MULTI-NODE NETWORKING

SOLUTIONS GUIDE

JULY 2016

Mitel®

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.

Trademarks

Multi-node Neworking
Release 10.0
July 2016

CHAPTER 1: INTRODUCTION

CHAPTER 2: MULTI-NODE NETWORK DESIGN

Chapter 1

INTRODUCTION

Introduction

This guide describes the factors that go into choosing to install a multi-node voice network and what decisions must be made as you plan your multi-node network.

The purpose of this guide is to discuss how to plan a voice network with more than one node. It does not cover Multi-node Management. For detailed information about Multi-Node Management applications, refer to *Mitel Voice Cluster Design and Implementation*, and the MiVoice Business System Administration Tool Help.

Although the graphics in this document show Mitel 3300 ICP controllers, MiVoice Business on ISS or MiVoice Business Virtual controllers can be used instead, except where the controller is connected to the PSTN.

Reasons to set up a multi-node solution

There are several main reasons why you would choose to deploy a multi-node network:

- You need more capacity than you can get with just one controller.
- You have multiple business groups with different needs that are easier to address if they are served by different nodes.
- You have branch offices that need to be connected to head office.
- You have multiple locations that need to access the PSTN through TDM interfaces (as opposed to a multi-site hosted).
- from a single node).
- You need a high availability network with additional nodes for failover (resilient network).

Note: This guide uses the terms **node**, **controller**, and **network element** interchangeably.

Types of networks

Multi-node networks can be located all in one building, or they can be spread over many locations world-wide. They can be set up in clusters with System Data Synchronization (SDS), and they can be set up to be resilient, if necessary.

Implementing a cluster architecture gives you the ability to manage large groupings of nodes in such a way that users think they are connected to just one large network. Users dial an extension number to reach a user on another controller. Features and feature codes function in the same way regardless of the controller.

SDS Sharing is crucial for large networks. You can program one node, and SDS propagates programming data and telephone directories to all the other nodes in the cluster. For detailed information about SDS, see Using System Data Synchronization, available on Mitel OnLine.

Also refer to the *Mitel Voice Cluster Design and Implementation Guide*.

Acronyms and terms used in this guide

ACRONYM	TERM
ARS	Automatic Route Selection
controller	A MiVoice Business platform, whether it is hosted on a 3300 ICP, an industry standard server, or a VMware virtual machine. Also called a node or network element.
CESID	Customer Emergency Services ID
HA	High Availability. A VMware feature that moves a VM to another host if the original host fails.
ICP	IP Communications Platform
KPML	Key Press Markup Language - KPML is a markup language that enables presentation-free User Interfaces as described in the Application Interaction Framework. The Key Press Stimulus Package is a SIP Event Notification Package that uses the SUBSCRIBE and NOTIFY methods of SIP. The subscription filter and notification report bodies use the Keypad Markup Language, KPML. (Description taken from IETF Sipping Draft.)
LAN	Local Area Network
MAN	Metropolitan Area Network
MAS	Mitel Applications Suite (now called MiCollab)
MCD	Mitel Communications Director (now called MiVoice Business)
MICD	Multi-Instance Communications Director (now called MiVoice Business Multi-instance)
MiVB	MiVoice Business controller
Multi-node network	A network containing more than one node.
MNM	Multi-Node Management: A set of embedded applications (in the System Administration Tool) for managing multiple nodes in the same Administrative Group, including Application Reach-Through, Fault Management, and Backup and Restore.
node or network element	MiVoice Business, whether it is hosted on a 3300 ICP, an industry standard server, or a VMware virtual machine. Also called a controller.
PSAP	Public Safety Answering Point. Used for directing emergency services.
QoS	Quality of Service - Usually refers to network prioritization mechanisms, but can also refer to availability of a service.
RDN Synchronization Mode	The Mitel data model used in MCD Release 4.0 and later releases and MiVoice 7.0+.
SDS	System Data Synchronization
TDM	Time Division Multiplexing
vMCD	Virtual Mitel Communications Director (now called MiVoice Business Virtual)
WAN	Wide Area Network

Chapter 2

MULTI-NODE NETWORK DESIGN

Planning your network

When designing and deploying a multi-node network, you need to make many decisions.

Table 1 provides a list of items for consideration before undertaking the design of your multi-node network. Use the table to record your network requirements, and add to the table, as necessary, to include any other requirements that must be included in the design.

Also refer to the *MiVoice Business Site Planning Guide*.

Table 1: Planning your multi-node network

NETWORK REQUIREMENT OR PARAMETER		YOUR NETWORK
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	
	In the case of analog trunks & phones, do the locations require different loss plans & tone plans?	
If there are multiple locations:		
	Do the locations have different time zones?	
	Do the locations have different language types?	
Type and number of IP phones required		
	Agent phones (in the case of contact centers)	
	User phones	
	Number of resilient IP phones	
	Number of non-resilient IP phones	
	Number of analog phones, on premise and off premise	
	Number of analog Fax end points	
	Number of T.38 fax channels	

Table 1: Planning your multi-node network (continued)

