine is being installed in.
13. At the zone ID prompt, enter the number corresponding to the zone number that this virtual machine is being installed in.
14. At the application ID prompt, enter the application ID that should be used for this Zone Controller installation:
    - For the Zone Controller on VMS01 in a Tsub, enter `1`.
    - For the Zone Controller located in a zone core, enter: `1` on VMS01, `2` on VMS02, `3` on VMS09, `4` on VMS10.

    NOTICE: The VMS number depends on the location of the server in a core or subsystem of a specific type:

    - VMS01: non-redundant cores (K cores, L1 and M1 cores), redundant cores (L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites.
    - VMS02: redundant cores (L2, M2, M3) and redundant DSR primary cores
    - VMS09: DSR backup cores
    - VMS10: redundant DSR backup cores
15. **DSR systems only:** At the M3 DSR core prompt, perform one of the following actions:
    - If this Zone Controller virtual machine is being installed in an M3 DSR core, enter: `y`
    - Otherwise, enter: `n`
16. At the syslog prompt, perform one of the following actions:
    - If Centralized Syslog Servers are part of the system configuration, enter their IP addresses or hostnames. Separate multiple entries with a colon.
    - Otherwise, press Enter.

    A summary of the selected options appears.
17. At the confirmation prompt, verify that the input is correct. Enter: `Y`.

The identity configuration for the Zone Controller virtual machine is applied. The virtual machine is restarted.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.10 Joining a Domain for Centralized Authentication

You can join the Zone Controller (ZC) to an Active Directory domain locally at the ZC.

Procedure:

1. From a Windows-based device, launch the **VMware vSphere Client**.

   A desktop shortcut was created during installation.
2. Log on to the ESXi server hosting the Zone Controller virtual machine as root by entering the IP address of the server and the root credentials.

   The **vSphere Client Inventory** window appears.
3. In the navigation pane on the left, select the Zone Controller virtual machine. Click the **Console** tab.
4. In the **Console** tab, log on to the Zone Controller virtual machine as root.
5. At the prompt, enter: `admin_menu`
6. In the **Main Menu**, enter the number for the **Services Administration** option.
7. In the **Services Administration** menu, enter the number for the **Manage AAA Client Configuration** option.
8. In the **Manage AAA Client Configuration** menu, enter the number for the **Join a Domain** option.

If…	Then…
If the Zone Controller is not currently joined to the Active Directory domain,	a list of Active Directory domains appears. Go to step 9.
If the Zone Controller is already joined to the Active Directory domain,	perform the following actions: **a** When the system prompts you to unjoin the current domain, enter: `c` **b** At the domain account prompt, enter the domain administrator account. **c** At the password prompt, enter the domain administrator account password. The Zone Controller is removed from the domain and a list of Active Directory domains appears.

9. Enter the number for the domain that you want to join.
10. At the domain account prompt, enter the domain administrator account.
11. At the password prompt, enter the domain administrator account password.

    The system begins the non-global zone configuration, the Zone Controller joins the domain. When the process is completed, a confirmation message appears.
12. In the **Manage AAA Client Configuration** menu, enter: **q**

    The Zone Controller prompt appears.

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.1.11 Applying the Platform Patch

You must update the virtual machine by applying the platform patch.

Prerequisites: Obtain the *PLATFORM PATCH* DVD or ISO for the current system release.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.
2. Log on to the ESXi server.
3. Verify whether the following path appears on the toolbar: **Home** → **Inventory** → **Inventory**.
4. In the left pane, navigate to the virtual machine that you want to update.
5. In the right pane, click the **Console** tab.
6. Connect the virtual machine to the local DVD drive or ISO:

If…	Then…
If you have the DVD,	perform the following actions: a Insert the DVD in the drive of the Windows-based device. b In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to *`<drive letter:>`*** where ***`<drive letter>`*** represents the drive with the DVD.
If you have the ISO,	perform the following actions: a Upload the ISO image to the Windows-based device. b In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to ISO image on local disk**.

7. Navigate to the location of the patch ISO and select it. Click **Open**.
8. Click anywhere in the **Console** tab and log on to the virtual machine as the root user.
9. Enter: `systemctl start autofs`

   If messages appear about the autofs service already running, ignore them.
10. Enter: `ls /media/cdrom0/`

    If the drive contains the updater script, the update directory appears.
11. If the update directory does not appear, enter: `ls /media/cdrom1/`
12. Enter one of the following commands:
    - If the updater script is on cdrom0, enter: `/media/cdrom0/update/updater`
    - If the updater script is on cdrom1, enter: `/media/cdrom1/update/updater`
13. Change the directory to root by entering: `cd /`
14. Enter: `systemctl stop autofs`

    If messages appear about the autofs service, ignore them.
15. Remove the DVD or ISO:

a Disengage the cursor from the console by pressing left CTRL + ALT.

b In the VMware vSphere Client, click the disc icon on the top toolbar and disconnect the DVD or ISO from the virtual machine.

c If prompted, confirm the operation.

16 Click anywhere in the **Console** tab.

17 Press ENTER.

18 Enter: `exit`

Related Links

Deploying the Zone Controller Virtual Machine on page 36

3.2
Configuration on ESXi-based Server

This section includes the configuration procedures for the Zone Controller on the ESXi-based server.

3.2.1
Information Assurance Configuration

Information Assurance (IA) configuration can be performed locally in the Zone Controller application.

For more information on how to perform the following IA procedures locally in the Zone Controller application hosted on VMS platform, see the following sections in the Zone Controller Operations on page 56 chapter:

- For centralized authentication, see Joining a Domain for Centralized Authentication on page 49.
- For centralized logging, see Centralized Logging on page 70.
- For centralized backup, see Centralized Backup and Restore (BAR) Service for Zone Controllers on page 94.
- For SNMPv3 configuration, see SNMPv3 USM Administration on page 71.
- For SSH key rotation, see Key Rotation Overview on page 75.

3.2.2
Zone Controller Redundancy and Switchover

You can perform tasks related to the zone core Zone Controller redundancy and switchover administration locally from the Zone Controller administration menu or the Unified Network Configurator (UNC) application.

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

IMPORTANT: Due to the system impact of a manual switchover event, initiate a switchover **ONLY** when necessary. Before performing a manual switchover, verify the health and status of the standby Zone Controller first from the network fault management application.

For more information, see “Zone Controller Quick Commands” in the *Unified Network Configurator* manual.

Related Links

Redundancy and Switchover Overview on page 25

3.2.2.1 Setting a Standby Zone Controller to Active

A manual switchover between Zone Controllers in the zone core must be initiated from the Standby ZC.

Manually switching a Standby ZC to Active causes all sites in the zone to go into site trunking. No wide area communications are possible in the zone for up to two minutes. Thereafter, only limited services are available until subscriber and talkgroup affiliation tables have been uploaded from the sites to the newly Active ZC.

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

Procedure:

1 Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.

2 Enter: `admin_menu`

The **Zone Controller Main Menu** appears.

3 Enter the corresponding number for **Application Administration**. Press Enter.

4 Enter the corresponding number for **Manage System Redundancy and Resilience**. Press Enter.

5 Enter the corresponding number for **Manage Controller Redundancy Configuration**. Press Enter.

6 Enter the corresponding number for **Change Application Redundancy Object State**. Press Enter.

The following message appears, followed by the Set HA Redundancy State menu:

```
Common Application State: Enabled
Common Application Cause: Normal
Application Redundancy Object State: Standby
------------------------------
***WARNING***
A transition to Active will cause the currently Active Controller to
reset
```

7 Enter the corresponding number for **Request a state of Active**. Press Enter.

The following prompt appears:

```
Are you sure you want to do this?
```

8 Enter: **y**

The following message appears, followed by the Zone Controller Administration menu:

```
SNMP Set of the Redundancy state was successful
```

3.2.2.2 Setting the Zone Controller to User Requested Standby

For upgrade purposes, you can set the Zone Controller in the zone core to User Requested Standby mode. Perform upgrades on the Standby ZC.

IMPORTANT: If both ZCs are in User Requested Standby mode, neither ZC can become active and all sites in the zone go into site trunking.

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter: `admin_menu` command at the prompt.

   The Zone Controller Main Menu appears.
3. Select **Application Administration** from the menu. Press Enter.

   The Services Administration menu appears.
4. Select **Manage System Redundancy and Resilience**. Press Enter.

   The Manage System Redundancy and Resilience menu appears.
5. Select **Manage Controller Redundancy Configuration**. Press Enter.

   The Manage Controller Redundancy Configuration menu appears.
6. Select **Change Application Redundancy Object State**. Press Enter.

   The Set HA Redundancy State menu appears.
7. Select **Request a state of User Requested Standby**. Press Enter.

   The following prompt appears:

   ```
   Are you sure you want to do this?
   ```

   CAUTION: A transition of **Active to User Requested Standby** will cause the Zone Controller to reset.
8. Enter: **y**

   The following message appears, followed by the Zone Controller Administration menu:

   ```
   SNMP Set of the Redundancy state was successful
   ```
9. Enter: `b`

   The Manage Controller Redundancy Configuration menu appears.
10. Select **Display Application Status** from the Manage Controller Redundancy Configuration menu. Press Enter.
11. Enter: `q`

    The prompt appears.

3.2.2.3 Setting the User Requested Standby Zone Controller to Active or Standby

Once an upgrade has been performed, you can set the Zone Controller that was set to User Requested Standby mode before the upgrade to either Active or Standby mode.

Redundancy and switchover operations do not apply to the Trunking Subsystem (Tsub) ZC. The Tsub ZC is always active. Sites that lose connectivity to the zone core, connect to the Tsub ZC for local area operation.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter: `admin_menu`

   The **Zone Controller Main Menu** appears.
3. From the menu, select **Application Administration**. Press Enter.
4. From the **Services Administration** menu, select **Manage System Redundancy and Resilience**. Press Enter.
5. From the **Manage System Redundancy and Resilience** menu, select **Manage Controller Redundancy Configuration**. Press Enter.
6. From the **Manage Controller Redundancy Configuration** menu, select **Change Application Redundancy Object State**. Press Enter.
7. From the **Set HA Redundancy State** menu, select **Request a state of Active** or **Request a State of Standby**. Press Enter.

