

MiVoice Business

Clustering Design and Implementation

RELEASE 9.2

SEPTEMBER 2021



Notice

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>.

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2020, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	Introduction	1
	About this Document	1
	Document Organization	1
	What's New?	2
	Mitel MiVoice Business Release 9.2	2
	Mitel MiVoice Business Release 9.0	2
	Mitel MiVoice Business Release 8.0	2
	Mitel MiVoice Business Release 7.0	2
	Mitel Communications Director Release 6.0	2
	Mitel Communications Director Release 5.0	2
	Who Should Read This Book?	2
	Related Documentation	3
	Other Information Sources	3
	Text Conventions	4
 Chapter: 2	 Voice Networking Fundamentals	 5
	About Mitel Voice Networks	5
	Benefits of a Network	5
	Common Network Topologies	6
	Star Networks	6
	Fully Meshed Networks	6
	Choosing a Topology	6
	Characteristics of a Mitel Voice Network	7
	About Mitel Voice Clusters	7
	Cluster Topologies	8
	Characteristics of a Voice Cluster	9
	Call Routing in the Network	10
	Key Components of Network Call Routing	10
	The Primary Node Identifier	10
	Local and Remote Directory Numbers	10
	Cluster Element (CE) Digits and Cluster Element Identifier (CEID)	11
	Routing Examples	11

Routing Calls between Cluster Elements11
Routing an Inbound Call from Outside the Cluster13
Resiliency and Clustering14
The Impact of Resiliency on Network Design15
Key Design Considerations15
Recommended Resilient Topologies15
Resilient Single-site Environment16
Resilient Distributed Network16
Resilient Hybrid Network17
Network Management18
About System Data Synchronization18
Sharing Scopes - How the extent of data distribution is controlled	19
Sharing Scope Examples19
About Multi-Node Management Applications22
About Administrative Groups23
Bandwidth Management23

Chapter: 3 Planning the Cluster 24

Overview24
Completing the Pre-requisites24
Optional Components25
Identifying the Network Requirements26
Collecting Form Data28
Network Element Information28
Cluster Information28
Numbering Plan and ARS29
Resiliency Requirements30
Resiliency Rules30
Class of Service and Class of Restriction31
User and Device Data31
IP Trunking Data31
Choosing a Database Programming Strategy32

Chapter: 4 Installation and Configuration 33

Overview33
Prepare Controllers33
Install Hardware and Upgrade Controller Software34
Create the Import Files (Optional)34
Rules for creating .csv Files34
How many worksheets do you need?36
Cluster the Network Elements38
Creating a Resilient Device or Hot Desk User38
Testing Resiliency38
Changing the Secondary Controller39
Disabling Resiliency39

Configuring Resiliency for Trunks, Groups, and Agents39
Configure Resiliency40
Complete Data Programming40
Import User and Device Data41
Test Your Cluster Configuration42
COS and COR Group Data43
IP Trunk Data43
ARS Data44
Cluster Element IDs and Feature DNs44
Program (or Import) the Cluster System Data45
Define the Administrative Groups45
Configure your Browser for Application Reach-Through46
Checking for Data Distribution Errors46
Synchronizing the Network Elements47
Start Sharing Data via SDS47
Create the Cluster48
Populate the Network Elements Form49
Prepare Elements for Clustering51

Chapter: 5

Using Multi-Node Management Applications	52
Overview52
Conditions52
Creating an Administrative Group53
Application Reach-Through53
About Application Reach-Through53
Typical Application Reach-Through Tasks54
How is Application Reach-Through Supported in the Forms?54
Application Reach-Through - Conditions54
Using Application Reach-Through55
Before You Start55
Accessing a Form on a Remote Element56
Application Reach-Through: Examples56
Troubleshooting57
Fault Management60
About Fault Management60
Overall Alarm Status60
Alarm Status Summary60
Fault Management Conditions60
Obtaining an Alarm Summary for the Group61
Obtaining the Alarm Details61
MNM Backup and Restore61
About MNM Backup and Restore61
Conditions and Restrictions61
Performing a Backup62
About Backups62
What Data is Backed Up?63

Back Up a Single System	63
Back Up Databases from an Administrative Group	64
Performing a Restore	65

Chapter: 6	Using the Import Spreadsheet	67
	Overview	67
	Requirements and Conditions	67
	Requirements	67
	Conditions	67
	Obtaining the Import Spreadsheet	68
	Creating Sub folders for the Cluster Elements	69
	Rules and Guidelines for Importing Data	71
	Entering Data into the Worksheets	71
	Creating the Import File from the Import Spreadsheet	72
	Setting Call History Records Capacity	73
	Previewing the Import Data	73
	Importing the Data into the MiVoice Business System	74
	Troubleshooting Import Errors	74
	Validation Errors	74
	Import Errors	75

Chapter: 7	Cluster Maintenance	76
	Overview	76
	Enabling and Disabling SDS	76
	Performing Backups and Restores	77
	Performing a Backup	77
	Performing a System Restore	77
	Adding a New Element to an Existing Data-Sharing Community	78
	Start Sharing with a New Element at the Network Level	79
	Start Sharing with a Network Element at a Cluster Level	79
	Removing an element from a data-sharing community	79
	Removing an Element from a Cluster	81
	Moving an Element to a Different Data- sharing Cluster	81
	Correcting Inconsistent Remote Directory Numbers	81
	Changing the Data Distribution Scope	81
	Splitting a Data-Sharing Cluster	82
	Merging Data-Sharing Clusters in the same SDS Network	83
	Resolving Data Distribution Errors and Pending Updates	84
	About Automatic Retry	85
	Repairing Data	85
	Moving Users to a Different Cluster Element	86
	On the source MiVoice Business System	86
	On the Destination MiVoice Business System	89

Chapter: 8	Glossary	91
-------------------	---------------------------	-----------

Introduction

About this Document

This document explains how to build and manage a resilient network of Mitel MiVoice Business systems.

Key topics covered:

- Fundamentals of Mitel voice networks
- Clusters
- Resiliency
- Network Management (System Data Synchronization and Multi-Node Management Applications)
- Bandwidth Management

The objectives of the document are to:

- Introduce MiVoice Business networking concepts.
- Highlight the major design considerations that must be addressed to provide a highly reliable infrastructure with fail over protection against network traffic interruptions.
- Provide best practices to ensure that the network has been properly provisioned and implemented to support IP telephony services.
- Provide a comprehensive overview on using the network management tools embedded in the MiVoice Business system.

Although the document contains plenty of detailed information on network design and implementation, the focus is on building a basic network of resilient MiVoice Business systems. For more complex network deployments, you may want to get the assistance of Mitel Professional Services. Contact a Mitel sales representative for more information.

Document Organization

- [*The Fundamentals of Mitel Voice Networks*](#)
Introduces the key concepts of voice networking using Mitel technology with emphasis on clustering and resiliency.
- [*Planning the Network*](#)
Describes the pre-installation preparations necessary for setting up a network of MiVoice Business systems.
- [*Installation and Configuration*](#)
Describes, step-by-step, how to install and configure a resilient cluster of MiVoice Business systems.
- [*Using Multi-Node Management Applications*](#)
Explains how to use Application Reach-Through and other management tools embedded in the MiVoice Business software to manage a network of MiVoice Business systems.
- [*Using the Import Spreadsheet*](#)
Describes the Import Spreadsheet and how to use it to program a cluster of MiVoice Business systems.
- [*Cluster Maintenance*](#)

Covers various tasks involved in maintaining an operating network, from adding and removing systems to software upgrades and database backups.

What's New?

Mitel MiVoice Business Release 9.2

Minor updates to the splitting a data sharing cluster section. See, [Splitting a Data-Sharing Cluster](#).

Mitel MiVoice Business Release 9.0

No updates.

Mitel MiVoice Business Release 8.0

No updates.

Mitel MiVoice Business Release 7.0

For software changes in MiVoice Business 7.0 pertaining to clustering and other subjects discussed in this document, see "What's New in This Release" in the System Administration Tool Help.

Mitel Communications Director Release 6.0

For software changes in MCD 6.0 pertaining to clustering and other subjects discussed in this document, see "What's New in This Release" in the System Administration Tool Help.

Mitel Communications Director Release 5.0

This document is completely new for MCD 5.0. It supersedes the "3300 ICP Multi-Node Management Clustering" and "Voice Clustering (Portable Directory Number)" documents from earlier 3300 ICP/MCD releases.

For software changes in MCD 5.0 pertaining to clustering and other subjects discussed in this document, see "What's New in This Release" in the System Administration Tool Help.

Who Should Read This Book?

This document is for certified Mitel MiVoice Business technicians and system administrators who plan, install, and maintain MiVoice Business networks.

It assumes that the reader understands general data networking principles and has a fundamental understanding of IP networking technologies and protocols.

To get the most from this document, the reader must have a thorough understanding of, or experience with


- MiVoice Business on 3300 ICP or industry-standard servers
- MiVoice Business System Administration Tool
- MiVoice Business Automatic Route Selection
- MiVoice Business Resiliency

Related Documentation

For the latest MiVoice Business documentation, see the Mitel Customer Documentation web site ([Document Center](#)). There, you'll find these and other information sources on installing, configuring, and using the MiVoice Business/3300 ICP:

- The *MiVoice Business Engineering Guidelines* highlight specific areas of the product that you must consider before installation. Use this guide to help plan site installations.
- The *MiVoice Business Site Planning Guide* also helps you prepare to install an MiVoice Business system. Use the questionnaires and checklists in this guide to collect site information and identify customer requirements and system engineering considerations that must be addressed before installation.
- The *MiVoice Business Resiliency Guidelines* provides the information required to understand, plan, and implement a failure resistant network using the MiVoice Business Resiliency solution.
- The *3300 ICP Technician's Handbook* provides installation, upgrade, maintenance, and troubleshooting instructions for the latest generation of MiVoice Business and 3300 ICP products.
- The *3300 ICP Hardware Technical Reference Manual* contains hardware specifications for the 3300 ICP and its components.
- The MiVoice Business System Administration Tool Help is the main source for information on programming and maintaining MiVoice Business software, the operating system for the 3300 ICP.

NOTE: All of the above documents, except the *MiVoice Business Engineering Guidelines*, are

included in the MiVoice Business 7.0 System Administration Tool Help. Use the  button in the Help viewer to access them. Also, be sure to check the [Document Center](#) web site for newer versions of these documents and for other MiVoice Business-related information sources, including the *MiVoice Business Engineering Guidelines*.

Other Information Sources

The following documents are from the Mitel Solutions Series collection on [Document Center](#). They cover some of the same topics discussed in Chapter 2 of this document but for a more general audience.

- *Multi-node Networking*
- *Using System Data Synchronization*

Text Conventions

Key terms are *italicized* the first time they are used and defined. These terms are also in the glossary at the back of the document.

NOTE: Notes point out areas of special concern or interest that merit consideration.

Warning Warnings and Cautions draw attention to anything that could damage equipment, cause the loss of data or service, or that could help you avoid certain mistakes or pitfalls.

Bold is used exclusively in procedures to denote interface elements, such as buttons and fields, under discussion or that you are required to click.



Denotes a hyperlink. This icon appears immediately after references to content outside of this document. Clicking the icon takes you directly to that content. You'll only see the icon when viewing the document from within the System Administration Tool Help for MiVoice Business 7.0. References to Help content that is not hyperlinked can quickly be found using the search in the Help—just copy the text reference into the Search form and follow the first link in Search results to the content.

Voice Networking Fundamentals

About Mitel Voice Networks

A voice network is a group of interconnected MiVoice Business systems, each referred to as a network *element*.

MiVoice Business networks can be deployed in a campus environment, on a city-wide, regional, national, or international basis, or all of the above in combination. Figures and 2.2 are examples of MiVoice Business networks, one showing elements that are geographically co-located (i.e., in the same building or campus), the other showing elements that are dispersed among several cities.

NOTE: The elements shown in Figures and 2.2—and throughout this document—are 3300 ICPs but they could also be industry-standard servers running MiVoice Business software or virtual MiVoice Business systems.



Figure 2.1: Local Area Network Application



Figure 2.2: Wide Area Network Application

Benefits of a Network

A network of MiVoice Business systems offers the following benefits:

- provides more lines than a single system.
- multi-site enterprises are able to operate as an integrated unit by forming their own private networks and can achieve operational efficiencies and cost savings by routing traffic across their own network rather than through the more expensive public network. Other opportunities for savings:
 - Centralizing attendant and voice mail management functions.
 - Using least cost routing (a feature of *Automatic Route Selection*) to ensure that the most economical option is used for routing any call, including routing calls through the private network before exiting at the cheapest point closest to the public destination.
 - Using the *Multi-Node Management Applications* embedded in each network element (requires MCD 5.0 software) which provides a single point of access for all network configuration and maintenance.
- 1
- operational resiliency and redundancy to ensure continuous service in the event of a network failure and for avoiding out of service or busy links through the use of alternative routes.
- ease of access to work colleagues in geographically dispersed locations, often just by dialing an extension number.
- support for MSDN/DPNSS features, such as calling line ID, callback when free, camp-on, conference and call forwarding between all network sites.

1. Supported in networks of up to 20 elements per Administrative Group. See for more information.

- allows business groups or communities of interests within an organization, each with different needs, to be serviced by their own system while remaining in a common network.

Common Network Topologies

Topology refers to the arrangement or physical layout of the PBXs, cables, and other components on the network. There are many ways to arrange—or design—a network. Most are variations on two basic topologies—star and fully-meshed—in use for decades, in both data and voice networks.

Star Networks

The star network uses an intervening PBX called a *tandem* switch. Each and every PBX is connected via a single tandem switch. Star configurations are normally employed when traffic levels between PBXs are comparatively low. The key feature of such networks is device isolation whereby a failure in any link between switches only takes down network access to some devices and not the entire network. (If the tandem switch fails, however, the entire network also fails.)



Figure 2.3: Typical Star Network

Fully Meshed Networks

A fully meshed network is one in which each and every PBX is connected by trunks to each and every other PBX. Mesh networks are trunk intensive and are used when there are comparatively high traffic levels between PBXs and the geographic or economic conditions justify the expensive trunking required.

The key feature of such networks is link redundancy, which provides alternative communications paths between some or all devices for times when inter-switch links are busy or disabled. Fully meshed networks also reduce the number of network elements—and therefore the number of potential bottlenecks—involved in each call to just the two end points.



Figure 2.4: Typical Mesh Network

Choosing a Topology

Topology selection depends on many factors, including:

- physical locations of the networked elements
- network size (number of lines)
- call traffic between elements
- usability
- interoperability with other enterprise applications
- cost
- future growth (scalability)

- the requirement for resiliency.

Whether you are building the network from scratch or adding voice to an existing data network, the goal is the same: the converged network must not compromise the quality of voice or data traffic.

NOTE: Traffic measurement and voice quality are beyond the scope of this document. For information on these subjects, see the *MiVoice Business Engineering Guidelines*. See also the *Voice Quality Troubleshooting Guide* and the *Voice Quality Solutions Guide*.

Characteristics of a Mitel Voice Network

Below are the distinguishing characteristics of a voice network built on Mitel proprietary PBX/IP-PBX technology:

- Can consist of standalone network elements and *cluster* elements (described below).
- Can comprise
 - EX controller
 - MiVoice Business platforms (3300 ICP, MiVoice Business for ISS, and MiVoice Business for VMware virtualized environments)
 - Mitel 200 ICP (via IP trunks)
 - Mitel 5000 Communication Platform (via SIP)
 - Non-Mitel systems (via QSIG and SIP)
- Users are required to dial ARS digits to call extensions on another network element.
- Databases on each network element can be completely different. No need for uniform configuration.¹
- Elements are interconnected by IP trunks and/or DPNSS or QSIG over TI/EI trunks.
- MiVoice Business systems can be at different software levels.

About Mitel Voice Clusters

A cluster is a group of interconnected elements that are configured together in such way that it appears to end users that they are connected to a single large system. A user can make a call from one system in the cluster to another just by dialing an extension number. For calls within the cluster, there is no indication on the display of the called extension that the call originated from another element in the cluster.

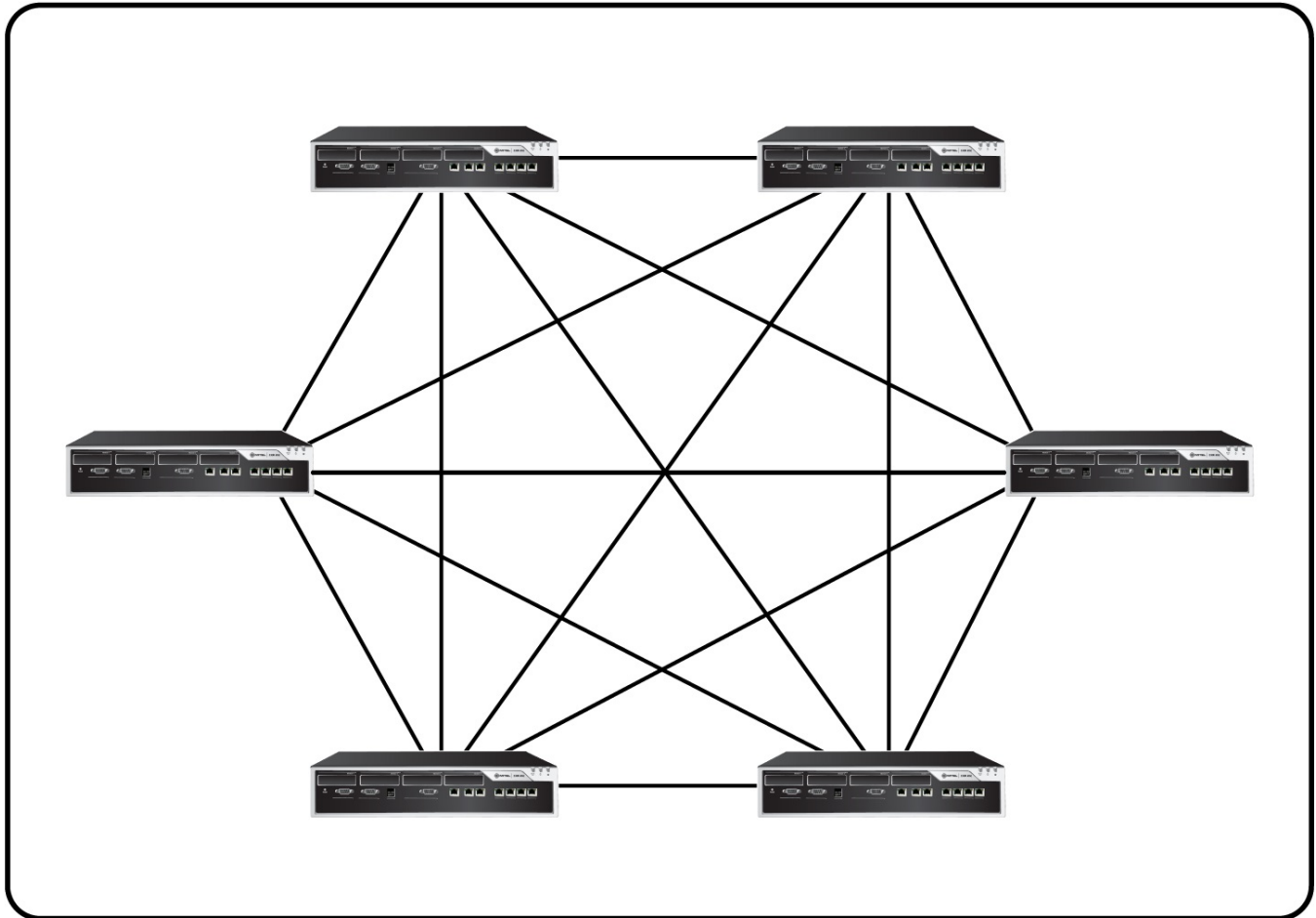
Each element in the cluster shares the directory entries of all the other elements, and system programming is standardized across all the elements. When network elements are configured in a cluster, you can

- reassign a directory number to any extension in the cluster without changing ARS programming,
- call any extension or other device in the cluster without dialing ARS leading digits.
- implement resiliency.

1. If required, the *System Data Synchronization* feature of MiVoice Business can be used to achieve and maintain database uniformity among network elements. See about

Cluster Topologies

Elements in a cluster can be arranged in all the same configurations as a non-clustered network. For clusters of 20 nodes or fewer, a fully meshed configuration (*Fully-meshed Cluster*) is simple to deploy, but as each new node is added, there is additional management overhead on every existing unit to add the new IP trunk.



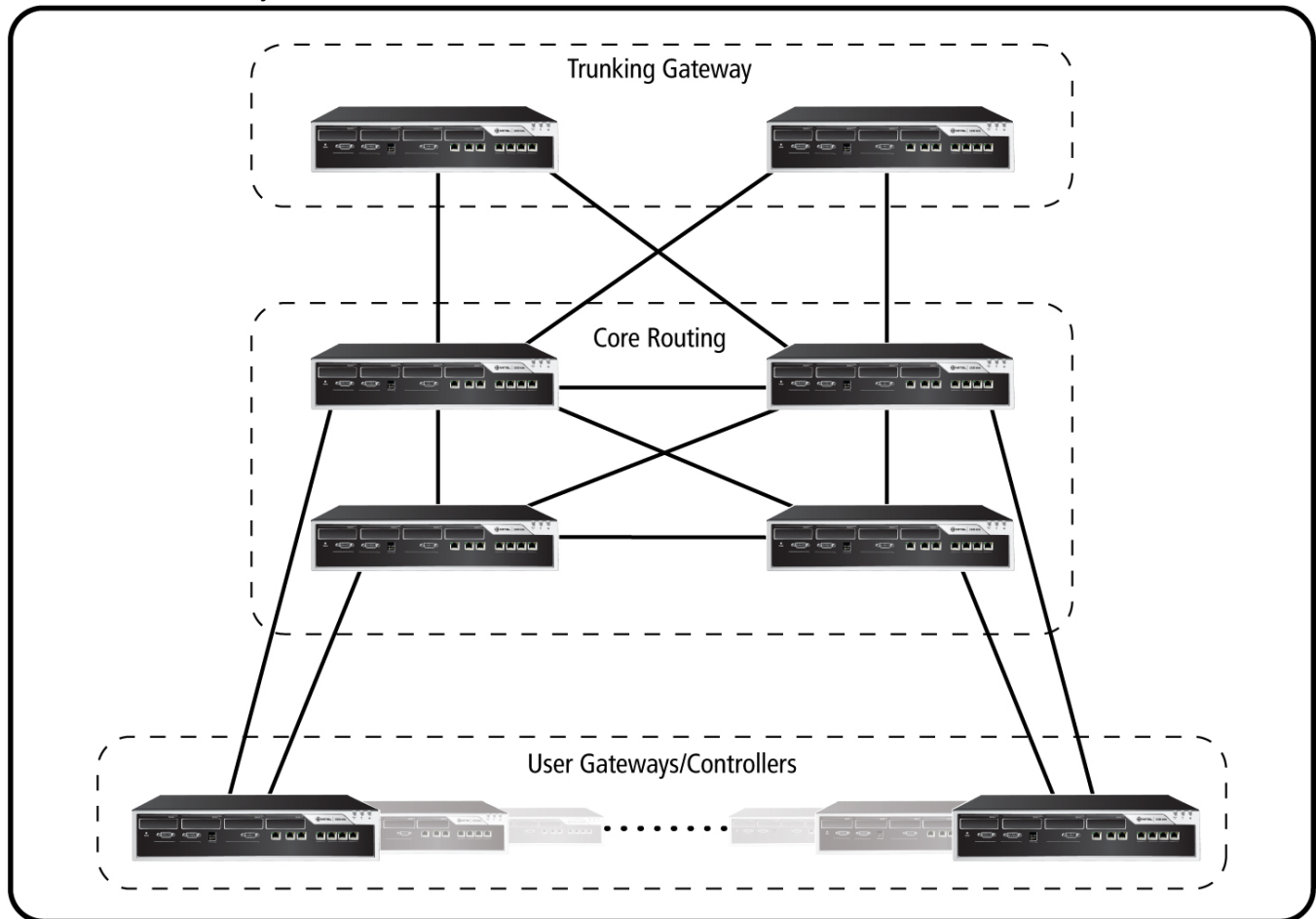
IP1436

Figure 2.5: Fully-meshed Cluster

Every node requires $N-1$ IP trunk connections. The number of trunks required is half that number. So for 20 nodes, there are 190 IP trunks $(20 \times (20-1))/2$. That means there are 380 end-points to be programmed.

For larger networks, especially those with many smaller remote nodes, it may be more practical to deploy a hierarchical network (*Figure 2.6*). In a hierarchical network, a central group of core routing switches are fully meshed, but only one or two links are required to connect to the remote nodes. Additional nodes then only require an update at the central group and at the new remote site.

The example 20-node network might therefore only need 38 IP trunks, with 76 end-points to be programmed. Adding the 21st node would require programming of four additional IP trunks, compared to 40 for the meshed system.



IP1437

Figure 2.6: Hierarchical Network with Fully-Meshed Nodes

Characteristics of a Voice Cluster

The features that distinguish a Mitel voice cluster from a voice network are as follows:

- A cluster can be part of larger MSDN/DPNSS network.
- A single network may consist of multiple clusters.
- A cluster has a uniform number plan with transparent extension dialing (i.e., no ARS digits to dial).
- A cluster and its telephone directory are managed entirely by *System Data Synchronization* through the MiVoice Business System Administration Tool.¹
- The maximum size of a single cluster (with all elements running 3300 Release 8.0 UR3 software or later) is 999. (Single clusters that large cannot be managed with SDS).^{2,3}

1. It is possible, but not advisable, to build clusters without SDS. Data for each node in such clusters would have to be programmed manually or imported from a spreadsheet. Nodes running MCD 4.0 or later and those running older software can be in the same network but only the former can share data.