	NETWORK REQUIREMENT OR PARAMETER	YOUR NETWORK
	Number of audio conference units	
	Number of video conference units	
Number of trunks required		
	Number of Digital E1/T1 Trunks and their location	
	Number of SIP Trunks (Note 1)	
	Analog (LS) trunks required for local connectivity or for connectivity during a massive power failure.	
Numbering Plan		
	DID ranges • Can they be ported (moved) to the new system? • If merging networks that are currently separate, will there be duplication of DID numbers?	
	Continued use of existing numbering plan or change of extension numbering system?	
Required features and applications, and number of users		
	Voice Mail Is voice mail centralized or distributed?	
	Auto-attendant	
	Will Active Directory be required?	
	MiVoice Border Gateway (MBG): (Note 1) • Teleworker phones using MiNET • External hot desk users (over SIP trunk) • SIP trunks	
	Dynamic Extension • Programmable ring groups (PRG) / twinning • External Hot Desk Users / KPML • Group presence (user can be moved in or out of group)	
	Property Management System (PMS)	
	Key system features	
	MiCollab Client (formerly called UCA)	
	Unified Communicator Express (UCX)	
	Hot Desking	
	Audio, Web, and Video Conferencing	

Table 1: Planning your multi-node network (continued)

	NETWORK REQUIREMENT OR PARAMETER	YOUR NETWORK
	Voice mail requirements	
	Analog phone requirements	
	Fax requirements and location	
	ACD Agents	
	Additional third-party software, if needed	
Networking		
	Network equipment (routers & switches & UPS requirements)	
	Cabling requirements	
	Power over Ethernet (PoE) & UPS requirements	
	Bandwidth between sites (type & how much)	
	Connections: dedicated to voice, or shared with data	
	Quality of Service (QoS), Priority settings for L2 & L3 (See Mitel recommended settings)	
Emergency services (for example, 911, 999, and so on)		
	Emergency phones sets that remain operational during a power outage	
Resiliency - There are many kinds of resiliency:		
	Do you need call control resiliency?	
	Voice mail resiliency?	
	Resiliency for critical applications?	
	PSTN/SIP trunk resiliency?	
	Do you need additional nodes and connections?	

Note:

1. MiVoice Border Gateways (MBGs) may be needed to provide IP address isolation and SBC functionality between the customer network and the SIP service provider. (SBC is Session Border Controller.

After determining the functionality required, consider the type of solution you need. You can work with your Mitel sales engineer to decide which of the following options best meets your requirements.

- Fully-hosted solution (central hub in one or two data centers)

  A Mitel reseller or the enterprise hosts and manages the network. The network can be hosted on-site or off-site.

- Local solution with local resiliency

  The resilient network solution is located on one site or across sites.

- Local solution with no resiliency

  The non-resilient network solution is located on one site or across sites.

- Hotel or motel

  Multiple MiVoice Business controllers used with resiliency and possibly in separate fire zones. Also refer to the *Hospitality Solutions Guide*.

- Cruise ship

  Multiple MiVoice Business controllers used with resiliency and possibly in separate fire zones, and separation of staff from clients. In cruise ships, connection to the Also refer to the *Hospitality Solutions Guide*.

MiVoice Business platforms

You can use one or more of the following MiVoice Business platforms in your network:

- MiVoice Business running on the Mitel 3300 ICP hardware platform

  The 3300 ICP platform running the MiVoice Business software provides analog interfaces for connecting to the PSTN.

- MiVoice Business Virtual running on a VMware or Microsoft Hyper-V host

  MiVoice Business Virtual controllers allow you to host communications applications on the same servers as your other business applications. This option is a cost-effective way to host multiple MiVoice Business controllers without requiring proprietary hardware.

- MiVoice Business and MiVoice Business Multi-instance (formerly called MICD) running on an industry standard server

  You can run one or more instances of MiVoice Business controllers that do not need connection to the PSTN. This option is a cost-effective way to host multiple MiVoice Business controllers without requiring proprietary hardware.

Multi-node networking considerations

The following sections give brief overviews of the many network planning and deployment considerations:

Note: Although the graphics in this document show Mitel 3300 ICP controllers, MiVoice Business on ISS or MiVoice Business Virtual controllers can be used instead, except where the controller is connected to the PSTN.

When and why to use a MiVoice Business cluster

A cluster is a separate group of elements within a network that shares a common telephone directory, even with elements spread over different locations. Your entire network may be encompassed in just one cluster, or you might have multiple clusters in your network.

For example, businesses with distinct geographic locations can be set up with a cluster at each location in a common network. Clusters can also be built around functional or business groups, while remaining in a common network. Hotels and motels are commonly organized this way, too.

Clustering and networking between units introduces additional performance overhead. To determine the impact of such configurations and use with users and applications, it is highly recommended that you discuss your needs with a Mitel Sales Engineer or Mitel Professional Services to gauge the headroom and overall impact of your proposed configuration.

You can network nodes with or without setting up a cluster, but nodes must be in a common cluster to be configured for resiliency. To achieve device resiliency, you must set up two or more MiVoice Business controllers in a resilient cluster, so that IP devices can fail over to a secondary controller if the primary controller fails or connection to it is lost.

Resilient devices can be configured to fail over from a primary to a secondary controller when the primary controller fails, or the connection to it is lost. If you need to do hot desking between controllers, the controllers must be in the same cluster. Even for a single controller, if you want to do hot desking, you need to program a cluster of one for Hot Desking to work.

In summary, use a MiVoice Business cluster if you need:

- Common extension numbering
- Resiliency
- Hot desking

Figure 1 illustrates the topology of a basic resilient cluster, in which IP phones have a primary and secondary MiVoice Business. For information about engineering a resilient network, refer to the *MiVoice Business Resiliency Guidelines*.