   The confirmation prompt appears.

   ⚠ **CAUTION:** A transition of Active will cause the currently Active Controller to reset.
8. Enter: **y**

   The successful message appears, followed by the **Zone Controller Administration** menu.
9. Enter: `b`
10. From the **Manage Controller Redundancy Configuration** menu, select **Display Application Status**. Press Enter.
11. Enter: `q`

3.2.2.4 Zone Controller Switchover Verification

After a manual zone core Zone Controller switchover has been performed either from the Unified Network Configurator (UNC) or the local administration menu, view the **Application Redundancy Object State** with the **Display Application Status** menu option.

See Viewing the Zone Controller Display Status on page 57.

3.2.3 Configuring the Network Management

The Unified Network Configurator (UNC) is an application used to configure and maintain operational parameters for a Zone Controller in a system. The UNC database stores configuration information for the Zone Controller.

Process:

1. Discover the Zone Controller. See “Device Discovery” in the *Unified Network Configurator* manual.
2. Configure the Zone Controllers to either active, standby, or User Requested Standby. See the “Zone Controller Quick Commands” table in the *Unified Network Configurator* manual.
3. To ping, test SNMP credentials, test credentials, or display HZM state. See the “Zone Controller Quick Commands” table in the *Unified Network Configurator* manual.
4. Perform a UCM Data Sync State for the Zone Controller. See “PM Data Sync State” in the *Unified Network Configurator* manual.
5. Delete the Zone Controller from a network. See “Deleting a Device” in the *Unified Network Configurator* manual.
6. Replace the Zone Controller in a network. See “Replacing a Device” in the *Unified Network Configurator* manual.

3.2.4 Dialing Restrictions Configuration

You can configure the disallowed dialing patterns as a part of the interconnect subsystem in the UNC configuration. By configuring the disallowed dialing patterns, you can add dialing restrictions. For more information, see “Configuring Disallowed Dialing Patterns” in the *Enhanced Telephone Interconnect Feature Guide* manual.

The Provisioning Manager (PM) is used to configure the dialing restrictions on a subscriber. The Exclusion Class ID field is used by the Zone Controller to map to the associated dialing restrictions. For more information, see “Interconnect Subsystem Configuration in the Provisioning Manager” in the *Enhanced Telephone Interconnect Feature Guide* and “Creating Records” in the *Provisioning Manager* manual.

Chapter 4

Zone Controller Operations

This chapter details tasks that you perform once the Zone Controller application is installed and operational on your system.

4.1

Logging On to a Zone Controller Application

The Zone Controller virtual machine resides on the Virtual Management Server (VMS) with the ESXi operating system. You can log on to the common Unix administration menu of the Zone Controller virtual machine on the VMS by using the VMware vSphere Client.

You can also log on to the Zone Controller by using PuTTY. For more information, see "Using PuTTY to Access an SSH Server from a Windows-Based Device" procedure in the *Securing Protocols with SSH* manual.

Prerequisites: From your system administrator, obtain the following information:

- IP address of the VMS hosting the Zone Controller virtual machine
- Password for the root user account

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.
2. Log on to the VMS hosting the Zone Controller virtual machine with local administrator root account credentials.

   The **vSphere Client Inventory** window appears.
3. On the pane on the left, right-click the Zone Controller virtual machine and click **Open Console**.
4. In the **Console** tab, log on to the Zone Controller virtual machine with the appropriate user account credentials.

   For more information about Active Directory user accounts, their authentication roles, and the administration menu operations they are authorized to perform, see Zone Controller Administration Menu on page 90.

   You can log on to the Zone Controller administration menu, by entering `admin_menu`.

Related Links

Viewing the Zone Controller Display Status on page 57
Setting the Heartbeat Key on page 61
Setting ZC-ISGW (ISSI 8000/CSSI 8000) Shared Secret on page 62
Resetting the Application on page 62
Requesting InterZone Capable for Local Zone on page 63
Requesting Zone Isolated for Local Zone on page 63
Checking Zone Call Processing Status on page 64
Registering Centralized Backup and Recovery Client on page 67
Resetting Zone Controller BAR Client on page 67
Verifying BAR SSH Keys on page 67
Getting BAR SSH Keys on page 68

Turning Off/On Zone Controller Messages on page 68
Changing Passwords on page 69
Displaying Domain Membership Status on page 69
Viewing the Centralized Logging Menu on page 70
Configuring SNMP Common Agent on page 71
Changing the IP PBX Server User Name on page 71
Changing the IP PBX Server User Password on page 72
Adding Centralized Logging Servers on page 70
Removing Centralized Logging Servers on page 70
Showing the Status of the Centralized Logging Server on page 70

4.2 Logging Off the Zone Controller Application

Use the System Administration menu to log off from the Zone Controller application.

CAUTION: For security purposes, always log off when you are finished administering a Zone Controller. Never leave a Zone Controller application open at the administration menu. Sessions time out after 15 minutes of inactivity on their own, but for security reasons, you must log off when you have finished administering a Zone Controller application.

Procedure:

At the Zone Controller prompt, enter: `exit`

Depending on the method that you used to log on to the Zone Controller virtual machine, you are either logged off from the Zone Controller **Console** in the VMware vSphere Client or the PuTTY session ends.

4.3 Zone Controller Administration

This topic lists the Zone Controller administration tasks.

4.3.1 Viewing the Zone Controller Display Status

The **Display Status** function checks the HA state, paths/links, and replication as either Up or Down.

The status of each Zone Controller is indicated as either Up or Down in the network fault management application of the zone.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter: `admin_menu`
3. Enter the corresponding number for **Application Administration**. Press Enter.
4. Enter the corresponding number for **Manage Application Status**. Press Enter.
5. Enter the corresponding number for **Display Application Status**. Press Enter.

   The message with three sections showing the current status of the ZC appears: HA State Info, HA Link/Path Info and Replication Info.

```
HA Link/Path Info
-------------
```

```
Common Application State: Enabled
Common Application Cause: Normal
Application Redundancy Object State: Active
```

Related Links

HA Link/Path Info Example on page 58
Zone Controller Common Application States on page 59
Zone Controller Common Application Causes on page 59
Zone Controller Application Redundancy Object States on page 59
Zone Controller Link States on page 59
Zone Controller Link Causes on page 60
Zone Controller Path States on page 60
Zone Controller Path Causes on page 60
Zone Controller Replication States on page 61
Zone Controller Replication Causes on page 61

4.3.1.1 HA Link/Path Info Example

Table 3: Example of HA Link/Path Info and Replication Info

HA Link/Path Info -----------------		
Link State Cause	ZC01 LinkUp Normal	ZC02 LinkUp Normal
--		
Path 1 State Cause	PathUp Normal	PathUp Normal
--		
Path 2 State Cause	PathUp Normal	PathUp Normal
--		
Path 3 State Cause	PathUp Normal	PathUp Normal
Press Enter key to continue		
Replication Info ----------------		
Replication to ZC01	Replication State synchronizationIn Progress synchronization Complete	Replication Cause Normal Normal

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.2 Zone Controller Common Application States

Enabled
Zone controller is operational.

Enabling
Zone controller is loading Configuration Data.

CritcalMalfunction
Zone controller is unable to support Call Processing.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.3 Zone Controller Common Application Causes

Normal
This is a normal operational state.

UserRequested
State (Enabling) is the result of a requested reset.

SoftwareError
State (CriticalMalfunction) is the result of software failure.

CommunicationFailure
State (CriticalMalfunction) is the result of router communication failure.

NoConfiguration
State (CriticalMalfunction) is the result of Configuration Data missing configuration sufficient to establish router communications.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.4 Zone Controller Application Redundancy Object States

Active
Performing Call processing for the zone.

Standby
Becomes Active automatically if capable and no other active Zone Controller exists.

UserRequestedStandby
User has requested the Zone Controller to remain in standby. The Zone Controller does not become active until the user requests a different redundancy state.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.5 Zone Controller Link States

N/A
Redundant Peer does not exist.

LinkUp
HA Link with peer Zone Controller is up.

LinkDown
HA Link has failed.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.6
Zone Controller Link Causes

N/A
Redundant Peer does not exist.

Normal
State (LinkUp), a normal operating mode.

AllPathsDown
State (LinkDown), due to all paths failing.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.7
Zone Controller Path States

N/A
Redundant Peer does not exist.

PathUp
Path on NET0, NET1, and NET2 to peer Zone Controller is operational.

PathDown
Path on NET0, NET1, and NET2 is peer Zone Controller is not operational. If peer Zone Controller is operational, check routers, cables, and other transport equipment for problems.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.8
Zone Controller Path Causes

N/A
Redundant Peer does not exist.

Normal
State (PathUp) is a normal operating mode.

CommunicationFailure
A significant number of properly authenticated packets from the peer Zone Controller have not been received.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.9

Zone Controller Replication States

N/A

Redundant Peer does not exist.

noSynchronization

Replication is not operating.

criticaldataSyncInProgress

The replication of critical database records is in progress. Avoid manual switchovers at this time.

noncriticalSyncInProgress

The replication of critical database records is complete and non-critical data replication is now in progress. Avoid manual switchovers at this time.

synchronizationComplete

The replication of mobility information has reached steady state. Replication occurs in lockstep with mobility notifications received by the Zone Controller. The system is as ready as possible for switchover to the target Zone Controller.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.1.10

Zone Controller Replication Causes

N/A

Redundant Peer does not exist.

normal

Replication is operating properly (InProgress or Complete).

linkDown

No replication is occurring due to communications problem.

zcVersionMismatch

Replication link is up but replication is not possible due to different Zone Controller versions.

otherZcIsNotActive

Replication link was established with a controller that is not active. The link drops and re-establishes with the new active Zone Controller.

Related Links

Viewing the Zone Controller Display Status on page 57

4.3.2

Setting the Heartbeat Key

The heartbeat key is used for authentication of the heartbeat packets sent between all Zone Controllers in a zone. The heartbeat key must be the same on all the Zone Controllers in the zone. If it is different, authentication fails, and the Zone Controllers do not recognize one another. The Set Heartbeat Key function sets the key to either ASCII based or hexadecimal based.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Application Administration**. Press Enter.

