A MITEL
PRODUCT
GUIDE

MiVoice MX-ONE

System Redundancy – Description

Release 7.5
80/1551-ANF 901 14 Uen A 2023-01-17

January 2023

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Introduction 1

This chapter contains the following sections:

This is a description of the System Redundancy feature in MX-ONE. System redundancy is achieved by adding a dedicated alternate system to the network. The alternate system has the ability to take over the tasks of the primary system when the latter fails or becomes unavailable. The System Redundancy feature is designed to be used in environments where reliable layer 2 (MAC/LLC) network monitoring is not possible. The feature is available to IP endpoints; that is, SIP terminals, clients or trunks. If the primary system fails or becomes unavailable, these extension types can register with the alternate system. This is, however, not done immediately, but with a delay. The delay is due to the time it takes for the alternate system to detect that the primary system is out of order as well as the time it takes for each extension to register with the alternate system.

1.1 Scope

This document provides a high-level description of the System Redundancy feature.

1.2 Target Group

This document is intended for system administrators.

1.3 Glossary

Active LIM

The LIM that currently provides the telephony services. If server redundancy is configured, the active LIM can run on the cluster regular server or the cluster standby server.

Active system

The MiVoice MX-ONE that currently provides the telephony services.

Alternate system

A system that can provide telephony services while the primary system is out of order.

Data backup

Exchange data is stored on disk by backing up data.

Exchange data mirror

An exchange data mirror contains all data backup files from all LIMs.

IP endpoint

SIP terminal, SIP trunk, or an other SIP client.

IP translation table

The IP translation table exists in the alternate system and is created at configuration. The table contains IP addresses from the primary system and the corresponding IP addresses in the alternate system. The table also contains LIM FQDNs. The table is used to adjust the exchange data for the alternate system.

LIM

Line Interface Module, an MX-ONE Service Node plus at least one media gateway.

Master server

The server referred to as 'Master Server' at new installation of a system. Normally the master server is the LIM 1 server. If LIM 1 has server redundancy, master server is the LIM 1 regular server. Maintenance is usually performed from the master server.

MS

Media Server, a "software-based" media gateway, in this context for use in the MX-ONE.

Network control address

An address in the network that is used to verify connectivity to terminals, trunks, and other clients.

Network redundancy

The network redundancy used with MX-ONE is a switched network redundancy with Ethernet bonding for the Service Nodes.

Passive system

The system that currently does not provide the telephony services.

Primary system

The MiVoice MX-ONE that normally provides the telephony services.

Primary system server

Either a LIM or a standby server in the primary system.

Redundancy

The duplication or multiplication of a certain function, which makes it possible to retain the function, at least partially, by accessing another system.

Takeover

The change over from the primary system to the alternate system or from the alternate system to the primary system. The passive system becomes the active system.

For a complete list of abbreviations and glossary, see the description for ***MiVoice MX-ONE Abbreviations, Acronyms, and Glossary***

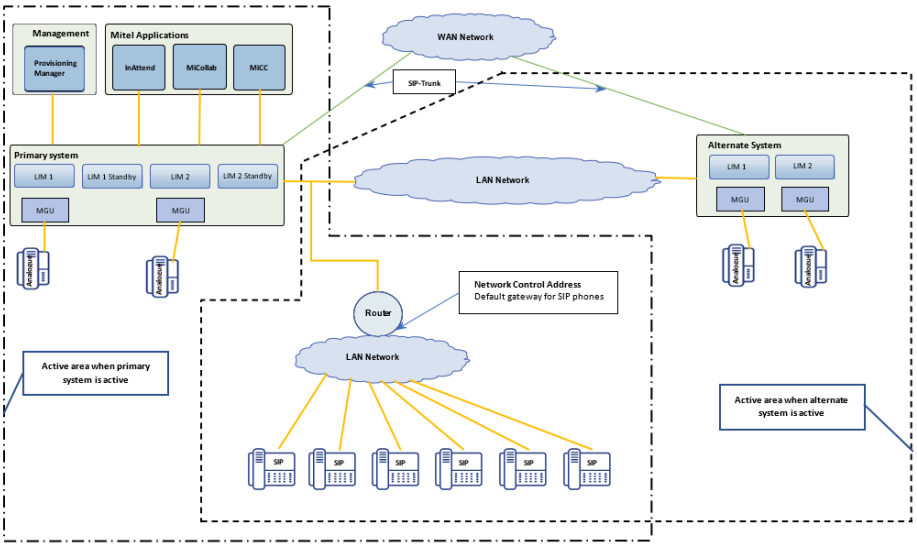
Functions 2

This chapter contains the following sections:

2.1 Overview

System redundancy reduces the likelihood of events such as power outages, floods, HVAC (Heating, Ventilation, and Air Conditioning) failures, lightning strikes, impact of tornadoes, and building fires that would disrupt telephony services.