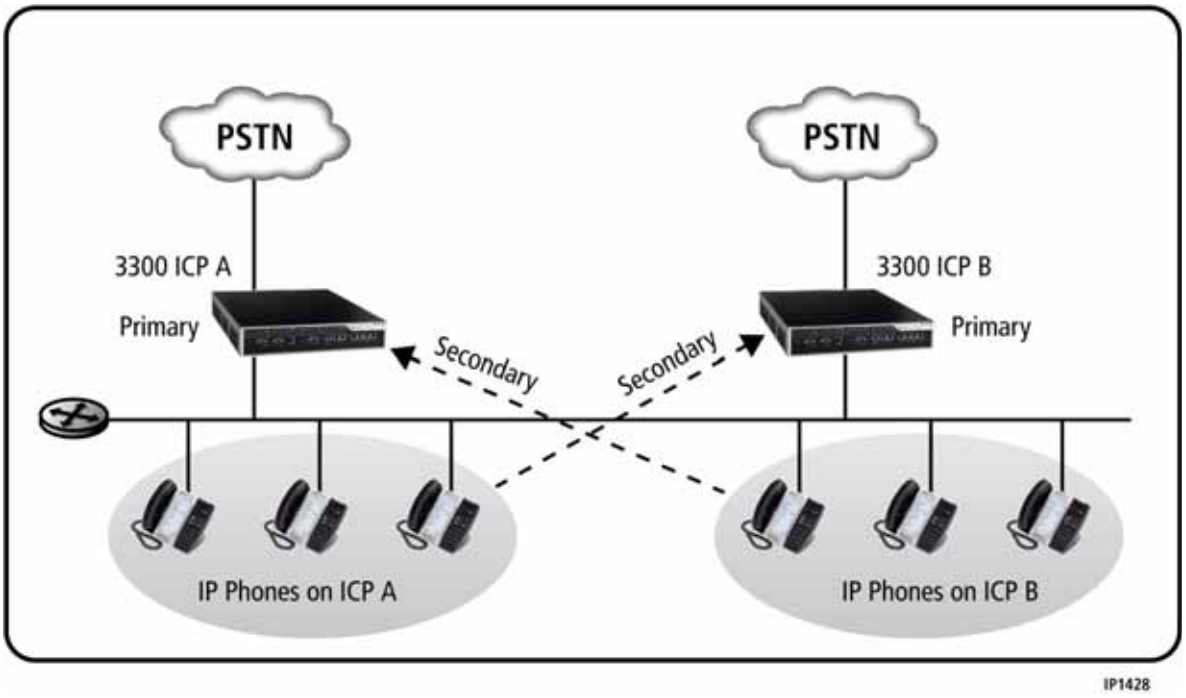

Figure 1: Basic resilient cluster

A resilient cluster is managed using the MiVoice Business System Administration Tool. Each node in the cluster must be running MCD Release 4.0 or later software, and be using Remote Directory Number (RDN) Synchronization. A resilient cluster contains:

- A cluster of 3300 ICPs or MiVoice Business controllers
- SIP trunks connected to multiple gateways to provide primary and secondary routes
- Applications that behave like IP phones, such as MiCollab Client (formerly UCA). (MiCollab Client cannot be made resilient, but it can be part of a resilient cluster.)
- Connections to MiVoice Business controllers outside of the cluster, but part of the overall network

Plus the following optional additions:

- 5xxx-series IP phones and IP consoles that support resiliency
- Interfaces to PSTN trunks that are connected to MiVoice Business controllers inside the cluster
- SIP trunks connected to multiple gateways to provide primary and secondary routes

RDN Synchronization Mode

Prior to MCD Release 4.0, system data was shared between nodes of a network using OPS Manager (Classic Mode). At MCD Release 4.0, with the change to RDN Synchronization Mode, this data sharing was integrated into MCD.

A distinct upgrade step is required when migrating through MCD Release 4.0 from earlier releases. MCD Release 4.0 and higher releases comply with the RDN Sync requirements, and use System Data Synchronization (SDS) to share network information.

After migration to RDN Sync Mode, which is required after MCD Release 4.0, OPS Manager can no longer be used for data sharing. After making the transition to RDN Sync Mode, you cannot go back to Classic mode. This is a one way transition. For details, refer to the following Solutions Guides, available on Mitel OnLine:

- *Migrating to RDN Synchronization Mode Solutions Guide*
- *Using System Data Synchronization Solutions Guide*
- *Network Upgrades Solutions Guide*

How to design administrative groups and clusters

Every network element must be defined in the **Network Elements** form, but an element may or may not belong to a cluster. To share user-related information within a cluster, the element must be part of that cluster. Most SDS data sharing is done at the cluster level. For more information about SDS sharing, see “About System Data Synchronization (SDS)” on page 14.

Administrative groups are logical sub-groups of elements within a network. Each element may or may not belong to an **Administrative Group**. If SDS sharing is enabled, each network element configured for sharing is automatically put into the **System Defaulted Administrative Group**, if it has not been explicitly added to a different Admin Group. Administrative groups are generally used to group network elements so they can easily be managed by one administrator using the Reach-Through feature.

Admin Group Size

It is recommended that Administrative Groups contain a maximum of 20 network elements to help maintain required performance of SDS and Reach-Through operations.

For MCD Releases 5.0+, the system will disable an Admin Group when there are more than 20 nodes in that group. A log file entry will be generated when the group becomes disabled. New administrative groups can be created and nodes moved to the new group. If a group is reduced to fewer than 20 nodes, the Admin Group is re-enabled, and a log entry generated.

Note: When moving nodes to a new group, ensure there is at least one managed node (a 3300 ICP, 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 will 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.

Reach-Through

The Reach-Through feature allows you to manage all the nodes in the same Administrative Group from one node. On any form, you can “reach through” to view and change the same form on another node in the group.

Starting with MiVoice Business 7.2 and MiCollab 7.0, Reach-Through can also be used from the MiCollab server when it is connected to a network of MiVoice Business controllers through SDS. Refer to the MiCollab Server Manager Help for details.