3. Enter the corresponding number for **Manage System Redundancy and Resilience**. Press Enter.
4. Enter the corresponding number for **Manage Controller Redundancy Configuration**. Press Enter.
5. Enter the corresponding number for **Set Heartbeat Key**. Press Enter.
6. Enter the corresponding number for either **Set ASCII Based High Availability Heartbeat Key** or **Set Hexadecimal Based High Availability Heartbeat Key**.
7. Enter the key. Press Enter.

   The Zone Controller administrative menu appears.

4.3.3
Setting ZC-ISGW (ISSI 8000/CSSI 8000) Shared Secret

The ZC-ISGW shared secret is used for authentication and encryption of the ZC-ISGW packets sent between the Zone Controller and ISGW in the ISGW zone. The ZC-ISGW shared secret must be the same on all the Zone Controllers and Intersystem Gateway devices in the zone. If they are different, the Zone Controller will not be able to send subscriber authentication information to a foreign system.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Application Administration**. Press Enter.
3. Enter the corresponding number for **ZC-Specific Management and Operations**. Press Enter.
4. Enter the corresponding number for **Manage ISGW - ZC Shared Secret**. Press Enter.
5. Enter the corresponding number for either **Set ASCII Based ISGW - ZC Shared Secret** or **Set Hexadecimal Based ISGW - ZC Shared Secret**.
6. Enter the shared secret. Press Enter.

   The Zone Controller administrative menu appears.

4.3.4
Resetting the Application

Resetting an Active Zone Controller is another way to force it into a Standby state causing the Standby Zone Controller to become the Active Zone Controller. The Active Zone Controller stops all call processing services and goes into a CriticalMalfunction state. The Standby Zone Controller then goes into an Enabling state, causing it to become the newly Active Zone Controller. Once the newly Active Zone Controller is in the Enabled state, call processing services restart and data from persistent storage loads. Data from the Zone Controller now in Standby is replicated.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Application Administration**. Press Enter.
3. Enter the corresponding number for **Manage Application Status**. Press Enter.
4. Enter the corresponding number for **Reset the Application**. Press Enter.

   The following warning and prompt appear:

   ```
   *** WARNING ***
   ```

```
You are about to reset the Application.
Are you sure you want to do this? [Yy/Nn]:
```

5 To continue, enter: **y**

The following message appears, followed by the Zone Controller Administration menu:

```
Resetting....
```

4.4

Zone Call Processing Administration

In order to administer zone call processing in a multi-zone configuration, make InterZone capable for a local zone, isolate a z zone for a local zone, and check the zone call processing status.

4.4.1

Requesting InterZone Capable for Local Zone

Normally, a Zone Controller is InterZone capable. This means that the zone communicates with the other Zone Controllers in the system, which allows calls from the local zone to include talkgroup members in other zones (InterZone trunking). This also allows individual radio-to-radio calls to be made from the local zone to radio users in other zones. However, if the Zone Controller is set to Zone Isolated, no InterZone calls take place. Interconnect calls from other zones are also not supported when the Zone Controller is set to zone isolated.

Procedure:

1 Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.

2 Enter the corresponding number for **Application Administration**. Press Enter.

3 Enter the corresponding number for **ZC-Specific Management and Operations**. Press Enter.

4 Enter the corresponding number for **Request InterZone Capable for Local Zone**. Press Enter.

The success message appears.

5 Enter: **q**

The **System Administration** menu appears.

4.4.2

Requesting Zone Isolated for Local Zone

In multizone systems, you can isolate the local zone from the other Zone Controllers in the system, if necessary, for troubleshooting, upgrade, or other purposes. Use the Request Zone Isolated function to isolate the zone. When the zone is isolated, the local Zone Controller cannot communicate with the other Zone Controllers in the system. This prevents talkgroup calls in the local zone from including talkgroup members in other zones (InterZone). This also prevents radio-to-radio calls from the local zone to radio users in other zones.

Procedure:

1 Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.

2 Enter the corresponding number for **Application Administration**. Press Enter.

3 Enter the corresponding number for **ZC-Specific Management and Operations**. Press Enter.

4 Enter the corresponding number for **Request Zone Isolated for Local Zone**. Press Enter.

The warning prompt appears.

5 Enter: **y**. To send the request to isolate the Local Zone, press ENTER.

The success message appears.

6 Enter: **q**

The **System Administration** menu appears.

4.4.3 Checking Zone Call Processing Status

Check the status of the InterZone paths and see what is known about the relative status of the Zone Controllers in the other zones. Relative status means the InterZone trunking capability of the remote Zone Controllers as it appears to the local Zone Controller.

When a remote Zone Controller reports that it is not InterZone capable, it is incapable of InterZone communication with the local zone making the query. It does not imply that remote Zone Controller is down, or that it cannot talk with the other zones in the system. The status only applies to the relationship between the remote zone and the local zone.

Procedure:

1 Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.

2 At the prompt, enter:`admin_menu`

3 Enter the corresponding number for **Application Administration**. Press ENTER.

4 Enter the corresponding number for **ZC-Specific Management and Operations**. Press ENTER.

5 Enter the corresponding number for **Check Zone Call Processing Status**. Press ENTER.

Messages similar to the following appear (depending on system states).

```
LOCAL ZONE STATUS:
 Zone 1: NOT IZ TRUNKING CAP - NO LOCAL CORE RP

INTERZONE TRUNKING STATUS:

SUMMARY OF SITE LINK STATUS:
 ALL SITE LINKS DOWN
```

6 Press **b**. Press ENTER.

The ZC-Specific Management and Operations menu appears.

7 Press **b**. Press ENTER.

The Zone Controller administrative menu appears.

Related Links

Call Processing Statuses for the Local Zone on page 65
Call Processing Statuses for Remote Zones on page 65
Call Processing Statuses for Site Links on page 66

4.4.3.1 Call Processing Statuses for the Local Zone

Table 4: Call Processing Statuses for the Local Zone

Status	Reasons	Definition
UNKNOWN STATUS		An internal problem with the local Zone Controller prevents it from making a query. The local zone cannot know or infer any information about itself or the remote zones.
IZ TRUNKING CAPABLE		The local zone is fully capable of InterZone (IZ) trunking.
IZ TRUNKING CAPABLE	NO LOCAL IND ID MAP	The local zone is capable of InterZone trunking, but its individual ID mappings are not present.
NOT IZ TRUNKING CAP	NO LOCAL TG ID MAP	The local zone is not capable of InterZone trunking as the talkgroup ID maps are not present.
	NO ZONE ID	The local zone is not capable of InterZone trunking as its zone ID is not set.
	LOCAL USER REQUEST	The local zone is not capable of InterZone trunking as it has been set to zone isolated by the user.
	NO LOCAL CORE RP	The local zone is not capable of InterZone trunking as the Zone Controller cannot communicate with its local core routers.

Related Links

Checking Zone Call Processing Status on page 64

4.4.3.2 Call Processing Statuses for Remote Zones

Table 5: Call Processing Statuses for Remote Zones

Status	Reason	Definition
UNKNOWN STATUS		An internal problem with the local Zone Controller prevents it from making a query. The local zone cannot know or infer any information about itself or the remote zones.
IZ TRUNKING	MISMATCH IND ID MAPS	The remote zone has InterZone trunking with the local zone, but the remote zones individual ID map does not match the local zones individual ID map.
	NO LOCAL IND ID MAP	The remote zone has InterZone trunking with the local zone. However, the local zones individual ID map is not present.
	NO REMOTE IND ID MAP	The remote zone has InterZone trunking with the local zone. However, the remote zone does not have the individual ID map.
IZ TRUNKING CAPABLE	MISMATCH IND ID MAPS	The remote zone does not have InterZone trunking with the local zone as the individual ID map at

Status	Reason	Definition
		the remote zone does not match the individual ID map at the local zone.
NO IZ TRUNKING	NO IZ DATA COMM	The remote zone does not have InterZone trunking with the local zone due to a problem with the data communication path between the two zones.
	NO LOCAL CORE RP	The remote zone does not have InterZone trunking with the local zone as the local zone cannot communicate with its core routers.
	NO REMOTE CORE RP	The remote zone is not in InterZone trunking with the local zone as the remote zone cannot communicate with the core routers in its zone.
	NO LOCAL TG ID MAP	The remote zone does not have InterZone trunking with the local zone as the local zone does not have the talkgroup ID map.
	NO REMOTE TG ID MAP	The remote zone does not have InterZone trunking with the local zone as the remote zone does not have the talkgroup ID map.
	MISMATCH TG CZ MAPS	The remote zone does not have InterZone trunking with the local zone as the talkgroup ID map at the remote zone does not match the talkgroup ID map at the local zone.
	LOCAL USER REQUEST	The remote zone is not in InterZone trunking with the local zone as the user has set the local zone to zone isolated.
	REMOTE USER REQUEST	The remote zone is not in InterZone trunking with the local zone as the user has set the remote zone to zone isolated.
	NO ZONE ID	The remote zone does not have InterZone trunking with the local zone as the local zone does not have its zone ID.

Related Links

Checking Zone Call Processing Status on page 64

4.4.3.3
Call Processing Statuses for Site Links

Table 6: Call Processing Statuses for Site Links

Status	Definition
ALL SITE LINKS DOWN	The Zone Controller does not have a connection to any IVD/HPD/3600 trunked sites.
AT LEAST ONE SITE LINK UP	The Zone Controller has at least one IVD/HPD/3600 trunked site link up and is trying to or has brought the site into wide trunking.

Related Links

Checking Zone Call Processing Status on page 64

4.5 Zone Controller Backup Administration

The zone configuration database contains the zone infrastructure information. This section covers the centralized Backup and Recovery (BAR) service topic.

For information on restoring data, see Data Restore Information on page 80.

4.5.1 Registering Centralized Backup and Recovery Client

The BAR is enabled on the server by default and the BAR Client is periodically registered at the BAR server. To manually register Centralized Backup and Recovery client, perform this procedure.