As with voice networks, MiVoice Business elements in the cluster are interconnected via IP trunks and/or DPNSS over T1 trunks. In some situations, SIP trunks may be used between network elements, or to connect to an external SIP trunk service provider.

Call Routing in the Network

This section compares the way ARS works in a network versus a cluster. Understanding the differences is important since ARS configuration is a crucial component of network design.

Below is a summary of the process followed by a more detailed explanation:

In a network of standalone elements, dialed digits translate to an ARS entry that matches the destination network element's *Primary Node Identifier (PNI)*, if used. This, in turn, selects an ARS route identifying a trunk group to the destination element. In the absence of PNIs, ARS and digit modification are used to strip off the leading route selection digits before sending the remaining digits (the extension number) to the element.

In a cluster, the system prefixes the dialed digits with ARS digits that match a number string (the *Cluster Element Digits*) assigned to the remote cluster element. The modified string is then delivered to ARS, which completes the routing by identifying a trunk group to the destination element.

Key Components of Network Call Routing

The Primary Node Identifier

As mentioned earlier, a network can consist of standalone network elements and one or more clusters of elements. In a network of both standalone and clustered elements, each standalone element and each cluster is assigned a Primary Node Identifier (PNI). The PNI is used by ARS to route calls between standalone network elements, between standalone network elements and a cluster, or between multiple clusters. (If it helps, think of each standalone element as a unique cluster that consists of a single network element.)

In a single cluster network, PNIs are optional, although programming a common value at each network element is still recommended.

To place a call to an extension on another standalone element or cluster, a user must dial ARS digits (which the called party may see on their telephone display) in addition to the extension number.

Local and Remote Directory Numbers

The directory numbers in the Telephone Directory forms of each element are classified as either local directory numbers or remote directory numbers. A local directory number belongs to a device, such as an IP phone, that is provisioned on that element. A remote directory number belongs to a device that is connected to another element in the cluster. Thus, the directory number for a local device on element A is a remote device in relation to element B and appears in the Remote Directory Numbers form of element B. Conversely, a local device on element B would appear in the Remote Directory Numbers form of element A.

-
2. For cluster sizes over 20 elements, a multi-hub configuration in which calls between peripheral elements in the cluster transit through designated hubs is recommended. At more than 249 nodes, a multi-hub configuration is mandatory.
 3. A cluster can include any MiVoice Business platform, including MiVoice Business Multi-instance and MiVoice Business for virtualized environments, as well as Mitel MiCollab. See "Completing the Prerequisites" on page 34 for specific software version requirements.

Local numbers registered to a particular network element (its host element) that are not shared within the cluster appear in the Local-only Directory Number List form on each element. Such numbers can only be reached from their host element. Devices on the same element can dial the number directly. Devices on other elements dial ARS routing digits in addition to the number.

The information in these three forms is used to determine what additional ARS digits need to be added to correctly route the call. If the called number is local to an element, ARS digits are not added. The Remote Directory information is shared cluster-wide, allowing the user to dial the extension of another user within the same cluster without the need for ARS digits.

To the user the entire cluster looks like a single system, even though the end devices may be distributed across multiple physical elements.

Cluster Element (CE) Digits and Cluster Element Identifier (CEID)

Each network element in a cluster is assigned a unique Cluster Element digit string in the Cluster Element form. The string is used to route calls between the cluster elements and so must appear in the Cluster Element form of all cluster members.

Each CE digit string is also assigned a Cluster Element Identifier (CEID). The CEID is the PBX number assigned to the network element in the Network Element form. Assigning the PBX Number/CEID of a remote cluster element to a directory number classifies that directory number as a remote directory number.

When a user on a cluster element (A) dials the remote directory number of an extension on a remote cluster element (B), element A automatically inserts the CE digits of element B in front of the dialed directory number. ARS then routes the call to the remote cluster element based on the CE digits. The user does not dial the CE digits to call a remote directory number nor do the digits appear on telephone displays for calls within the cluster.

Routing Examples

The process of call routing in a cluster begins by identifying where (i.e., which element) the dialed destination is located. The PNI is the first clue. It tells the element receiving the call whether it is destined for an element in its own cluster or to another cluster or standalone element in the network. Remember that all elements in a cluster share the same PNI, making it appear as a single network element to inbound calls. When a cluster element receives a call it looks at the PNI prefixed to the dialed number to see whether it matches its own. If it doesn't match, it means the call is bound for a destination outside the cluster. If it does match, the PNI is stripped off, leaving just the extension number. All that remains to complete the call is to determine which element in the cluster the dialed extension is connected to. The following examples explain how that is done.

Routing Calls between Cluster Elements

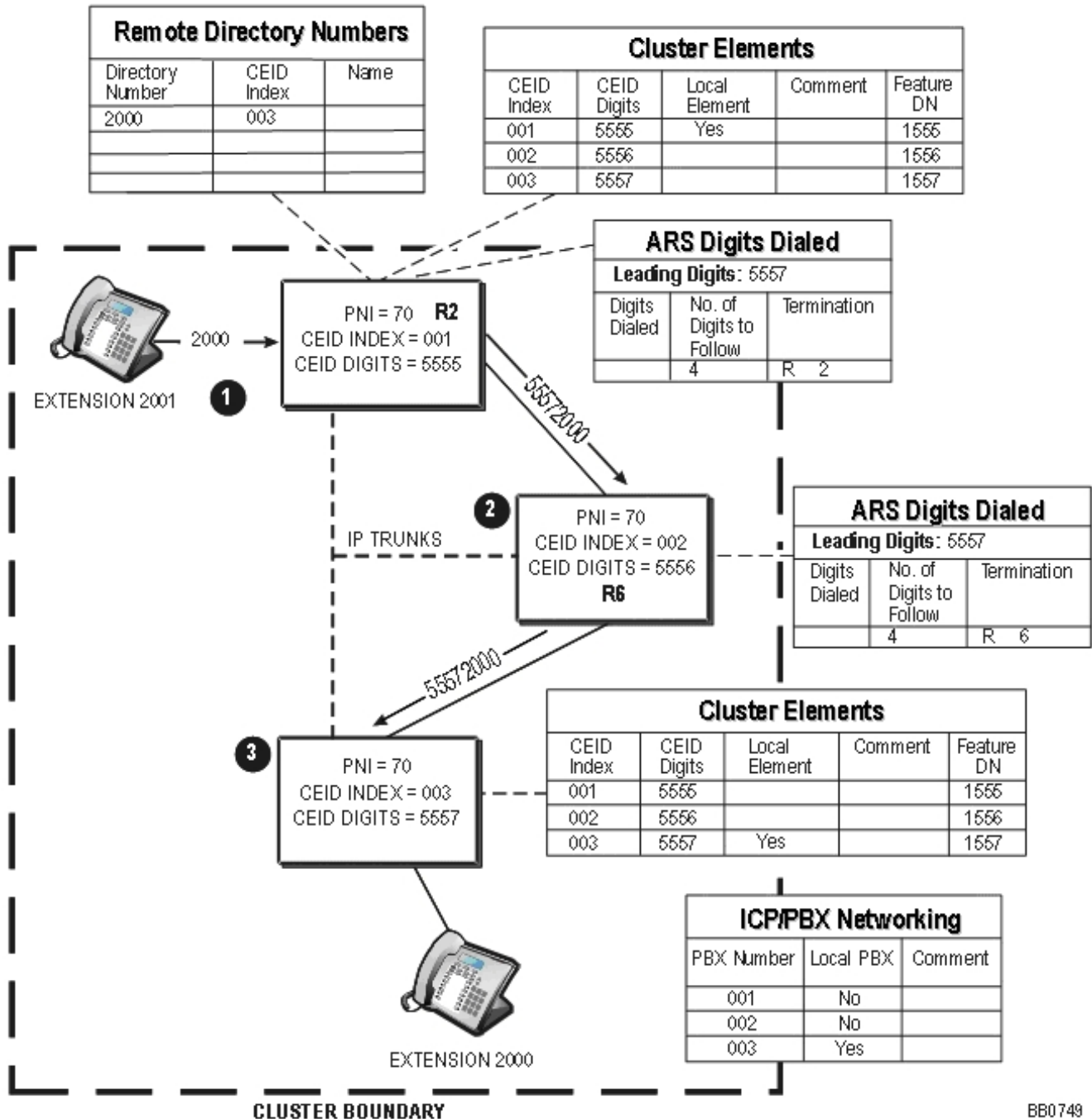
Figure 2.7 illustrates how a call is routed from an extension on one cluster element to an extension on another element in the cluster.

Stage 1 - caller at 2001 on the first cluster element dials 2000. The element checks for a dialable string of 2000 in its digit tree. It finds 2000 in its Remote Directory Numbers form. The CEID index for 2000 is 003. This number indexes the Cluster Elements form, which translates 003 to 5557. Digit string 5557 is the ARS string that all elements within the cluster use to direct calls to the third element. The element

prefixes the 5557 to 2000 and delivers 55572000 to ARS. ARS identifies Route 2 (by looking in the ARS Digits Dialed form) as the termination point for the digits 5557 and dials 572000 on Route 2.

Stage 2 -second element receives 55572000. It checks for a dialable string of 55572000. It finds 5557 followed by any 4 digits in its ARS table. ARS points to Route 6. The element dials 55572000 out to the third element.

Stage 3 - third element receives 55572000. It checks for a dialable string of 55572000 in its digit tree. The element's digit tree indicates 5557 is in its Cluster Elements form. The Local field in the form is set to "Yes", which indicates that the extension is a local device. The element then strips off the 5557 and rings extension 2000.



BB0749

Figure 2.7: Call Routing: Inter-element Calls

NOTE: Users in a cluster do not dial the PNI or CEID digits of a cluster element when they call other extensions in the cluster. Dialing the extension number is sufficient for calling any user within the cluster.

Routing an Inbound Call from Outside the Cluster

Figure 2.8 illustrates how a cluster handles an inbound call from another element in the network.

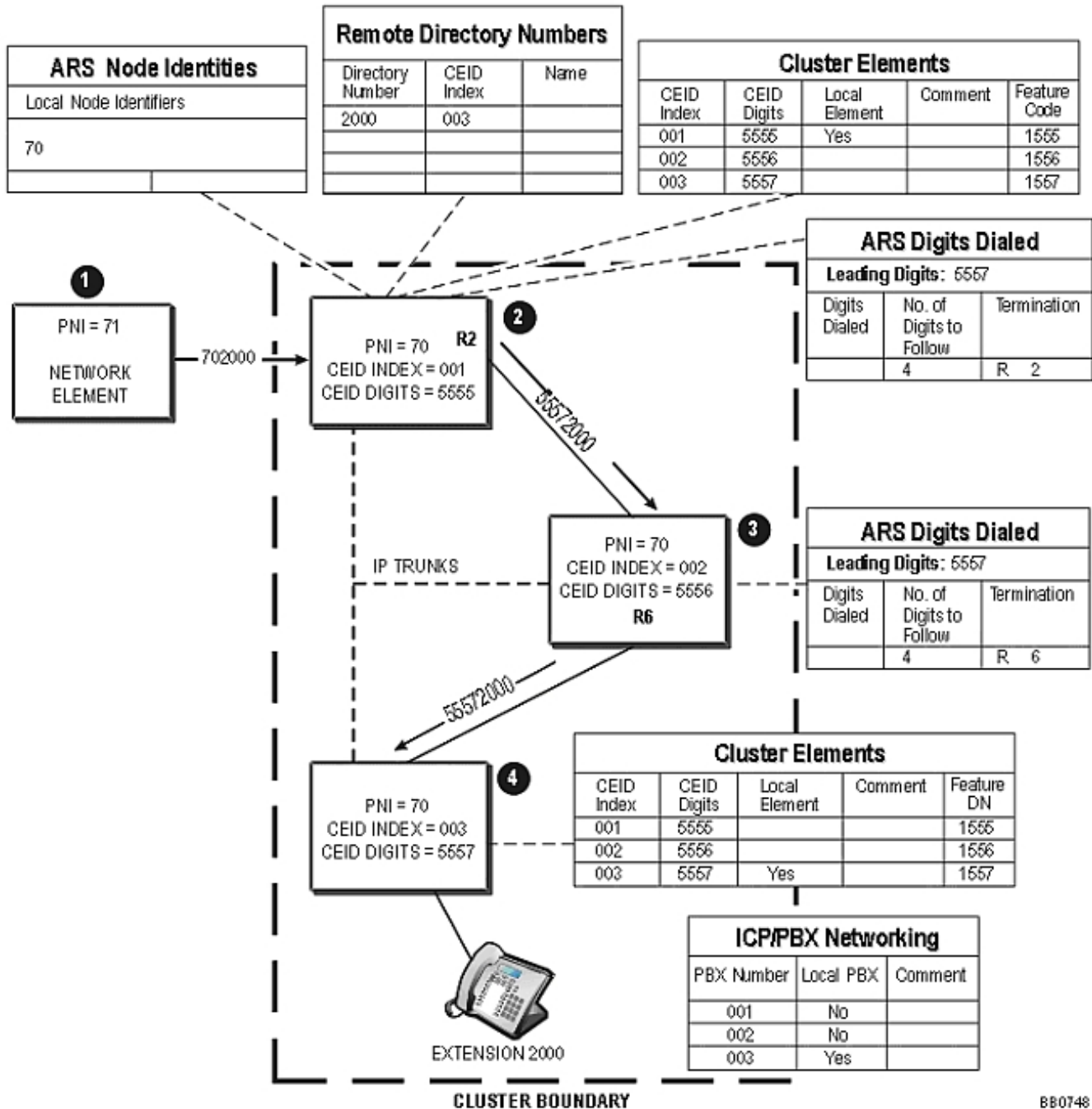
Stage 1 -A caller on network element with a PNI of 71 dials 702000. Network element (PNI 71) sends the digits to an element in the cluster that has a PNI of 70 (each cluster element has 70 as its PNI).

Stage 2 - The cluster element receiving the call identifies the 70 as its own PNI. It strips off the PNI and checks for a dialable string of 2000 in its digit tree. When it determines that 2000 is a Remote Directory Number, it references the CEID index for 2000, which is 003. This number indexes the Cluster Elements form which translates 003 to 5557. The digit string 5557 is the ARS string that all elements within the cluster use to direct calls to the third element. The element prefixes the 5557 to 2000 and delivers 55572000 to ARS. ARS then identifies Route 2 (R2) and dials 55572000 on Route 2.

Stage 3 -The second element receives 55572000. It checks for a dialable string of 55572000 in its digit tree. It finds 5557 followed by any 4 digits in its ARS table. ARS points to Route 6. The element dials 55572000 out to the third element.

Stage 4 -The third element receives 55572000. It checks for a dialable string of 55572000 in its digit tree. The element's digit tree indicates 5557 is in the Cluster Elements form. The Local field in the form is set

to "Yes", which indicates that the extension is a local device. The element then strips off the 5557 and rings extension 2000.



BB0748

Figure 2.8: Inbound Call Routing

Resiliency and Clustering

Resiliency refers to the ability of a MiVoice Business network to continue operating in the event of an ICP/ MiVoice Business system or network infrastructure failure. It works by designating a primary and

secondary (or backup) ICP/ MiVoice Business system for devices or users. Under normal operating conditions, service is provided by the primary system. When a failure occurs, the devices and users on the affected primary systems, transfer seamlessly (or "fail over") to the secondary system. A return to the primary is automatic upon resolution of the failure.

Resiliency operates at the cluster level, meaning the primary and secondary systems must belong to the same cluster.

NOTE: Before MCD 4.0, you had to use OPS Manager to provision resiliency. MCD 4.0 offered the option of using either OPS Manager or migrating to using RDN Synchronization via SDS. After migration, which is mandatory in MCD 4.1 and later, OPS Manager can no longer be used for provisioning resiliency.

The Impact of Resiliency on Network Design

Resiliency imposes special demands on network design. The key ones are summarized here; for the others, refer to the *MiVoice Business Resiliency Guidelines*, particularly the chapter on planning, which also describes several recommended resilient topologies (summarized below).

Key Design Considerations

- Clustering and networking between ICPs and MiVoice Business systems can introduce additional limitations to the system that may reduce its capacity. (See the *MiVoice Business Engineering Guidelines* for more information.) You may also want to use the System Engineering Tool to verify the configuration you are planning. If you are unsure how to do this, contact Mitel Professional Services.
- Multiple paths to the PSTN should be considered so that a single gateway or ICP/ MiVoice Business failure will not result in loss of PSTN connectivity to the entire network. Remote sites, as in a branch-office/headquarters configuration, should also consider providing local PSTN access. This is mandatory for E911 services where the remote sites and headquarters reside in different PSAP locations).
- You can decide which users/devices in your system to make resilient. You may want to make all devices resilient or only those required for critical services. You can also select which system each device will fail over to.
- Devices and users belonging to designated work groups should be supported by the same primary and secondary ICPs. This helps to preserve the work group capabilities of these devices during a failure.
- There are additional licensing requirements when setting up a resilient cluster. While each IP phone and each ACD agent only has to be licensed on the primary system, voice mail resiliency also requires that they be licensed on the secondary system.
- MCD 4.0 systems migrated to RDN Synchronization via SDS and higher cannot provide resilient operation with pre MCD 4.0 or with MCD 4.0 in legacy (OPS Manager) mode.

Recommended Resilient Topologies

The following highly-scalable topologies are recommended for resilient deployments:

- Resilient Single-site Environment—for small to medium-sized businesses.
- Resilient Distributed Network—for large enterprises.
- Resilient Hybrid Network—for combinations of single sites and geographically distributed sites.

The 3300 ICPs in the networks shown in this section can be replaced by any combination of the following:

- MiVoice Business running on the Mitel 3300 ICP hardware platform.
- MiVoice Business running on a VMware host.

- MiVoice Business running on an industry standard server.
- MiVoice Business Multi-instance (multiple MiVoice Business instances running on an industry standard server).

Resilient Single-site Environment

In a resilient single-site environment, a number of ICP/ MiVoice Business systems are clustered together, with each capable of functioning independently if it has its own PSTN access. Systems are connected through a local area network (LAN) of IP or TDM trunks. This topology is suitable for a small to medium-sized organization located at a single-site (no branch offices).

The resilient cluster in [Figure 2.9](#) shows a single-site network with the addition of a second 3300 ICP with PSTN access.

PSTN trunk access is available from both ICPs. If alternative routing is programmed, devices on either ICP can access the PSTN through the other ICP if their own ICP is operational, but the link from their current ICP to the PSTN has failed. When planning a resilient installation, consider providing PSTN access for all phones on a secondary ICP.

If all trunks on one of the ICPs are busy, the ICP can route to the other over IP networking to seize a trunk, if it is programmed to do so.



Figure 2.9: Resilient Single-site Network

Resilient Distributed Network

A locally distributed network connected through a local area network (LAN), metropolitan area network (MAN), or most typically, a WAN, is ideal for larger enterprises, organizations, or institutions that consist of several local branch offices or departments. These branches can be dispersed throughout a city as in the case of a restaurant chain, or throughout a campus environment, as in the case of an educational institution.

NOTE: In the PSTN case, if you are connecting system elements across a MAN or WAN, you must ensure that local emergency services remain available to devices that have failed over to secondary ICPs at other sites. This means ensuring that the secondary ICP is programmed with PSAP information for the devices that have failed over from the primary.

In a resilient distributed network, for ease of maintenance, scalability, and feature operation, it is common to dedicate each ICP to one specific function, such as:

- user controller
- trunking gateway
- tandem trunk gateway
- application gateway

For example, you might have a number of ICPs in a central location, some functioning as dedicated TDM gateways and others as central voice mail servers for group controllers, or ICPs that are dispersed throughout branch offices, buildings, or departments.

Setting up the ICPs throughout a large geographic area and hosting the resilient hardware in separate locations minimizes the possibility of a total system outage, should one of the sites become unavailable, for instance, because of water damage or fire that can bring down a more centralized system; dispersed PSTN connectivity is less vulnerable than centralized PSTN connectivity.

In [Figure 2.10](#), nodes A, B, and C form one resilient cluster in which devices from ICP A fail over to ICP C, devices from C fail over to B, and devices from B fail over to A. Note that each site can also become independently resilient with the addition of a second ICP, so that devices fail over to an ICP at the same site.

In the Figure, PSTN access is added at node B. Node B can provide PSTN access to the devices it hosts, and if automatic route selection (ARS) is programmed appropriately, node B can also provide PSTN access to devices at node C. This example has the minimum requirement of two PSTN access points, but a third can also be installed at node C for greater resiliency.

Part of the flexibility of a resilient network is that not all resilient devices on any given ICP must fail over to the same secondary ICP. They can be programmed to fail over to different ICPs in the resilient cluster. This further minimizes the effect of a failure in one area of the network.



Figure 2.10: Resilient Distributed Network

Resilient Hybrid Network

In a resilient hybrid network, you might have a main office with a distributed system (connected through a LAN throughout several departments) and one or more branch or single-site sites connected to the main network through a MAN or WAN connection. These branch sites can be part of the resilient cluster at the main office and have corporate PSTN access while also retaining PSTN access through a local group controller. In this way, branch sites can continue to operate independently and retain PSTN service for things like emergency services in the event of a failure of the MAN or WAN link to the main office. They could also be in different time zones.

[Figure 2.11](#) illustrates a resilient hybrid network in which the branch office has corporate and local PSTN access. The dotted lines illustrate optional resilient clustering in this topology. For example, sites A and B can both be resilient clusters; devices at site A can fail over to a secondary ICP at site A (same for site B). Alternatively, devices at site A can fail over to an ICP at site B and vice versa. In this way, sites A and B are part of the same resilient cluster. Branch site C can be clustered with A and B to fail over to an ICP at the main office, or it can be independently clustered and resilient with the addition of a second ICP at the branch office.



Figure 2.11: Resilient Hybrid Network

Larger networks may apply a hierarchy of functions within the network where user controllers, and trunk gateways are dedicated to specific ICP nodes. Larger networks may also employ the concept of tandem or core switching ICPs to provide IP trunk links between ICPs at remote locations and central applications or central controllers, as shown in [Figure 2.12](#).

The controllers at the company's headquarters (HQ) are resilient and connect through the core. These also provide connectivity to phones at Remote Office 2, so they appear to be located with HQ.

There are independent primary and secondary controllers at Remote Office 1. These connect to the remainder of the system through the central switching core.



Figure 2.12: Large Hybrid Network

Figure 2.13 includes a fully-meshed central switching core and specialized and dedicated ICPs. All traffic passes through this core. The trunk gateways are resilient and also connected through the core. With every ICP server dedicated to features and applications connected to every trunking gateway, there is always a viable communications path.



Figure 2.13: Resilient hybrid network with Dedicated Servers for Users, Applications, and Trunks

Network Management

Embedded in MiVoice Business are all the tools necessary to provision and manage a network of MiVoice Business systems. No external applications, including Mitel OPS Manager and MiVoice Enterprise Manager, are required.

The MiVoice Business network management tools are accessed through the System Administration Tool interface. They include the following:

- System Data Synchronization
- Multi-Node Management Application
- Bandwidth and Zone Management

About System Data Synchronization

In a network, certain configuration data, such as Interconnect Handling Restrictions, Feature Access Codes, and Class of Service Options, must be identical at each element. System Data Synchronization (SDS) keeps this data identical by sharing it among the elements and distributing changes to maintain consistency.

Without SDS, you would need to manually program the data to be the same on each element, or program a master database and restore it to each element. Then, you would need to make all configuration changes on each element to keep all the databases in the network or cluster in sync.

SDS reduces the time required to set up and manage networks and clusters by allowing you to

- compare the data in a programming form of one system against the data in same form on another system to uncover any inconsistencies.
- synchronize the form data of an element with other elements in the network or cluster.
- share form data among a network or cluster of elements.

SDS is part of the MiVoice Business System Administration Tool and runs on every element in the network or cluster. Enabled by default, SDS tracks all additions, modifications, and deletions to the data that you have designated as shared and automatically distributes them to the other elements in the cluster at the specified sharing scopes.

SDS is mandatory in resilient configurations where it ensures that data for resilient users and devices remains in sync on the primary and secondary controllers. It does this no matter where the changes are made—on the primary or secondary MiVoice Business system, from the phone, the System Administration, or other web-based configuration tool—or whether the phone is on the primary or failed over to the secondary.

SDS works in any topology of Mitel MiVoice Business system, regardless of location. The type of data and the level (or scope) at which it shares is also similarly unrestricted.

Note that, in the figures that follow in this section, the controllers could be any combination of:

- 3300 ICP controllers
- MiVoice Business running on industry standard servers (ISS)
- MiVoice Business Multi-instance (multiple MiVoice Business instances running on ISS)
- MiVoice Business for VMware virtualized environments

Sharing Scopes - How the extent of data distribution is controlled

A sharing scope defines which elements in the network form data is shared with—for example, all elements in the network or just the ones in the same cluster. Every form is assigned a scope by default.

¹The defaults work well for most applications. You can edit them, if necessary, but you probably will not need to.

The scope at which a form can be shared depends on whether its data is local (MiVoice Business specific) or global in nature. The User and Services Configuration form data is local so its scope is more limited than, for example, the data in the System Speed Call form which can apply network-wide.

The scopes are as follows:

- **All Network Elements:** Distribute updates to all network elements that support SDS.
- **All Cluster Members:** Distribute updates to all MiVoice Business cluster elements, including applications that connect using SDS—for example, MiVoice Enterprise Manager and Mitel MiCollab.
- **All MiVoice Business/3300 ICPs:** Distribute to MiVoice Business system in the network only. This includes all MiVoice Business and MiVoice Business Multi-instance elements and 3300 ICP appliances. Non- MiVoice Business elements—that is, applications that use SDS—are excluded.
- **Admin Group Members:** Distribute updates to all elements that belong to the Administrative Group. Use Administrative Groups to share data among groups of elements within the network.
- **Resilient Pair:** Distributes resilient user and device data between a primary and secondary controller.
- **Member Hosts:** Distributes group information and group member data (for example, cluster pickup groups information and cluster pickup group members) between all the elements on which the group members reside. This sharing scope does not apply to network hunt groups or resilient ACD hunt groups.
- **Host and Gateway:** Distribute data to the Guest Room DNs primary node and the hospitality gateway node.
- **None:** Do not distribute the form data

NOTE: In special cases, you may want to exclude certain records in a form from being shared with the other elements—for example, a particular Class of Service in the Class of Service Options form. The sharing scope of forms and contents is configured in the SDS Form Sharing form.