For more information about the Reach-Through feature, refer to the *Using System Data Synchronization Solutions Guide*.

The network example in Figure 2 shows a cluster with five Administrative Groups.

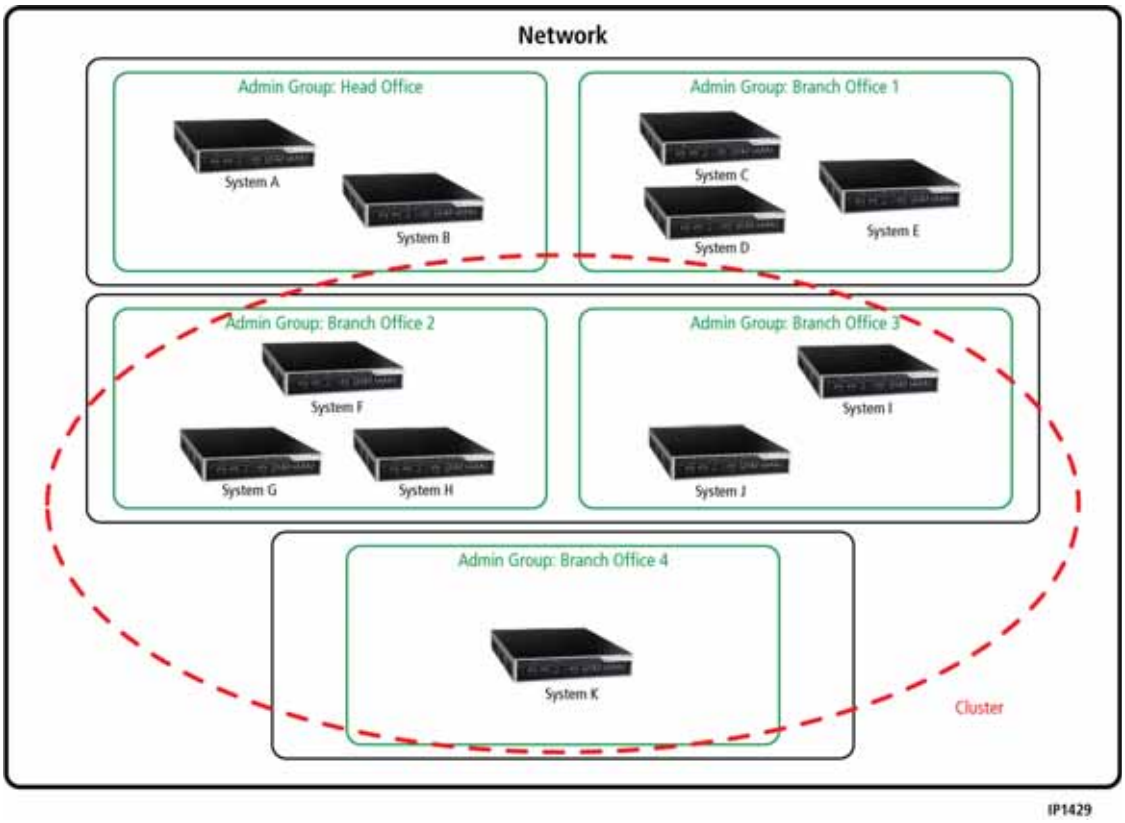

Figure 2: Administrative groups in a cluster

About System Data Synchronization (SDS)

System Data Synchronization, or SDS, allows data sharing and automatic data propagation throughout your network. SDS uses information presented in forms to populate and configure elements in a cluster. You can import form data into one element in the cluster and then share it with the other elements.

In a network of elements, certain programming data, such as **Interconnect Handling Restrictions**, **Feature Access Codes**, and **System Options**, must be identical at each element.

System Data Synchronization (SDS) reduces the time required to set up and manage networks or clusters of MiVoice Business controllers by automatically sharing data updates among the network elements. Programming updates do not have to be made separately on each network element. You can add a user on one network element and that user's data is updated in the databases of all network elements in the sharing scope.

Starting with MiVoice Business 7.2 and MiCollab 7.0, one MiCollab server can also be added to SDS sharing in the **Network Elements** form. This allows provisioning and ongoing synchronization with the MiCollab server. Note that all MiVoice Business nodes in SDS sharing with the MiCollab Server must be in the same Admin Group. Refer to the MiCollab Server Manager Help for conditions and limitations in the “Flow Through Provisioning” topics.

Certain forms in SDS are shared at the network level, by default; some at the cluster level, and some at the administrative group level. (Also see “How to design administrative groups and clusters” on page 13.)

Depending on the configuration, you may need to adjust the sharing scope (or level) of information on certain forms. You may also need to adjust some forms further, such that some database records are shared while others remain local to the specific nodes.

Most SDS sharing is done at the **All Cluster Members** scope; that is, the sharing is done among all network elements in the cluster.

Some SDS sharing is done at the **Administrative Group** scope, and data is shared only among the network elements in the Administrative Group. An example of information shared at the **Administrative Group** scope is alarms.

You can also share the forms that define resilient pairs. In the **User and Services Configuration** form, you can define a **Secondary Element** for each device to set up device resiliency.

There is also data that you do not want to share, but keep local to the node. This includes information relating to the trunks. Some examples of the kinds of data you might choose not to share with other network elements are:

- A common operator number local to a specific node, for local operation only.
- A trunking gateway. It may have some trunk numbers in common with the network, but local node (non-shared) numbers for digit handling.
- Number and extension information in a non-clustered network. Most number and extension information is shared within clusters, but not in a non-clustered network. (Through specific routing and number plans, however, it is possible to make calls between clusters within the network by dialing only the extension.)