To use Centralized Backup and Recovery (BAR), the Zone Controller BAR client needs to be registered with the BAR. For the backup procedures, see the *Backup and Restore Services* manual.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage BAR Client Configuration**. Press Enter.
4. Enter the corresponding number for **Register Client**. Press Enter.

   A success message appears.

4.5.2 Resetting Zone Controller BAR Client

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage BAR Client Configuration**. Press Enter.
4. Enter the corresponding number for **Reset BAR**. Press Enter.

   A message similar to the following appears:

   ```
   Registration at BAR_IP_ADDRESS> completed successfully
   Cleanup completed successfully
   ```

4.5.3 Verifying BAR SSH Keys

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage BAR Client Configuration**. Press Enter.
4. Enter the corresponding number for **Verify SSH Keys**. Press Enter.

   A message similar to the following appears:

```
KEY VERIFICATION FOR BAR CLIENT SUCCESSFUL
```

4.5.4 Getting BAR SSH Keys

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage BAR Client Configuration**. Press Enter.
4. Enter the corresponding number for **Get Host User Keys**. Press Enter.

   A message similar to the following appears:

   ```
   SUCCESS: Host Keys provisioned successfully
   SUCCESS: User Keys provisioned successfully
   ```

4.6 Zone Controller Message Administration

There are several tasks you must familiarize yourself with to get started with Zone Controller message administration.

4.6.1 Turning Off/On Zone Controller Messages

You can turn on and off technical and alert messages on the Zone Controller, which you might do if the condition of your system has deteriorated to the point that messages are affecting system and database performance, or if you do not find the messages useful.

IMPORTANT: Turn messages off and on only on the advice of an experienced service person.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Application Administration**.
3. Enter the corresponding number for **ZC-Specific Management and Operations**.
4. Enter the corresponding number for **Turn off/on Messages**.
5. Press the number indicated to turn on or off a particular message type.

   The following warning message appears on the screen:

   ```
   ********************************************************
   WARNING: You are changing a MAJOR functionality.
   This option is meant to be used as a tool
   to assist you if your system is getting too many
   alerts or tech messages.
   It is NOT intended to solve your problem,
   You need to address the cause of the alerts and tech messages.
   Once the messages are turned off you will not receive them
   again until you resume them.
   Be absolutely sure this is what you want to do.
   ********************************************************
   ```

```
Do you wish to continue? (y,n,q,?) [n]
```

6 To confirm the change, enter: `y`

Messages are turned on or off, depending on the option you selected.

4.7
Zone Controller Unix Administration

There are several tasks you must familiarize yourself with to get started with Zone Controller Unix administration.

4.7.1
Changing Passwords

To access the Zone Controller, use your personal domain account. Access rights and command execution is granted based on the Authorization Role membership of your personal domain account. For more info about those roles, see Table 10: Authentication Roles on page 91.

The username and password on the Zone Controller must match the username and password on the IP PBX server. The purpose of having the same user name and password on both the Zone Controller and IP PBX server is for authentication purposes on the SIP trunk during call set-up. To change the IP PBX server username, see Zone Controller Administration Menu on page 90.

Procedure:

1 Log on to the Zone Controller and stay at the prompt level. See Logging On to a Zone Controller Application on page 56.

2 Enter: `passwd`

3 Enter a new password for the user account. Press Enter.

4 Enter the new password again for verification.

The success message appears.

5 If password verification does not succeed, perform the procedure again.

4.7.2
Displaying Domain Membership Status

Procedure:

1 Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.

2 Enter the corresponding number for **Services Administration**. Press Enter.

3 Enter the corresponding number for **Manage AAA Client Configuration**. Press Enter.

4 Enter the corresponding number for **Display Domain Membership Status**. Press Enter.

If the Zone Controller is currently joined, the **Membership Status** displays **Joined**.

If the Zone Controller is currently not joined, the **Membership Status** displays **Not Joined**.

4.7.3 Centralized Logging

Centralized logging can be done locally at the Zone Controller, as well as in the VMS host. Use the Centralized Logging menu to Add or Remove a centralized logging server or to show the status of the centralized logging server.

4.7.3.1 Viewing the Centralized Logging Menu

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage Syslog Client Configuration**. Press Enter.

4.7.3.2 Adding Centralized Logging Servers

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage Syslog Client Configuration**. Press Enter.
4. Enter the corresponding number for **Add Centralized Logging Server**. Press Enter.

   The following prompt appears:

   ```
   Enter centralized syslog server to add (q=quit) :
   ```
5. Enter the syslog server. Press Enter.

4.7.3.3 Removing Centralized Logging Servers

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.
3. Enter the corresponding number for **Manage Syslog Client Configuration**. Press Enter.
4. Enter the corresponding number for **Remove Centralized Logging Server**. Press Enter.

   The following prompt appears: `Which centralized syslog server would you like to remove? (1-#, a=all, q=quit):`
5. Enter the syslog server. Press Enter.

4.7.3.4 Showing the Status of the Centralized Logging Server

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **Services Administration**. Press Enter.

3. Enter the corresponding number for **Manage Syslog Client Configuration**. Press Enter.
4. Enter the corresponding number for **Display Centralized Logging Status**. Press Enter.

   A prompt similar to the following appears. (This example is when no logging servers have been added.)

   ```
   Centralized Logging is disabled.
   ```
5. Enter the syslog server. Press Enter.

4.7.4 SNMPv3 USM Administration

The implementation of SNMPv3 provides enhanced security and requires USM user passphrases to access the SNMP common agent. The SNMP common agent is used to administer network elements that operate using the Unix operating system.

You can use the SNMP common agent to administer the following settings:

- SNMP user configurations
- SNMP inform configurations
- MotoAdmin passphrases

For more information about using the SNMP common agent or recovering passphrases, see the *SNMPv3* manual.

4.7.4.1 Configuring SNMP Common Agent

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **OS Administration**. Press Enter.
3. Enter the corresponding number for **Security Provisioning**. Press Enter.
4. Enter the corresponding number for **Manage SNMP Passphrases**. Press Enter.
5. Enter the corresponding number for **Configure Agent SNMPv3**. Press Enter.
6. When prompted, enter the passphrase for the following:
   - **MotoAdmin Authentication Passphrase**
   - **MotoAdmin Encryption Passphrase**

   The SNMP common agent grants access. For detailed procedures, see the *SNMPv3* manual.

4.7.5 Changing the IP PBX Server User Name

The username and password on the Zone Controller must match the username and password on the IP PBX server.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **OS Administration**. Press Enter.
3. Enter the corresponding number for **Security Provisioning**. Press Enter.
4. Enter the corresponding number for **Configure PBX User**. Press Enter.

5. Enter the corresponding number for **Change user name and password**. Press Enter.

   The following message is displayed:

   ```
   Enter user name or q to back out:
   ```

6. Enter a new name for the IP PBX server user. Press Enter.

   Username may have lower and upper case letters and must be between 2 and 64 characters in length.

   The following message is displayed:

   ```
   Enter passphrase or q to back out
   ```

7. Enter the password for the new user. Press Enter.

   The passphrase must be 15 – 64 character long and contain at least one each of the following:

   - number
   - uppercase letter
   - lowercase letter
   - special character

   The following message is displayed:

   ```
   Reenter passphrase or b to back out:
   ```

8. Reenter the password for the new user. Press Enter.

   The following message appears, and then the Security Provisioning reappears:

   ```
   sending user new username>
   SNMP Set of the user name and password successful
   ```

4.7.6

Changing the IP PBX Server User Password

The username and password on the Zone Controller must match the username and password on the IP PBX server. The purpose of having the same user name and password on both the Zone Controller and IP PBX server is for authentication purposes on the SIP trunk during call set-up.
The IP PBX Server is present only when the optional Enhanced Telephone Interconnect feature is implemented. For more information, see the *Enhanced Telephone Interconnect Feature Guide*.

Procedure:

1. Log on to the Zone Controller. See Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **OS Administration**. Press Enter.
3. Enter the corresponding number for **Security Provisioning**. Press Enter.
4. Enter the corresponding number for **Configure PBX User**. Press Enter.
5. Enter the corresponding number for **Change password for user**. Press Enter.

   The following message is displayed:

   ```
   Enter passphrase or q to back out
   ```

6. Enter the password for the new user. Press Enter.

   The passphrase must be 15 - 64 character long and contain at least one each of the following:

   - number
   - uppercase letter

- lowercase letter
- special character

The following message is displayed:

```
Reenter passphrase or b to back out:
```

7 Reenter the password for the new user. Press ENTER.

The following message appears, and then the Security Provisioning reappears:

```
SNMP Set of the user name and password successful
```

Related Links

Changing Passwords on page 69

4.8 Upgrading Linux-Based Virtual Machines

Prerequisites:

- Disable the application, if applicable.
- Prepare installation media for the RedHat Enterprise Linux (RHEL) operating system and any applications to be installed.

Procedure:

1 Insert the application update disc into the optical drive.

2 Open **My Computer** and navigate to the optical drive.

The application update `.iso` is shown as the contents of the disc.

3 Copy the application update `.iso` to the desktop.

4 Eject the application update disc from the optical drive.

5 Insert the RHEL installation media into the optical drive of the Windows-based device.

6 Open **My Computer** and note the optical drive letter.

The ***<drive letter>*** is needed in next steps.

7 Launch the **VMware vSphere Client**.

A desktop shortcut was created during installation.

8 Log on to the server as a root user:

a Enter the IP address of the ESXi server that serves as the Virtual Management Server (VMS) host.

b In the user name field, enter `root`

c In the password field, enter the corresponding password.

9 In the **vSphere Client Inventory** window, perform the following actions:

a In the left pane, click the virtual machine you want to update.

b In the right pane, click the **Console** tab.

The **Console** appears.

10 In the vSphere Client, click **Connect/disconnect the CD/DVD devices of the virtual machine**.

11 In the **CD/DVD device** menu, select **CD/DVD drive 1** → **Connect to *<drive letter>***.

12 In the vSphere Client, click **Connect/disconnect the CD/DVD devices of the virtual machine**.

13 In the **CD/DVD device** menu, select **CD/DVD drive 2 → Connect to ISO image on local disk**.

The **Open** window appears.