Sharing Scope Examples

Data Sharing at the Network and Admin Group Scope

[Figure 2.14](#) shows an example of Feature Access Codes (FAC) being shared at the network scope, and Call of Restriction (COR) settings being shared at the Administrative Group scopes.

In the following illustration:

1. See "What Data Can Be Shared?" in the System Administration Tool Help for default scopes.

- All systems, A, B, C, D, E, F, G, and H, share FAC data at the Network Scope.
- Systems C and D share COR data at the Admin Group 1 Scope.
- Systems G and H share COR data at the Admin Group 2 Scope.

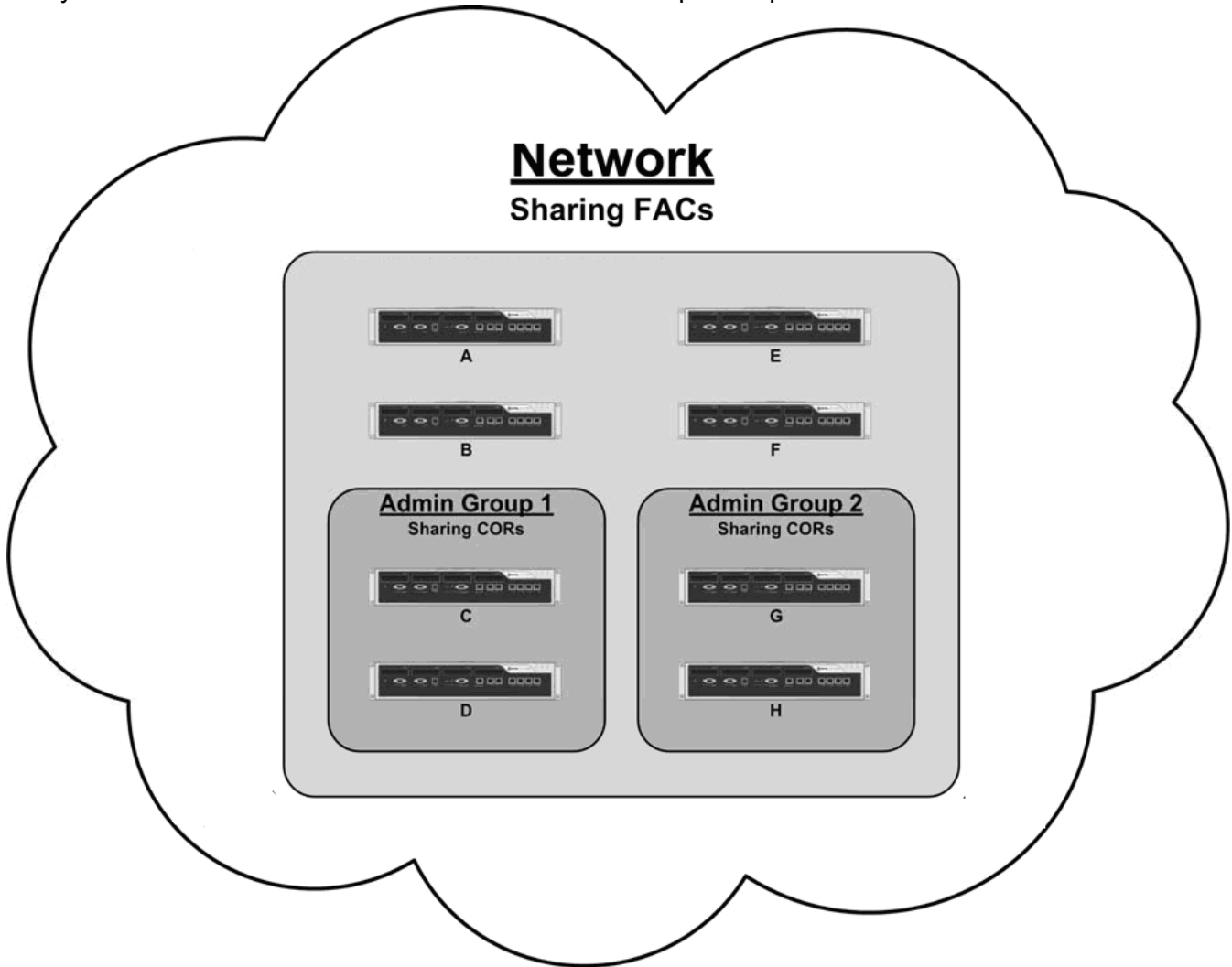


Figure 2.14: Data Sharing at Network and Administrative Group Scopes

Scope of Data Sharing at Network and Cluster

Figure 2.15 shows an example of FACs being shared at the network scope while the COS settings are shared at the cluster scope only. In the following illustration:

- Systems A, B, C, and D share FAC data at the network scope.
- Systems A and B share COS data at the cluster scope.
- Systems C and D share COS data at the cluster scope.

SDS would be configured such that:

- COS changes on A would only be distributed to B; and COS changes on B would only be distributed to A.
- COS changes on C would only be distributed to D; and COS changes on D would only be distributed to C.

- FAC changes on any of the four systems would be distributed to A, B, C, and D.

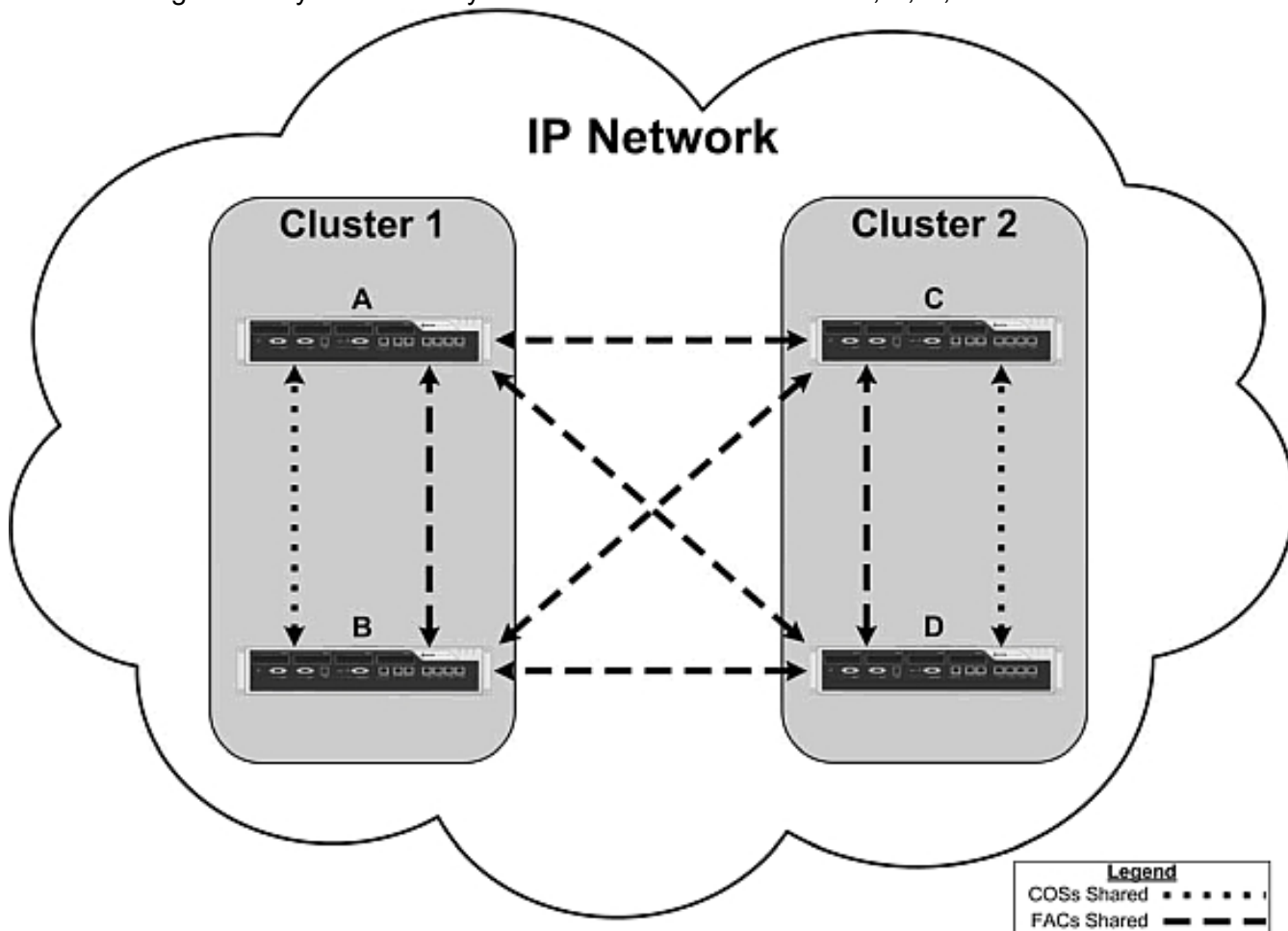


Figure 2.15: Data Sharing at Network and Cluster Scopes

Scope of Data Sharing at Resilient Pair

At the resilient pair scope, SDS shares the selected device data, user data, and user-managed data¹ between the primary and secondary ICPs.

In the following example, SDS would be configured such that:

- User and device changes on A, the primary ICP, would only be distributed to B, the secondary ICP.

1. Data associated with features configured or invoked from the user's set or via the Desktop Tool.

- User and device changes on B, the secondary ICP, would only be distributed to A, the primary ICP.

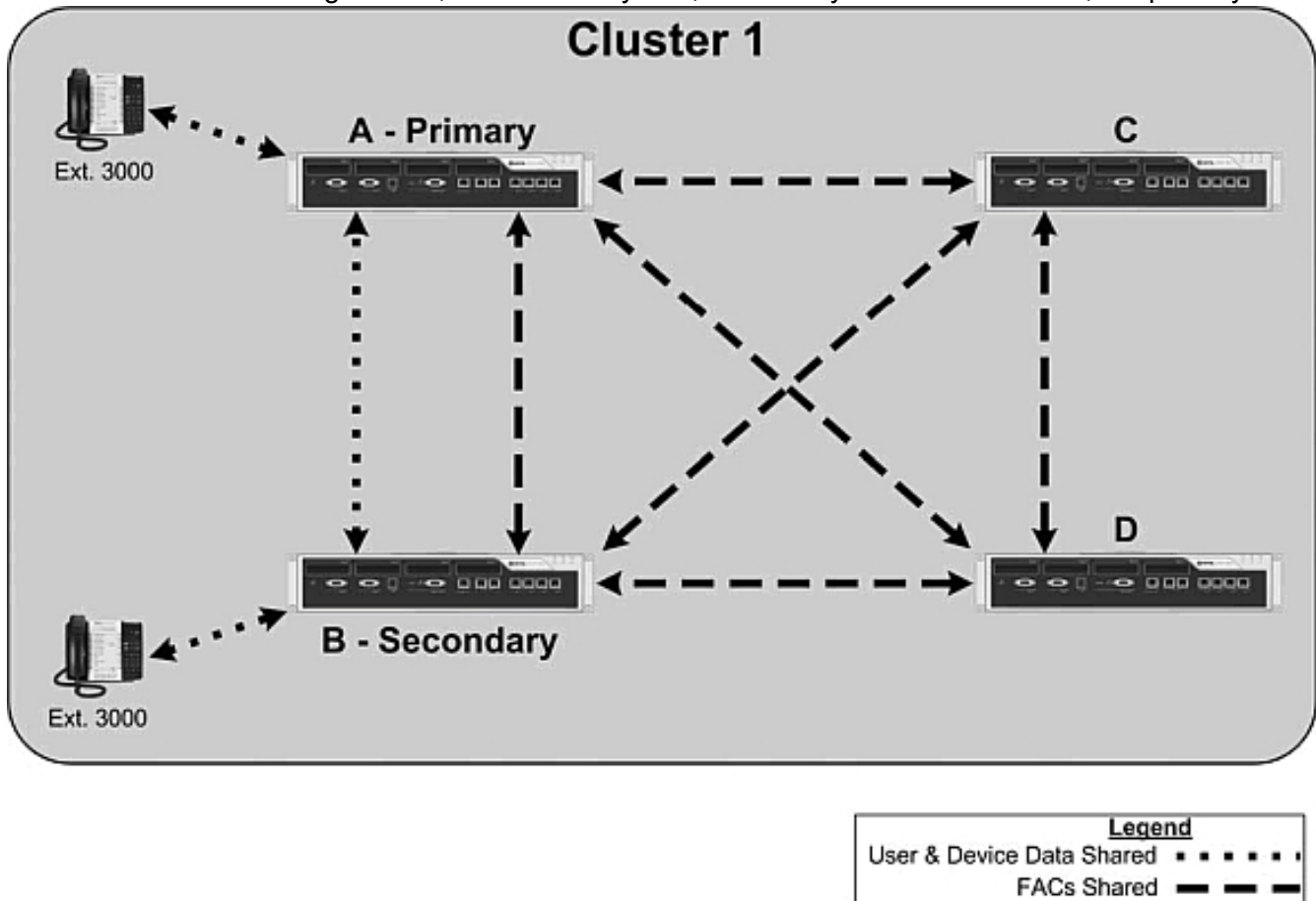


Figure 2.16: Data Sharing at Resilient Pair Scope

About Multi-Node Management Applications

Like SDS, Multi-node Management (MNM) applications are built into the MiVoice Business System Administration Tool. They allow you to maintain network elements that are grouped together in an *Administrative Group* (described in the next section).

You can log in to a System Administration Tool session on any element in the Administrative Group and perform the following management tasks:

- **Application Reach-through** - access and program system forms hosted on the elements in the Administrative Group from a single log on session.
- **Fault Management** - monitor a summary of alarms for the Administrative Group or view the alarm details for each member node.
- **Backup and Restore** - perform database backups from one or all of the elements in the Administrative Group, or restore a database backup to a remote element in the Administrative Group.

Refer to Using Multi-Node Management Application for more information about MNM Applications.

About Administrative Groups

Administrative Groups (shortened to Admin Groups) divide large clusters or networks into smaller domains for data sharing and management purposes. To manage an element using the MNM Applications it must belong to an Admin Group.

The number of Administrative Groups is not limited. However, the number of network elements that can belong to a single Administrative Group is limited to 20. Networks or clusters that exceed 20 nodes can still use the MNM services, provided they are partitioned such that each participating Administrative Groups does not exceed 20 nodes. Additional Administrative Groups can be created as more network elements are added. Network elements can be moved freely within these new groups.

In MCD 4.2 and later, if the Administrative Group Management option is enabled and the installer exceeds 20 members in the Administrative Group, the MNM features for the group will be automatically disabled. MNM will be automatically re-enabled once the size of the group is reduced to 20 or fewer members. SDS Sharing within the group will continue regardless of the size and/or setting of the Administrative Group Management option.

For more information on Admin Groups, see .

Bandwidth Management

Bandwidth Management (BWM) is the process of measuring and controlling traffic (packets) on a network link to avoid congestion. MiVoice Business has built-in BWM features that track and manage bandwidth consumption by the VoIP media stream. With BWM, you can do the following for the voice data packets at predetermined bottleneck points in the network.

- Measure and report consumed and available bandwidth.
- Set maintenance alarms when bandwidth consumption exceeds configured threshold levels.
- Provide Call Admission Control (CAC), rejecting new calls through a specific bottleneck point when consumed bandwidth exceeds maximum configured levels.

BWM may be based on a need to:

- Limit the bandwidth used by voice to allow sufficient bandwidth for data-based applications, such as banking transactions, which voice traffic must not degrade.
- Define the limit at which the voice quality may suffer.

To configure BWM, you need to analyze at your network to see where the bottlenecks are. Once you have this view, you model the network into groupings or zones. In essence, you put an overlay onto your network that defines zones for controllers, devices, sets, consoles, and so forth, that need to be "virtually" (in software) co-located in the same zones to allow bandwidth to be measured.

The resulting measurements and collected statistics on bandwidth consumption are viewed in the Bandwidth Management form.

For more information on Bandwidth Management, see "Voice Networking > Manage Network > Bandwidth Management" in the *System Administration Tool Help*.

NOTE: Bandwidth Management is more often used in star-topology networks where bandwidth is restricted. Hierarchical networks also use because they have a topology that is partly star-based. Its use in fully-meshed networks is less common.

Planning the Cluster

Overview

Planning is the most important phase of a successful cluster deployment. The better your plan, the easier your cluster will be to implement and maintain.

The planning described here is specific to clustering and resiliency. There are other preparations that apply to VoIP deployments, in general, that you need to make, too. These include assessing the current network to gauge whether it can support voice traffic; establishing QoS mechanisms to protect voice quality; and ensuring that business-critical applications have adequate bandwidth. Refer to the *MiVoice Business Engineering Guidelines* for assistance with this planning.

With the general planning done, you can begin to plan your resilient cluster using the tools and information in this chapter. The planning steps are as follows:

- Complete the Prerequisites
- Identify the Network Requirements
- Choose a Resiliency Architecture
- Collect the Network Element Information
- Collect the Cluster Information (includes Admin Group membership)
- Plan Automatic Route Selection
- Identify Users and Resiliency Requirements
- Define Class of Service and Class of Restrictions
- Collect User and Device Data
- Plan IP Trunking

Completing the Pre-requisites

Building a resilient cluster requires the following components:

Hardware and Software	Version	Comments/Additional Requirements
Mitel 3300 ICPs	MCD 4.0*	At least two ICPs/ MiVoice Business systems are required for resiliency.

Hardware and Software	Version	Comments/Additional Requirements
Mitel Communications Director	MCD 4.0+*	<p>The following feature options must be enabled at each element in the cluster:</p> <ul style="list-style-type: none"> • The System Type as specified on the AMC is “Enterprise.” (MCD 5.0 and later). • Networking Option enabled in the License and Option Selection form (pre MCD 5.0 only). • System Data Synchronization must be enabled in the System Options form (this option is enabled by default)*.
Microsoft ® Excel ® (for using the planning spreadsheets and the 3300 ICP Import/Export spreadsheets)	Excel 97 (SR-2) or later	
* Each node in the cluster must be running MCD 4.0 or later software, and be using Remote Directory Number (RDN) Synchronization.		

Optional Components

The following additional components are compatible with clustering:

Hardware and Software	Version	Comments/Additional Requirements
MCD / MiVoice Business for Industry Standard Servers.	MCD 4.0*	At least two MCD/ MiVoice Business systems are required for resiliency.
Multi-Instance Communications Director / MiVoice Business Multi-instance	1.0	
Mitel Applications Server (MAS) / Mitel MiCollab	3.0 SP1	
Mitel Integrated Configuration Wizard	4.0	Can be used for initial cluster setup and provisioning of MCD/ MiVoice Business systems.

Hardware and Software	Version	Comments/Additional Requirements
* Each node in the cluster must be running MCD 4.0 or later software, and be using Remote Directory Number (RDN) Synchronization.		

Identifying the Network Requirements

Use the table below as a supplement to your network planning research. Although the table does not cover network design for every environment, it does provide a basis to start you thinking about your own deployment.

After determining the functionality and capacity required, you, along with your Mitel sales engineer, can decide on a solution that best meets your customer's needs

Number of Users
Number of IP users (by location)
Number of TDM users (by location)
Number of Locations
Number of nodes
Platform (Mitel 3300 ICP or industry-standard server)
Centralized deployment with a hub, or distributed
Type and Number of IP Phones Required
Number of Agent phones
Number of User phones
Number of Trunks Required
Number of Digital E1/T1 Trunks and their location
Number of SIP Trunks *
Numbering Plan
DID ranges <ul style="list-style-type: none"> • can they be ported to the new system (can they be moved)? • if merging networks that are currently separate, will there be duplication of DID numbers?
Continue use of existing numbering plan or change plan?

Required Features and Applications
Voice Mail (Is voice mail centralized or distributed?)
Auto-attendant
Do you need MiVoice Border Gateway? <ul style="list-style-type: none"> • Personal groups (PRG)/twinning • External Hot Desk Users / Dynamic extension • Group presence (user can be moved in or out of group)
Property Management System (PMS)
Key system features
Unified Communicator Advanced (UCA)
Unified Communicator Express (UCX)
Dynamic Extension
Hot Desking
ACD Agents
Audio Web Conferencing
Voice mail requirements
Analog phone requirements
Fax requirements and location
Additional third-party software such as PrairieFyre ACD
Networking
Network equipment (routers and switches)
Cabling requirements
Power over ethernet (POE)
Bandwidth between sites (type and how much)
Connections: dedicated to voice, or shared with data (especially important with SIP)
Quality of Service (QoS)
Emergency Services (for example, 911, 999)
Resiliency

How reliable is your network - do you need additional nodes and connections?

* MiVoice Border Gateways may be needed to provide IP address isolation between the customer network and the SIP provider.

Collecting Form Data

Two Microsoft Excel spreadsheets are provided to help with collecting the information required to provision a cluster. The first spreadsheet is filled with sample data and is intended to illustrate how to configure a cluster in an orderly fashion. The second spreadsheet is a blank version of the first. Use it to enter the data for your cluster. Afterwards, you can use the Data Import feature of the System Administration Tool to bring the data into your cluster elements, rather than entering it all again by hand.

- ClusterPlanning_Example.xls
- ClusterPlanning_Blank.xls

Network Element Information

Record the information for your network /cluster in the Network Info worksheet of the ClusterPlanning spreadsheet. The information required is as follows:

- Names of the elements in the network/cluster.
TIP: Append the PBX Number/CEID Index to the element name. This helps to keep things straight in your mind when programming forms.
- Type of elements. Note that typically only 3300 ICP and MiVoice Business elements share data via System Data Synchronization. Some applications, but not all, may also connect via SDS to share certain specific user information.
- IP address that you will assign to each network element.
- Whether the element will share data with other elements. Data sharing is supported between MiVoice Business systems only.
- Version of system software on each cluster.

Cluster Information

Refer to [Figure 3.1](#) for an example of the required information. Record your information in the **Cluster Info** worksheet of the ClusterPlanning spreadsheet.

The information required is as follows:

- A cluster name
The name you enter here must match the cluster name you entered in the Network Info worksheet.
- Primary Node Identification (PNI) number .
The PNI is a digit string that identifies clusters and standalone network elements within a network. Automatic Route Selection for the network is set up to route calls to clusters and standalone elements based on their PNIs. The PNI is not required in a single cluster network.
- Administrative Group membership
By default, all elements are members of the System Defaulted Administrative Group. If you do not need to create additional Administrative Groups, all elements can remain in the default group. Geo-

graphically dispersed elements can be in the same group provided they are also in the same cluster. For other recommendations, see [“Define the Administrative Groups”](#).

- Element names
Re-enter the names from the **Network Info** worksheet.
- PBX Number / CEID Index
Each element in a cluster requires a unique PBX Number/CEID Index from 1 to 999. The index identifies the host element of a DN in the Remote Directory Number form, which lists all DNs in the cluster.
- System IP information for each element
Obtain information below from the site IT administrator. The first item is mandatory for cluster programming; the remainder are required to complete the system IP properties programming at each element.
 - System IP Address or RTC IP
 - Host Name
 - E2T (or Media Server) IP Address
 - Subnet Mask
 - Gateway IP Address
 - Layer 2 Switch IP Address
 - Domain Name
 - Primary DNS Server
 - Secondary DNS Server



Figure 3.1: Cluster Information

Numbering Plan and ARS

Assign unique *CEID Indexes*, *CEID Digits*, *Feature DNs* and a directory number range to each element in the cluster. Enter this information in the **Routing** worksheet of the ClusterPlanning spreadsheet.

The digit length of all of the above, except the CEID Index, must match to avoid dialed number resolution conflicts.

The CEID Digits are used by ARS to route calls between the cluster elements.

A Feature DN is a directory number that allows features, such as Busy Lamp Fields, Direct Page, and Group Page to function across a cluster of elements. These features require an element to send the status of one of its devices to another device on a different element. Status messages are sent to a Feature DN on the element that hosts the device, rather than being sent directly to the set. This approach reduces the number of status messages that are sent across the network.

At each element, base the numbering scheme on the last digits of the element name as shown in [Figure 3.2](#). Use consecutive numbering.

Provisioning IP trunks from each element to every other element in the cluster creates a fully-meshed network. Meshed networks are optimal for clusters of up to 10 elements. Larger meshed configurations are possible, but may add some management and routing complexity. They may be difficult to manage if certain routes need to flow through specific elements to support functionality such as bandwidth management, or remote nodes across a WAN link.

Define ARS routes between the elements that correspond to the last digit(s) in the destination element names.



Figure 3.2: ARS Between Cluster Elements

Resiliency Requirements

Record the user and device resiliency requirements in the **Resiliency** worksheet of the ClusterPlanning spreadsheet. Resiliency is supported for

- IP devices
- Hot Desk users
- SIP endpoints (line side)
- Groups (hunt, pickup, etc.)
- T1/E1 trunks
- ACD agents

[Figure 3.3](#) shows an example of how you could plan user resiliency in a cluster.

The information you need to record includes the following:

- number and type (Standard, Hot Desk, or Teleworker) of users at each element.
- number of resilient users
- primary (home) and secondary controller for each resilient user
- user and device licenses required at each element.



Figure 3.3: Resiliency Requirements

Resiliency Rules

Below are some rules to observe when planning resiliency.