Refer to the *Using System Data Synchronization Solutions Guide* for more information.

Note: If you have started making sharing changes in SDS and you would like to revert back to the defaults, refer to the System Administration Tool Help, in the topic called “What Data Can Be Shared”. This topic contains a table describing the default settings.

CAUTION: After you start SDS sharing among the elements, do not stop sharing unless directed to do so by Mitel Product Support.

Do not stop sharing while voice traffic is running in the system.

About Flow-through Provisioning

Flow-through Provisioning is available when all MiVoice Business controllers are at Release 7.2+ and the MiCollab Server Release is at 7.0+.

Flow-through Provisioning uses System Data Synchronization to provision MiVoice Business through the MiCollab.

Which sites must be connected to the outside world through PSTN trunks?

When deciding which sites must be connected through PSTN trunks, consider where access is now, and where it needs to be. The location of the PSTN trunks affects placement of your Mitel nodes. Consider the following:

- Where are the PSTN trunks connected in your current network?
- Do you need external trunk access to a branch office?
- Do you need additional PSTN trunks, either connected to your main control center, or to branch offices, to provide increased reliability?
- Are you adding SIP trunks?
- Do you need local trunk access for fax?

Note: Typically, you program Automatic Route Selection (ARS) separately on each individual node.

Emergency services, local call routing, and power backup

Careful planing of the PSTN access is required to ensure that emergency call routing is supported correctly. If local gateways are provided, then trunk access for emergency calls may be provided from the local trunks. If all trunking is provided out of a central point, emergency calls may need to be forwarded to the correct public safety answer point by the trunk provider (sometimes known as PSAP forwarding). Ensure that you plan call routing not only for normal operation, but also to ensure that if a user is connected to the resilient controller, emergency services are still routed correctly.

Note: In MCD 6.0/MiVoice Business 7.0+, the CESID can contain up to 12 digits. For MCD Release 5.0 and previous releases, the maximum number of digits is 10.

Keep in mind that if a phone is powered using PoE (Power over Ethernet), then the PoE switch, network switches, and routers must be backed up with a properly sized UPS to ensure that calls can be made in the event of a power outage. This is a rather expensive solution. As an alternative, an ONS phone, a 3300 ICP with an LS trunk and power fail programming can be used even if the entire building has no power. For a detailed discussion of this topic, see the *MiVoice Business Engineering Guidelines*.

IP consoles should be considered as critical phones, and at least one should always be provided with power backup. This is mainly to provide a callback point and emergency services.

MCD Release 6.0 introduced Location-based call routing. With Location-based call routing, a call from an extension to a service or destination such as Emergency (911 or 999, for example), Directory Assistance (411), or a corporate Help Desk is sent to the service located in the same network zone as the originating device. For example, when a New York-based hot desk user logs into a phone in Chicago and dials 911, the system routes the call to the Chicago Public Safety Answering Point (PSAP), not to the New York PSAP. For detailed information about configuring Location-based call routing, refer to the System Administration Tool Online Help.

Starting in MCD Release 6.0, a Ring Group can be configured to function as an emergency answering point and trigger an SNMP trap to notify Mitel Emergency Response Adviser whenever the group receives a call.

Connectivity to applications

Applications like MiCollab or NuPoint UM can be distributed or central. Your current voice mail configuration may be distributed among your office locations, for example, and you can decide to centralize all voice mail functionality with one MiCollab UM installation in a central location. This provides a network-wide Unified Messaging solution, while making management easier. For increased resiliency, however, you may plan to have application support at the branch offices to ensure that service is not lost if the connection to the main site is lost.

With MiCollab Single-Point Provisioning, when you add or delete information for a single user on the MiCollab server, you can optionally update the MiVoice Business system database at the same time. When the Single-Point Provisioning option on the Network Element tab is enabled, new configuration data entered on the MiCollab server (such as phone and mailbox creation, COS option setup, Call Forwarding, and Desktop Monitor setup) is automatically updated in the MiVoice Business programming database at the same time.

Similar functionality is available when MiCollab (beginning with MAS Release 5.0) is connected directly to the corporate Active Directory (AD) user database. MiVoice Business can be updated at the same time, along with most MiCollab applications. For more information, refer to the *Provisioning Users Solutions Guide*, available at Mitel OnLine.

Analog end-point requirements

You will need analog trunks if you have any of the following requirements or legacy equipment:

- You need to provide emergency service access, even in the case of network failure and/or complete power outage without a UPS system.
- You need to use fax machines (if fax is not supported over the SIP trunk).
- You plan to continue to use an existing TDM switch.

Basic resiliency

Voice system resiliency allows you to minimize the impact of network element or connection failure. There are four main aspects to resiliency.

- MiVoice Business call control resiliency
- Mitel end-points can be configured to continue working by failing over to a secondary call controller.
- Network (LAN/WAN) resiliency is an expected pre-requisite of installation of a Mitel solution.
- A second PSTN access point ensures continued voice operation if one PSTN connection fails

We recommend the following highly-scalable, resilient topologies. These topologies are discussed in detail in the *MiVoice Business Resiliency Guidelines*.

- Resilient single-site environment for small to medium-sized businesses

  In a resilient single-site environment, a number of MiVoice Business controllers are clustered together; each MiVoice Business controller can function independently if it has its own PSTN access. MiVoice Business controllers are connected through a local area network (LAN), or through IP trunks or TDM trunks. This topology is suitable for small to medium-sized business, organizations, or institutions that use a single-site (no branch offices).

