

# Server Redundancy

OPERATIONAL DIRECTIONS



## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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](mailto: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>.

© Copyright 2019, Mitel Networks Corporation

All rights reserved

# 1 GENERAL

This document describes server redundancy and how to configure it in MX-ONE. Server redundancy is achieved by adding one or more standby servers to the network. A standby server has the ability to take over the tasks of a faulty LIM server.

The document is intended for those who want to know more about the functionality as well as technicians that want to learn about certain procedures and specific behavior of the function.

## 1.1 WHAT IS SERVER REDUNDANCY

Using server redundancy, a standby server can take over the tasks of a regular server suffering from, for example, hardware failure. This way, a faulty server can be replaced with a minimum of disturbance.

When using server redundancy, regular servers and an additional standby server are grouped as a cluster. The standby server is prepared with data from the regular servers in the cluster and ready to start an instance of any of these servers in case of a server fault.

To build a real fault tolerant cluster, network redundancy can be combined with server redundancy.

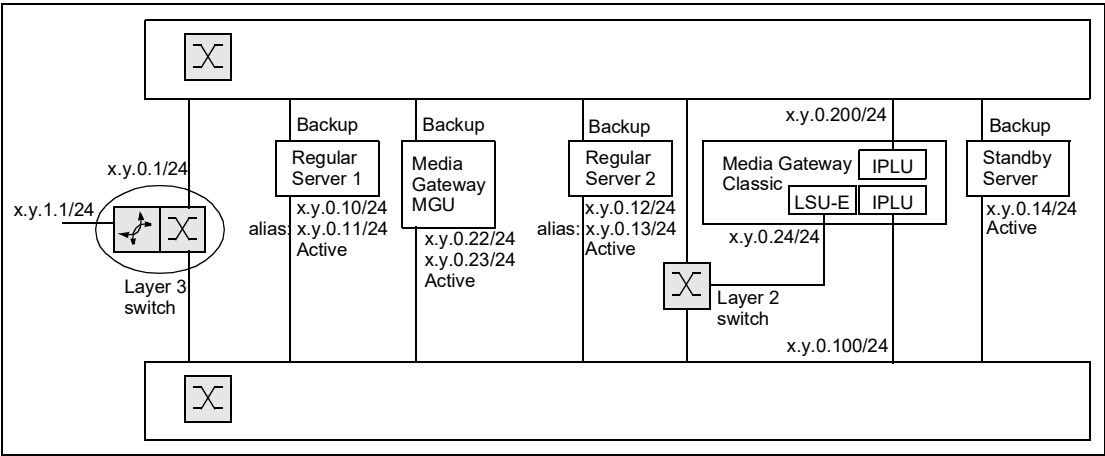


Figure 1: Server redundancy with Ethernet bonded network redundancy.

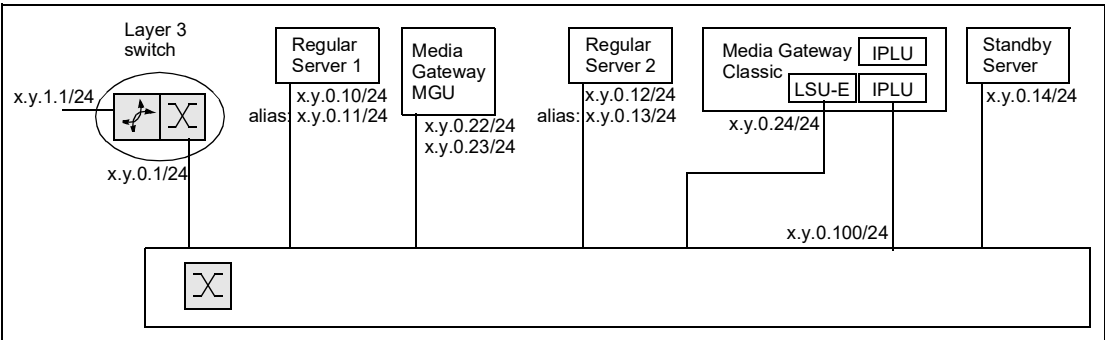


Figure 2: Server redundancy without network redundancy.

Each server in a cluster supervises the state of the other servers. In case of a server failure or lost network connection with the regular server, the software running on the faulty regular server will be started on the standby server. The standby server will also manage the media gateways of the faulty regular server.

Particularly, when the network connection is lost, the regular as well as standby server will run the MX-ONE Service Node service. Subsequently when the network connection is restored and the regular server and the standby server detect each other running the MX-ONE Service Node service, the regular server will stop running the service. A preloaded cluster behaves as a non-preloaded cluster in this regard. Network redundancy reduce the likelihood of both servers running the service simultaneously.