- Each node in the cluster must be running MCD 4.0 or later software, and be using Remote Directory Number (RDN) Synchronization.
- Only certain device and user types can be resilient. See the *MiVoice Business Resiliency Guidelines* for a list of them.
- The primary and secondary elements must reside within the same cluster.
- Routing must be provided to the secondary elements for resilient devices via TDM or IP trunks.
- Sufficient IP user licenses must be provisioned at each primary resilient element. A resilient user will use one user license on the primary element but none on the secondary element. (This requirement is addressed in MCD 6.0 by provisioning systems with an Enterprise license.)
- "Voice," or "Voice Mail Hunt," and "Recorder" type hunt groups can be resilient.
- To provide embedded voice mail for a user on the secondary element, a voice mail box must be provisioned on the secondary element. A sufficient number of voice mail boxes must be provided for the secondary element.
- Ring Groups can be resilient.
- Agent Skill Groups can be resilient.

- A Personal Ring Group is resilient if its prime member is resilient.

Class of Service and Class of Restriction

A Class of Service (COS) and Class of Restriction (COR) define the features and dialing permissions that can be assigned to individual users and trunks. Assign COS 1 and COR 1 to basic service (most restrictive). Create other classes based on site requirements with ascending numbers and increasing service levels.

The same Classes of Service and Classes of Restriction should be used across all the elements in the cluster. Refer to the **COS and COR** worksheet in the ClusterPlanning spreadsheet for examples.

User and Device Data

Input all the set and user data for the cluster in the **User and Device** worksheet of the ClusterPlanning spreadsheet.

It may be possible to export some of the required user data (for example, last name, first name, department, and location) from Microsoft Windows® Active Directory® or other on-site directory service.

Also record any directory numbers that you want to designate as local-only to the database of a cluster member. A local-only directory number is not listed in the Remote Directory Number forms of the cluster elements and is therefore not dialable across the cluster using the DN alone. A user on the same element can call a local-only directory number just by dialing its DN. However, a user on a remote element cannot. To call a local-only DN, a user on a remote element must dial the CEID digits followed by the local-only extension digits. Refer to the following book in the online help for complete information on local-only directory numbers: Voice Networking -> Manage Network -> Local-only Directory Numbers.

IP Trunking Data

There are two ways to provision IP trunks in a voice network or cluster. One way uses traditional IP/XNET trunk groups and profiles; the other, which is available in MCD 5.0 and later, uses a special ARS route (Direct IP Route) that bypasses the need for such groups and profiles. Using the traditional way, you have to set up the COS, COR, and Interconnect Restrictions that define the service levels, signaling, and other attributes of the IP trunks.

The Direct IP Route does not require this setup. Instead, it uses factory-set attributes, which allow for more rapid trunk provisioning, especially in a new installation of MCD 5.0 (and later) systems. IP/XNET trunk groups and profiles can still be used if an issue arises that requires some IP trunks in the network or cluster to have a different COS or COR than the others.

Enter the IP trunk data into the **IP Trunking1** and **IP Trunking2** worksheets in the ClusterProgramming.xls spreadsheet. Ignore the shaded parts of the worksheet if you are using the ARS Direct IP Route method to provision IP trunks.

In the **IP Trunking2** worksheet, you must assign IP/XNET Trunk Profile numbers to the outgoing IP trunks at each element. The actual settings (Trunk Service Number, Interconnect Number, etc.) in each trunk profile can be the same at each element in the cluster, or they can be different at each element. [Figure](#)

3.4 shows an example of how to set up the trunk profiles. The table above the figure shows the data for lcp554.



Figure 3.4: Planning IP XNet Trunk Profiles

Choosing a Database Programming Strategy

Each element in a cluster has a database and programming forms for entering data into the database. The data includes the system's settings, hardware profile, telephone directory entries, Automatic Route Selection programming, and so forth.

Across a cluster of elements, the data in these forms is either common, similar with some differences, or specific to the element. Data that is common is programmed into a master element and distributed by SDS to other (*slave*) elements in the cluster. The unique data, such as user and device data, is programmed into each element, on an element by element basis.

There are several ways to program a database:

- "Gold" Database (Foreign Database Restore)
Using the Database Backup and Restore facilities of MiVoice Business together with SDS is a quick way to start building a cluster. With just a single system and minimal licensing, a dealer can create a "gold" database in his lab that has the cluster elements programmed in the Network Elements form and the common system data (COS, COR, System Options, etc.). Next, the resulting database is backed up and taken to the customer's site where it's restored to a single element in the pending cluster. SDS is then used to share and sync the data to the other elements, thereby creating the cluster. Adding the IP trunks and ARS routing to connect the elements completes the basic cluster provisioning.
For more information, "Restoring a Foreign 3300 ICP Database" in the *Sys Admin Tool Help*.
- Mitel Integrated Configuration Wizard (MiCW)
MiCW Release 3.0 supports cluster creation without IP trunk and ARS route provisioning, which must be completed using the System Administration Tool after the cluster is created. The wizard also allows you to join a system to an existing cluster and to provision resilient devices and applications. Using MiCW to provision a cluster is suitable for new installations only. See the *MiCW Help* for more information.
- Import Spreadsheet
The Import Spreadsheet is a collection of Microsoft Excel worksheets that correspond to the programming forms in the System Administration Tool. They save you configuration time by reusing data from your planning spreadsheet for import into the master element of your cluster. SDS can then distribute the shared portion of the data to the other elements in the network or cluster.
Use the Import Spreadsheet for forms that contain large amounts of data. This is the programming method featured in the next chapter on cluster programming.
- Manual Method
The manual method involves entering data by hand into the System Administration Tool forms at each cluster element. Manual data entry can be time-consuming and error-prone, even with SDS helping by distributing shared data to the other cluster elements. As such, it's not recommended for large networks with many users.

Installation and Configuration

Overview

You can configure the controllers in a lab, or other off-site location, and then deliver them to the customer premises. However, the controllers must be programmed with IP addresses on the customer's network before you can install them. To satisfy this requirement in a lab setting, ask your IT administrator to create a separate subnet for you. Then, assign the IP addresses obtained from the customer to the controllers.

As discussed in the previous chapter, there are several ways to program data into an MiVoice Business system. This chapter describes how to set up a new cluster by importing data using the Import Spreadsheet and .csv files. No matter how you program the data, for forms that are shared via SDS, you only need to get it into a single master element within the cluster. SDS takes care of distributing the data to the other elements. For forms that are not shared, you have to program the data into those forms on each element, either by logging into the element directly, or by using Application Reach-Through from the master element.

To install and configure a cluster, complete the following tasks:

- Prepare Controllers
- Create the Import files
- Create the Cluster
- Configure your Browser for Application Reach-Through
- Define the Administrative Groups
- Program (or Import) the Cluster System Data (COS, COR, IP Trunk, ARS, etc.)
- Test the Cluster Configuration
- Program (or Import) Set and User Data
- Complete Data Programming
- Configure Resiliency
- Make Database Modifications via Application Reach-Through

Prepare Controllers

Although you can have a mix of releases in your cluster (for example, some MCD 5.0 and some MCD 4.x), the minimum is MCD 4.0. Furthermore, the 4.0 systems must be using SDS, not OPS Manager, to synchronize RDNs across the cluster.

Before you can upgrade a controller to MCD 5.0, you must ensure that it has been configured to use SDS for RDN synchronization. For information on how to do this, see the Global Data Model Migration document on [Document Center](#).

Install Hardware and Upgrade Controller Software

1. Perform initial installation and setup of each controller.
 - Refer to *Chapter 2: Initial Setup* and *Chapter 3: Installation* in the **3300 ICP Technician's Handbook**.
 - See also [“Completing the Pre-requisites”](#) for networking-related licensing and option requirements.
2. Use the MiVoice Business Software Installer Tool to upgrade each controller to MCD 5.0 or later software.
 - See the *MiVoice Business Software Installer Tool Help* for instructions.

Create the Import Files (Optional)

If you are using a different method to program the elements in your network or cluster, skip this section and go to [Cluster the Network Elements](#).

The Import Spreadsheet is supplied with the MiVoice Business software. Each release of MiVoice Business has its own version of the spreadsheet, which can only be used to create import files for that release. If you have used the spreadsheet before, proceed with the instructions below; otherwise, read *Using the Import Spreadsheet* first, and then come back and follow the instructions here.

Have the ClusterPlanning spreadsheet filled out and open on your PC. You will be copying data from this spreadsheet to the Import Spreadsheet and creating .csv files for import into the MiVoice Business systems.

To create the import files:

1. Download the Import Spreadsheet.
2. Create folders in Windows Explorer in which to save the .csv import files.
3. In the Import Spreadsheet, create worksheets for the forms listed in below. See also the next section to calculate how many worksheets you will need.
4. Take the data from your ClusterPlanning spreadsheet and copy it into the columns in the worksheets.
5. Save the completed worksheets for import into the cluster elements.

Rules for creating .csv Files

Observe these rules and conditions when creating .csv files for the following forms:

Form	Conditions
------	------------

Cluster Elements - Members	<ul style="list-style-type: none"> • Complete the Name, PBX Number/Cluster Element ID, Local, and Comments field. Set the Local field to "Yes" for the master element (the element into which you will import the data for distribution to the network/cluster). • Set the remote elements to "No". • Leave the Cluster Element ID Digits and Feature DN fields blank. • Leave the Existing Network Element field blank.
ICP/PBX Networking	Leave the Local ICP/PBX column blank.
User and Services Configuration	<ul style="list-style-type: none"> • When you import data into the User and Services Configuration form, some common data, such as directory number and device type, is also written into the following forms: <ul style="list-style-type: none"> – Multi-line IP Sets – Wireless IP Sets – Telephone Directory • Although it is useful to create one large spreadsheet that allows you to view all user entries, when you import the entries, you must import them in blocks of 1000 entries or less. See for details. • When you validate your data (by clicking the Check Data Format button), if errors are highlighted in the User and Services Configuration worksheet, ensure that you correct them before you import the data into the system. Otherwise, the errors could be propagated to other forms, such as the Telephone Directory, that have data written to them by the User and Services Configuration form.

	<p>Before you begin importing the user data:</p> <ul style="list-style-type: none"> • Set the Call History Records field in the System Options form to 0 at each element. The system limit is 56000 Call History records. However, by default, the system assigns 20 call records to each user which restricts the import to 2800 users. Since not all sets require or support Call History (for example 53xx IP Phones or analog sets), set the default to 0. • Set the Call History Records capacity in the Dimension Selection form on each section based on set requirements (See Set the Call History Capacity) • After importing the users, manually update the entries that require call history records through the Multiline IP Sets form.
Multiline IP Sets (optional)	<ul style="list-style-type: none"> • Importing the Multiline IP Sets form is optional because the data is imported via the User and Services Configuration form. However, you may want to import this form to modify certain fields. • Set the cells in the "Max Call History Records" column of the "Multiline IP Sets" import spreadsheet to 0. Although the default is 20 in the spreadsheet, the import may fail if the cells are not set to 0.

How many worksheets do you need?

The System Administration Tool has over 200 programming forms. In an SDS sharing network, about 10-15% of these forms must be shared. These include the Cluster Elements, Admin Groups, and Network Elements forms. Of the remaining 85-90%, there are some forms you cannot, or would not share, because the data in them is unique to each controller. The System IP Properties and User and Services Configuration form in a non-resilient cluster are examples of such forms. (In a resilient cluster, this form must be shared between the primary and secondary controllers). The balance can be shared, or not shared, depending on the customer's needs. For example, you may want to use the same Classes of Service on every element in the cluster, in which case the Class of Service (COS) form would be shared. It's also possible for a form, such as the COS form, to share some of its data but leave the rest unshared.

You can distinguish the forms that are always shared from those that aren't by the way they are listed in the SDS Form Sharing form. The forms that are always shared have their names dimmed (grayed out) and italicized. For most deployments, the system defaults will allow a fully operational cluster to be built.



Figure 4.1: SDS Sharing Form

For shareable forms, if you want to share the form data across the network or cluster, create one worksheet for the network or cluster. If your network or cluster consists of multiple Administrative Groups create one worksheet per Administrative Group.

TIP: When implementing a new SDS network, limit data-sharing to these forms to prevent data from being overwritten in error. After the SDS network is operational, enable data-sharing for other forms as required.

[Table 4.1](#) shows the forms that require programming to provision a cluster with users and PSTN trunks. Note that the IP/XNET forms are listed as optional. These forms are used to set up IP trunks between the cluster elements. They don't require programming if you opt for the ARS Direct IP Route method of provisioning IP trunks.

Table 4.1: Forms to Program in a Typical Cluster

Unique (Not Shared)	Shared
ARS Digit Modification Plans	ARS Call Progress Tone Detection (if provisioning Loop Start Trunks)
ARS Digits Dialed	Class of Restriction Groups
Digital Link Descriptors	Class of Service Options
Digital Links	Cluster Elements - Members
Digital Trunks	Network Elements
Hunt Group Members	System Account Codes (Optional)
Hunt Groups	Trunk Attributes (for IP trunks connecting cluster elements)
ICP-PBX Networking	User and Services Configuration (in resilient deployments)
ICP-PBX Networking - Members	ARS Routes (sharing optional; see for details.)
IP/XNET Trunk Groups (Optional)	
IP/XNET Trunk Profiles (Optional)	
ISDN Protocol	
MSDN-DPNSS-DASS II Trunk Circuit Descriptor	
Multiline IP Sets (Optional)	
Multiline Set Keys (Optional)	
Trunk Attributes	
Trunk Group Members	
Trunk Groups	
User and Services Configuration (in non-resilient deployments)	
Wireless IP Sets (Optional)	

NOTE: Do not create a .csv file for the Network Synchronization form. If you need to program this form, you must program it manually through the System Administration Tool.

Cluster the Network Elements

Creating a cluster is a four-step process:

- Prepare the elements by programming the IP properties, date and time, and optionally, designate an element to act as the DHCP server for the entire cluster.
- Populate the Network Elements form with systems you intended to cluster.
- Create the cluster.
- Start data sharing in the cluster.

Creating a Resilient Device or Hot Desk User

1. Log into the element you want as the home (primary) element for the resilient device or user. The element that you are logged into when you create the new device or user is the home (primary) element.
2. Do one of the following:
 - To create a resilient IP phone or hot desk user, navigate to the User and Services Configuration form, or
 - To create a resilient IP console, navigate to the IP Consoles form.
3. Do one of the following:
 - To create a new resilient device or hot desk user, click **Add**.
 - To add resiliency to an existing device or hot desk user, click **Change**.
4. Select the name of the secondary element from the list of cluster members.

NOTE: You can select any element in the cluster to be the secondary element. However, to support resiliency for the device or user, the selected element must be sharing data with the local (primary) element. To confirm that they are sharing, check the Network Elements.
5. Click **Save**.
6. Click **Save**. SDS shares the device data at the Resilient Pair scope between the device's primary and secondary element.

Testing Resiliency

After you have configured the system, you should test the resilient IP phones:

1. Disconnect the resilient IP Phone's primary controller from the network while the phone is on hook.
2. Ensure that you can place calls from the resilient IP Phone to verify Fail-over.
3. Ensure that you can make calls to the resilient IP Phone from another set on the secondary controller to verify call routing.

4. Ensure that you can make calls to the resilient IP Phone from each of the other controllers in the cluster to verify call routing in the cluster.
5. Plug the primary controller back into the network. After the primary controller has restarted, ensure that you can make calls (verifies that IP phone has returned to its primary controller.).
6. While on a call at the resilient IP Phone, disconnect the IP Phone's primary controller from the network. Listen for two beeps while you are on the call. If resiliency has been set up correctly, your call will be maintained. However, you will not have access to any other features (this verifies call survival).
7. Hang up and then go off-hook. After you go off-hook your set should have re homed to its secondary controller and you should have access to all the system phone features.
8. Reconnect the primary controller to the network; the IP phone fail backs to its primary.

Perform the above procedure on the IP console to verify its resiliency programming. If any of the above tests fail, refer to "Troubleshooting a Resilient System" in the *3300 ICP Troubleshooting Guide*.

Changing the Secondary Controller

Changing the secondary element of a resilient device from the User and Services Configuration or IP Consoles forms is a two-step two operation. First, disable resiliency for the device (by setting the "Secondary Element" field to "Not Assigned" and clicking Save). Then, re-enable resiliency for the device and assign a different secondary element.

Disabling Resiliency

To disable resiliency from a IP phone, hot desk user, or IP console:

1. On the home (primary) element, navigate to the User and Services Configuration form (IP phone or hot desk user), or IP Consoles form.
2. Select the directory number of the resilient device, and then click **Change**.
3. In the Secondary Element field, select **Not Assigned**.
4. Click **Save**. The entry for the resilient device is automatically deleted from the secondary controller.

Configuring Resiliency for Trunks, Groups, and Agents

Refer to the *MiVoice Business Resiliency Guidelines* for instructions on how to configure:

- Resilient Groups (Pickup, Hunt, Ring, etc.)
- T1/E1 Resiliency
- Resilient ACD Agents and ACD Hot Desk Agents

Configure Resiliency

A device or hot desk user becomes resilient when its *hosting data* is shared between its home (or primary) controller and a secondary controller in the same cluster.

After data sharing has been initiated, SDS automatically keeps the data in synch on the two controllers. It also keeps feature data, such as DND settings and feature keys, synchronized when changes are made on the primary or secondary controller.

Complete Data Programming

Now that the cluster is established and operating, you can program (manually or by importing) the data for TDM trunks, hunt groups, pick groups, applications, and so forth. Remember that data for shared forms only needs to be programmed into the master element. Data for forms that are not shared must be programmed into each element.

You must program the forms in the order in which they are listed in the System Administration Tool "View by Category" menu ([Figure 4.8](#)). If you try to import a form out of order, the system may block your attempt due to data dependencies between forms.

NOTE: When programming digital (TDM) trunks, if you want to assign an external clock source for network Synchronization, you must program the "Network Synchronization" form manually. Do not import the data into this form.

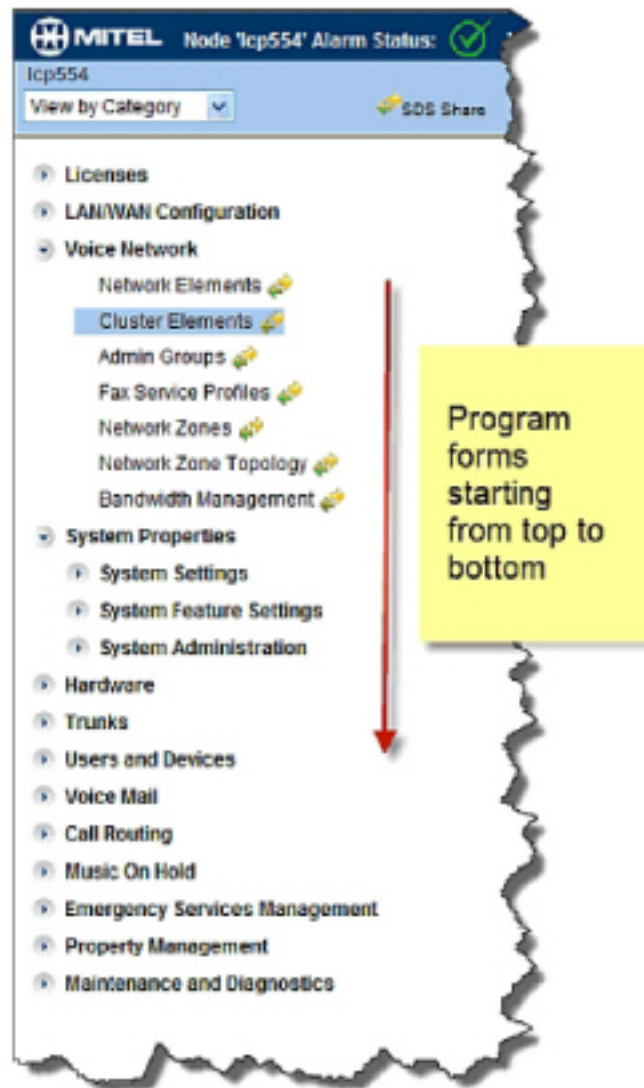


Figure 4.2: Form Programming Order

Import User and Device Data

Using Application Reach-Through, access each element and import the user and device data. Afterwards, check the SDS Distribution Errors - All form and resolve any pending SDS updates or errors. See the "Resolving Pending Updates or Errors" topic in the System Administration Tool Help for instructions.

NOTE: When importing user and device data, it is strongly recommended that you perform database backups at regular intervals during the import process. Every 1000 records is the recommended interval.

1. Navigate to the Network Elements form on the master element and perform an SDS Sync operation to ensure the databases of the cluster elements are synchronized.
2. Set the "Call History - Default Call History Records" field in the System Options form to 0 at each element.
3. Import the user configuration data into each element. The following rules apply when importing:
 - For large databases with more than a 1000 records, import the records in blocks of 1000 or less. Do not attempt to import more than 1000 records at a time.
 - Before performing the import, exit any other non-essential applications on the client PC. The client PC must be running the minimum number of applications when importing large quantities of data into an element.
 - After you complete an import, before proceeding with the next import, ensure that the "SDS Distribution Errors - All" form is clear on the local and remote elements.
4. (Optional) Enter data in the following forms at each element if required:
 - Multiline IP Sets
 - Wireless IP Sets
 - Multiline Set Keys

Test Your Cluster Configuration

At this stage, you should test your cluster configuration by programming an IP phone on each element and placing calls between them.

To speed up programming, use Application Reach-Through to navigate between elements.

1. In the System Options form on each element, program a Set Registration Access Code and a Set Replacement Access Code.

NOTE: The Set Registration and Replacement Access Codes must be identical on all controllers in the cluster.
2. In the User and Services Configuration form on each element, program a user with an IP phone. Assign names that will identify the element that the user belongs to. For example:

First Name:TESTphone
 Last Name: lcp554
 Extension:1554
 First Name:TESTphone
 Last Name: lcp555
 Extension:1555
 . . . and so forth.

SDS will share the local entries to the databases of the remote elements.
3. Check the Remote Directory Numbers forms on each element to ensure that the directory numbers of the phones on the remote elements are listed.
4. Check the Telephone Directory forms on each element. The local number will be listed as "internal". The other numbers will be listed with their CEID Index number.

5. Connect the phones to the LAN.
 6. Register each phone with its controller by entering its PIN number.
 - Enter the Set Registration Code followed by the extension number of the phone.
 - Depending on the phone type, you need to press the Hold key, Send softkey, or Superkey to send the PIN number to the controller.
- If necessary, refer to Programming > Programming Devices > Register IP Telephones in the System Administration Tool Help for instructions. See also "About IP Phone Registration in a Cluster."
7. Place calls between all the phones to verify that IP trunking and ARS is configured correctly.
 8. When verification is complete, delete the test phone entries from the User and Services Configuration forms on each element.

COS and COR Group Data

Since the Class of Service and Class of Restriction Group data should be the same across all elements in the cluster, you only need to program it on the master element. SDS will then automatically distribute the data to the other elements in the cluster.

Use the COS and COR data from your ClusterPlanning spreadsheet to identify the required services, then log in to the master element to program the COS and COR forms. Or, proceed as follows to import the data:

1. In the Import Spreadsheet, create worksheets for the Class of Service Options and Class of Restriction Group forms.
2. Copy the COS and COR definitions from your ClusterPlanning spreadsheet into the import worksheets and modify the default settings as required.
3. Save the worksheets as .csv files for import.
4. Log into the master element, and then import the worksheets into the Class of Service Options and Class of Restriction Groups forms. SDS shares the data to the other elements in the cluster.

IP Trunk Data

Skip this section if you are using the ARS Direct IP Route method to provision IP trunks between cluster elements.

The method described here uses IP/XNET trunk groups and profiles and the data you entered in the second of the two IP trunking worksheets of your ClusterPlanning spreadsheet.

If you are using the Import Spreadsheet to program the elements, create .csv files with data from your planning spreadsheet and import them into the following forms and elements:

- Trunk Attributes form data into the master cluster element
- IP/XNET Trunk Profile form data into each cluster member element
- IP/XNET Trunk Group form data into each cluster element

For manual programming, enter data into the same elements and forms as above.

See "IP Networking Programming" in the System Administration Tool Help for more information on IP trunk provisioning.

ARS Data

Program ARS using the data in the Routing worksheet of your ClusterPlanning spreadsheet. If you are importing the data, you'll need to create .csv files for the following forms in the Import Spreadsheet:

- ARS Digit Modification Plans
- ARS Routes
- ARS Digits Dialed
- System Account Code (optional)

To define ARS routes between the cluster elements:

1. Program (or import) the ARS Digit Modification Plans form data into the database of each element.
2. Program (or import) the System Account Code data, if required, into a master element. SDS shares this data by default to the other cluster member elements.
3. Program (or import) your ARS Routes form data. By default, SDS does not share this data. If your routing data is identical on each element, share the route data but reserve some other routes as non-shared. The non-shared routes can be configured differently on each element and used, for example, by digital trunk links to the PSTN:
 - Navigate to the SDS Form Sharing form and select the ARS Routes form from the list of shareable forms.
 - Click **Change**.
 - Share the ARS Routes form at the "All Cluster Members" scope.
 - Select **All records except those specified below**.
 - Click **Add criteria**.
 - Select **Route**, then select **is between**, and then enter a range of route numbers that you want to exclude from sharing. You can use these route numbers at each element to create element-specific routes.
 - Click **Save**.
4. Using Application Reach-Through, program (or import) the ARS Digits Dialed data into the ARS Digits Dialed form on each element.

Cluster Element IDs and Feature DNs

Return to the Cluster Elements form and manually program the CEID digits and Feature DNs for the elements. You cannot import this data using the Import Spreadsheet.

Refer to the Cluster Info worksheet of your ClusterPlanning spreadsheet for the data.

By default, SDS shares this information, so you only have to enter it on the master element.

1. Log into the master element and navigate to the Cluster Elements form.
2. Click **Change Members**.
3. Manually enter the CEID Digits and Feature DNs for each element.