- Resilient distributed network for large enterprises

  A locally distributed network connected through a LAN, 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 locally throughout a city as in the case of a restaurant chain, or throughout a campus environment, as in the case of an educational institution.

- Resilient hybrid network for a combination of single-site and distributed topologies

  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 networks 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.

- Resiliency with MiVoice Business Virtual in a VMware vSphere environment to create resilient topologies

  Any of the network topologies can use MiVoice Business Virtual as a primary or secondary controller, or you can run your entire network on virtual nodes. For physical PSTN access such as T1/E1, BRI or analog interfaces, a PSTN gateway is needed, such as the 3300 ICP with MiVoice Business. The virtual MiVoice Business and physical MiVoice Business, in the form of a 3300 ICP hardware platform, can work together. The MiVoice Business

Virtual does not have physical connections to the PSTN, but it can be used as a trunk controller when connected to external SIP trunks.

Note: For a MiCollab server in the SDS network, the MiCollab server does not fail-over to a secondary MiVoice Business.

This limitation affects your network only if:

- You have a MiCollab server in your SDS Sharing network.
- You are using Flow Through Provisioning.
- You are running MiVoice Business 7.2+ and MiCollab 7.0+.

The following considerations affect all of the resilient network topologies discussed in the following sections:

- It is recommended that devices belonging to designated work groups be supported by the same primary and secondary MiVoice Business controllers. This helps to preserve the work group capabilities of these devices during a failure.
- You must ensure that your secondary MiVoice Business controller knows how to route emergency calls for devices that are failed over from their primary controller if the primary and secondary nodes operate in different Public Safety Answering Points (PSAP).
- “MiVoice Business” refers to any of the following:
  - MiVoice Business running on the Mitel 3300 ICP hardware platform
  - MiVoice Business Virtual 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
- To configure device resiliency, you assign a secondary controller to each device. If the primary controller of a resilient device (IP Phone or IP Console/MiVoice Business Console) goes out of service, the device fails over to its secondary controller without loss of service.
- Compression zones and bandwidth management: for details, see the *MiVoice Business Engineering Guidelines*.

IP trunking models between nodes

Examples of fully-meshed and hierarchical network configuration networks are shown in Figure 3 and Figure 4.

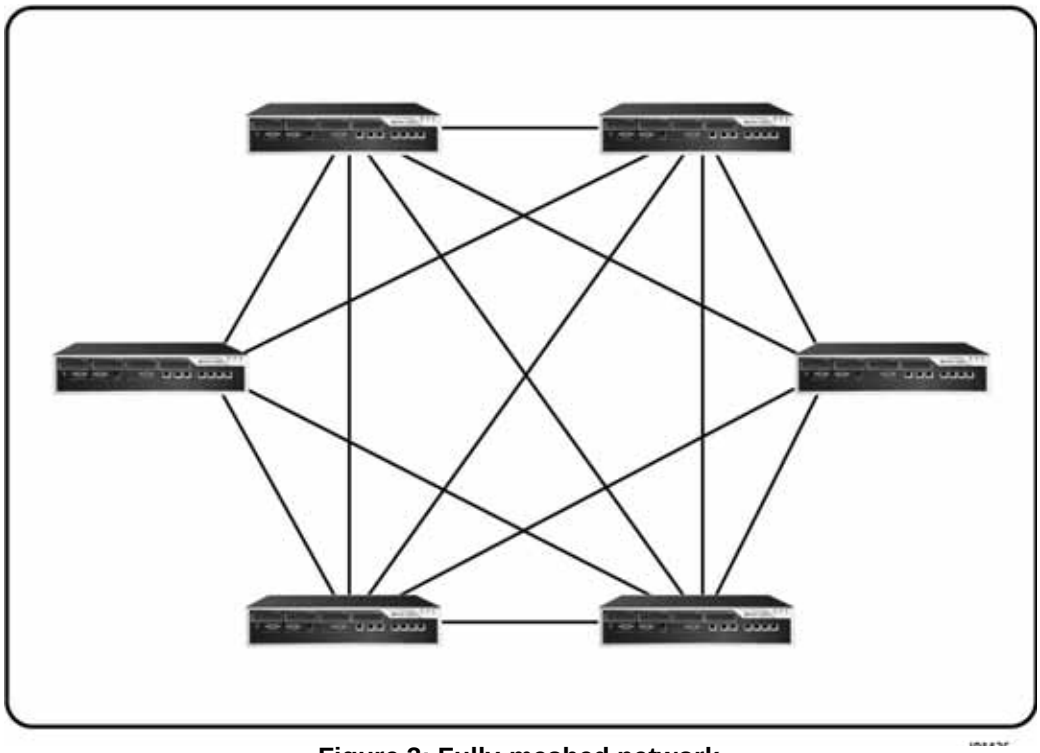

Figure 3: Fully-meshed network

In a fully-meshed network, every node is connected to every other node. The benefit of a fully-meshed network arrangement is that one, or even more than one, link can go down, and nodes can still reach each other—there are many alternative routes.

For deployments of 20 nodes or less, the fully meshed model is easy to deploy, but as each new node is added, there is additional management overhead on every existing unit to add the new IP trunk.

Every node requires N-1 IP trunk connections, so for 20 nodes, there are 380 IP trunks (20 x (20-1))—760 end-points—to be programmed.

For larger systems, especially for those with many smaller remote nodes, it may be more practical to deploy a hierarchical network.

In a hierarchical network, as shown in Figure 4, a central group of core routing controllers are fully meshed, but only one or two links are required to connect to the remote nodes, or to other applications. Adding a new node requires only an update at the central group and at the new remote site.