Two almost identical systems, a primary system and a dedicated alternate system, are configured. For details see the ***System Redundancy Functionality, Prerequisites*** section and the ***Capacity and Limitations*** section. The two systems should be deployed in different geographic locations.



Under normal circumstances the primary system is active and handles all telephony services. The alternate system is running but does not handle any telephony services; that is, it is passive.

When there is a disruption, (for example, power outage of the primary system), the alternate system can take over the tasks of the primary system. This way, the alternate system becomes active and provides the telephony services when the primary system

goes out of order. For more information, see details in the *Interaction with Other Features* section.

The IP endpoints should be so configured that these can register with both the primary system and the alternate system.

The alternate system is prepared with exchange data from the primary system.

The takeover in the event of failure (takeover by the alternate system from the primary system) and recovery from failure (takeover by the primary system from the alternate system) can be configured to be manual or automatic. The recommended configuration is automatic takeover at failure and manual takeover at recovery.

If automatic takeover is configured, network redundancy between the primary and alternate system reduces the likelihood of both the systems running telephony services simultaneously.

If manual takeover is configured, the takeover must be ordered by using the system redundancy maintenance utility.

External applications and equipment must also be able to detect that the primary system is out of order (for example, calls via SIP trunks must be routed to the alternate system).

All servers used in the primary and the alternate systems must have similar capacities for a well-functioning environment.

2.2 System Redundancy Functionality

2.2.1 Prerequisites

The following types of generic extensions are supported:

- SIP extensions (terminals sending register request)

The following requirements and limitations apply for configuring system redundancy:

- Network connectivity between the alternate system and the primary system is required. Protocols ICMP and TCP are used and must be allowed by firewalls.
- The two systems, primary and alternate, must be set up such that that no duplicate IP address conflicts occur.
- The same license file is to be installed on both the primary and the alternate systems. The license must be issued for both the primary and the alternate systems. The license file must be in place in both systems before configuring the alternate system.
- The number of LIMs and the LIM numbers of the alternate system must be the same as of the primary system.

- Hardware within a LIM; that is, media gateways and boards, must be placed in the alternate system exactly as placed in the primary system.
- Media servers must be added to the alternate system in the same way as in the primary system.
- The number of system databases in the alternate system can differ from that in the primary system.
- If TLS is to be used, certificate(s) must be issued for both systems, the primary and the alternate. The certificate(s) must be installed on both systems.
- Configuration files, such as announcement prompts, must be installed and loaded in both systems.
- The two systems, primary and alternate, must be up and running.
- Appropriate exchange data must be configured in the primary system.

2.2.2 Configuration

The System Redundancy feature is configured in the alternate system by the system administrator. For configuring system redundancy, the system version running in the alternate system must be the same as that running in the primary system.

During system redundancy configuration, the system administrator is required to confirm the IP translation table and to add optional network control addresses used in the takeover process.

At configuration, an exchange data mirror is made in the primary system. The mirror is copied to the alternate system and a system reload is performed in the alternate system in order to apply exchange data from the primary system into the alternate system.

To keep the exchange data in the alternate system up to date with the exchange data in the primary system, a new exchange data mirror is made in the primary system, copied and applied to the alternate system by a system reload.

In order to perform supervision and exchange data handling, data about the primary system is stored at configuration in the alternate system.

2.2.3 Supervision

The alternate system supervises the primary system servers by using IP address over the protocols ICMP (default) or TCP. The alternate system will contact the primary system servers at configured intervals and if there is a response from any of the servers the primary system is considered working. Lack of response from servers can be due to a server failure or network connection loss. The supervision is performed regardless of whether the alternate system is active or passive.