4. Using Application Reach-Through, navigate the Cluster Elements form on each remote element to ensure that SDS has shared the cluster membership data and Feature DNs to the remote elements.

Program (or Import) the Cluster System Data

The Cluster System Data consists of the following:

- Class of Service (COS) and Class of Restriction (COR) data
- IP Trunk Data
- Automatic Route Selection data and System Account Code data (if required)
- Cluster Element IDs and Feature DNs

You can program the data manually or put it in a .csv file and import it. Some of the data is shared among the cluster elements, while the balance is element-specific. The shared data is programmed once at the master element. The element-specific data is programmed in to each element individually.

Define the Administrative Groups

Within the network, you can create groups of elements and use SDS to share specified data among the member elements at the Admin Group Members scope.

By default, all elements are members of the System Defaulted Administrative (or Admin) Group. You do not need to create any new Admin Groups unless you want more than one.

The number of elements allowed per Administrative Group, is unlimited, although 20 is the maximum that you can manage using the Multi-Node Management services. So to use MNM, you should also keep your Administrative Groups to 20 or fewer elements.

Other recommended practices:

- Create additional Admin groups for each region in a geographically dispersed cluster. This is mandatory for elements located in different time zones. For each time zone-based Admin group, you need to share the Date and Time form among the member elements at the Admin Group scope. Once they are sharing, set the system date and time on one element in each group.
- Rename the default group by choosing a more appropriate description early in the installation.

To create a new Admin group or to move elements to an existing group, the elements must be must be at MCD 4.0 or later and sharing data via SDS. SDS must be sharing data among the elements in order to update the group membership on the remote elements.

To change the name of the local Admin group from System Defaulted:

1. Navigate to the Admin Groups form on your local element. The name of the group to which the local element belongs is displayed in the Admin Groups frame.
2. Click **Change**, enter the new name (for example, Kanata) and then click **Save**.

NOTE: You can only view the member elements of the local group (that is, the group to which the local element belongs). To see a list of member elements of another group, you must log into an element that belongs to that group and open the Admin Groups form.

3. Select the elements that you want to include in the renamed group, and then click **Move**.
4. Click **Existing Group**, and then select the renamed group.

5. Click **Save**.

To create the other Admin Groups (for example, Chandler):

1. Ensure that the elements are sharing data via SDS.
2. Using Application Reach-Through, navigate to the Admin Groups form on an element that you want to include in the group. See page 84 for instructions on how to use Application Reach-Through.
3. In the Group Members frame, select each element that you want to move to the new group.
4. Click **Move Member(s)**.
5. Select **New Group**, and then enter a group name (for example, Chandler).
6. Click **Save**.
7. Using Application Reach-Through, navigate to the Administrative Group forms on one of the elements in the new group to view a list of the group members.
8. Proceed to "Program (or Import) the Cluster System Data."

Configure your Browser for Application Reach-Through

Before you can use Application Reach-Through, you must first add the IP addresses of all the elements that belong to the Administrative Group to Internet Explorer (IE) ¹ on your PC. You add the IP addresses as web sites in the Local Internet zone in IE. See [Before you Start](#) for instructions. The addresses must also be added to the Compatibility View list in IE11 (if using). The list is in the browser's Tools menu.

NOTE: You cannot access the DHCP Server form on another element via Application Reach-Through unless the local login element also supports a DHCP server. We recommend that you log into the element directly and set up the DCHP server. This restriction also applies to other forms, including some digital trunk forms.

Checking for Data Distribution Errors

Distribution errors can occur during the process of synchronizing data among cluster elements. Although unlikely in a new installation (because databases in the cluster all contain default data), they should be addressed as promptly as possible. Left unresolved, the errors will compound with each successive SDS update, making them more difficult to fix, and potentially causing problems with the operation of the cluster.

Data distribution errors are collected and displayed in the SDS Distribution Errors forms of the element where you initiated the Start Sharing operation. The forms also display pending updates, which are updates that have not yet been applied to the destination element's database.

For more information on data distribution errors and pending updates, see .

1. Not required for Mozilla Firefox.

Synchronizing the Network Elements

After you initiate sharing in the network, you need to synchronize the data among the member elements. A sync makes the form data identical across the network.

To synchronize the network elements:

1. On the master element, navigate to the Network Elements form.
NOTE: When adding a new element to an existing cluster, start the synchronization from an existing network element, not the new element. This effectively "pushes" existing data to the new element. It also minimizes updates to other existing nodes that already have existing data.)
2. Select the network elements in your sharing community, and then click **Sync**.
3. In the Confirm Synchronization dialog box that appears ([Figure 4.7](#)):
 - Leave **Data Migration** selected.
 - In the **Shared Forms To Be Synchronized** list, leave all the check boxes unselected (the default). The defaults are sufficient because all the forms needed to establish the pending cluster are already sharing at this stage. Later, after the user and device data is added, it will be necessary to revisit this dialog box and do another sync, but this time with the corresponding forms selected.
 - Click **OK**.
4. Check for Data Distribution Errors; see the next section for more information.



Figure 4.3: Confirm Data Synchronization

Start Sharing Data via SDS

With the cluster created, you are ready use SDS to start sharing data among the elements, and to perform a Sync operation to make the required data consistent across all the elements.

The Start Sharing operation establishes the sharing community of member elements and the rules that define which forms will be shared among them, and at what scope—for example across the entire cluster or at an Administration Group level only. **With certain exceptions Start Sharing does not make forms identical across elements.** The exceptions are the Network Elements form, the membership data in the Cluster Elements form, and other internal SDS-related data. These are all made identical (i.e., “synchronized”) among all network elements by the Start Sharing operation.

If you start sharing, and, for example, the COS forms on two controllers have different programming for COS 35, COS 35 will still be different on the controllers and will stay that way until you perform a Sync. At that point, the change is shared with the other controller and COS 35 would then be identical.

The forms that need to be shared for clustering are set up for sharing at the correct scope by default. Use the SDS Form Sharing form to make any changes before the next step: network element synchronization—or *network sync* for short). For example, if elements in the cluster are in different time zones, you'll have to set the sharing scope for the System Date and Time form to None or Admin Group. You'll also need to set the date and time on each element or on the master element of the Admin Group.

WARNING: Install the required Internet Explorer registry file on your PC before starting to share data. The registry file extends your Internet Explorer session and prevents it from timing out before a Start Sharing

or Synchronization operation is complete. Refer to Mitel Knowledge Base article 07-3849-01068 on Mitel Online for instructions.

WARNING: All remote System Administration, Group Administration, Desktop Tool, and M iXML sessions, are terminated after you click Start Sharing and will remain blocked until the operation IS complete.

To start sharing data among the elements:

1. Log in to the master element and navigate to the Network Elements form.
2. Select the check boxes of the elements you want sharing data—which would be all the elements in the cluster.

The Data Sharing column identifies whether or not the element is configured to share data. Selecting the check box located in the top left-hand corner of the frame (next to "Name") selects all network elements in the list that are eligible for sharing.



Figure 4.4: Selecting Elements for Sharing

NOTE: For successful sharing, the names in the System IP Properties forms of the remote elements must match the names that you entered in the Network Elements form.

3. Click **Start Sharing**. The local system begins communicating with the elements that you selected for sharing. A confirmation window lists the elements that will start sharing data and the forms that will be shared.

WARNING: After you start SDS sharing, do not abort sharing unless absolutely necessary or especially while there is voice traffic in the system.



Figure 4.5: Confirm Start Sharing

4. Verify that the correct elements are listed.
5. Click **OK** to proceed with the start sharing operation. When operation is complete, the **Data Sharing** field for the selected elements in the Network Elements form will change from NO to YES ([Figure 4.6](#)).
6. Proceed to the next task, .



Figure 4.6: Sharing Enabled

Create the Cluster

To create a cluster, you give it a name and then add elements to it from those previously entered in the Network Elements form.

WARNING: Networks or clusters can exceed 20 elements and be managed using the Multi-Node Management (MNM) service provided they are partitioned into multiple Administrative Groups of 20 elements or fewer each. For more information, see [Define the Administrative Groups](#).

From the same element you were logged into to populate the Network Elements form:

1. Navigate to the Cluster Elements form.
2. Click **Create Cluster**. The cluster is created and the local element is added as a member by default.
3. Assign a name to the cluster (for example: Mitel).
4. Assign a unique 1- to 7-digit PNI to the cluster (for example: 569).
5. Do one of the following:
 - Import the .csv file that you created from the **Cluster Elements - Members** worksheet making sure to leave the CEID digits and Feature DNs blank. You will enter this information manually later in the procedure.
 - For each remote element you want to include in the cluster, click **Add Member**, select the element, and then click **Save**, leaving the other fields to be completed later.

When all the elements are added, the Cluster Elements form should look similar to [Figure 4.3](#).

6. Proceed to the next stage, .



Figure 4.7: After Creating the Cluster

Populate the Network Elements Form

To define a cluster, you start by networking the remote elements. This is done by adding the elements to the Network Elements form of the local element. SDS then distributes (shares) the network element data from the local element to the remote elements.

The local element is the element that you are logged into. The other elements in the cluster are remote to the local element.

NOTE: Although you can create the network from any pending member element, you are advised to initiate data sharing from one master element. That way, you can monitor data distribution errors from that one master element. If data is shared from multiple elements, then you must log in separately to each element (or use Application Reach-Through) and check for distribution errors.

To define the members of the network:

1. Log into a System Administration Tool session at the master element.
2. Check that the "IP Address or FQDN" field of the LOCAL (master) element is programmed as an IP address and not an FQDN. SDS requires an IP address.

NOTE: The IP Address of the local system is programmed in the System IP Properties form.
3. (Optional) If you are using Bandwidth Management and want to assign this element to a different zone, do the following in the Network Elements form:
 - Click **Change**.
 - Enter the Zone Number (default 1) for the IP media stream originating or terminating at this network element.
 - Click **Save**.
4. Click **Add** to begin adding remote elements to the network.

5. Enter a unique system name of up to 9 characters in length for the first remote element. Use the names that you have assigned to the elements in your planning spreadsheet.
6. Set the type of element to "3300 ICP". SDS does not support other element types.
7. Enter the IP address of the remote element. The address must match the IP Address that you assigned to the remote element.
8. (Optional—skip if not using Bandwidth Management) Enter the Zone Number (default 1) for the IP media stream originating or terminating at this network element.
9. Click **Save**. The new element record is added to the Network Elements form.
10. Repeat steps 4 to 9 to add the remaining remote elements. When all the elements are added, the Network Elements form should look similar to [Figure 4.2](#).
11. Proceed to the next stage, "Create the Cluster."

Although the Network Element form doesn't show it, each element is added to the same Administrative Group as the local element (the element that you are currently logged in to). See [Creating an Administrative Group](#).

The screenshot shows the Mitel Network Elements configuration interface. The top bar includes the Mitel logo, node information (Node 'Icp554' Alarm Status: No Alarm 2011-Jul-25 18:13:43), and navigation links (Message Board, About, Help, Logout). The main header shows 'Network Elements on Icp554' with a search bar and a 'Show form on' dropdown set to 'Not Accessible'. Below the header are buttons for 'Add', 'Change', 'Delete', 'Start Sharing', 'Sync', 'Print...', 'Import...', 'Export...', and 'Data Refresh'.

The 'Network Elements' table lists the following elements:

Name	Type	FQDN or IP Address	Data Sharing	Version	Zone
Icp554 (Local)	3300 ICP	10.40.129.21	---	11.0.0.96	1
Icp555	3300 ICP	10.40.129.23	NO	11.0.0.96	1
Icp556	3300 ICP	10.40.131.22	NO	11.0.0.96	1
Icp557	3300 ICP	10.40.130.21	NO	11.0.0.96	1
Icp558	3300 ICP	10.40.131.23	NO	11.0.0.96	1
Icp559	3300 ICP	10.40.130.24	NO	11.0.0.96	1

Below the table, the 'Name' field is set to 'Icp554'. The 'Type' is '3300 ICP'. The 'FQDN or IP Address' is '10.40.129.21'. The 'Data Sharing' is '---'. The 'Local' checkbox is checked. The 'Version' is '11.0.0.96' and the 'Zone' is '1'.

The '3300/SX-2000 Properties' section shows:

- Member Of Cluster (Mitel): True
- PBX Number/Cluster Element ID: 569
- Primary Node Id (PNI): 569

Figure 4.8: Populating the Network Elements Form

Prepare Elements for Clustering

Complete the following programming **on each element**:

1. Navigate to the System IP Properties form and complete the fields with the information that you entered in your ClusterPlanning spreadsheet.

NOTE: Each element must be programmed with both a System IP Address and Host Name. The System IP Addresses and Host Names must be unique at each element. It is recommended that this Host Name be exactly the same as the PBX Name. Check that the name is compatible with MiVoice Enterprise Manager (if using).

2. Navigate to the Network Elements form and complete the following:

- Click **Add**, and enter the Network Element Name.
- Enter the IP address for the system.
- Set **Type** to 3300 ICP.
- Leave the other fields blank.

3. Navigate to the Date and Time form, click **Change** and do one of the following:

- Set the system date and time manually
- Specify the DNS address of a Network Time Protocol (NTP) server.

NOTE: You only have to set the System Date and Time on the master element. After you start sharing data via SDS from the master element, the other elements will be updated with the settings in this form.

4. Navigate to the Maintenance Command form and enter the DBMS SAVE command.

5. (Optional) If you want one of the elements to act as the DHCP server for the entire cluster, complete the DHCP programming on that element. See the *3300 ICP Technician's Handbook* and System Administration Tool Help for instructions. The following conditions apply:

- You must populate the DHCP Subnet form with the subnets that you want the DHCP server to respond to. By default, this form is assigned the subnet 192.168.1.0. If different subnets will be used in your installation, then delete this default subnet. Enter the subnets to be used in your installation.
- In the DHCP Options form, configure the options that you want applied to the subnets. Apply each option to the defined subnets at one of the following scopes: Global, Subnet, or Range. The DHCP server responds with option information to DHCP requests based on the priority of the scope setting. The highest priority is Range, followed by Subnet, and lastly, Global. Note that the scopes only apply to subnets that you have defined in the DHCP Subnet form. A request from a subnet, or scope, that is not defined in this DHCP Subnet form will not elicit a DHCP response.
- If you deleted the default subnet of 192.168.1.0 from the DHCP Subnet form, the associated DHCP option information for this subnet is ignored. However, you should delete any DHCP options assigned to this subnet from the DCHP Options form as a precautionary measure.

Using Multi-Node Management Applications

Overview

Multi-node Management (MNM) Applications are embedded in the MiVoice Business System Administration Tool. They allow you to maintain a group of network elements from a single System Administration Tool session on one of the member elements. MNM applications are supported for network elements that are grouped together in an Administrative Group.

You can log in to a System Administration Tool session on an element in the Administrative Group and perform the following management tasks:

- Application Reach-Through - access and program system forms hosted on the elements in the Administrative Group from a single log-on session.
- Fault Management - monitor a summary of alarms for the Administrative Group or view the alarm details for each member node.
- Backup and Restore - perform database backups from one or all of the elements in the Administrative Group, or restore a database backup to a remote element in the Administrative Group.

Conditions

The following conditions apply to Multi-node Management Applications:

- To support the MNM applications, elements must
 - be an MiVoice Business system (3300 ICP, MiVoice Business, or MiVoice Business for VMware virtualized environments)
 - have MCD 4.0 or later software
 - belong to an Administrative Group
 - be sharing data via SDS.
- The MNM applications are intended for Admin Groups of up to 20 nodes. If the number of nodes exceeds 20, then the application will stop processing ALL Multi-node Management (MNM) functions for ALL nodes in the group. Two software logs are also generated: one when the 20-node threshold is reached and a second when it is exceeded. Reduce the number of nodes in the Admin Group to 20 or fewer to restart MNM processing.
- When moving nodes to a new group, ensure there is at least one managed node (a 3300ICP, for example) in the new group. This will allow you to login to that node through the System Administration Tool to see the group members. If an Admin group has only SIP Peer elements, you would not be able to "see" that Admin group. Alternatively, the Admin Groups and associated functions, including Reach-Through and alarm consolidation can be ignored, if not required, and the system will automatically disable groups with more than 20 nodes, such as would be encountered at default installation.
- The User Authorization Profiles must be shared across all members of the Administrative Group.
- The current date and time must be set on each MiVoice Business system in the Administrative Group.
- Interoperability with MiVoice Enterprise Manager:
 - You can reach through to a System Administration Tool session on an element in an Administrative Group and then use the MNM applications among the member elements.

- If there multiple Administrative Groups that support Multi-node Management applications in the network, you must launch a session on a member element in the specific group to use the applications within that group.
- To simplify management of Administrative Groups, the MiVoice Enterprise Manager administrator should configure user-defined groups that match the network Administrative Groups.
- Multi-node Management applications do not require licensing.

Creating an Administrative Group

To manage an elements using the MNM Applications it must belong to an Administrative Group. In MCD 4.0 and later, all elements in the network belong initially to the default Administrative Group (System Defaulted).

NOTE: Multi-node Management is supported only in SDS Administrative Groups that contain 20 or fewer elements.

To specifically configure an Administrative Group:

1. Upgrade all elements that you want include in the Administrative Group to MCD 4.0 or later. See the *Migrating to RDN Synchronization Mode* Solutions Guide on [Document Center](#).
2. Check the System Options and Network Elements form to confirm that SDS is enabled and that all the elements are sharing and synchronized.
3. In the Admin Group form, move the member elements from the default Administrative Group to a new group (see "Define Administrative Groups" in the System Administration Tool Help).
4. Assign administrators with access rights (see "Assigning Administrators" in the System Administration Tool Help).
5. In the SDS Form Sharing form,
 - Ensure that SDS is sharing the User Authorization form data at the Admin Group Members scope. See "Specifying the Shared Data" in the System Administration Tool Help.
 - Define the data that you want shared across the Administrative Group at the Admin Group Members scope (see "Specifying the Shared Data" in the System Administration Tool Help).

Application Reach-Through

About Application Reach-Through

Application Reach-Through is available for Administrative Groups that support Multi-node Management applications. From the System Administration Tool session on any member element, you can "reach through" to the System Administration tool of any remote member element in the group and perform programming tasks.



Figure 5.1: Cluster (SDS Enabled and Sharing Data Among Elements)

Typical Application Reach-Through Tasks

Typically, you use Application Reach-Through to perform the following tasks on a remote element:

- Change user settings through the User and Services Configuration form.
- View logs, statistics, and alarm details.
- Issue maintenance commands.
- Modify hardware programming (for example, Card Assignment, Resilient T1/E1 Framers, or Quad BRI Framers).
- View and modify system-specific settings (for example, DHCP settings, Firewall Control, Licenses and Option Selection, or System Capacity).
- View or modify IP Network settings (for example, Spanning Tree, LAN Policy, or Layer 2 Switch) for an element.

How is Application Reach-Through Supported in the Forms?

To support Application Reach-Through, the System Administration Tool has been modified in MCD 4.0 and later software versions. The following image highlights the most significant modifications:



Figure 5.2: Auto Reach-Through to Lab 3 Disabled



Figure 5.3: Auto Reach-Through to Lab 3 Enabled

Application Reach-Through - Conditions

The following conditions apply:

- Application Reach-Through is only available in an Administrative Group that supports Multi-Node Management (MNM) applications.
- SDS must be sharing data among the elements in the Administrative group. If elements are not sharing data, they will not be available for Application Reach-Through.
- All nodes must be reachable from the administration station (PC) on the network in order for Reach-Through to work between nodes.
- If the system administration policy of the user on the remote element is different than the system administration policy of the user on the login node, the user access is governed by the policy on the remote element.
- The network elements in the Admin Group have to be either
 - all migrated to RDN Synchronization, or
 - all NOT migrated to RDN Synchronization
- Before you can use Application Reach-Through, you must install the Mitel Root Certificate on the client PC and add the IP addresses of all the elements in the Administrative Group as web sites in the Local Internet zone of your browser. ¹ You should also turn off the pop-up blocker in the browser (the

1. Local Internet zones apply to Internet Explorer only.

command is in the Tools menu); otherwise, you'll get a prompt and have to respond to it before you are allowed to continue with the reach-through.

- The current date and time must be set on each MiVoice Business system in the Administrative Group. You set the system "Date and Time" with the WriteDateTime maintenance command or through the Group Administration Tool.
- If Application Reach-Through is available you can click on the **Show form** on field to display a list of the elements in the Administrative Group.
- If Application Reach-Through is not available for a form, the Show form on field displays "Not Accessible".
- It's possible to reach through to forms that contain data from elements that do not belong to the Administrative Group. For example
 - A reach-through to the SDS Distribution Errors form on an Administrative Group member element could show updates that were initiated at sharing scopes greater than the Administrative Group scope.
 - You can reach through to the SDS Form Comparison form on an another Administrative Group member element and then compare form data from that member with a network element that is not a member of the Administrative Group.
 - You can reach through to the Hunt Groups form on an another Administrative Group member element and then assign a secondary element for hunt group resiliency. The secondary element can be an element outside of the current Administrative Group.

Using Application Reach-Through

Before You Start

Before you can use Application Reach-Through, you must first add the IP addresses of all the elements that belong to the Administrative Group to Internet Explorer¹ on the client PC. You add the IP addresses as web sites in the Local Internet zone of your Internet Explorer browser.

To add the IP addresses of the Administrative Group elements:

1. Navigate to the Admin Groups form and record the names of the elements that belong to the group.
2. Navigate to the Network Elements form and record the IP address of each element that belongs to the group.
3. Open your Internet Explorer browser.
4. Click **Tools**, and then click **Internet Options**.
5. Click the **Security** tab, and then click **Local Intranet**.
6. Click the **Sites** button.
7. Click **Advanced**. Leave all boxes in this dialog box checked.
8. Enter the IP addresses of the Administrative Group elements.
9. Click **Add**.

1. Not required if you are using Mozilla Firefox.

10. Click **Close**, and then click OK.

NOTE:

1. You can add a single range of IP addresses that includes all the IP addresses in the group by using asterisks as wild cards. For example, 10.37.*.*
2. You must install the Mitel Root Certificate on the client PC in order to use Application Reach-Through.

Accessing a Form on a Remote Element

To access a form on a remote element,

1. In the left-hand menu, select a form. The local form is displayed in the right frame.
2. Select the desired element from the **Show form on** field. The form for the remote element is reloaded in the right frame.
3. Modify the form as desired.
4. Click the Auto-Reach Through button () to stay on this element, and select another form. Or, select another form without clicking the button return to the local element.

Application Reach-Through: Examples

The following examples describe how you can use Application Reach-Through to manage the elements in an Administrative Group.



Figure 5.4: Cluster (SDS Enabled and Sharing Data Among Elements)

Example 1: Change a Users's Settings

You have logged into a System Administration Tool session on lcp554 and want to modify the settings of a user's who is hosted on a another element (for example lcp556) in the Administrative Group.

1. Select the User and Services Configuration form in the form tree menu. The User and Services Configuration form of the local element (lcp554) is displayed.
2. Set the **Search Scope** to **Admin Group**.
3. Set the **Find** field to "Number", enter the extension number of the user (for example, extension 2244), and then click **Search**. The search result displays the record of the extension number.
4. Click **Change**. The Change window for the user's record is displayed. If the user is on a remote element, the title at the top of the Change window indicates the host element (for example, "User Configuration on lcp556").



Example 2: View Logs on a Remote Element

To view logs on a remote element in the Administrative Group

1. Log into a System Administration Tool session on a local system—for example, ipbxL09 ([Figure 5.5](#)).
2. From the list box at the top of the navigation pane, select **View Alphabetically**.

- 3. From the alphabetical list of forms, click **Maintenance Logs - All**. The Maintenance logs for the local system, Element A, are displayed in the right frame.
- 4. Select the desired remote element—for example, t80 ([Figure 5.5](#))—from the Show form on field and then click Go. The form for the remote element is reloaded in the right frame.



Figure 5.5: View Logs on Remote Element

- 5. Click the desired log to display the log information in the lower frame.
- 6. Click any form in the left-hand menu to access that form from the local element (ipbxL09). The form is loaded into the right frame.

Example 3: Enter Maintenance Commands on a Remote Element

As an example, you may need to adjust the alarm threshold for a particular alarm category on all the elements in the Administrative Group:

- 1. Log into a System Administration Tool session on the local system—for example, ipbxL09 ([Figure 5.6](#)).
- 2. In the navigation pane, choose **Maintenance and Diagnostics**, then click **Maintenance Commands**. The Maintenance Command form for the local system (ipbxL09) is displayed in the right frame.
- 3. Use the Set Thresholds maintenance command to adjust the alarm threshold on the local element.
- 4. Next, select a remote element—for example, t80—from the **Show form on** field and then click **Go**. The form for the remote element is reloaded in the right frame.



Figure 5.6: Enter Maintenance Commands on Remote Element

- 5. Enter the Set Thresholds maintenance command to adjust the alarm threshold on t80.
- 6. Enter the command on the other remote elements. Navigate to the Maintenance Command. Select the remote element in the **Show form on** field and click **Go**. Then, enter the command in the command line.

Troubleshooting

Error	Probable Cause	Solution
-------	----------------	----------

Cannot reach through to an element in the Administrative Group.	Element has pre-MCD 4.0 software installed.	Upgrade element to MCD 4.0 or later software. See the <i>Migrating to RDN Synchronization Mode</i> Solutions Guide on Document Center .
	Form incompatibility. The requested form is not supported. The local element has a later software version than the remote element and the selected form does not exist in the software version on the remote element	Upgrade elements to same software version.
	Form not licensed. Some forms, such as the FAX Service Profiles form must be licensed on the element before they are available. If a form is licensed on the local element, but not licensed on the remote element, you cannot modify it.	License the functionality associated with the form on the remote node.