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

If you have the network set up with each MiVoice Business controller dedicated to a specific function, there is no need for a fully-meshed architecture.

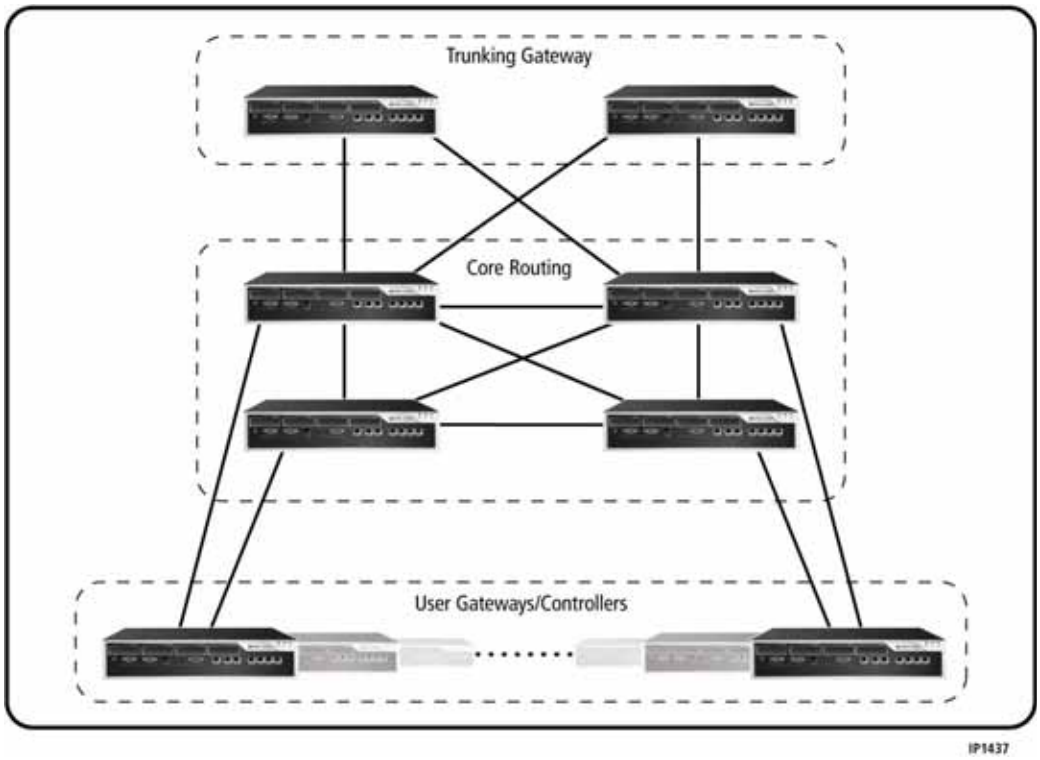

Figure 4: Hierarchical network

For systems that include more than twenty nodes, it is strongly recommended to follow the hierarchical network design. Twenty nodes is also the working limit of an Administration Group, and is a good point at which to break the system into distinct functions, as used within a hierarchical design.

It is still possible within a hierarchical design to mesh nodes within certain function groupings to simplify local call routing. For example, the core routing can be meshed, but the connections to the user gateways need to be limited to certain nodes. Likewise, there may be groupings of users within the user gateways, for example HQ versus a remote office, where local meshing would be more beneficial for local call routing.

For a large, potentially geographically dispersed, system, however, the hierarchal design is the recommended option. With the advent of cloud hosting and centralized SIP trunks, the hierarchical design also makes sense.

It is possible to mesh large systems, but experience has shown that it becomes cumbersome and difficult to install and maintain due to the increasing number of route configurations that are needed. Route configuration is also not shared through SDS, so must be manually completed on each node at both ends of the link.

An additional consideration is that only 249 external active trunks are possible from any one node, even if more routes are programmed. The default setting is that established routes will maintain connection once established, to minimize communication between nodes and time to make calls. This means that the first 249 routes will be established and any others will fail, resulting in failed calls and call blocking.

It is possible to overcome this “stickiness” of established IP-Trunk connections by setting the IP-Trunk timer to a low value, with one second being a recommended minimum value. This needs to be the same value at both ends of the trunk, as the higher value will take precedence. A link that is always established is considered to have infinite timeout, i.e. never clear. Earlier releases of Mitel Communications Director (MCD) software may not include an IP-Trunk timeout option. In this case, you use the ISDN timeout value, which will perform the same function for these releases.

Use of the timeout timer may introduce delays in establishing calls, and if an IP-Trunk is unavailable, it could result in call setup blocking. It is, therefore, not recommended for systems with high levels of traffic.

Use of the timeout timer results in more network communications between nodes to establish the initial connection, and to clear it after traffic is no longer carried on the link. For low bandwidth connections; for example, to a remote site, this increased traffic may result in additional bandwidth consumption, and increased performance impact on the controllers or gateways; that is, not for high traffic situations.

Multi-node Hospitality

There are three main architectures you can use in setting up a hospitality solution:

- Standalone

  In a Standalone hospitality solution, one Mitel 3300 ICP running MiVoice Business acts as the controller for the hotel or motel.

  - Networked Standalone: Standalone hospitality controllers each manage their own guest and staff groups, but they can be networked to exchange information. In this configuration, each controller has its own Property Management System (PMS) and each database is kept separate from all the others; there is no sharing among them.

- Clustered

  In this configuration, the MiVoice Business controllers are clustered so that hospitality features can be offered to large hotels or hotel chains that require multiple controllers.