If there are more than one faulty regular servers in a cluster, the standby server will only replace one of the faulty servers. Other faulty servers will not operate. Which of the faulty regular servers the standby server will replace depends on the regular servers priority to run on the standby server. If the priority is equal, the first regular server started on the standby server will continue running. If a server with higher priority to run on the standby server fails, while the standby server is already running a regular server, it will be replaced by the server with higher priority.

Each regular server in a cluster is configured with two addresses, a base IP address and an alias IP address. The standby server is configured with only a base IP address. In case of a faulty regular server, the standby server will take over the alias IP addresses of the faulty server.

When a regular server recovers from a failure, the MX-ONE Service Node programs running on the standby server can fallback to the regular server.

Two types of fallback exist:

- Manual fallback  
A command has to be used to do the fallback to the regular server.
- Automatic fallback  
The fallback will take place as soon as the regular server has recovered.

During fallback, the MX-ONE Service Node software is stopped on the regular and standby servers, and then started on the regular server.

If a cluster server finds another cluster server with the same alias address active, one of the servers will remove the alias address and stop running the telephony programs. Which server that will stop depends on configuration. Normally the regular server will be stopped and then the fallback is executed, either automatically or manually. By this measure the consequences of Split brain is avoided.

If the alias IP address is found in use by some other network equipment (none cluster server), it can result in that the LIM is not started. This is an example of faulty network configuration.

## 1.2 HANDLING OF SERVER DATA

The standby server is prepared with data from the regular servers in the cluster and is ready to start an instance of any faulty regular server within the cluster. Reload and LDAP data is copied from the regular servers in the cluster to the standby server after every data backup and once every 24-hour period.

For a correct data synchronization, the server's clock have to be in sync and NTP configured properly. This is normally configured during system installation. If manual adjustments of the clocks are performed make sure servers clock are in sync. The reload data files modification times are used to select data sync direction between regular and standby servers.

Data backup is not allowed if LDAP master server is out of order, any data changes meanwhile gets lost when LDAP master server recovers.

## 1.3 PRELOADED CLUSTER

A standby server is preloaded with program and data to make failover faster. This is only possible for a cluster consisting of one regular server and one standby server.

**Note:** The preloaded cluster function is not supported with LSU-E based media gateways.

In a preloaded cluster the alias address is started in both servers at the same time, but it is blocked in the Linux kernel in the passive side. If the regular server fails, the blocking of the alias address is removed and the standby server is functional.

The passive side is updated with reload and LDAP data from the active side when the `data_backup` command is used on the active side. A data reload is then executed automatically in the passive side to prepare it for failover.

The time to detect a server as failed is lower in a preloaded cluster than in a regular cluster, 30 seconds.

A shorter fail detection time increases the risk for faulty detection of server failure. This puts higher requirements on the cluster servers and networks. Ensure that the cluster is configured with high performance servers. Use network and storage with enough bandwidth. Use of Network redundancy is recommended.

Failover or fallback can occur to a server (LIM) that is currently loading, but has not yet reached the preloaded state. If this happens the time to recover will be longer than with a server that has reached the preloaded state.

Using automatic fallback for instance, if the regular server is reloaded, fallback will occur as soon as the two servers have found each other. This will happen while the regular server (LIM) is still loading. The traffic disturbance at recovery using automatic fallback is in this case longer than if manual fallback is used. The manual fallback can be ordered when the reloaded server has reached the preloaded state. Manual fallback is a better alternative for preloaded clusters.

The LIM running on the preloaded server is isolated from the other LIMs in the system. In a multi-LIM system, the other LIMs are system blocked from a standby LIM point of view. You can have different alarms such as 'Broken connection to master LDAP', 'LIM out of order' in the preloaded LIM because of the isolation.

## 1.4 GLOSSARY

### ARP

Address Resolution Protocol. Used to find out on what hardware address (MAC) an IPv4 address is used.

### Alias IP address

An alias IP address tied to a specific network interface. IP aliasing is the process of adding more than one IP address to a network interface.

### Base IP address

The normal IP address for a network interface.

### Cluster

A number of regular servers and a standby server are grouped together in a cluster.

**Data backup**

Exchange data are stored on disk by doing a data backup.

**Gratuitous ARP**

An ARP announcement of a MAC and IP address combination.

**HLR redundancy**

The HLR backup or redundancy feature in MX-ONE. It provides a possibility for H.323 and SIP extensions, on certain conditions, to temporarily register to a backup HLR in another server instead of to the regular HLR server.