The Application Reach-Through request fails.	User authorization profile is out of sync on the remote node	Use SDS to sync the User Authorization Profile form across the Administrative Group.
	A network problem is preventing the local element from connecting to the remote element.	Contact your IT Support administrator.
	You do not have permission to access the requested form on the remote element. The Admin Policies form is not synchronized across all the elements in the Administrative Group.	Ensure that SDS is sharing the Admin Policies form to all elements in the Administrative Group.
	<p>SDS was turned off and then on following a system reboot. Another reboot is required before Application Reach-Through will work. In general, if access to a form is granted without a reboot, then other nodes cannot reach through to this newly granted form. To illustrate, consider the following example involving two switches, A and B:</p> <ol style="list-style-type: none"> 1. Switch A has access to Form1 but Switch B does not. 2. Enable licensing on B such that now B has access to Form1 but don't reboot. 3. If a reach through is performed from A to B, there would be a reach-through failure. 4. After rebooting B, A can perform a reach through to B. 	Reboot the switch that can't be reached.
Cannot find user on remote element.	The user information was not distributed to the remote element by SDS.	Resolve any SDS pending updates or errors on the local element. See Resolving Data Distribution Errors and Pending Updates .

After you select a remote element in the Show form on field and click Go , Internet Explorer does not open the form of the remote element.	The IP address of the remote Administrative Group element has not been added to the Local Internet zone of the Internet Explorer browser on your client PC.	Add the IP address of the element. See <i>Before you Start</i> .
Remote element missing from Show form on field in Firefox.	Remote element running MiVoice Business software that is incompatible with Firefox.	Upgrade element to MCD 6.0 SP1 (or later) or switch to Internet Explorer 8.0 (or later).

Fault Management

About Fault Management

This Multi-Node Management application provides you with the following alarm information:

- the highest alarm status among all the elements in the Admin Group, and
- a summary of the alarm severity for each member element in the MNM Administrative Group.

Overall Alarm Status

If you log into a System Administration Tool session on any element that belongs to a Admin Group, the alarm status for the group is displayed in the top-left corner of the screen (see *Figure 5.7* for an example). See "Alarm Status Levels" in the System Administration Tool Help for details on the alarm indications.

Alarm Status Summary

To display a summary of the alarms for the Admin Group elements, navigate to the Admin Group Alarm Summary form. An example of the screen is show below.

The Alarm Summary form presents the following information:

- Administrative Group name
- overall highest alarm status for the Administrative Group
- name of each element (left column)
- alarm level for each element (right column).



Figure 5.7: Alarm Status Summary

Fault Management Conditions

Fault Management is only available in an Administrative Group that supports Multi-Node Management (MNM) applications.

Obtaining an Alarm Summary for the Group

To display a summary of the alarms for the MNM Administrative Group elements:

1. Navigate to the Admin Group Management form and enable fault management for the group.
2. Navigate to the Admin Group Alarm Summary form to view the alarm status for the member elements.

Obtaining the Alarm Details

To obtain the alarm details:

- From the Admin Group Alarm form, select the element in the Name column to obtain its alarm details. This will show you any/all alarms on that element.

NOTE: A "nameless" element (one that has had its name deleted in the Network Elements form) can still be selected by clicking on the blank space where the name would otherwise appear.

To go back to the local system after viewing alarm details on a remote element, do any of the following:

- Click the local navigation tree on the left side of the page.
- Select the local system from the **Show form on** list in the top-right corner of the page.
- Click the Alarm Status area at the top of the page. Depending on the alarm status, you are taken back to the local Admin Group Alarm Summary form (or Alarm Details form if the system is not in an Admin Group), License Distribution Management form, or SDS Distribution Errors - All form.

NOTE: Navigating via the Alarm Status display only works when reaching from an MCD 5.0 or later system to another MCD 5.0 or later system.

MNM Backup and Restore

About MNM Backup and Restore

Multi-node Management (MNM) backup and restore allows you to perform database backups and restores from a System Administration Tool session on any member element in a MNM Administrative Group. From a System Administration Tool session on a local element, you can

- Back up the database of another Administrative Group member element to an FTP server.
- Back up the databases of all member elements in the Administrative Group to an FTP server.
- Restore a database to any element in the Administrative Group.

The Restore can be done using a backup file a local PC drive or from the FTP server.

Conditions and Restrictions

The following conditions apply:

- MNM Backup and Restore is only available in an SDS Administrative Group that supports Multi-Node Management (MNM) applications.
- To support database backups from multiple elements, you must have an external FTP server in the network where the system can save the backups. You must configure the path to the FTP server and other FTP server parameters in the External FTP Server form.

- By default, the FTP Server Parameters are shared by SDS among the elements at the "Admin Group Members" scope. If you want to specify different FTP servers for different elements, disable the sharing of the FTP Server Parameters by setting the sharing scope to "None" in the SDS Form Sharing form.
- You need to ensure that the FTP server
 - is working properly and that there is sufficient disk space on the server for the database files
 - supports the required number of concurrent client sessions. To perform database backups from multiple elements a concurrent client session is required for each element in the Administrative Group. For example, if the Administrative Group has 10 elements, the FTP server must support a minimum of 10 concurrent client sessions.
- You can still use the Backup form in the System Administration Tool to save the database of the local system to the hard drive of the System Administration Tool client PC.
- The backup and restore databases will include the following FTP server information:
 - IP address
 - Port
 - Login user name
 - Login password
 - Path (optional)
- The list of Admin Group member elements are saved in the database backup file and can be restored from the backup file.

Performing a Backup

About Backups

You can back up the system database

- to the hard drive of the System Administration Tool client PC, or
- to an external FTP server.

In addition, if the MiVoice Business system belongs to an Administrative Group that supports Multi-Node Management applications, you can choose to back up the databases of all elements that are members of the Administrative Group (see the previous section for details).

A scheduling option is available, enabling you to back up the local node's system database automatically. You can schedule backups to be performed once, on a particular date and time, or repeatedly, on a daily, weekly, monthly, or yearly basis.

NOTE:

1. During a system backup, no other users can access any of the web-based tools (Visual Voice Mail, Desktop Tool, Group Administration Tool, or System Administration Tool), access Visual Voice Mail, or save changes. To avoid blocking other users, we recommended that you perform system backups outside of business hours.
2. When backing up system information on a single MiVoice Business system that shares data through the System Data Synchronization feature, the backup applies only to the element you are logged in to. During a system backup, the network element rejects all data update distribution attempts. See "Performing Backups and Restores" in the Sys Admin Tool Help for more information on performing and managing backups on SDS network elements.

What Data is Backed Up?

For 3300 ICP controllers, a backup includes call control data, system data (COR, COS, System Options, etc.), internal DHCP server configuration, and voice mail settings (with or without messages). For hospitality systems, a backup includes the following additional data:

- Wakeup data
- Room status data (occupancy and condition)
- Call Restriction data (internal, local, long distance, etc.)
- Number of calls
- Message Registration data
- Credit Limit
- Message Waiting status

For the AX controller, you cannot include voice mail messages in a system backup.

NOTE:

1. Embedded voice mail is only supported for an AX Controller that is configured with a 4 GB flash card. If you use embedded voice mail on an AX controller that only has a 512 MB flash card and then initiate a back up of the system database, the backup may fail because there is not enough space available.
2. The amount of disk space available for voice mail backup is 4 GB. Messages must be deleted to reduce the voice mail file size to this level before attempting a backup.

Back Up a Single System

NOTE: You can also schedule the backup to be performed at a later date and time. See "Scheduling Backups" in the Sys Admin Tool Help.

To back up the database of a single system:

1. If System Data Synchronization is enabled, resolve all pending updates and errors.
2. Select Maintenance and Diagnostics > Backup/Restore.
3. Do one of the following:
 - To perform the backup immediately, click Backup and proceed to the next step.
 - or
 - To schedule the backup to be performed at a later date and time, see "Scheduling Backups" in the Sys Admin Tool Help.
4. Click **Selected Node only**. This option allows you to back up the database of the currently accessed element (that is, the local element or the element that is selected in the **Show form on** field).
5. Choose the location of the backup file:
 - Choose **FTP server configured on node** to save the database to an FTP server in the network. Configure the FTP server parameters in the External FTP Server Parameters form before you use this option.
 - Choose **Local hard drive** to save the database backup to the client PC. Click **Browse** to launch the Save As dialog box, then navigate to the folder on your local drive where you want to save the backup file (for example C:\3300_ICP\backup). Click **Open**.

NOTE: To browse to a folder for the backup file and to perform a backup, your current user account on the computer must have Java Plug-in version 1.6.0_01 or later installed.

6. In the Backup file prefix field, enter a prefix to apply to the database file names. The databases will be saved to the FTP server using filenames in the following format:
`<prefix>_<node name>_<release version>_<timestamp>.tar`
The prefix must be all lowercase and contain only letters and numbers. Spaces are not allowed.
7. Select **Call History records** and/or **Voice mail messages** if you want to include them in your backup. Including these messages and records can increase the backup time and required space significantly.
8. Click **Start Backup**.
System will display progress by a "back-up complete" message.
9. Click **OK**.
10. Verify the presence of the backup on the local drive.

Back Up Databases from an Administrative Group

To back up the databases from all the member elements of an SDS Administrative Group:

NOTE: The Administrative Group must support Multi-Node Management applications (that is, the group must contain 20 elements or fewer and all MiVoice Business elements in the group must have MCD 4.0 or later software).

1. Ensure that an external FTP server has been configured in the External FTP Server form. The databases are saved to the external FTP server specified in this form.
2. Resolve all pending updates and errors.
3. Select Maintenance and Diagnostics > Backup/Restore.
4. Click **Backup**.

NOTE: You must be logged into the System Administration Tool of the local element to perform a backup of the Administrative Group databases (that is, the Show form on field must be set to the local node that you are logged into).
5. Click **All reachable nodes** (possible only from <local node>).
6. Enter a prefix to apply to the database file names. The databases will be saved to the FTP server using filenames in the following format:
`<prefix>_<node name>_<release version>_<timestamp>.tar`
The prefix must be all lowercase and should contain only letters and numbers. Spaces are not allowed.
7. Select Call History records and/or Voice mail messages if you want to include them in your backup. Including these messages and records can increase the backup time and the space required.
8. Click **Start Backup**.
The system will display progress followed by a "back-up complete" message.
9. Click **OK**.
10. After the operation is finished, you will see a message box indicating that the backups are complete. Verify the presence of the backups on the FTP server.

Performing a Restore

If the system database becomes corrupted, you will need to restore an uncorrupted database to the system from a recent backup file.

You can restore a database backup file

- from the hard drive of the System Administration Tool client PC, or
- from an external FTP server.

WARNING: You must reboot the controller after restoring a database. Service will be LOST for the duration of the reboot.

NOTE:

1. You may restore a database from one MiVoice Business system to a another with a different IP address. There are rules you must follow when doing this; see "Restoring a Foreign 3300 ICP Database" in the Sys Admin Tool Help.
2. When restoring system information on an MiVoice Business system that shares data through the System Data Synchronization feature, the restore applies only to the element you are logged in to. During a system restore, the network element rejects all data update distribution attempts. For more information on performing and managing restores on SDS network elements, see "Performing Backups and Restores" in the Sys Admin Tool Help.
3. You can only restore a Release 3.3 or later database onto a system running 3300 ICP Release 4.1 (as opposed to MCD 4.1) or later software. You may not restore a database saved on software prior to Release 3.3.
4. You may not restore an LX or 700-user database onto an MX controller if the database had CIM 3 or 4 configured. You must first delete the unsupported CIM configuration.
5. You can only restore an AX controller database to an AX controller. You cannot restore a database from another type of controller to an AX controller.

To restore a database:

1. Navigate to the Restore form.
2. Choose the location of the backup file (archived file) that you want to restore:
 - Click **FTP server configured on node** to obtain the file from an FTP server in the network. The FTP server parameters must be configured in the External FTP Server form.
 - Click **Local hard drive** to obtain the file from the client PC. Type the location of the database that is being restored, or use the browse facility.
3. Click **Include Guest Room information** if you want to include Hotel/Motel wake-up information in your restore.
4. Choose the Dimension Selections:
 - Click **From archived file** to use the Dimension Selections from the backup file, OR
 - Click **Use current** if you are restoring the database after programming new Dimension Selection information. See Change Licenses and Options for more information about changing the system dimensions.
5. Click **Start Restore**.

NOTE: To perform a restore, your current user account on the computer must have Java Plug-in version 1.6.0.1 installed. Later versions are not supported.

6. Click **OK**. The system shows an "in progress" message.
7. When the status window shows "complete", click **OK**.
8. Enter the "Reset System" maintenance command. When the reboot is complete, the database is converted, and the system automatically resets.
9. If you have programmed Dimension Selection, the system reboots automatically one more time.

NOTE:

1. The system does not allow you to log in during the restore and reset period. After the system has completed the restore and reset, you should see "deleting/ ipservicesdb.tar" in the RTC. This is an indication that you can log back in to the System Administration Tool.
2. While the System Administration Tool is restoring the database, no other users can access any of the web-based tools (Visual Voice Mail, Desktop Tool, Group Administration Tool, or System Administration Tool), access Visual Voice Mail, or save changes. To avoid blocking other users, we recommend that you perform restores outside of business hours.
3. If you chose to back up the Call History records, they will be restored during the database restore process. If you do not want to keep the Call History records, then you can delete them using the History Delete All maintenance command.

TIME: The system takes approximately 30 minutes to restore an average-sized database, during which time the files are copied to the controller. Once the files have been copied, you must reset the controller. Note that the system can take up to an additional 30 minutes to reset. The process is faster on MiVoice Business for ISS

Using the Import Spreadsheet

Overview

Importing data can save you considerable configuration time and reduce the likelihood of data-entry errors. It's especially useful for adding a large number of users and devices during initial system configuration.

The Import Spreadsheet is a Microsoft® Excel® spreadsheet that is supplied with the MiVoice Business software. It consists of a series of worksheets that correspond to the System Administration Tool programming forms. You enter your programming data into the Import Spreadsheet forms and then use the tool to import the data, form by form, into the system database of a master element. The System Data Synchronization application then distributes that shared data to the other elements in the network or cluster.

Requirements and Conditions

Requirements

- The client PC must have at least 2 GB of committed memory and a minimum of 512 MB of RAM (1 GB is recommended).
- Due to the large size of data import files, it is recommended that you close all non-essential programs to ensure that the largest possible amount of memory is available. A large data import can use up to 1.5 GB of memory.
- You need a file archiver and compressor application like WinZip® installed on your client PC to open the Import Spreadsheet form after downloading it.
- You need Microsoft Excel 97 (SR-2), Excel 2000 (SP 3), Excel 2003 (SP 2) or higher installed on your client PC in order to download and read the Import Spreadsheet form, and to manipulate the data to be imported to the system database. For .csv files containing characters in the extended ASCII character set—that is, characters above 128—use UTF-8 file encoding when saving the file.

Conditions

- Import files created with an Import Spreadsheet from previous MiVoice Business releases are incompatible with the current release and vice versa.
- The Import Spreadsheet should only be used on PCs with North American versions of Microsoft Windows. Using the spreadsheet on non-North American versions of Windows could produce errors caused by incorrectly translated characters.
- .csv files generated by the Import Spreadsheet and subsequently modified using Microsoft Excel may cause errors when imported into the MiVoice Business system. Use Windows Notepad or another text editor to edit the file, or edit the original worksheet in the Import Spreadsheet and regenerate the .csv file.

- The User and Services Configuration, Key Assignment, and Telephone Directory work-sheets are not listed in the All Forms worksheet so they cannot be recreated if deleted. If deleted, you must obtain a new Import Spreadsheet.
- Import adds and updates existing data in the MiVoice Business database; it never deletes records.

Obtaining the Import Spreadsheet

You download the Import Spreadsheet from the System Administration Tool.

1. Log into a System Administration Tool session.
2. Navigate to the User and Services Configuration form.
3. Click **Import**. The Import dialog box opens.

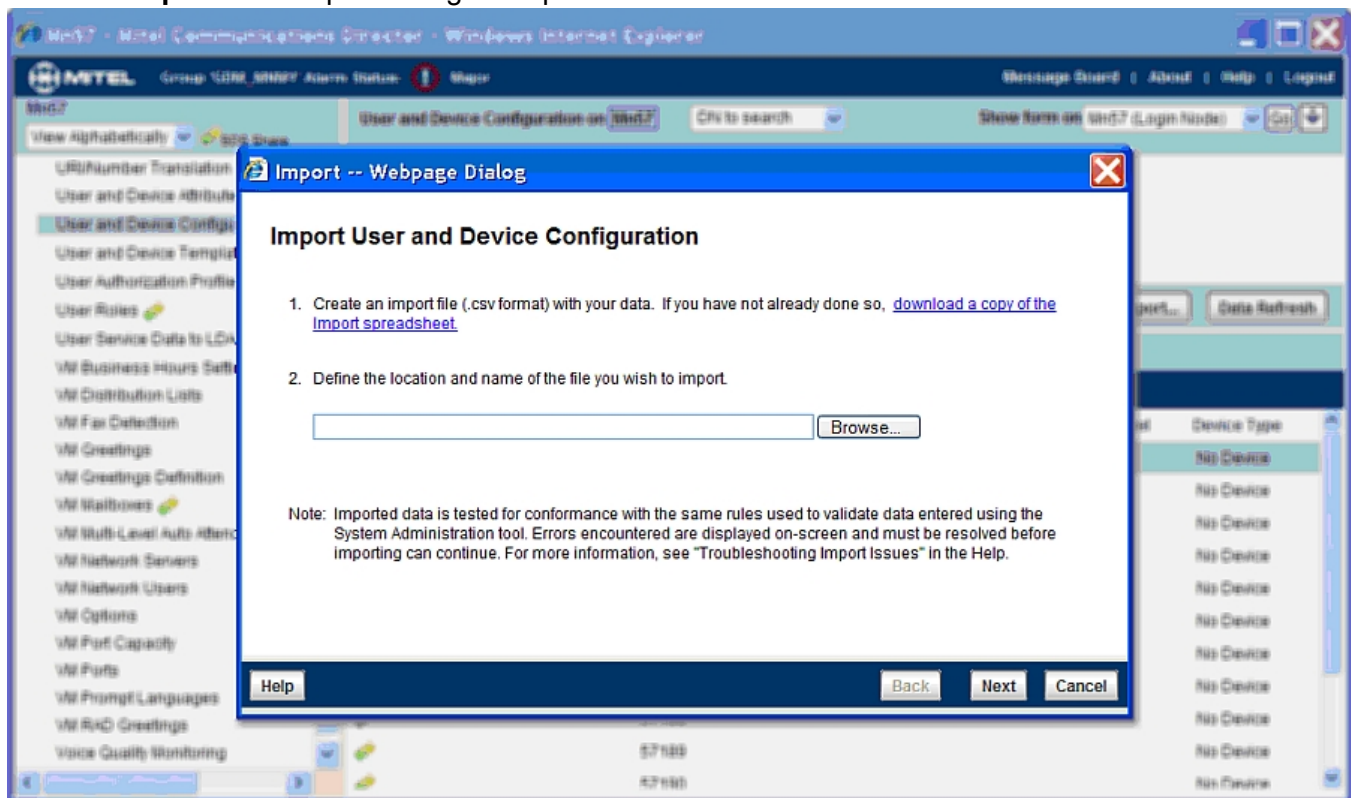


Figure 6.1: Import Dialog Box

4. From the Import dialog box, click **download a copy of the Import spreadsheet**.
5. Click **Save** to save the .tar file to your PC.
6. Open the .tar file using WinZip.
7. Extract the .xls and .txt files using WinZip to the same directory, then launch the spreadsheet (.xls file) from that directory. This ensures that all columns are present in the spreadsheet. The columns correspond to the fields in the System Administration Tool forms and are derived from data contained in the .txt file.

WARNING: You must extract both the .xls and .txt files to the same directory before opening the spreadsheet (.xls) file. Otherwise, you will not get the latest version of the spreadsheet.

8. Set the Platform type and set the synchronization mode to RDN Synchronization via SDS before you save the spreadsheet to a new folder.

Creating Sub folders for the Cluster Elements

In Windows Explorer, inside the Spreadsheets folder, create separate subfolders for each of the elements in your cluster. [Figure 6.2](#) shows an example:

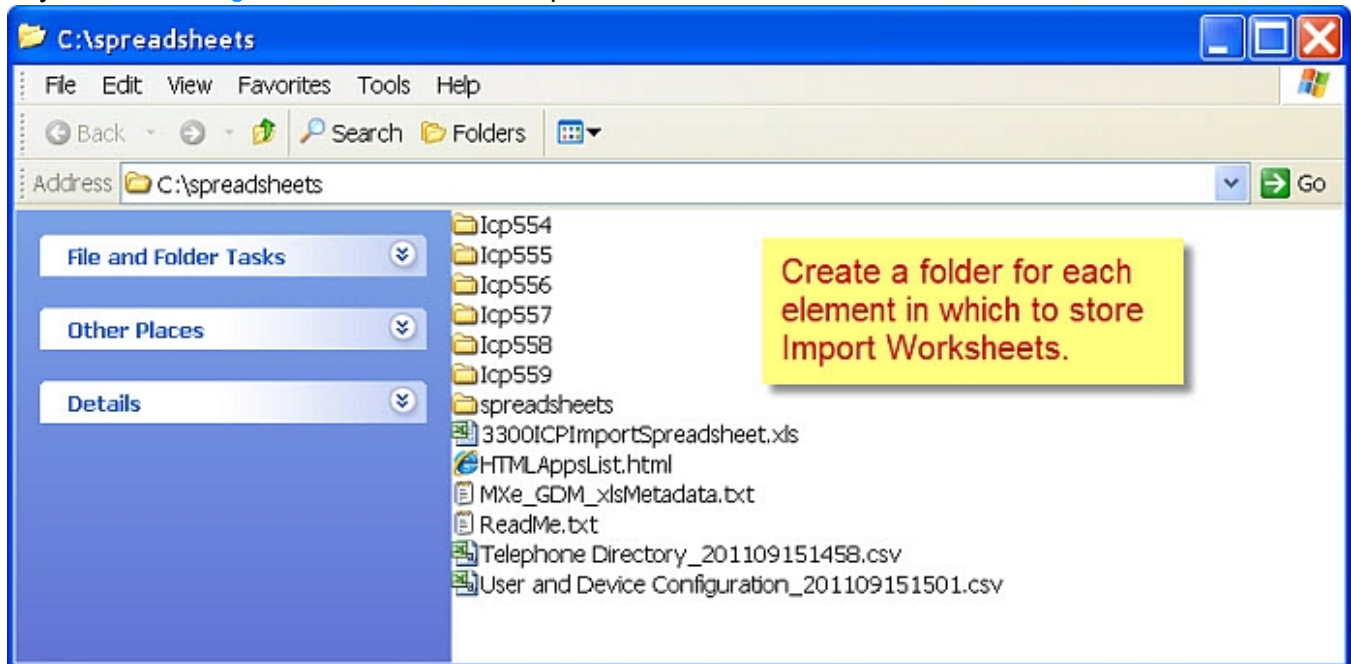


Figure 6.2: Create Subfolders for Import Spreadsheets

When you create .csv files from the import worksheets, you will save the files that contain data that is common to the cluster, such as Class of Service, in the folder for a master element. After you import common data into the master element, it is shared via System Data Synchronization to the other cluster elements.

Save the .csv files that contain non-SDS shared data, such as trunk data, into each associated element folder.