14 Make the application update disc available to the Virtual Machine:

a Navigate to the location of the application update `.iso` file on the desktop and select it.

b Click **Open**.

The application update disc image is now available to the Virtual Machine.

15 Click in the right pane and log in to the Virtual Machine as `root`.

16 At the command line prompt, enter: `service autofs start`

Ignore messages about the **autofs** service already running if they appear.

17 At the command line prompt, enter: `/media/cdrom0/update/updater`

If the command returns a message that says it could not be found, run: `/media/cdrom1/update/updater`

The software status displays as installed with the current software and media version.

18 To confirm the updates, enter: `y`

The update process executes, and the Virtual Machine may restart.

19 Click in the right pane and log in to the Virtual Machine as `root`.

20 Select **Eject All**.

The following message appears.

```
Please remove media and press <ENTER> to continue.
```

21 In the **vSphere Client Inventory** window, click **Connect/disconnect the CD/DVD devices of the virtual machine**.

22 In the **CD/DVD device** window, select **CD/DVD drive 1 → Disconnect from *`<drive letter>`***.

23 In the **Disconnect Device** window, click **Yes**.

24 In the **Remote Disconnect Device** window, click **OK**.

The optical drive is disconnected from the virtual machine.

25 In the **vSphere Client Inventory** window, click **Connect/disconnect the CD/DVD devices of the virtual machine**.

26 In the **CD/DVD device** window, select **CD/DVD drive 2 → Disconnect from *`<ISO file location>`***.

27 In the **Disconnect Device** window, click **Yes**.

28 In the **Remote Disconnect Device** window, click **OK**.

The DVD drive on the network management (NM) client is disconnected from the virtual machine.

Postrequisites: UCS only: Once the system is operational, synchronize the databases for Unified Network Configurator and Provisioning Manager and force initialize configuration. See “Publishing Infrastructure Data to the PM” in the *Unified Network Configurator* manual and “Distributing Full Configuration (Force Initialize Configuration)” in the *Provisioning Manager* manual.

Chapter 5

Zone Controller Maintenance

This chapter provides maintenance information relating to the Zone Controller.

5.1

Key Rotation Overview

Key rotation is the process of deleting existing keys and generating/propagating new keys. The following features require their own key generation. Frequency of key rotation is determined by your organizations policies.

- SSH
- SNMPv3
- Router Encryption
- Voice and Data Confidentiality Encryption
- Heartbeat Key
- ISGW Shared Secret

For further details on key rotation, see the *Information Assurance Features Overview* manual.

5.2

Zone Controller Backup Administration

The zone configuration database contains the zone infrastructure information. This section covers topics related to backup administration.

- Software Backup Guidelines on page 75
- Backing Up and Restoring Data on page 76

5.2.1

Software Backup Guidelines

Follow these guidelines for backing up the Zone Controller.

IMPORTANT: Perform backup and migration of data from storage only on the standby Zone Controller. Backup and migration on the active Zone Controller can severely impact system performance.

- Institute and document a backup program. There are disasters specific to certain regions (such as tornadoes or earthquakes) that may require other storage considerations. Rebuilding a damaged site is much easier when valid configuration data is available for reload.
- Perform a backup anytime a maintenance action may affect the system data or configuration. This ensures restoring properly configured software and data if you find a problem after maintenance.
- Schedule backups on the Zone Controllers at times that affect the fewest users.
- Automated backups can be enabled on the BAR server after enabling the IBS software on the Zone Controller.

5.2.2
Backing Up and Restoring Data

When and where to use:
Migration data is used to maintain the data when upgrading a Zone Controller.

Procedure:

1 Log on to the Zone Controller. If needed, see Logging On to a Zone Controller Application on page 56.

2 Enter the corresponding number for **Backup and Restore Administration**. Press ENTER.

5.2.2.1
Backing Up Data to Persistent Storage

Procedure:

1 Log on to the Zone Controller. If needed, see Logging On to a Zone Controller Application on page 56.

2 Enter: `admin_menu`

The **Zone Controller Main Menu** appears.

3 Select **Backup and Restore Administration** from the menu. Press ENTER.

The **Backup/Recovery Administration** menu appears.

4 Select **Backup Administration**. Press ENTER.

The following message appears:

```
Do you want to continue with the back up operation(s)?
The Existing files and/or configuration will be overwritten. (y/n):
```

5 Enter: `y`

The following message appears, followed by the Backup and Restore Administration menu:

```
Copying migration data to persistent storage...
Migration data successfully copied to persistent storage.
```

6 Enter: `q`

5.2.2.2
Restoring from Persistent Storage

Prerequisites: Send the Zone Controller backup data from the Backup and Restore (BAR) server to the Zone Controller server. See “Executing a BAR Client Data Restore” in the *Backup and Restore Services* manual.

Procedure:

1 Log on to the Zone Controller. If needed, see Logging On to a Zone Controller Application on page 56.

2 Enter the corresponding number for **Backup and Restore Administration**. Press ENTER.

3 Enter the corresponding number for **Restore Administration**. Press ENTER.

4 Enter the corresponding number for a desired restore operation. Press ENTER.

5 To continue with the restore operation, enter: `y`

The Zone Controller object in the UEM client corresponding to the Zone Controller where the restore is being performed must be deleted and then rediscovered.

The UNC application must be disabled and then enabled.

A message similar to the following appears, followed by the **Restore Administration** menu:

```
Migrating data from persistent storage...
Restoring SSH keys and configuration...
SSH keys and configuration complete, restored global ssh
settings and user settings.
Restoring miscellaneous configuration...
Successfully restored High Availability authentication key.
Successfully restored Subscriber Authentication KI key.
Miscellaneous configuration restored.

Restoring MotoAgent Database...
MotoAgent Database restored.

All data migrated successfully.
```

Postrequisites:
Complete the restore procedures and ensure that the data restore is completed successfully. See the “UEM Operation” chapter in the *Unified Event Manager* manual and the “UNC Operation” chapter in the *Unified Network Configurator* manual.

Chapter 6

Zone Controller Troubleshooting

This chapter includes guidelines and procedures to troubleshoot the zone controller once it has been identified as the faulty device.

For hardware troubleshooting, see the *Virtual Management Server Hardware* manual.

For VMware vSphere Client or VMS Host troubleshooting, see the *Virtual Management Server Software* manual.

6.1 General Troubleshooting for Zone Controllers

Follow these troubleshooting steps to resolve general Zone Controller problems.

1. In the Unified Event Manager (UEM), check the condition of the troubled Zone Controller and links. Also verify the condition of the LAN switch. See Unified Event Manager (UEM) Usage to View Zone Controller Status and Alarms on page 79 for details.
2. If for some reason the newly active controller is not functioning properly, you may need to switch the standby controller back to active. See Setting a Standby Zone Controller to Active on page 52.
3. In the Zone Controller administration environment, check the Zone Controller status. See Viewing the Zone Controller Display Status on page 57 for details.
4. Check UNC diagnostics. See the *Unified Network Configurator* manual for details.
5. Determine the functional problem the Zone Controller is experiencing. See Zone Controller Functional Problems on page 85 for details.
6. View the Zone Controller log files. See Viewing Zone Controller Logs on page 88 for details.
7. Check for any sharp bends or kinks in cabling. Test any suspected cabling for noise, continuity, attenuation, and crosstalk. Replace the cabling if necessary.
8. Run `ping`, `pathping`, and other network administration commands to identify any link or intermediate devices (switch or routers) with high latency or connection problems to the Zone Controller.
9. Reset the Zone Controller application. See Resetting the Application on page 62.
10. Reinstall the operating software and application software, if necessary. See Zone Controller Installation and Configuration on page 36.

    NOTICE: Reinstallation of the Zone Controller is a serious system operation. Contact system support before attempting to reinstall the Zone Controller.

6.2 Troubleshooting SNMPv3 Configuration Loss

The SNMPv3 Common Agent may lose the content of the configuration file after a Zone Controller power failure or hard reset.

When and where to use:

- If Unified Event Manager (UEM) displays the **CommFailure** alarm for a Zone Controller that experienced a power failure or a recent hard reset.

- If an application cannot communicate over SNMPv3 to or from a Zone Controller that experienced a power failure or a recent hard reset.
- If you cannot select the **Configure SNMPv3 Agent/Manager** option from the **Manage SNMP Passphrases** menu in the main Zone Controller administration menu despite using the correct MotoAdmin credentials.

Procedure:

1 Perform one of the following actions:

If…	Then…
If a configuration backup file is available,	restore critical data from the backup file, including the SNMPv3 configuration: **a** Perform the restore operation. **b** Check if the communication problem persists.
If a configuration backup file is not available or too old, or you do not want to restore critical data from the backup file along with the SNMPv3 configuration,	reset the SNMPv3 credentials manually: **a** Reset the MotoAdmin credentials to be able to change other users' credentials. See "Recovering MotoAdmin Passphrases" in the *SNMPv3* manual. **b** Configure the rest of SNMPv3 users on the affected Zone Controllers. See "Configuring USM User Security for Zone Controllers" in the *SNMPv3* manual. Make sure to fix all SNMPv3 paths to/from the Zone Controllers based on the "SNMPv3 Communication Matrix" in the *SNMPv3* manual. **IMPORTANT:** This has to be done on the Zone Controllers and all servers which communicate with it over SNMPv3. **c** Verify that the updated communication paths are operational.

6.3

Unified Event Manager (UEM) Usage to View Zone Controller Status and Alarms

You can view status and alarm messages for the Zone Controller (ZC) by using the Unified Event Manager (UEM).

The UEM provides the following fault management functions for the ZC:

- Discovering devices
- Handling faults
- Detecting and reporting loss of communication and synchronization

The UEM processes fault notifications (SNMP traps) sent by the ZC and reports any loss of communication. The UEM application also provides management functions such as the ability to troubleshoot faults and send commands to the ZC.

The UEM uses maps to provide a quick summary of the status of physical devices and their links. Each icon represents a subnet or a group of subnets that contain the devices and links managed by the UEM. The following zone physical map views are available:

Summary View

Displays smaller icons and a larger number of subnets on the screen.