**LDAP**

A database used for configuration data in MX-ONE.

**Network redundancy**

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

**NTP**

Network Time Protocol.

**Regular server**

A Service Node server where a LIM normally is running.

**Standby server**

A server that can take over for a faulty regular server.

## 2 PREREQUISITES

The following requirements and limitations apply for installations using server redundancy:

- A cluster can have up to ten LIMs.
- A cluster can have only one standby server.
- It is possible to have as many clusters as there are LIMs in the system (with a maximum of one standby server per LIM server).
- A standby server can belong to only one cluster.
- A LIM server can belong to only one cluster.
- All servers in a cluster must reside on the same subnet. Gratuitous ARP is used in the network to announce that a standby server has taken over the alias IP address of a faulty regular server. (ARP is a link layer protocol, operating on the local subnet.)
- The Alias IP address must be on the same subnet as the base IP address.
- A standby server must have performance enough to be able to replace any regular server in the cluster.
- A standby server must have enough free hard disk space to store two data backups (LDAP data included) of each regular server in the cluster.
- There must be enough bandwidth within a cluster for efficient transfer of data backups to the standby server.
- Failover behavior preloaded is used only for clusters consisting of one regular and one standby server.
- Failover behavior preloaded is not supported if LSU-E based media gateways are used.

### 2.1 KNOWN LIMITATIONS OF THE SERVER REDUNDANCY FUNCTIONALITY

#### 2.1.1 AUTOMATIC FALLBACK

After a server failure using automatic fallback to the regular server, fallback will take place when the server is functioning again. This can create problems if the regular server starts and stops repeatedly during a short period of time.

#### 2.1.2 SEVERAL REGULAR SERVERS FAILING AT THE SAME TIME

If there are more than one faulty regular servers in a cluster, the standby server will only replace one of the faulty servers. Other faulty servers will not operate. Which of the faulty regular servers the standby server will replace depends on the regular servers priority to run on the standby server. If they have equal priority the first started on the standby server will continue to run. Only servers with higher priority will replace an already running server.

### 2.1.3 LIMITATIONS WHEN A LIM IS RUNNING ON THE STANDBY SERVER

It is not possible to perform data backups when LDAP master server is out of order. See chapter 2.1, Handling of Server Data.

If the failing server contains the LDAP master database, all functions that updates the LDAP database will not work when running on the standby server. The LDAP master database is not moved to the standby server.

The management system, running on the primary server, is not started on the standby server.

The media server, running on the primary server, is not started on the standby server.

The CSTA Phase III Web Service Application function, possibly running on the primary server, is not started on the standby server.

## 2.2 OTHER CONSIDERATION

### 2.2.1 WHEN TO USE BASE OR ALIAS IP ADDRESSES

The base IP address of a server in a cluster is used for connecting to applications on the specific server.

The alias IP address of a server in a cluster is used for applications moved between regular and standby server

For more information on when to use base and alias addresses, see the installation instructions for *INSTALLING AND CONFIGURING MIVoice MX-ONE*.

### 2.2.2 ARP CONSIDERATION

For IPv4 Gratuitous ARP is used to update ARP caches when an alias IP address is moved between a regular server and the standby server. Routers and switches have to be configured to accept Gratuitous ARP.

If Gratuitous ARP is not accepted, the failover time will equal the ARP cache timeout time, which is normally not acceptable.

To prevent too long delay in the failover, the ARP cache timeout time should not be too long. Gratuitous ARP is sent periodically to make sure network caches are updated.

### 2.2.3 USE LIM LOCKING AT USER CONTROLLED SERVER REBOOT

Locking the LIM to regular server is recommended before doing user controlled server reboot, especially in clusters configured for manual fall-back. This will keep the LIM on the regular server when the reboot is completed. Do not forget to unlock the LIM when the reboot is done.

## 3 AIDS

-



## 4 REFERENCES

-

## 5 PROCEDURE

### 5.1 CONFIGURING AND USING SERVER REDUNDANCY

Cluster configuration is performed after system installation. It can be executed in a running system, preferable in low traffic time.

Every regular LIM server needs an extra IP address in the cluster. This address, which is entered during cluster configuration, will become the new base address. The old base address will be used as alias address. This trick will remove the need for restarts during configuration.

The cluster configuration are performed using the *MX-ONE Maintenance Utility*. Log-in as user *mxone\_admin*, and key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` and select option *Cluster handling*

The following actions are possible:

- List all clusters
- Show status
- Create new cluster in system
- Change fallback type or priority
- Change failover behavior to preloaded
- Add a lim to existing cluster
- Remove a lim from existing cluster
- Delete cluster in system
- Move lim from standby to regular server
- Lock lim to server
- Unlock lim from server
- Sync exchange data within cluster

Some of the actions listed above will remove old xdata-versions (reload and LDAP data) that are incompatible with current configuration.