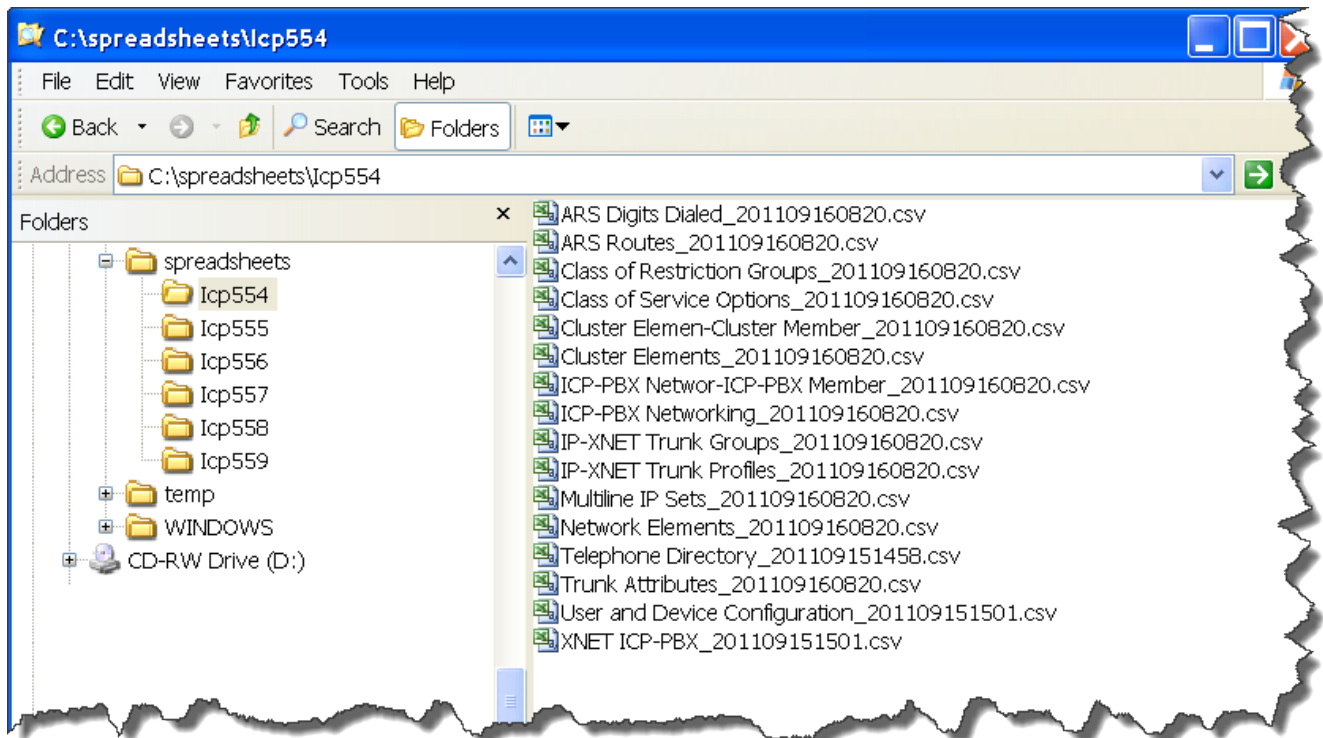


Figure 6.3: Shared and Non-Shared .csv Files for Master Element Icp554

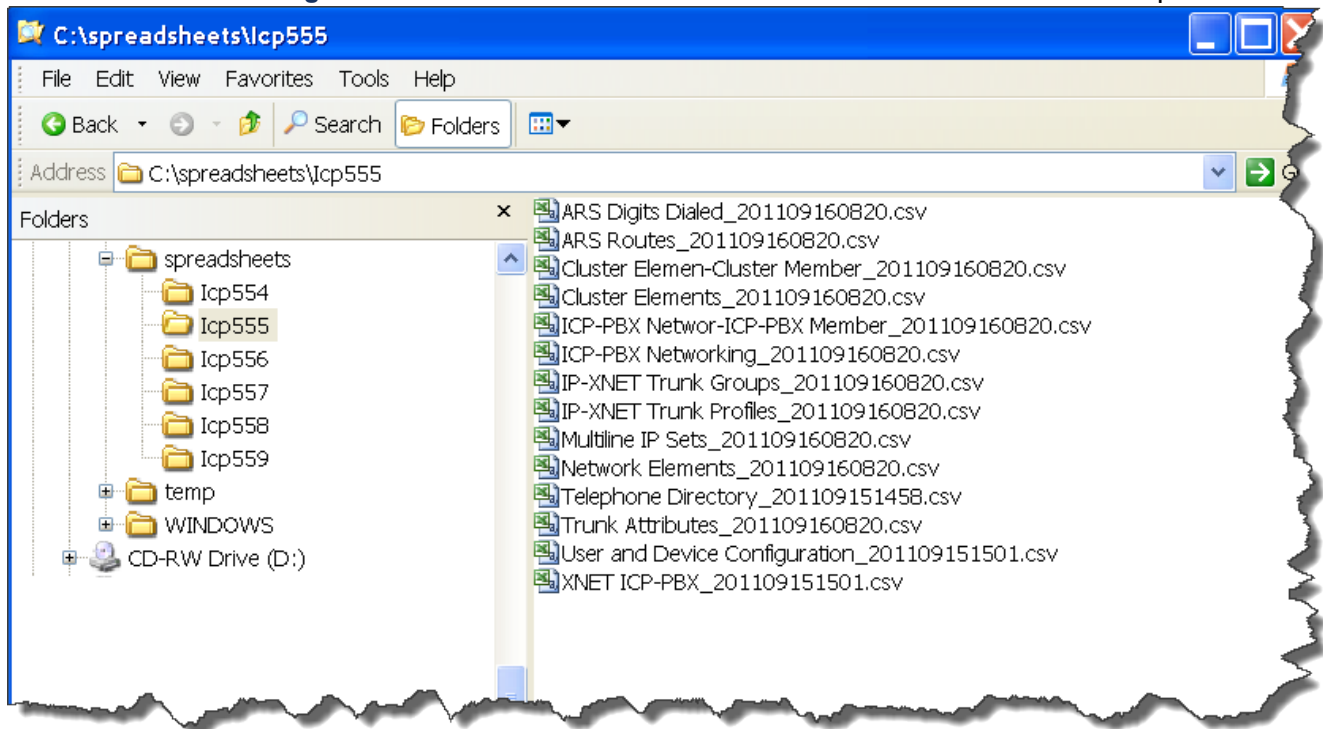




Figure 6.4: Non-shared .csv files for Element Icp555

Rules and Guidelines for Importing Data

This section details the rules and guidelines for importing data using the Import Spreadsheet.

- **Ensure that the correct Platform type is selected.**
The spreadsheet varies by platform type (AX, CX, MXe, etc.). Make sure the correct Platform type is selected each time that you open the Spreadsheet Tool.
- **Expand Worksheet Column Titles**
Increase the width of the worksheet columns to see the full title of each column.
- **Correct Errors**
The Spreadsheet validates the data in the worksheet before you can import it. Data errors or missing data are indicated in the worksheet with red borders. You must correct any errors before you can proceed with the import.
- **Use the Logs Viewer**
To get additional detail about errors found during the validation process, check the logs in the Logs Viewer.
- **Data in Shared Forms is Distributed to the Cluster**
You only have to import the data for shared forms into a master element. By default, SDS distributes the data in shared forms to all elements in the cluster. Shared forms are identified by the  icon in the System Administration Tool form menu.
- **Data for Unshared Forms Must be Imported into each Element**
Forms that are not shared must be imported individually into each element. Unshared forms have no  icon. For example, the System Options data for element lcp554 must be saved in a separate worksheet and then imported into the System Options form of lcp554. The System Options data for element lcp555 must be saved in another worksheet and imported into the System Options form of lcp555.
An exception to this rule is the User and Services Configuration data. You must import the local user data into each element using a separate User and Services Configuration worksheet for each element. Although SDS shares the User and Services Configuration data by default, it writes the data only to the Remote Directory Number forms of the remote elements. In your ClusterPlanning.xls spreadsheet, you can sort the user entries by PBX Number and then copy the columns of entries into the element worksheet.

Entering Data into the Worksheets

The Import Spreadsheet consists of a series of worksheets, each corresponding to a configurable form. Four worksheets are displayed by default, one each for the User and Services Configuration, Key Assignment, and Telephone Directory forms, and a fourth for creating additional worksheets for other forms.

The User and Services Configuration and Telephone Directory worksheets allow you to enter programming data for as many users as your system supports; however, by default, the worksheets display 50 rows. If you wish to add more than 50 users, click **Add 50 Records**.

The spreadsheet adds 50 more rows with the same default column values.

To enter data for import:

1. Open the Import Spreadsheet, and click **Enable Macros** if prompted.
2. Select **Open the 3300 ICP Import Spreadsheet**.
3. Ensure that the Platform type is set correctly.

4. Save the import spreadsheet with a unique name.
5. Follow the instructions on the All Forms worksheet to create the required worksheets.
6. Copy the columns of data from your ClusterPlanning.xls spreadsheet into the corresponding data columns in the worksheet(s).

	Last Name	First Name	Number	Local-only DN	Department	Location	Role Name	IDS Manageable	Email
10	Smith	Mike	5001	No	Sales	5th Floor	Full-time	Yes	Mike_Smith@abc.com
11	Green	Ted	5002	No	Sales	5th Floor	Full-time	Yes	Ted_Green@abc.com
12	Black	Jack	5003	No	Sales	5th Floor	Full-time	Yes	Jack_Black@abc.com
13	White	Sally	5004	No	Sales	5th Floor	Full-time	Yes	Sally_White@abc.com
14	Brown	Gordon	5005	No	Sales	5th Floor	Temp	Yes	Gordon_Brown@abc.com
15	Jones	Tom	5006	No	Training	6th Floor	Full-time	Yes	Tom_Jones@abc.com
16	Sacamano	Bob	5007	No	Training	6th Floor	Full-time	Yes	Bob_Sacamano@abc.com
17	Thomas	Jane	5008	No	Training	6th Floor	Temp	Yes	Jane_Thomas@abc.com
18	Matthews	Sarah	5009	No	HR	2nd Floor	Full-time	Yes	Sarah_Matthews@abc.com
19	Johns	Matt	5010	No	HR	2nd Floor	Full-time	Yes	Matt_Johns@abc.com
20	Paulson	Peter	5011	No	HR	2nd Floor	Full-time	Yes	Peter_Paulson@abc.com

Figure 6.5: User and Services Configuration Worksheet

NOTE: If you need to import over 1000 records, you must import the records in blocks of 1000 records or less. For example, if you need to import 5000 records, create five import files of 1000 records each.

Creating the Import File from the Import Spreadsheet

Click **Check Data Format** to check the selected worksheet or **Check All** on the All Forms worksheet to check all worksheets. The Import Spreadsheet validates the data and highlights cells with errors. Note the following:

- Some True/False cells may appear highlighted. You need to select a value from the drop-down menu in the cell to avoid getting a validation error. Typically, you need to select a Yes/No value.
- Validity checking determines whether the data make sense (numbers fall within an allowable range, numeric data are all digits, there are no illegal characters, etc.). The checking does not "verify" that the data is correct. Verification occurs when the data is imported into the MiVoice Business system at which time it is checked for conflicts and conformance with database configuration rules.
- Checks for out-of-range values are based on the maximums allowed by the MiVoice Business database. Some of these values are dependent on Flexible Dimensioning and may not correspond to the maximums allowed by the Import Spreadsheet. Any such out-of-range values in the spreadsheet will generate errors during the import process.
- The Check Data Format process can take a considerable amount of time, depending how much data you are adding, and on the speed of your PC. To minimize the amount of time required to complete a Check Data Format or a Save, do not switch to any other applications until the operation is finished.

- Cells with errors are highlighted with red borders. Correct errors in the cells, and then click **Check Data Format** again. Repeat the process until the spreadsheet is free of errors.
- Click **Save for Import**. The import file is saved as a .csv file in the same folder that contains the Import Spreadsheet. The system automatically appends a date and timestamp to the saved file.
- In Windows Explorer, copy the .csv file to the appropriate element folder and append the element name to the form name: for example, User_Configuration_Icp554_200902101147.csv.

NOTE: If the Browse button is available in the worksheet, you can click **Browse** and save the file directly to the appropriate element folder.

Setting Call History Records Capacity

Before importing a large number of devices that support Call History recording, set the maximum number of call history records at each element. To set the maximum number of call history records for an element:

1. Identify the number of devices in the import file that support Call History recording.
2. Multiply that number by the device's default Call History records value plus the number of Call History records that you wish to allocate to the device. For example, if your import file contains 10 devices that support Call History recording, each device has a default Call History value of 20, and you wish each device to have a Call History record value of 10, multiply $10 \times (20 + 10) = 300$. The maximum number of Call History records is 56000.
3. Navigate to the Dimension Selection form.
4. Click **Change**.
5. Ensure that the value in the Call History field in the "Dimension Selection" form is larger than the value obtained in Step 2 above. If it is not larger, enter the value you obtained in Step 2.
6. Click **Save**.

WARNING: The maximum number of call history records must not exceed the number of call history records allocated on a system-wide basis through the Dimension Selection form.

Previewing the Import Data

Preview the import data before you import it.

1. Log into a System Administration Tool session.
2. Navigate to the form into which you want to import data.
3. Click **Import**.
4. From the Import <form name> dialog box, click **Browse**.
5. Navigate to the .csv file (for example, User and Services Configuration_Icp554_201109151501.csv).
6. Click **Next**. A Validating Data dialog appears.
7. Review the data listed in the Import Preview window. If no errors are detected, proceed to see *"Importing the Data into the MiVoice Business System"* below.

8. If the Import Preview window displays errors, select from the following options:
- **Previous** - to return to the Import dialog box, revise the import file data, and begin the import process again.
 - **Show Only Errors/Show All Data** - to show records with errors, or to show all records. By default, the Preview window shows only entries with errors.
 - **Print** - to print the Preview window to keep a record of the errors. Note that Print is enabled only when you are in the Show Only Errors view (that is, when Show All Data is displayed at the bottom of the screen).
 - **Cancel** - to cancel the import and return to the form. After you cancel, you can modify data in the import file, or exit the form and try the import process at a later time.

NOTE: The Import button is disabled if there are data format errors. You cannot import erroneous configuration data. See below for information on how to resolve errors.

Importing the Data into the MiVoice Business System

Before you attempt to import data, review the data import rules outlined in the previous sections.

NOTE: Import adds and updates existing data; it never deletes.

1. Log into a System Administration Tool session on the element.
2. Navigate to the form into which you want to import data.
3. Click **Import**.
4. Click **Browse**.
5. Browse to the Import Spreadsheet worksheet file (for example, User and Services Configuration_lcp555_201109151501.csv).
6. Click **Next**.
7. When the import is successfully completed, click **Finish** to return to the form.
8. Review the form for errors.
9. If necessary, manually correct any import errors in the System Administration Tool form.

Troubleshooting Import Errors

Import errors fall into two main categories:

- Validation Errors are displayed in the Import Preview window. You must resolve these errors before you can continue and complete the Import.
- Import Errors are displayed in a Summary window. The records containing the errors are ignored and the Import continues. You can either correct the errors in the import file and re-import or modify the form directly.

Validation Errors

Validation errors result from invalid data formats in the Import Spreadsheet.

To avoid validation errors, ensure that the entries for each cell in the Import Spreadsheet meet the requirements for valid data entries (numbers fall within an allowable range, numeric data are all digits, there are no illegal characters, and so forth).

Validation errors are detected before the data is actually imported into the system database.

The errors are displayed in an Import Preview window.

The appearance of the Import Preview window depends on whether there are errors:

- No errors detected - displays all data records from the Import Spreadsheet.
- Errors detected - displays an ERROR FOUND IN DATA message and records that contain data format errors. Fields with errors are highlighted.

The Error column may display error messages such as

- Too many characters in name field
- Too many digits in Directory Number

You cannot import erroneous configuration data. You must resolve errors before attempting the import again.

Import Errors

Import errors occur when data from the Import Spreadsheet form conflicts with existing system data. For example, you could import a user profile that has the same Directory Number as a profile that already exists in the system database. Alternatively, you could import a user whose name is exactly the same as the name of an existing user. In both cases, the imported data conflicts with existing system data, so import errors occur.

Import errors are detected during the import process—that is, while the data is imported or written to the system database. A record of these errors is displayed in a Summary window.

The Summary window displays different information, depending on whether there are import errors:

- No errors detected - displays all data records from the Import Spreadsheet.
- Errors detected - displays an ERROR FOUND IN DATA message and records that contain data format errors. Fields with errors are in bold text.

The Error column may display error messages such as

- Directory Number already exists
- Name already exists

Import errors must be resolved after the import is complete. Resolve these errors in the form that is receiving the imported data.

Cluster Maintenance

Overview

This chapter contains information about maintaining an established cluster. Topics covered are as follows:

- Enabling and Disabling SDS
- Performing Backups and Restores
- Upgrading Software in the Cluster
- Adding a New Element to an Existing Data-Sharing Community
- Removing a Element from a Data-Sharing Community
- Moving an Element to a Different Data-Sharing Cluster
- Correcting Inconsistent Remote Directory Numbers
- Changing the Data Distribution Scope
- Splitting a Data-Sharing Cluster
- Merging Data-Sharing Clusters in the same SDS Network
- Repairing Data
- Moving users to a different cluster element

WARNING: Do not attempt the procedures in this section unless you understand how SDS works. Severe service disruptions can result from failing to observe the conditions and rules for configuring and maintaining an SDS network. See the "Voice Networking > Manage Network > System Data Synchronization" section in the Sys Admin Tool Help for the required information OR The *Using System Data Synchronization* Solutions Guide on [Document Center](#).

NOTE: For assistance with SDS-related problems encountered while performing the maintenance procedures in this chapter, see the *3300 ICP Troubleshooting Guide* - "Chapter 8: Voice Networking, System Data Synchronization."

Enabling and Disabling SDS

SDS is enabled by default. On a system where the SDS feature is disabled, the SDS-related forms (SDS Distribution Errors, SDS Form Comparison, and SDS Form Sharing) are missing from the navigation pane in the System Administration Tool.

Certain operations, such as removing an element from an data-sharing community, require that you disable SDS.

WARNING: Before disabling SDS on a member element, ensure that the elements are sharing data at the network or cluster scope.

To enable or disable SDS:

1. Log in to the system and navigate to the System Options form.
2. Click **Change**.
3. Click **Yes** to enable or **No** to disable System Data Synchronization.

Performing Backups and Restores

In an SDS-enabled network or cluster, you typically perform backups and restores locally on each element, and the backup or restore only applies to the element that you are logged in to.

However, if the element belongs to an SDS Administrative Group that supports Multi-node Management applications, you can choose to back up the databases of all elements that are members of the Administrative Group; see ".

While the backup or restore is processing, data distribution updates sent by other data-sharing elements are rejected. Update errors caused by the rejected distribution updates are logged on the member element that attempted the distribution.

NOTE:

1. When you restore a backup file, if the backup is significantly older than databases on the other elements in the network or cluster, you should synchronize from another node in the SDS network or cluster to ensure that the local element has the latest data from the other elements.
2. During a system backup, no other users can access any of the web-based tools (Visual Voice Mail, Desktop Tool, Group Administration Tool, or System Administration Tool) or save changes. To avoid blocking other users, we recommended that you perform system backups outside of business hours.

Performing a Backup

To back up the database on a data-sharing MiVoice Business system:

1. Log in to the element you want to back up.
2. Perform the backup. See "Performing Backups and Restores" in the Sys Admin Tool Help.
3. After the backup is complete, synchronize the SDS network. See "Synchronizing Data" in the Sys Admin Tool Help.
4. If necessary, resolve any pending updates or errors. See "Resolving Pending Updates or Errors" in the Sys Admin Tool Help.

Performing a System Restore

To restore a database to a data-sharing MiVoice Business system:

1. Log in to the element you want to restore.
2. Restore the database. See "Restore Database" in Sys Admin Tool Help.
3. After the restore is complete, synchronize the SDS network from another element in the network that has the latest data. See "Synchronizing Data" in the Sys Admin Tool Help.
4. If necessary, perform an event retry to resolve data distribution errors. See "Resolving Pending Updates or Errors" in the Sys Admin Tool Help.

NOTE: If you are restoring an old database from another element that has never been shared, to a network element that belongs to a data-sharing community, you must re-enable data sharing on that element. To re-enable data sharing, enable the System Data Synchronization (Data Sharing) option in the System Options form, and then perform a Sync operation from one of the other member elements.

Adding a New Element to an Existing Data-Sharing Community

After you have set up a data-sharing network or cluster, you can add new elements to the network or cluster at any time. Once you have added new elements, you can start sharing with the new elements, if desired.

When you add a new element, you must always bring it into an existing data sharing community from an element that is already in the data-sharing community—that is, you must always grow the data sharing community from an element within the SDS network. The following illustrations illustrate this requirement:

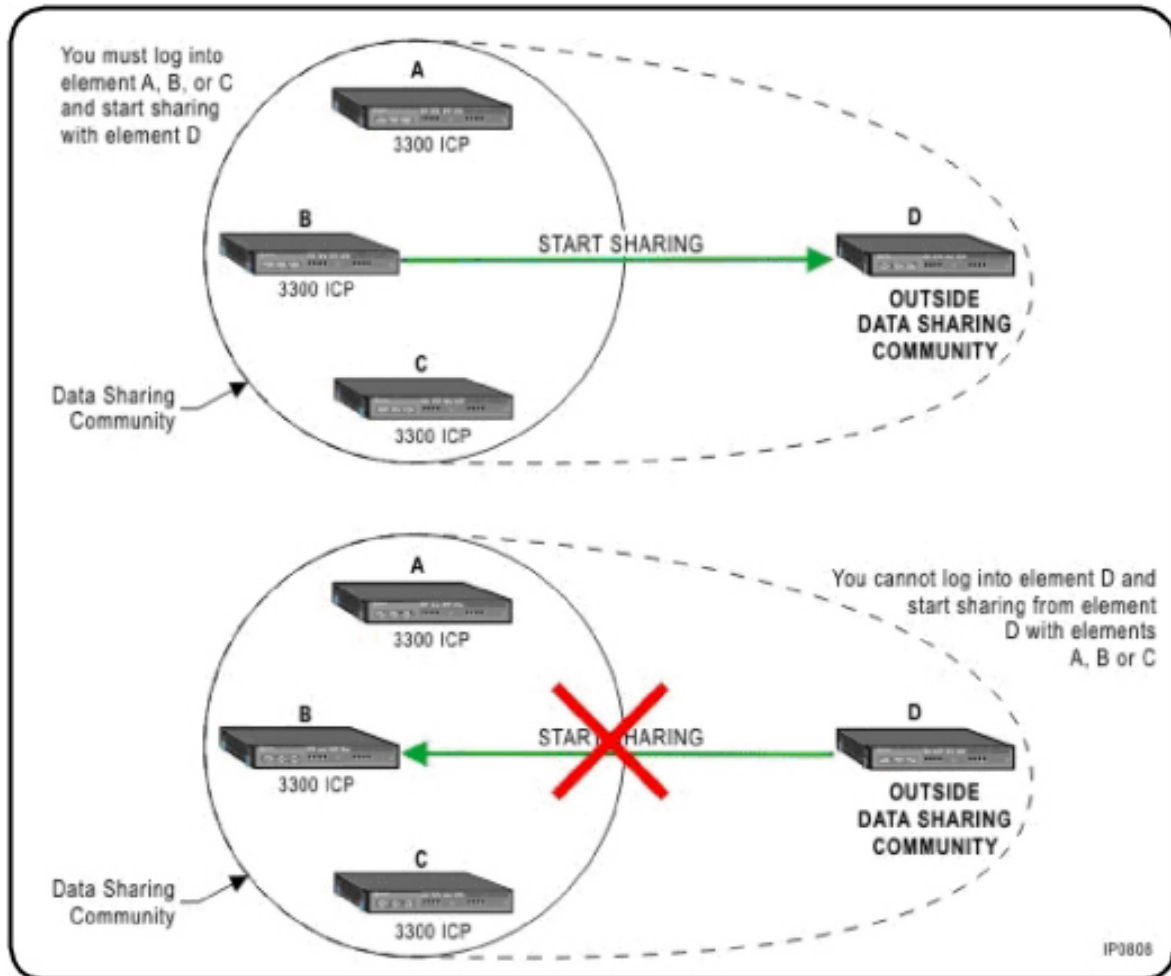


Figure 7.1: Adding a New Element to a Data-Sharing Community

NOTE: You can add a cluster element or network element to an existing data-sharing network without including that element in a data-sharing relationship. For information about adding new network elements without enabling data-sharing, see [Populate the Network Elements Form](#).

There are three possible scenarios for starting to share with a new element:

- Start sharing with a new element at the network level.
- Start sharing with a network element at a cluster level.
- Start sharing with a new element at the network level and cluster level at the same time.

After you add the network elements to the sharing community, you must synchronize the network elements with each other. The one exception to this rule is if both network elements are new, and no data-base changes have been made.

You can attempt to synchronize all of the network elements at the same time, but a prioritized approach generally saves time. It is recommended that you perform the Sync operation on one element at a time, particularly if there are elements that are significantly out of sync. Then, you repeat the Sync procedure, adding forms to synchronize, and then progressing to other network elements.

Start Sharing with a New Element at the Network Level

Follow this procedure to start sharing data at the network level with an element that is new to the data-sharing network.

1. Ensure that the element has been upgraded to 3300 ICP Release 6.0 or later. Refer to the *3300 ICP Technician's Handbook* for information on upgrading the system software.
2. Ensure that the element is not currently a member of any other data-sharing network. An element can only be a member of one data-sharing network at a time. If the element is sharing data with another network, remove the element from that network. See [Removing an element from a data-sharing community](#) for more information.
3. Log into an element that is within the existing data sharing community (an element that is already part of the SDS network). From the Network Elements form, add the new element to the local SDS network. See [Populate the Network Element Form](#).
4. Start sharing. See "Start Sharing Data" in the Sys Admin Tool Help.
5. Synchronize the network elements. See "Synchronizing Data" in the Sys Admin Tool Help.

Start Sharing with a Network Element at a Cluster Level

You may wish to enable a network element to start sharing data within a cluster in the same network. The element is not new to the data-sharing network, but it is a new cluster member.

NOTE: To add an element to a data-sharing cluster, you must first add the element to the network in which that cluster resides.

To start sharing at a cluster level:

1. Ensure that the element has been added to the cluster. If not, see "Adding Cluster Elements" in the Sys Admin Tool Help for more information.
2. Start sharing. See "Start Sharing Data" in the Sys Admin Tool Help.
3. Synchronize the network elements. See "Synchronizing Data" in the Sys Admin Tool Help.

Removing an element from a data-sharing community

You can remove an element from its data-sharing community at any time. However, before removing it, you must disable SDS on it. By disabling SDS, the element ceases to participate in data-sharing at any scope. If you want the element to resume data sharing at any scope (either in the same network or another network), you must re-enable SDS (see [Enabling and Disabling SDS](#)) and start sharing again (see "Start Sharing Data" in the Sys Admin Tool Help).

NOTE: The following procedure is for removing an accessible element—i.e., one that you can log on to from the Sys Admin Tool. If the element has failed and it is not possible to log on to it, use the REMOVE-SHARINGNE maintenance command in the Sys Admin Tool to remove it from the data-sharing community. See the Sys Admin Tool Help for more information.

WARNING: Before Disabling SDS on a member element, ensure that the elements are sharing data at the network or cluster scope.

In the following procedure, element A is the master for the operation and element B is the element that you are removing from the cluster.