Detail View

Displays a distinctive icon for each individual subnet type and displays the subnet name.

For more information on using the UEM, see “UEM Operation” in the *Unified Event Manager* manual.

Fault Reporting for Tsub ZC in UEM

The Trunking Subsystem (Tsub) ZC only reports to the UEM on link status for the following Tsub devices:

- Consoles
- Dynamic Transcoders

6.4
Unified Network Configurator

The Unified Network Configurator provides diagnostics for the Zone Controllers in the zone. See “UNC Troubleshooting” in the *Unified Network Configurator* manual.

6.5
Data Restore Information

If, for any reason, the Zone Controller software and data were lost due to a hard drive replacement, perform Restoring from Persistent Storage on page 76 to enter the Restore Administration menu to restore all Zone Controller software and data.

SSH Keys Restore and Configuration

Perform Restoring from Persistent Storage on page 76 to restore the SSH keys and configuration on the Zone Controller.

Configuration Database Restore

Restoring Zone Controller data requires activation of the configuration database.

Restoring from Persistent Storage on page 76 describes how to restore the configuration database.

Miscellaneous Configuration Information Restore

Restore miscellaneous configuration information that is SNMPv3 related to a Zone Controller using Restoring from Persistent Storage on page 76.

All Data Restore

Perform Restoring from Persistent Storage on page 76 to restore the SSH keys and configuration, along with the configuration database, and all other miscellaneous configuration in a single step.

Related Links

Zone Controller Backup Administration on page 67

6.6 Automatic Switchover

Some Zone Controller failures cause automatic switchover. Automatic switchover occurs when a failure event within the server causes a loss of wide area trunking for all sites or loss of dispatch operations. The failure event is either software or hardware-based.

Failures that Cause Automatic Switchover

CPU failure

A CPU failure affects all the controller functions, consequently affecting all sites and causing an automatic switchover.

Both power supplies fail

If both power supplies fail, there is no source of operating voltages for any of the controller cards. Consequently, an automatic controller switchover occurs.

HP DL380 port failure

In case of failure check NIC ports 4 and 8 that are used for CP1 and CP2. Failure causes a loss of Wide Area Trunking (WAT) capability, which causes a switchover.

Reset the zone controller from the local Administration menu

If the active zone controller is reset from the local Admin menu and the standby zone controller is able to support wide area trunking, an automatic zone controller switchover occurs. This action is not advisable due to the system impact of a switchover event.

IMPORTANT: Before performing any manual switchover or action that results in a zone controller switchover, verify the health and status of the standby controller subsystem in the network fault management application.

Zone Controller Failures that Do Not Directly Cause Automatic Switchover

IMPORTANT: Failures of the following components do not directly cause an automatic switchover. However, such failures can indirectly cause an automatic switchover if they cause one of the critical components to fail.

Single Power Supply failure

The controller only requires one power supply to run. Failure of a single power supply does not cause a zone controller switchover, since the zone controller chassis features redundant power supplies.

Hard disk failure

A failure of the hard disk drive does not cause a zone controller switchover immediately since all necessary information is loaded into Synchronous Dynamic Random Access Memory (SDRAM). Hard disk failure however may cause overstating ZC capability. When the operating system wants to use the hard disc and either deadlock a ZC process or panic the kernel, it will influence performing of the ZC and ESXi server all together and cause the ZC switchover.

Optical media drive failure

A failure of the optical media drive does not cause a zone controller switchover since the optical media drive is only used to load zone controller operating software and patches.

6.6.1 System Behavior During Automatic Switchover

When an automatic switchover to the standby zone controller is commanded, the following sequence of events takes place.

- A failure of any one of the critical components listed in Automatic Switchover on page 81 causes the active zone controller to reset and causes a standby zone controller to compare its operational health against the health of an active zone controller. An automatic switchover is initiated if a standby zone controller is capable of wide area trunking. The standby zone controller informs all zone controllers through the Ethernet link that it is going active, and the active zone controller must go into standby.

- All sites in the zone lose connectivity to the zone controller and subsequently enter site trunking mode. If the zone controller has malfunctions, the switch to site trunking has probably already occurred.
- All active wide area calls are ended, including Talkgroup, Multigroup, Interconnect, Private, and Emergency. The active talkgroup and emergency calls revert to in-cabinet and repeat for sites and subsystems. Simulcast subsystems still simulcast within the subsystem. All console patches are lost.
- All subscriber radios, upon receiving the site trunking system status Outbound Signaling Packet (OSP), leave their current site and search for a site in wide area trunking. Since all sites are in site trunking mode, the subscribers return to the original site and inform the radio user of the site trunking mode through audible tone and, when so equipped, with a visual indication.
- The sites constantly send link requests to the controller. Once the newly active controller is online, it acknowledges the link requests to bring the sites into wide area trunking.
- As each site transitions to wide area trunking from site trunking, it transmits a wide area System Status OSP to inform the subscriber radios of the change. The time duration to transition from wide area trunking to site trunking and return to wide area trunking varies depending on the system size and configuration, but it should take less than two minutes.
- If the subscriber radios ended up on a site other than their starting point during their search for a wide area trunking site, they transmit an affiliation Inbound Signaling Packet (ISP).
- The newly active zone controller begins gathering the current location of subscriber radios and talkgroup members from the affiliation tables sent from the sites.

  NOTICE: Only limited wide area services are available until the controller receives all site affiliation tables. The time to recover the site affiliation information varies depending on the number of active subscribers, talkgroups, and the number of sites in the system, but should be less than 20 minutes.
- For multizone systems, if the active zone controller is the controlling zone for an InterZone call, it must also receive talkgroup affiliation information from the other zones before those zones are included in call requests. The time required varies depending on the number of subscribers and talkgroups in the system but in general should be less than 25 minutes. Prior to this being completed, InterZone services to other zones may be affected.

6.6.1.1 Possible Call Processing Behavior During Recovery

The following table lists the types of call processing disruptions that may occur during the recovery of the primary Zone Controller. These disruptions could be caused by incomplete location and configuration data.

Table 7: Call Processing Behavior During Recovery

Call Type	Possible Disruptions
Private Calls/Telephone Interconnect Calls	Calls to target subscriber radios whose affiliation is not yet known to the controller are not successful.
Talkgroup/Multigroup Calls	Talkgroup members need to have at least one affiliated member known by the controller at their site, to be included in talkgroup calls.

6.6.1.1.1 Subscriber Scatter

All sites transition to site trunking mode regardless of whether a controller switchover is automatic or user-initiated. The sites notify the subscribers of this change through a System Status OSP. Upon receiving this OSP, the subscribers automatically start scanning the adjacent site list for another site that is still in wide area trunking mode unless the site that the subscriber is currently affiliated to is set to Always Preferred in the subscriber programming. When no wide area site is found, the subscriber stops scanning and returns the original site.

NOTICE: Some subscribers can be affiliated at more than one site during the Zone Controller switchover. Multiple affiliations can occur if a radio happens to affiliate to a new site while the radio is also searching the adjacent site list for a wide area site. Because connectivity to the controller is temporarily lost during controller switchover, the entries in some of the site affiliation tables do not get updated to reflect subscribers who have changed sites. Normally, the controller de-affiliates subscribers when they roam out of a site. However, during a controller switchover the communications path from the controller to the site is temporarily unavailable, preventing the controller from performing de-affiliation.

The site transitions to wide area trunking mode when the site reestablishes a link with the controller. The site then notifies the subscribers of the change through System Status OSP.

The wide area feature called Dynamic Site Assignment requires that the controller have up-to-date affiliation tables. All sites need to upload the affiliation tables to the controller. After the controller receives all uploads from the sites, it looks through the compiled affiliation table for subscribers that are registered on more than one site. If the controller finds duplicate affiliations, it requests, through all sites where the subscriber shows affiliations, that the subscriber reaffiliate. This must happen before Dynamic Site Assignment guarantees all intended parties are included in the call.

The length of time it takes to update the affiliation tables depends on the number of sites, subscribers, and talkgroups in the system, but in general it should be less than 20 minutes from the time the first site transitions back to wide area trunking.

6.7 Manual Switchover

You can perform a manual switchover from the Unified Network Configurator (UNC) or the Zone Controller local administration menu. A manual switchover is typically used when performing a software upgrade or performing maintenance such as replacing a faulty Field Replaceable Unit (FRU) that did not cause an automatic switchover.

IMPORTANT: Due to the system impact of a switchover event, initiate a manual switchover **ONLY** when necessary. Before performing a manual switchover or take any action that results in a Zone Controller switchover, verify the health and status of the standby Zone Controller in Unified Event Manager (UEM).

For more information, see the "Zone Controller Quick Commands" in the *Unified Network Configurator* manual or Zone Controller Redundancy and Switchover on page 51.

6.7.1 Manual Switchover in the Zone Controller Verification

After a manual switchover has been performed, view the Application Redundancy Object State in the Display Status menu. See Viewing the Zone Controller Display Status on page 57.

6.7.2

Switching Back to the Standby Zone Controller

If the newly active controller is not functioning properly, you may need to switch the standby Zone Controller back to active. This can cause the Zone Controller database to become out-of-sync. At this point, the only way to get the Zone Controller back in sync is to perform a force initialization procedure via the PM GUI.

IMPORTANT: Upon switchover, the mobility information is replicated to the new standby Zone Controller. This should take approximately one hour. During this time, manual switchovers should be avoided to prevent the need to rebuild the mobility information from other system devices.

For more information, see "PM Data Sync State" in the *Unified Network Configurator* manual.

6.7.2.1

Radio User and Talkgroup Record Download

After the channel capabilities have been verified, the Network Management Subsystem begins sending subscriber and talkgroup records to the Zone Controller. The time required for this download varies, depending on the number of subscribers and talkgroups in the system. Typically, this takes approximately 30 minutes for a system with 15,000 subscribers. A system with 64,000 subscribers could take as long as two hours.

NOTICE: Conducting a Force Initialize command from the PM to various devices may take from 1.5 hours to 6 hours to complete, depending on the number of subscribers and size of the data.