After these actions only one xdata-version exist:

- Create new cluster in system
- Change fallback type or priority
- Change failover behavior to preloaded
- Add a lim to existing cluster
- Remove a lim from existing cluster

- Delete cluster in system

## 6 EXECUTION

### 6.1 ADD A CLUSTER

1. Install new server.  
For detailed information, see *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.
2. On LIM 1 log in as user *mxone\_admin*.
3. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
4. Select option *Server in system* to add a new server to system.  
Follow the procedure as instructed on screen.
5. Select option *Standby server in system* to convert free server to standby server.  
Follow the procedure as instructed on screen.
6. Select option *Cluster handling* to create a new cluster in system.  
Follow the procedure as instructed on screen.

### 6.2 REMOVE A CLUSTER

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to delete cluster in system.  
Follow the procedure as instructed on screen.
4. Select option *Standby server in system* to convert standby server to free server.  
Follow the procedure as instructed on screen.
5. Select option *Server in system* to remove server to system.  
Follow the procedure as instructed on screen.

### 6.3 ADD A LIM TO A CLUSTER

A LIM can be added to a cluster. An additional IP address has to be entered. This IP address will be the new base address for the interface. Use utility: `/opt/mxone_install/bin/mxone_maintenance -> cluster -> add`

1. On LIM 1 log in as user *mxone\_admin*.

2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to add lim to existing cluster.  
Follow the procedure as instructed on screen.

## 6.4 REMOVE A LIM FROM A CLUSTER

A LIM can be removed from a cluster. If the last LIM in the cluster is removed, the complete cluster will be removed.

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to remove lim to existing cluster.  
Follow the procedure as instructed on screen.

## 6.5 PRINT CLUSTER STATUS

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to show status of all clusters.

## 6.6 PRINT CLUSTER CONFIGURATION

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to list all clusters.

## 6.7 CHANGE FALLBACK TYPE AND LIM PRIORITY

The fallback type and the LIM priority to run on the standby server can be changed.

Fallback type can be automatic or manual

A lower priority value, gives higher priority to run on the standby server.

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to change fallback type or priority.

## 6.8 CHANGE FAILOVER BEHAVIOR TO PRELOADED

A cluster consisting of one regular and one standby server is configured and preloaded.  
(To remove pre-loading, cluster must be removed).

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to change failover behavior to preloaded.

## 6.9 EXECUTE MANUAL FALLBACK TO REGULAR SERVER

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
`sudo -H /opt/mxone_install/bin/mxone_maintenance` to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to change failover behavior to get preloaded.

## 6.10

## EXECUTE A MANUAL ORDERED SYNCH OF DATA

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
*sudo -H /opt/mxone\_install/bin/mxone\_maintenance* to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to synch exchange data within cluster.

## 6.11

## LOCK OR UNLOCK A LIM TO A SPECIFIC SERVER

A LIM can be locked to a regular server or a standby server to prevent failover.

When a LIM is unlocked from a server, failover actions can occur again.

If a LIM locked to the standby is unlocked, the clusters configured fallback type determines what will happen. With automatic fallback, the LIM will fallback to regular server (if it is functional). With manual fallback the user has to manually order the fallback.

1. On LIM 1 log in as user *mxone\_admin*.
2. Key command  
*sudo -H /opt/mxone\_install/bin/mxone\_maintenance* to start MX-ONE Maintenance Utility.
3. Select option *Cluster handling* to lock lim to server.  
or  
Select option *Cluster handling* to unlock lim from server.

## 7 ALARMS

This chapter describes MX-ONE alarms related to server redundancy.

### 7.1 LIM IS RUNNING ON STANDBY SERVER

This alarm is received when a LIM is running on the standby server.

The alarm indicates that a regular server has a network problem, faulty hardware, or is rebooting. If the fault is of a more serious character, manual measures might be needed.

### 7.2 STANDBY SERVER IS OUT OF ORDER

This alarm is received when contact with a standby server is lost.

The alarm indicates that the standby server has a network problem, faulty hardware, or is rebooting. If the fault is of a more serious character, manual measures might be needed.

### 7.3 STANDBY CLUSTER HAS FAILED TO SYNCHRONIZE DATA

This alarm is received when a standby server has failed to synchronize exchange data with the regular servers in a cluster.

## 8 TERMINATION

-