1. Log into a system administration tool session on element B. De-program all group features and devices that are hosted on element B.
 - delete any page group entries.
 - delete any call rerouting first/second alternative references.
 - delete the devices from the User and Services Configuration form. This step also deletes the telephone directory entries. The RDN entries and hosted service entries for these devices are automatically removed from the cluster element databases via SDS.
 - delete the group features using the appropriate group forms. This step blanks the directory numbers of the telephone directory entries. For devices, SDS automatically removes the RDN/hosted service entries.
2. Check the SDS Distribution Errors form, and resolve any errors that have appeared.
3. Log into element A. Remove resiliency from any devices or groups that use element B as the secondary.
 - In the User and Services Configuration form, remove resiliency from the devices that use Network Element B as their secondary.
 - Remove group resiliency by changing the secondary element assignment to Not Assigned in the associated form.
 - ACD Agent Skill Groups
 - Hunt Groups
 - Page Groups
 - Personal Ring Groups
 - Pickup Groups
 - Ring Groups
 - Trunk Groups
4. Repeat step 2 on any other cluster elements that have resilient devices or groups that have element B assigned as the secondary controller.
5. Log into element B and disable the SDS option in the System Options form.
6. Log into element A, navigate to the Cluster Elements form and delete element B as a cluster element.
7. Reinstall the system software on element B to remove the cluster programming data (PNI for the cluster, CEID indexes and CEID digits for the other elements, etc.) from element B.

Removing an Element from a Cluster

MCD 6.0 provides a maintenance command, `REMOVEDNE`, that facilitates the removal of a non-local element from a cluster and from its data-sharing community (if applicable). See the Sys Admin Tool Help for more information.

Moving an Element to a Different Data-sharing Cluster

Moving an element from one data-sharing cluster to another requires removing it from its cluster and then adding it to the other cluster. See the procedures above for instructions.

Correcting Inconsistent Remote Directory Numbers

To remove inconsistent RDNs (where a directory number of a resilient device appears only in the database of one of the resilient pair controllers rather than on both):

1. Use the SDS Form Comparison form to compare the Multiline IP Sets, Single Line IP Sets, and Wireless IP Sets forms of the primary and secondary controllers.
2. From the results of the compare operations, record any directory numbers that appear only on the secondary controllers. Any directory numbers for resilient devices that appear only on the secondary controllers are inconsistent RDNs. So are numbers that appear as remote DNs in some controllers in the network, but have no local DN to match anywhere else in the network or vice versa.
3. Navigate to the Network Elements form on the primary element.
4. Click the check boxes beside the primary and secondary element(s) that you want to synchronize.
5. Click **Sync**.
6. Select the **Data Repair** option in the Confirm Sync to Element(s) window.
7. Select only the following form data for synchronization:
 - Service Hosting Data
 - System Level Call Handling
8. Click **OK**. When the synchronization operation is complete, the inconsistent RDNs are removed from the RDN forms. If you don't want them removed, you must add them manually to the other controller(s) before the Sync.

Changing the Data Distribution Scope

After your data-sharing network is established, you can change the scope at which a given form shares its data.

To modify the data-sharing of a shareable form:

1. Using the SDS Form Sharing form, identify the scope and records you wish to share. For more information on how to modify the data shared, see "Specifying the Shared Data" in the System Admin Tool Help.
2. Synchronize the network elements. See "Synchronizing Data" in the System Admin Tool Help.

NOTE:

1. To change records within the SDS Form Sharing form, your user profile must be assigned System Data Synchronization Admin access rights. See "Assign Administrators" in the System Admin Tool Help.
2. The data in the SDS Form Sharing form is shared with other elements and appears in the SDS Form Sharing forms of the other elements.

Splitting a Data-Sharing Cluster

Each cluster is assigned a Global Unique Identifier (GUID) that the system software uses to identify the cluster. GUIDs do not appear in any of the System Administration Tool forms. Before a data-sharing cluster can be split into two distinct SDS clusters, you must reset the GUID on one of the existing cluster elements. There are two procedures that you can use to do that:

- Reset the GUID of one of the cluster elements from an element outside the cluster.
- Remove all the elements from the Cluster Elements form in one of the elements in the smaller cluster and create a new cluster.

NOTE:

- Cluster A has elements MiVB1, MiVB2, MiVB3, and MiVB4.
- Cluster A is to be split into two clusters; Cluster A with elements MiVB1 and MiVB2, and Cluster B with elements MiVB3 and MiVB4.
- MiVB5 is an element that does not belong to any cluster, which is to be used to split Cluster A.

To split a data-sharing cluster:

1. Perform a full cluster-wide SDS share. Resolve any errors.
2. Login to MiVB3
3. Disable SDS sharing between MiVB3 and MiVB4. After disabled, re-enable it.
4. In the Network Elements form, verify that the **Data Sharing** column shows **NO** for all the elements.
5. Reset the GUID for the new Cluster B:

Option 1 (recommended):

- Reset the cluster GUID of MiVB3 from MiVB5.
- From MiVB5, create a virtual cluster by adding MiVB3 to the Cluster Elements form and then start SDS share with MiVB3. The system automatically configures MiVB3 with the hidden GUID of the new Cluster B.
- Disable SDS share with MiVB3.
- From MiVB3, run the **REMOVE** maintenance command to remove MiVB5 that was used to create the virtual cluster.
- Proceed to step 6.

Option 2:

- Remove all the elements from one of the element's in the smaller cluster and create a new cluster.
 - From MiVB3, run the **REMOVE** maintenance command to remove MiVB1, MiVB2, and MiVB4. Remove the dependent data from ARS programming and the ICP/PBX Networking form.
 - Create a new Cluster B on MiVB3 and then add the member elements as required.
 - Proceed to step 6.
6. From MiVB3, enable SDS sharing and start sharing with MiVB4.
 7. Update the new cluster name and Primary Node Identifier (PNI) as required.

Merging Data-Sharing Clusters in the same SDS Network

SDS does not support the merging of independent data-sharing communities. If two SDS communities have been created independent of each other, the system rejects all attempts to start sharing from one community to the other. If you wish to start sharing between independent communities, you must disassemble one of the communities (preferably, the community with fewer elements) by removing the member elements (see [page 106](#)), and then add the individual elements to the existing larger community (see [page 104](#)).

Complete the following procedure to merge two existing data-sharing clusters that belong to the same SDS network.

Pre-requisites

- Verify that no dialing plan conflicts, including ARS, exist between the element that you selected to be the master element and the elements to be added from the other cluster.
 - Ensure that the chosen master element contains the data that you want to share with all the elements in the new, merged cluster. (The data from the master takes precedence over data on other elements - slaves - in the sharing scope.)
 - Ensure that all elements to be merged are 3300 ICP type elements in the Network Elements form.
1. In the cluster with the fewest elements (for example cluster A), turn SDS off and then on again at each of the cluster elements. See .
 2. Choose a member element from the larger cluster (for example, element B1 from cluster B) as the master element.
 3. Log into element B1 and add all elements from cluster A to the Network Elements and to the Cluster Elements forms of element B1.
 4. While logged in to element B1, complete the cluster programming that is not shared (CEID Index, CEID Digits, Feature DN number, and ARS) for each newly added cluster element in the Cluster Elements form on element B1.
 5. For each element that initially belonged to cluster A, update the cluster Name and PNI in the Cluster Elements form to match the name and the PNI configured for elements in cluster B.

NOTE: Make sure that the name is an exact match (upper/lower case).
 6. From the master element B1, start sharing with all the elements added to cluster B. See "Start Sharing Data" in the Sys Admin Tool Help.

7. From the master element B1, perform a full Sync operation with each newly added element (initially belonging to cluster A). See "SDS - Synchronizing Data" in the Sys Admin Tool Help.

NOTE: A full Sync with all other elements (initially belonging to cluster B) is recommended, but not mandatory.

Resolving Data Distribution Errors and Pending Updates

Data Distribution errors and pending updates are database changes that SDS has either failed to apply (errors) or has yet to apply (pending) to the destination elements. They happen for many reasons, including

- network outages or congestion
- MiVoice Business software incompatibilities
- mismatched country variant settings
- incorrect SDS configuration

Data distribution errors and pending updates are collected and displayed in the SDS Distribution Errors forms of the local element where you initiated the Sync operation. Check these forms frequently and resolve any problems found as quickly as possible before they get out of hand and cause serious trouble, including service outages.

NOTE: You must resolve data distribution errors at the element where the updates were initiated.

To resolve distribution errors from the originating element:

1. Navigate to the SDS Distribution Errors form. The number of data sharing errors is in the top left-hand corner of the form.
2. To view all records, in the **Display** field select **All** and then click **Retrieve**. Or, to view a subset of records, select first or last, select the desired number of records, and then click **Retrieve**. The main frame of the window lists the pending updates and the failed updates.
3. Click on the **Action ID** field heading to sort the errors by action ID. You can sort the errors based on any of the column headings by clicking on the desired heading (for example, Reason).
4. Select the check box next to the update record.

NOTE:

- a. You can check the boxes of multiple records and the operation that you choose will be applied to the checked records. To select all update records, click **Select All**.
 - b. When you select multiple records, the Retry and Force Change operations will be available only if the records selected are of the same type.
5. To resolve the pending update or error:
 - Click **Retry** to retry the update. "Retrying" appears before the Reason field in the record. If the update is successful the update record disappears from the list. If the update is unsuccessful, the update error record will be updated with the new time stamp.
 - Click **Force Change** to update the remote node with the record from the local node. (This action only applies to errors resulting from conflicting data.)
 - Click **Login** to launch the system administration tool of the remote system. You can then manually fix the error through the System Administration Tool of the remote element. To automatically login from the local element, the User Authorization Profile must share the profile of the logged in admin-

istrator with the remote element. If the login ID of the administrator is not defined on the remote element, the login page of the remote element will be displayed instead, and you must login using the user name and password of the remote element.

6. Click **Data Refresh** to update the main window.

NOTE: The system automatically retries "transport" errors. Updates that are fixed by the system will disappear from the SDS Distribution Errors window after a Refresh. See ["About Automatic Retry"](#) below for details.

7. After you have corrected an error, you may have to delete the error record. Go back to the SDS Distribution Errors form on the local element, select the error record and click **Delete**. The update error is removed from the main window and the error log is removed from the logs. You can also choose to delete an error record if you understand the error and determine that the update is not required.

WARNING: Deleting an error record could cause data inconsistencies that could cause subsequent retry operations to fail because of a dependency between the records.

About Automatic Retry

The system automatically retries data updates that are not successfully delivered to the destination element (due to a network or element failure).

The following data updates are not automatically retried:

- updates that fail because an application on the destination element was unable to write the data to its database
- updates that fail because the same data was updated concurrently. See "About Concurrent Synchronizations" in the Sys Admin Help.

The following conditions apply to system-initiated automatic retries:

- Automatic retries are started every 30 minutes.
- Updates are retried from oldest to newest based on the initial time stamps of the record.
- Automatic retries yield to manual retries and new updates.

Repairing Data

If the database of a controller is severely out of sync, you can restore the database from a backup. However, the backup database will not include the recent database changes that have been made to other systems in the cluster while the controller was down. After performing the data restore, you can bring the controller's database up to date, by performing a Data Repair operation from another controller in the network.

The Data Repair operation overwrites all the shared data, including the user and device data, on the slave controller with the shared data from the master controller.

1. Perform a data restore of the latest backup to the secondary controller. See .
2. Navigate to the Network Elements form of a controller in the cluster that has up to date data.
 - Synchronize the data from the local, master controller to the slave controller. For resilient networks, do the following before you confirm the synchronization operation:
 - Select the **Data Repair** option in the Confirm Sync to Element(s) window.

- Click the **Advanced** button.
- Set the Resilient User-Device Policy to "Synchronize data where <local element> is the PRIMARY and SECONDARY host for resilient devices".
- Click **Apply**.
- Click **OK**.

Moving Users to a Different Cluster Element

Moving a user from one cluster element to another is a multi-step process. First, identify the forms that contain records of the user's directory number. Then, record the relevant data so that you can use it when reprogramming the user on the destination MiVoice Business system. You can do the reprogramming either manually or by using the Import and Export facilities of the System Administration Tool.

Before beginning the move, ensure that the source and destination elements are properly licensed and that they are sharing and synchronized via SDS.

Also, be sure to read the notes at the end of this section for additional programming that may be required to complete the move.

On the source MiVoice Business System

1. In the User and Device Attribute form, export the records of the users you want to move. The information is used to reprogram Groups and Call Rerouting (if applicable) on the destination MiVoice Business system.
2. In the Hunt Groups form, find out whether the user DNs are members of non-resilient Hunt Groups anywhere within the cluster. If they are, record the number of the hunt group.
3. In the forms listed below, record the data associated with the user DN(s) you are moving. The information will be used when reprogramming the users on the destination MiVoice Business system ¹.

Form	Data to Record
5560 IPT Master/Slave Association	All
Associated Directory Numbers	All
Call Forwarding Profile	All
Call Rerouting Always Alternate / First Alternate / Second Alternative	Alternative Number that has the user DN programmed in the "Directory Number" field
DND	All
Guest Rooms	All
Multi-device Suites	All

1. If you plan to export this data and import it directly into the destination MiVoice Business system, you may need to edit the export data—for example, to remove unwanted users—before importing it. This is to ensure that the data is valid for import and can be saved on the destination.

Form	Data to Record
Multiline Appearance Groups	Group Directory Number(s) that has the user DN programmed as the Primary Directory Number in the Member list
Multiline Set Keys	DNs of line keys and the corresponding line type.
Remote Busy Lamps	Any number that has the user DN as the Remote Host Set Directory Number.
Suites	All
Telephone Directory	All
Trunk Attributes	Trunk Service Number has the user DN programmed as the "Non-dial In Trunks Answer Point - Day/Night 1/Night 2

4. In the User and Services Configuration form:

- a. Disable resiliency for users being moved (users must be local to the source system).

Single user

- Change **Secondary Element** to **Not Assigned**

Multiple Users

- Export all users.
- Update the .csv file to remove users you are not moving; delete the value of the Secondary Element for the remaining users.
- Import the modified .csv file into the source system.

- b. Clear the Home Element, User PIN, and User Profile Password, if applicable.

Single User

- Select the user (Use Search to Locate by DN).
- Click **Export**
- Select **Selected Record**

Multiple Users

- Export all users and delete the unwanted user records from the .csv file before proceeding.
- Edit the exported User and Services Configuration .csv file as follows:
 1. Delete the Home Element value.
 2. Replace "*****" in the User PIN and User Profile Password fields with a default password, if previously programmed.
 3. Save the modified .csv file.

5. In the VM Mailboxes form (for distributed voice mail configuration only).¹

- a. Export the VM mailbox records of users being moved.

Single User

- Select the user. (Use Search to locate by DN.)
- Click **Export**.
- Select **Selected Record**.

Multiple Users

- Export all VM Mailboxes.
- Update the .csv file to remove the VM Mailboxes whose users are not being moved.
- Save the modified .csv file.

- b. Edit the VM Mailboxes .csv file as follows:

- Replace ***** in VM Passcode field with a default password, if applicable.
- Save the modified .csv file.

6. In the Multiline Set Keys form:

- a. Export the key data for each user DN being moved.

Single User

- Select the user. (Use Search to locate by DN.)
- Click **Export**
- Select **Selected Record**.

Multiple Users

- Export all DNs.
- Update the .csv file to remove DNs that are not being moved and their corresponding key records.
- Save the modified .csv file.

- b. Edit the Multiline Set Keys .csv file as follows:

- Remove any "User Speedcall - Private" keys or replace ***** with a valid DN, if applicable.
- Ensure that all remote DSS/BLF numbers and user speedcall (non-private) numbers are valid on the destination MiVoice Business system.
- Save the modified .csv file.

7. If the user DN is used in the following forms, locate the references and delete them.

Form	Data to Record
Trunk Attributes	DN in the "Non-dial In Trunks Answer Point - Day/Night 1/Night 2" fields of individual Trunk Service Number records.
Call Rerouting Always Alternate/First Alternate/Second Alternative	DN in the "Directory Number" field of the Alternative Number records.

1. In a distributed voice mail configuration, a resilient user has two mailboxes, one on the primary system and one on the secondary. The user must program each mailbox separately (greetings, passwords, etc.). The system is programmed so that the user gets a message waiting notification when there is a voice message on either mailbox.

Form	Data to Record
Page Group	DN in the "Number" field of individual Page Group records.
Remote Busy Lamp	DN in the "Remote Host DN Number" field of individual Monitored Device record.
Guest Rooms	"Guest Room Number" record corresponding to the given DN.
Suites	"Directory Number" in the Suite Members of individual Suite Pilot Number records.
Multi-device Suites	"Directory Number" in the Multi-device Suites Members of individual Multi-device Suites Pilot Number records.
Multiline Set Keys	Line keys of the given user DN ¹

1. Alternatively, you can deprogram the line keys from the User and Services Configuration form (under Keys tab).
8. In User and Services Configuration form, delete the user(s) you are moving.
9. Check the SDS Distribution Error - Users form for any pending SDS updates or errors resulting from the deletion. Resolve any issues before proceeding.

On the Destination MiVoice Business System

1. In User and Services Configuration form, import the .csv file from the source MiVoice Business system.
2. If CESIDs are programmed, the "Enable Auto CESID Updating" field must be selected in the Default CESID form on the destination MiVoice Business system before importing starts.
3. In VM Mailboxes form, import the corresponding .csv file from the source MiVoice Business system.
4. In Multiline Set Keys form, import the corresponding .csv file from the source system.
5. Before importing, ensure that all numbers for call forwarding, speedcall, and DSS/BLF programmed on the source system are valid on the destination. ¹
6. In the User and Services Configuration form, re-enable resiliency for the users who are moved by assigning the appropriate Secondary system.
7. Re-program the user-associated data collected from the source system, as applicable.
8. Re-register users' devices for L2 to CESID mapping, if applicable. See "Emergency Services - CESID Programming" in the Sys Admin Tool Help for more information.

1. If you plan to export this data and import it directly into the destination MiVoice Business system, you may need to edit the export data—for example, to remove unwanted users—before importing it. This will ensure that the data is valid for import and can be saved on the destination system.

9. Inform users of their newly defaulted passwords (User PIN and User Profile Password), VM Passcodes; and remind users to reprogram their private User Speedcall numbers.¹

NOTE:

1. If the SDS sharing of any user-related or user-dependent form is disabled in the network, you will need to manually program the relevant user data on the destination MiVoice Business system to recreate the original user configuration.
2. The following non-shareable forms must be manually reprogrammed on the destination system to recreate the original user configuration: - Page Groups - Remote
3. Call Forwarding Profile and DND forms, although shareable, are user-specific. When a user is deleted from the source system, the call forwarding numbers and DND settings are also deleted. Which means they must be manually reprogrammed on the destination system.
4. The VM Network Server form (if applicable) must be manually reprogrammed if it was configured differently on the source and destination system. The same applies to the Call Forwarding used to dial voice mail.
5. Call Rerouting treatments assigned in the User and Device Attributes form may need to be updated on the destination system to recreate the original user configuration.
6. Any HTML Applications installed on the source system and assigned for use on phones in the User and Services Configuration form (Phone Application tab), must be installed and assigned on the destination.

1. Passwords/passocodes and user speedcalls do not get exported for security reasons and must be re-created.

Glossary

Administrative Group - System Data Synchronization allows you to share system form data among groups of elements at different sharing scopes. Administrative groups are sub-groups of elements within a network group. Elements that are members of an Administrative Group share SDS form data at the Administrative Group Members scope. Multi-Node Management applications are supported for SDS Administrative Groups.

Boundary node - a network element that actively routes calls between resilient MiVoice Business systems and non-resilient MiVoice Business/3300 ICP systems.

CEID Index - a 1- to 3-digit number from 1 to 999 that you assign to the CEID digit string of a cluster element in the Cluster Elements form. You use the CEID Index number to associate the CEID string in the form with the remote directory numbers in the Remote Directory Numbers form.

Cluster - a group of interconnected elements that share a common dialing plan. MiVoice Business systems can be interconnected via IP trunks and/or DPNSS over T1 trunks.

Cluster element - a single MiVoice Business/3300 ICP system that is a member of a cluster.

Cluster Element Identifier (CEID) Digits - a digit string used to identify an element in a cluster. In a cluster that is configured for the RDN feature, the CEID allows calls to be routed between the elements in the cluster. You assign unique CEID digits to each cluster element. You also assign a CEID index to each CEID. You must set up ARS to route calls between the cluster elements based on the CEID digits.

Common Data Distribution - See "RDN Synchronization."

Embedded Resilient Device Support - In a network or cluster that supports RDN Synchronization, you can configure resilient devices from the MiVoice Business System Administration Tool. Prior to MCD 4.0, you had to use OPS Manager to configure resilient devices.

Feature DN - a directory number that allows DPNSS features, such as busy lamp fields, direct paging and extension paging, to function across the cluster. You enter unique directory numbers in the Feature DN fields of the Cluster Elements form at each element in the cluster.

FQDN - Fully Qualified Domain Name. The complete domain name for a specific computer (host) on the Internet—for example, www.mitel.com.

Global Data Model - see "RDN Synchronization."

Global Unique Identifier (GUID) - used by the system software to identify a cluster. The GUID does not appear in any of the System Administration Tool forms.

ICP/PBX Networking form - a programming form in the System Administration Tool that sets up signaling links between elements and establishes how long the signaling session will stay up after the call is torn down. You must program this form for each element in the cluster (including the local element). You assign the local element a PBX Number that matches its CEID index. You then assign a PBX Number to each remote element. Each remote PBX Number must match the remote element's associated CEID index.

Local network or cluster element - the cluster element that supports the device (that is, the device's primary controller).

Local device - the devices (for example, IP Phones) that an element supports are considered local to that cluster element.

Master Element (or Controller) - In a network that is configured with the System Data Synchronization feature, the master element is the network element you are logged in to when you initiate the data sharing, and subsequent data sync, operation. Data from the master takes precedence over any of the data on any of the other elements (slaves) in the sharing scope.

Multi-Node Management Applications - Applications, such as Application Reach-Through, that are available to a system administrator within an Administrative Group. These applications support the management of the elements that belong to the Administrative Group.

Network - a group of interconnected elements, for example MiVoice Business/3300 ICP systems. MiVoice Business/3300 ICP systems can be interconnected via IP trunks and/or DPNSS over T1 trunks.

Network element - an element, for example a MiVoice Business/3300 ICP system, that is a member of a network.

Portable Directory Number - a call processing feature that is available in a cluster.

Primary Node Identifier (PNI) - a digit string that identifies a network element or a cluster within a network. Automatic Route Selection for the network is set up to route calls to the network elements based on the PNIs. Note that in a single standalone cluster, you do not need to assign PNIs to the cluster members.

QoS- Quality of Service. The performance of a communications channel or system is usually expressed in terms of QoS. The QoS comprises many aspects of a connection, including, SNR (Signal to Noise Ratio), BER (Bit Error Ratio), maximum and mean throughput rate, and reliability, priority.

Remote network or cluster elements - in relation to the cluster element that you are programming, the other cluster elements are considered remote.

Remote device - the devices in a cluster that are not hosted by a given local element (that is, the devices that are hosted by other elements in the cluster) are considered to be remote to that element. At each cluster element, you must assign the devices that are remote to that element with the CEID index of its local cluster element. You assign CEID indexes in the Cluster Elements form. The Remote Directory Numbers form lists the portable directory numbers of all the remote devices in the cluster.

Remote Directory Number - Local directory numbers are hosted on the element that you are logged into while remote directory numbers are hosted on another element in the cluster. Users can call remote directory numbers from any extension in the cluster by just dialing the number. The Remote Directory Numbers form lists the remote directory numbers in a cluster network. The Remote Directory Numbers forms of the cluster elements are updated via OPS Manager synchronizations or Remote Directory Number Synchronization.

Remote Directory Number Synchronization - (also known as Common Data Distribution) supports the synchronization of remote telephone directory entries across all the element databases in a network or cluster. If you migrate a network or cluster to support Remote Directory Number (RDN) Synchronization (recommended with MCD 4.0; mandatory with MCD 4.1 or later), any telephone directory entries that you add, modify, or delete at an element through the System Administration Tool are automatically distributed to the other elements.

Resiliency - allows a network to maintain calls in progress, handle new incoming and outgoing calls, and continue to provide voice mail service in the event of MiVoice Business/3300 ICP failure or a network-level failure. Resiliency is achieved by setting up a network of MiVoice Business/3300 ICPs in a resilient cluster, which is a specially-configured network of MiVoice Business/3300 ICPs that can direct IP phones and route and maintain calls.

Resilient Pairs - Devices (IP phones and IP consoles) can be configured to have a primary controller and a secondary controller, with the secondary controller available to immediately take over if the primary

controller fails. The primary and secondary controllers can be referred to as a resilient pair. SDS allows you to keep these two controllers synchronized so that the devices can be moved seamlessly from primary to secondary in the event of a controller failure.

Share (Data) - an SDS feature that allows you to maintain consistent system form data in a cluster by sharing data updates among the cluster elements. After sharing is enabled, the data that you identified in the SDS Form Sharing form will be shared among the selected elements. Then, if a record is added or modified in a shared form of one of the cluster elements, the update will be made automatically in the databases of the other cluster elements.

Sharing Scope - The data shared among network elements using SDS can be shared, for example, across the whole network, within the cluster or Administrative Group, or by resilient pairs.

Slave Element (or Controller) - In a network that is configured with the System Data Synchronization feature, a slave element has its database overwritten or merged with the data on the master element during a Sync operation.

System Data Synchronization - In a network or cluster of elements, certain programming data, such as Interconnect Handling Restrictions, Feature Access Codes, Class of Service Options, and System Options, must be identical at each element. The System Data Synchronization (SDS) application reduces the time required to set up and manage networks or clusters of MiVoice Business/3300 ICP systems by allowing you to

- compare the data in a programming form of one cluster element against the data in same form on another element in the cluster.
- synchronize the form data of a network or cluster of elements with the form data of a master element
- share system form data among a network or cluster of elements (MiVoice Business/3300 ICP systems).

Sync Operation - an SDS feature that allows you make the shared form data on one or more remote elements the same as the data on a local element. Before you can perform a sync operation, the remote elements must already be sharing data with the local element at the desired scope.

Standalone network element - a network element that is not included in the cluster.

Transit node - A cluster element that passively allows calls to be routed through it, on their way to a another MiVoice Business or 3300 ICP system.