The IP tables for blocking traffic are checked in both the primary and alternate system to ensure that the IP tables for traffic are correct.

2.2.4 Takeover

General

In the normal state, the primary system is active and handles all traffic. The alternate system is passive and blocked for traffic.

The IP tables block or unblock the systems for traffic.

In the configuration, a time limit is specified for repeated takeovers. This configured time must elapse after a takeover is executed before a new takeover is executed. This is to avoid switching back and forth due to intermittent network or power disturbances.

Before all IP endpoints have re-registered with the active system, all features do not fully work in the active system.

Network control address

Network control address(es) are checked for verifying connectivity to terminals, trunks, and other clients and is performed over the protocols ICMP (default) or TCP. A network control address can be the default gateway of a subnet to which IP endpoints are connected.

Conditions for Automatic Takeover by Alternate System

When the primary system is detected unreachable by the supervision, the primary system is considered faulty.

Before a takeover is executed, a check is done on the network control address(es). If at least one network control address responds, the takeover will be executed. If no network control address responds, the takeover will not be executed. If no IP endpoints are reachable from the alternate system, there is no point in executing the takeover.

If no network control address is configured, the takeover will be executed with no additional check.

Conditions for Automatic Takeover by Primary System

The supervision will detect when the servers are back in service.

If automatic takeover by the primary system is configured, the alternate system is blocked for traffic and the primary system will handle the traffic if there is at least one LIM responding.

2.2.5 Registration to the Active System after Takeover

General

When a condition for takeover has been detected by the alternate system, all users who can, will register with the active system. Propagation and detection of the takeover condition can take some time.

As an example, the time before detecting the conditions for takeover may be in the range 3-4 minutes, depending on the number of LIMs. In addition, there will be a delay of 0 to 10 minutes (or even more as this is specified in the configurable timer in the terminal) before the re-registration from the IP terminals is requested.

User Logged in at Takeover

The IP terminal must request registration in the active system.

User not Logged in at Takeover

The IP terminal will primarily try to register with the primary system. If that fails, the IP terminal must request registration with the alternate system by sending a new registration request.

Load Regulation of Registrations at Takeover

In view of overload risk and the risk of suppression of traffic execution, the MX-ONE Service Node must limit the number of registrations per time unit; that is, it must have a load regulation for the registration function. The periodic re-registration (keep-alive check) that is done for logged in IP terminals has a default period of 10 minutes and this is the interval at which re-registrations are triggered. The timer duration can be changed.

Rejection Cases

Re-registration with the active system can fail with the reasons specified in the ***MiVoice MX-ONE SIP Extension - Description*** document.

Abnormal Cases

Due to, for example, bad networks or malfunctioning network elements, the system could end up with isolated segments of LIMs that operate separately for a period.

2.2.6 Ongoing Calls at Takeover

SIP to SIP, non-gateway call, the session timer will timeout and the call will be disconnected.

SIP to SIP, gateway call, the call will be disconnected.

Re-registration will be done with the active system for both cases.

2.3 MITEL IP Endpoints

For more information about the redundancy functionality for Mitel 6900/6800/6700 terminals, see the ***Mitel 6900, 6970, 6800, and 6700 SIP Terminals for MiVoice MX-ONE*** document.

Interaction with Other Features 3

The functionality that is impacted by a takeover is described in this topic.

All dynamic data is lost at takeover. For example, a call queue is lost and a new call queue is established in the new active system.

The feature configuration (permanent and semi-permanent data) in the alternate system will be what was specified in the primary system and copied as exchange data to the alternate system.

All supported features are working in the active system.

ACD/CTI Group

The call queue is lost during a takeover.

Authorization Code

The authorization code lock information will be as what was copied from the primary system.

Automatic Registration of Extensions

-

Callback and On-hook Queuing

The queue for Callback and On-hook Queuing is lost during a takeover.

Call Information Logging

-

Call Waiting

The queue for Call Waiting is lost during a takeover.

Charging/Call Metering

-

Common Bell Group

The active system must have hardware required to support this feature.

Conference (and Intrusion)

All parties must be logged into the active system.

Cordless Extension Traffic (DECT)

Not supported.

CSTA Monitoring and Services

-

Diversion Services

The diversion services information will be as what was copied from the primary system.