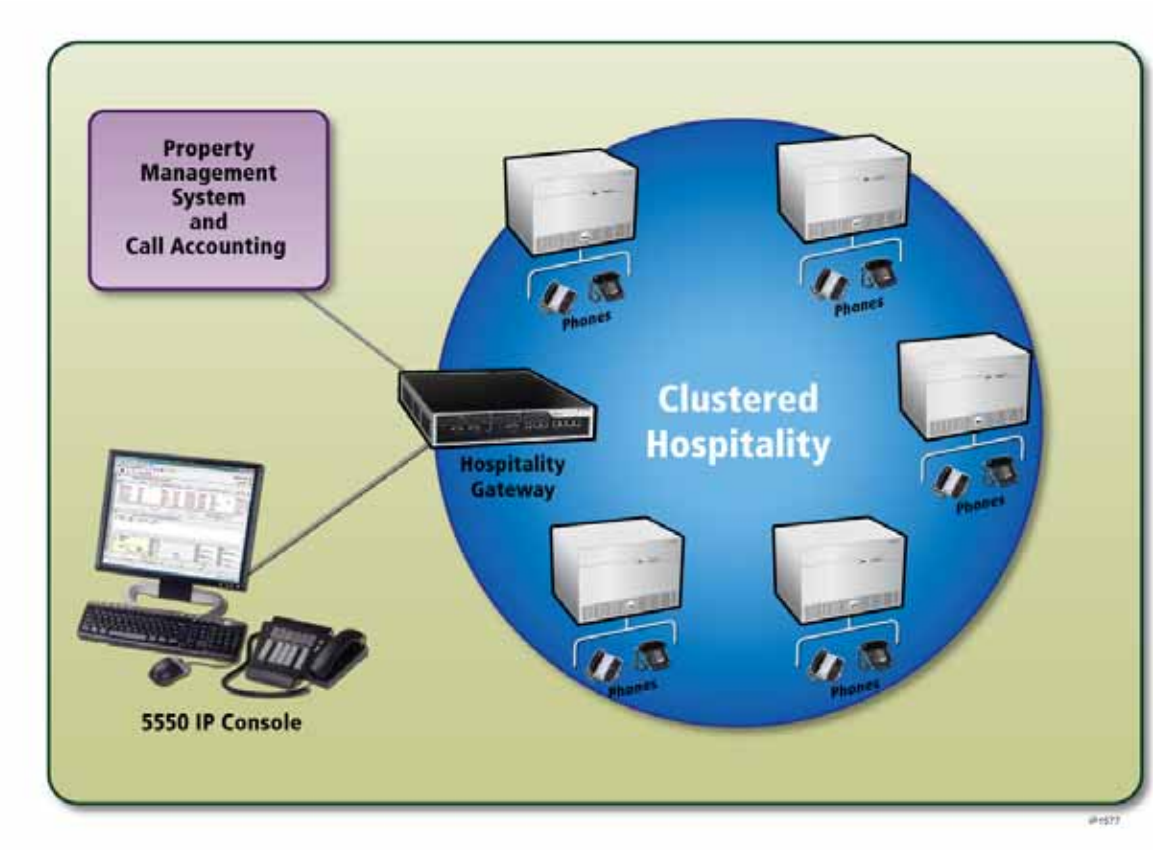

Figure 5: Clustered Hospitality components

- Centralized

  Calls come in through one MiVoice Business (running on ISS) or a Stratus Server, or occasionally, a 3300 ICP (MXe), and are sent to multiple AX controllers. The analog telephones are connected to the AX units. This provides support for large-scale analog

operations, while consolidating management to one console. This configuration also provides support for IP phones.

For more information about deploying a Hospitality network, refer to the *Hospitality Solutions Guide*.

Maintenance and troubleshooting

Voice system maintenance includes backup and restore, plus periodic log cleaning. Consider the following:

- Multi-node management (MNM) backup and restore allows you to perform database back-ups 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.

Note: Starting in MCD 6.0, anonymous FTP accounts are no longer supported on MXe Server, MiVoice Business Multi-instance, MiVoice Business on ISS, and MiVoice Business Virtual.

  - 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.
  - Back up individual machines from their local consoles.
  - Perform backups using MiVoice Enterprise Manager.
  - Perform backups through Software Installer (SI) Tool.

  When you restore a database, you can choose to restore the backup file from a drive on the local PC or from the FTP server.
- The number of logs generated depends on the logging settings. The MiVoice Business controllers generate many more logs in debug mode than they do in the default mode. Either way, the old log files should be removed periodically to reclaim disk space.

  You can back up old log files to tape or USB drive, or you can delete them. This should be a regularly scheduled task.

See Table 2 for a list of Mitel guides containing maintenance and troubleshooting information.

Table 2: Installation and Maintenance Guides

MITEL PRODUCT	GUIDE NAME
MiVoice Business	*MiVoice Business Installation and Administration Guide for Industry Standard Servers (ISS)* *MiVoice Business Troubleshooting Guide* *MiVoice Business Technician's Handbook*
MiVoice Business Multi-instance	*MiVoice Business Multi-instance Installation and Administration Guide*
MiVoice Business Virtual	*MiVoice Business Installation and Administration Guide for Virtual MiVoice Business Virtual*
MiCollab	*MiCollab Installation and Maintenance Guide*

Table 2: Installation and Maintenance Guides (continued)

MITEL PRODUCT	GUIDE NAME
MiCollab Unified Messaging (formerly NuPoint UM)	*MiCollab Unified Messaging Technician's Handbook*
MiContact Center Office (formerly Customer Service Manager)	*MiContact Center Office Technician's Handbook*