6.8

Synchronizing the UCS with the Zone Controller

When subscriber and infrastructure data is restored to the UCS, the PM data synchronization procedure has to be performed.

For information on how to determine whether a Zone Controller is out-of-sync and how to resynchronize, see “PM Data Sync State” in the *Unified Network Configurator* manual.

Zone Controllers Synchronized Status Verification

After synchronizing the Zone Controllers from the UNC, view the Replication State in the Display Status menu. See Viewing the Zone Controller Display Status on page 57.

6.9

Zone Controller Display Status

The Display Status function checks the states and causes of the Zone Controller.

See Viewing the Zone Controller Display Status on page 57.

6.10

Network Link and Speed Indicator LEDs

This section describes Zone Controller network link and speed indicators.

The network link indicator LED is located at the upper left of each Ethernet connector, labeled 03. The network speed indicator LED is located at the upper right of each Ethernet connector, labeled 03.

Table 8: Zone Controller Network Link and Speed Indicators on page 85 describes the network link and speed indicators if there is a problem with an Ethernet connector.

Table 8: Zone Controller Network Link and Speed Indicators

LED	Description	If there is a problem with an Ethernet connector...
Network Link Indicator	Network link status	• Green light steady on a link is established. • Green light off indicates link is not established. • Green blinking there is activity on this port.
Network Speed Indicator	Network speed status	• Amber on the link is operating as a Gigabit connection (1000Mbps). • Green on the link is operating as a 100Mbps connection. • Off the link is operating as a 10/100=Mbps connection.

6.11

Zone Controller Functional Problems

This section introduces troubleshooting steps for different Zone Controller conditions.

This section introduces troubleshooting steps for different Zone Controller conditions.

- Resolving Call Processing Problems
- Resolving Resource Management Problems
- Resolving Mobility Management Problems
- Resolving InterZone Communications Problems
- Resolving Audio Problems
- Resolving Reporting Problems
- Resolving Network Management Problems

6.11.1

Call Processing Problems

The Zone Controller is responsible for managing call processing in the zone. This includes registration, individual calls, and group calls. A failed Zone Controller results in the loss of system and zone trunking for that particular zone. All call requests, registration requests, and calls in progress are dropped. The zone also drops out of participation in all InterZone calls.

If there are problems with call processing in the zone, you can troubleshoot using the following steps:

- Verify that the most current Subscriber Access Control (SAC) and the configuration database records have been downloaded. You can verify this by viewing the Out of Sync flag in the UNC. In order to send the complete set of subscriber information, perform a forced initialization from the PM to the Zone Controller.
- If there are continual problems accessing a particular type of service or feature, check the Provision Manager (PM) records and profiles for radio settings, talkgroup settings, fleetmapping, system settings, encryption keys, and so on. Also, verify that zone-level settings (such as timeouts) in the UNC are configured appropriately.

- Check the loading of call traffic and InterZone channel utilization through the Historical Reports application. Reconfiguring the PM and UNC settings, adjust loading as necessary.
- Verify that timeouts and other subscriber settings are configured appropriately in the radios.
- Troubleshoot the CPU card. The CPU card processes all the activities in the zone and generates grant, busy, or reject messages to the subscriber radios. The CPU card actively manages all the registration resources and call management activities in the zone and mobility management for talkgroups that are mapped to the zone. The physical CPU is controlled by the ESXi-based host server. Use the terminal server, the network fault management application to evaluate the CPU card status.
- Troubleshoot the Ethernet ports. The Ethernet ports send command messages and retrieve feedback from all sites in the zone. The ports also communicate and send call processing command messages to other zones over the InterZone link. The physical Ethernet ports are controlled by the ESXi-based host server. Use the terminal server and the network fault management application to evaluate the Ethernet port status.

6.11.2 Resource Management Problems

The Zone Controller is responsible for managing all the resources for subscriber services, including dynamic site allocation and other infrastructure arrangements. A service is either granted, busy, aborted, or rejected. If a service request is busy, aborted, or rejected, the Zone Controller sends the message to the subscriber and releases all associated resources from the service.

- Verify that the most current configuration database records are downloaded to the Zone Controller.
- Check the site access profiles and adjacent control channel settings in the PM. Verify that the settings are correct.
- Check the zone-level settings in the UNC. Verify that all remote site settings are correct.

6.11.3 InterZone Communications Problems

The Zone Controller coordinates services with Zone Controllers in other zones. The Zone Controller shares command messages, mobility information, and coordinates audio calls with the other zones through the InterZone control path. A failed InterZone Control Path causes InterZone communications to cease. InterZone calls and sharing of mobility information with the failed zone also ceases.

- Check the zone call processing status for each affected Zone Controller. Verify that all the zones are InterZone trunking capable.
- Check the network configuration for each affected Zone Controller. Verify that the Zone Controller is given the appropriate zone number. If the Zone Controller is configured with the wrong zone number, then all the IP addresses for the Zone Controller are incorrect.
- Check the InterZone channel loading through the Historical Reports application. Adjust InterZone traffic by adjusting home zone mapping for talkgroups or subscribers as necessary.
- The Zone Controller sends and receives InterZone control information through the Cooperative WAN Routing, LAN switch, exit router, and gateway router. Verify proper operation of the devices.
- The CPU is responsible for managing all multizone operations that involve its zone. It also sends audio control routing command messages to other devices in the zone as required.

6.11.4 Audio Problems

The Zone Controller is not involved with the quality of audio. If there are any problems with audio quality, audio delays, and so on, check the base radio settings.

6.11.5 Reporting Problems

The Zone Controller generates air traffic information which is then gathered by the Air Traffic Router (ATR) for logging. The ATR distributes the information to the statistical servers, ZoneWatch clients, and any billing or accounting service hosts. The air traffic information also includes Radio Control Manager (RCM) feedback (such as a response or fulfillment of an RCM command). This RCM feedback is forwarded to RCM clients.

Air traffic information is stored in the ATR. The sites and the Zone Controller do not store or buffer any of the air traffic information.

- If an individual site falls into site trunking or if there is a Zone Controller outage, any air traffic information for the affected sites that is not received by the ATR is lost.
- Air traffic information passes to the ATR through the network management Ethernet link. Check the display status and the Ethernet card component status in the Zone Controller Administration menus.
- Verify the operation of the CPU if there are any problems with air traffic logging.

6.11.6 Network Management Problems

The Zone Controller receives its operating information from the Unified Network Configurator (UNC). The UNC downloads all the infrastructure and Subscriber Access Control (SAC), plus all the pending RCM commands from the bulk download of files to the Zone Controller. The Zone Controller arranges the SAC information accordingly in its location registers and stores the infrastructure information.

Problems with the network management links affect the fault management capabilities and remote command capabilities from the network management subsystem. Network Management problems can isolate the Zone Controller from any new information programmed in the PM or UNC, and information flow to the remote sites are also restricted.

If a network management problem is being experienced, check the following items:

- Check the Display Status in the Zone Controller Administration menus.
- Perform the `test credentials` command on the UNC. It will verify connectivity and check if the SNMP configurations are aligned.
- Check the Display Status in the Zone Controller Administration menus. The display status will show HA connections (in redundant zone configuration).
- Verify that the network configuration for the Zone Controller is set up for the appropriate zone in the administration menus. Also check the IP configurations for the UNC, network fault management application, and any other network management servers that are affected.
- The CPU, located on the VMS host, supports the network management link between the Zone Controller and the network management servers. Verify the operation of the CPU, if necessary. See the *Virtual Management Server Software* manual.

6.12 Getting Log Files

Getting log files combines multiple files into a single file for transferring the data off the Zone Controller. Follow the procedure steps to get different types of log files.

Procedure:

1. Log on to the Zone Controller. If needed, see Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **OS Administration**. Press ENTER.

3. Enter the corresponding number for **Get Log Files**. Press Enter.
4. Enter the corresponding number for desired log types to compress into a single file. Press Enter.

   A message similar to the following appears, followed by the Get Log Files menu.

   ```
   Getting logs files, this may take a while...
   Created /var/getlogs/NAME_OF_COMPRESSED_LOG_FILE>
   ```

6.13

Viewing Zone Controller Logs

After exhausting other Zone Controller troubleshooting options, trained support personnel may ask you to view the Zone Controller logs, which contain detailed information about Zone Controller functions.

For details on how to securely transfer diagnostic logs, see the *Securing Protocols with SSH* manual.

Procedure:

1. Log on to the Zone Controller. If needed, see Logging On to a Zone Controller Application on page 56.
2. Enter the corresponding number for **OS Administration**. Press Enter.
3. Enter the corresponding number for **Display Logs**. Press Enter.

   The View Logs menu appears.
4. Enter the corresponding number for desired log types. Press Enter.

   A list of available logs to view is displayed.
5. Enter the corresponding number for a log file to view. Press Enter.

   The requested log file appears.
6. Navigate within a log. Perform one of the following actions:
   - To go forward, press Space Bar
   - To go back, press B
   - To end viewing mode, press Q

   After viewing the log, the list of available logs to view reappears.

6.14

SNMPv3 Problems

If contact with the SNMP common agent is not allowed because MotoAdmin passphrases are lost or privileges (permissions) are not appropriate for the actions being performed, see the *SNMPv3* manual.

Chapter 7

FRU/FRE Procedures

For information on any FRU/FRE hardware replacement of the server, see the *Virtual Management Server Hardware* manual. For information on the Linux operating system, see the *Virtual Management Server Software* manual.

7.1

Restoring Zone Controller Application and Data

After replacing a server hard drive, perform this procedures to re-install the Zone Controller application and to restore all data.
For information about setting up Active Directory users so that they can perform specific administration menu procedures, see Zone Controller Administration Menu on page 90 and contact your Active Directory administrator.

Prerequisites: The firmware, operating system, and the server must be installed and operational.