Emergency Calls

Emergency calls are lost during a takeover.

Emergency Extension (Automatic Conference)

Emergency calls are lost during a takeover.

Emergency Switching

Emergency switching is lost during a takeover.

Feature Keys in Extensions

The feature keys will be as what was copied from the primary system.

Forking

-

Free Seating

Free Seating logon is lost during a takeover.

Group Call Pickup

The queue for Group Call Pickup is lost during a takeover.

Hunt Group

The queued calls and logon status for Hunt Group are lost during a takeover.

Individual Call Pickup

-

Last External Number Redial

The centrally stored Last External Number Redial (LNR) number is lost during a takeover.

Message Waiting and Manual Message Waiting

The queue for MMW and Message Waiting is lost during a takeover.

Because messages are stored in an external application, Message Waiting messages can be re-created if the external application is configured for and updates while the user is registered with the alternate system.

Multiple Representation of Extensions/MNS

-

Multiple Terminal Service

-

Operator Specific Services

The operator's queue is lost during a takeover.

Paging

-

Parallel Ringing

-

Parking, Inquiry, Alternation and Transfer

Single line access extensions lose the inquiry queue mission during a takeover.

Parking of trunk calls has a timed recall function, which is lost during a takeover.

Path Replacement

-

Personal Number (IRD Distribution)

Active personal number will be as what was copied from the primary system.

Recorded Voice Announcements

-

Remote Extension

The multiplicity number will be what as copied from the primary system.

Routing and Least Cost Routing

-

Single Number Indication

Single number indication will be as what was copied from the primary system.

SOM, Surveillance, Observation and Monitoring

-

SS7 trunk

-

Traffic recording

-

Administration 4

The system redundancy maintenance utility contains functions for managing the System Redundancy feature.

Manual changes to exchange data in the alternate system are not automatically transferred to the primary system.

The timer for the periodic keep-alive re-registration of IP extensions can be changed in the terminals, and thus affect the System Redundancy feature.

Removing System Redundancy

Removing of the System Redundancy feature is done in the alternate system and by the System Administrator.

At removal, supervision of the primary system is stopped and the system redundancy configuration is removed. Traffic status will remain as is after removal. If traffic was blocked before removal of System Redundancy, the traffic remains blocked after removal. If traffic was not blocked before removal removal of System Redundancy, it will continue to remain so after the removal.

After removal of the feature, the IP tables are not checked for blocking traffic in the systems. Thus, if a LIM server that is blocked for traffic is powered off, the LIM server will not be blocked for traffic after the server is powered on.

If the prerequisites for configuring System Redundancy are fulfilled, System Redundancy can be configured again after it is removed.

Terminating System Redundancy

After removal (see above), System Redundancy can be terminated. Terminating system redundancy includes removing redundancy settings from IP endpoints and removing one of the systems.

Upgrade 5

When the System Redundancy feature is in operation, the system version running in the alternate system must be the same as or later as that running in the primary system. This means that the alternate system can be upgraded before the primary system is upgraded. After the primary system is upgraded, the alternate system must be upgraded if not already done. If the system versions are different in the two systems, semi-permanent data cannot be loaded into the alternate system.

Capacity and Limitations 6

1+1 server redundancy can be used in the primary system, but not in the alternate system.

N+1 server redundancy is not supported.

HLR Redundancy feature cannot be used.

The primary system cannot be configured to be the alternate system for a third system.

A branch-office scenario is not suitable in combination with system redundancy.

FQDNs in exchange data other than those listed in the IP translation table, are not handled.

The System Redundancy feature must be re-configured after any repair of the LIM 1 in the alternate system.

Automatic takeover at recovery

If network connection between the primary and the alternate system is lost and restored in quick succession or if the primary system starts and stops repeatedly during a short period of time, the active system might move back and forth, causing telephony services to be interrupted. The System Redundancy feature has a functionality to prevent frequent repeated takeovers, but unstable networks can still result in takeover.

The recommended configuration is automatic takeover at failure and manual takeover at recovery.

Limitations When the Alternate System is Active

Some IP endpoints cannot be configured to use a backup/secondary server and those IP endpoints cannot automatically register with the alternate system.

Hardwired terminals (for example, analog terminals) can be used in either the primary system or the alternate system.