Process:

1. Log on to the server. See Logging On to a Zone Controller Application on page 56.
2. Load the Zone Controller application. See Deploying the Zone Controller Virtual Machine on page 36.
3. Discover the Zone Controller in the UNC. See the *Unified Network Configurator* manual.
4. Perform the redundancy and switchover configurations for a redundant configuration. See “Zone Controller Quick Commands” in the *Unified Network Configurator* manual or see Zone Controller Redundancy and Switchover on page 51.
5. Reset the Zone Controller. See Resetting the Application on page 62.
6. Discover the Zone Controller application in UEM. See the “UEM Description” and “UEM Operation” chapters in the *Unified Event Manager* manual.
7. Restore the Zone Controller data. See Data Restore Information on page 80.
8. Configure the Information Assurance. See Information Assurance Configuration on page 51.

Chapter 8

Zone Controller Reference

This chapter contains supplemental reference information relating to the Zone Controller.

8.1 Timers for a Zone Controller

This section describes Zone Controller step sizes.

In a trunking system, the UNC offers greater timer granularity than what is executed by the Zone Controller. Use the following table to determine the exact value of timers associated with the Zone object. Any entered value that is between two steps is rounded up by the Zone Controller, according to the step size indicated in the table. For example, if you enter a timer value of 22 minutes in the UNC, the Zone Controller rounds it up to 25 minutes.

Table 9: Zone Controller Step Sizes

Timer Value	Step Size
0 ms 10 ms	10 ms steps
100 ms 1000 ms	100 ms steps
1 sec 10 sec	500 ms steps
10 sec 2 min	1 sec steps
2 min 5 min	20 sec steps
5 min 20 min	2 min steps
20 min 60 min	5 min steps
1 hr 4 hr	1 hr steps
4 hr 72 hr	4 hr steps
3 days 7 days	1 day steps
1 week 4 weeks	1 week steps

8.2 Zone Controller Administration Menu

The Zone controller functions are accessed from the Zone Controller Administration menu.

The only local account on the ZC is root. All other accounts are domain controlled. Each user uses their personal account. Access to the ZC and command execution privileges on the ZC are based on the ASTRO® 25 system authorization roles assigned to a personal account. A domain group equates to an ASTRO® 25 system authorization role. Access and command execution privileges are determined by the domain group membership of the users account.

The following table lists the authentication roles users may be assigned to. For information on how to look up credentials that are required for particular operations and determine account privileges, see the *Authentication Services* manual.

WARNING: Users should check as they log on to see what other users are logged on to the same device (this information displays automatically) because if two users perform conflicting operations, they could damage the system.

Table 10: Authentication Roles

Role Name	AD* Group Name	Level of Access
Network Security Administrator	secadm	Handles keys and phrases. When key/phrase material is created, edited, or visible, it falls under this role. Also, OS and network level keys, such as SSH, SSL, and SNMPv3, are handled under this role.
Backup Administrator	bkupadm	Handles databases, software installations and configurations. Under this role, content can be restored back on a device. Has the ability to back up both platform/OS and application-specific information.
Installation Administrator	instadm	Performs OS, server, and application installations. Also, installs OS, server, and application patches. Has the ability to load license keys for the applications and enable features, using license keys. Has the ability to restore platform/OS and application-specific information from backup.
Domain Administrator	built-in AD domain admins group)	Creation and maintenance of centralized user accounts. Centralized and local authentication and authorization administration.
Network Administrator	netwadm	Configuration and administration of transport equipment.
Platform Administrator	platadm	Handles reboot and shutdown operations. Has control over local peripherals, Unix administration items such as NTP, local IP address, local log files related to device performance monitoring, and faults. Has the ability to enable/disable services, such as communication protocols.
System Audit Administrator	auditors	Handles the information related to user operation trail. Given the system architecture, this role entails auditing centralized logs, and auditing local logs.
Subscriber Infrastructure Administrator	infradm	Has the ability to add, configure and remove data, channels, voice channels, and console sites. Essentially this means ZCM and CSS administration and device local call processing configuration. Active standby control. Has the ability to load license keys required by applications to add additional resources, or enable additional functionality in existing applications. Also, manages databases.
Subscriber Security Administrator	subssec	Handles keys for radio operations, such as payload encryption and subscriber authentication.
Subscriber Administrator	subsadm	Ability to add, configure, and remove radio users. PM and Radio Programming Software Administrator. DB management of subscriber data.
Subscriber	subsusr	Fixed/Mobile terminal operator, such as: Dispatch console operator. Data terminal user.

[*] Active Directory (AD) users and groups are set up in Active Directory on the ASTRO® 25 system domain controllers.

Related Links

Logging On to a Zone Controller Application on page 56
Changing Passwords on page 69

8.2.1 Executing Menu Options from the Administrative Menu

Procedure:

1. Choose a desired option to execute from Zone Controller Administration Menu on page 90, as listed below, and then, going up towards the entry in the Menu column, identify the submenu names in all applicable submenu **(level 5)**, **(level 4)**, **(level 3)**, **(level 2)**, and **Menu** columns.
2. Log on to a server with available option to execute using your Active Directory account. If needed, see Logging On to a Zone Controller Application on page 56.
3. Enter the corresponding number for ***<DESIRED MENU OPTION>*** identified in the **Menu** column of the table from Zone Controller Administration Menu on page 90. Press ENTER.
4. Enter the corresponding number for ***<DESIRED MENU OPTION>*** identified in the **(level 2)** column of the table from Zone Controller Administration Menu on page 90. Press ENTER.
5. Perform one of the following steps:

If…	Then…
If the *<DESIRED MENU OPTION>* was chosen in step 4 is a submenu,	perform the following actions: **a** Repeat step 4 and step 5 for the **(level 3)** submenu. **b** Repeat for all subsequent lower-level submenus, as noted in step 1.
If the *<DESIRED MENU OPTION>* was chosen in step 4 is a command identified to execute in,	the ***<DESIRED MENU OPTION>*** is executed.
If the user has insufficient permissions,	the following message appears: `Insufficient Privileges for: DESIRED MENU OPTION >.` Log off, contact your Network Administrator for required permissions, and start again from step 1.

An asterisk (*) in front of a corresponding number for ***<DESIRED MENU OPTION>*** indicates insufficient permissions.

Postrequisites: Continue with another procedure that requires the same credentials or log off from the server application.

Chapter 9

Zone Controller Disaster Recovery

This chapter provides references and information for you to recover Zone Controllers in the event of a failure.

9.1 Virtual Management Server and DAS Recovery

The Virtual Management Server (VMS) and the Direct Attached Storage (DAS) devices need to be in a functional state before attempting to recover the Zone Controller. For the procedures to recover the VMS and/or the DAS, see “Virtual Management Server Disaster Recovery” in the *Virtual Management Server Software* manual.

9.1.1 Recovering the Zone Controller

Process:

1. Reinstall the Zone Controller virtual machine on the Virtual Management Server (VMS) host. See Deploying the Zone Controller Virtual Machine on page 36.
2. Recover data from the Backup and Restore (BAR) server. See Restoring Critical Data to a Zone Controller from the BAR Server on page 95.

Appendix A

Centralized Backup and Restore

This appendix provides disaster recovery information for the Zone Controller when utilizing centralized Backup and Restore (BAR) service.

A.1 Centralized Backup and Restore (BAR) Service for Zone Controllers

This section provides information about centralized backup and restore (BAR) services for Zone Controllers for an ASTRO® 25 system with a centralized Backup and Restore (BAR) server.

NOTICE:
If secure protocols are used for communication with the BAR server, correctly configure secure and clear protocols, provision SSH keys, and register the device with the BAR server. See the SSH configuration process for centralized backup and restore in the *Securing Protocols with SSH* manual.

The Zone Controller uses Domain Name Server (DNS) name resolution to communicate with the BAR server, so the DNS service must be available. The Domain Controller provides this service, so the Domain Controller must be online during recovery of a Zone Controller.

For more information, see the *Backup and Restore Services* manual.

A.1.1 Zone Controller Backup from the BAR Server

In addition to regularly scheduled Zone Controller backups from the Backup and Restore (BAR) server, perform backups whenever critical data has been modified:

- After changes to the zone configuration database
- Before and after changes to the SSH keys and configuration
- After clear/secure protocol settings have changed

If secure protocols are being used to communicate between the Zone Controller and BAR server, then configure SSH first. See the SSH configuration process for centralized backup and restore in the *Securing Protocols with SSH* manual.

For the procedure to perform data backups from the BAR server, see “Scheduling a One-Time Backup of a BAR Client” in the *Backup and Restore Services* manual. The procedure backs up critical data, as well as some non-critical log files that are used for diagnostic purposes. For the ZC, the critical data is:

- Configuration Database
- SSH keys and configuration (including secure/clear settings)

Tsub ZC Information Backed Up by BAR

The Trunking Subsystem (Tsub) ZC is also backed up by the zone core BAR server. Since the Tsub ZC has limited functionality, only SSH keys and credentials that the Tsub ZC needs to communicate with the zone core servers are backed up by BAR. The backed up information includes:

- UEM SNMP credentials
- UNC SNMP credentials

- SSH credentials
- Syslog configuration

For more information on how to schedule a backup for the Tsub ZC, see the *Backup and Restore Services* manual.

A.1.2
Restoring Critical Data to a Zone Controller from the BAR Server

NOTICE: For information about setting up Active Directory users so that they can perform specific administration menu procedures, see Zone Controller Administration Menu on page 90 and contact your Active Directory administrator.

Process:

1. Execute a client data restore from the BAR server. See “Executing a BAR Client Data Restore” in the *Backup and Restore Services* manual.

   NOTICE: Executing a client data restore from the BAR server puts the data in a temporary directory. It does not apply any configuration changes and does not activate the database.

2. Perform the data recovery by selecting **Restore All Critical Data** from the **Restore Administration** menu. See Data Restore Information on page 80.
3. Determine whether the UNC is available to download the Configuration Database to the Zone Controller. See Viewing the Zone Controller Display Status on page 57. If the UNC is available to download, see the *Unified Network Configurator* manual for the procedure to download the Configuration Database to the Zone Controller.
4. If Secure Shell (SSH) is used in the system, then the SSH keys and configuration can be recovered from the BAR server. See Restoring from Persistent Storage on page 76.
5. Restore additional configuration data. See Restoring from Persistent Storage on page 76.

Related Links

Recovering the Zone Controller on page 93