UC Enterprise Solution

BLUEPRINT

Release 3.0

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

Mitel and MiCollab Unified Messaging are trademarks of Mitel Networks Corporation.

Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Blackberry® is a registered trademark of Research in Motion Incorporated.

Google®, and Android™ are registered trademarks of Google Incorporated.

Hewlett-Packard, HP, and the HP logo are all registered trademarks of the Hewlett Packard Company.

iOS®, iPAD®, iPhone®, and Apple® are registered trademarks of Apple Incorporated.

Microsoft®, Microsoft Active Directory are registered trademarks of Microsoft Corporation.

Salesforce®, and Salesforce.com are registered trademarks of Salesforce.com Incorporated.

Sun Microsystems, Sun, and the Sun logo are all registered trademarks of Oracle Sun Microsystems Inc.

VMware, VMware vMotion, VMware vCloud, VMware vSphere, ESX, and ESXi are trademarks of VMware Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

UC Enterprise Solution Blueprint
Release 3.0
September 2018

CHAPTER 1: UC ENTERPRISE SOLUTION OVERVIEW

CHAPTER 2: UC ENTERPRISE SOLUTION TOPOLOGIES

CHAPTER 3: APPLICATIONS

CHAPTER 4: END-USERS AND DEVICES

CHAPTER 5: AVAILABILITY AND RESILIENCY

CHAPTER 6: TRAFFIC AND SCALING CONSIDERATIONS

CHAPTER 7: EXTERNAL CONNECTIVITY

CHAPTER 8: MANAGEMENT CONSIDERATIONS

CHAPTER 9: NETWORK AND NETWORKING CONSIDERATIONS

CHAPTER 10: LICENSING CONSIDERATIONS

APPENDIX A: GLOSSARY

Chapter 1

UC ENTERPRISE SOLUTION OVERVIEW

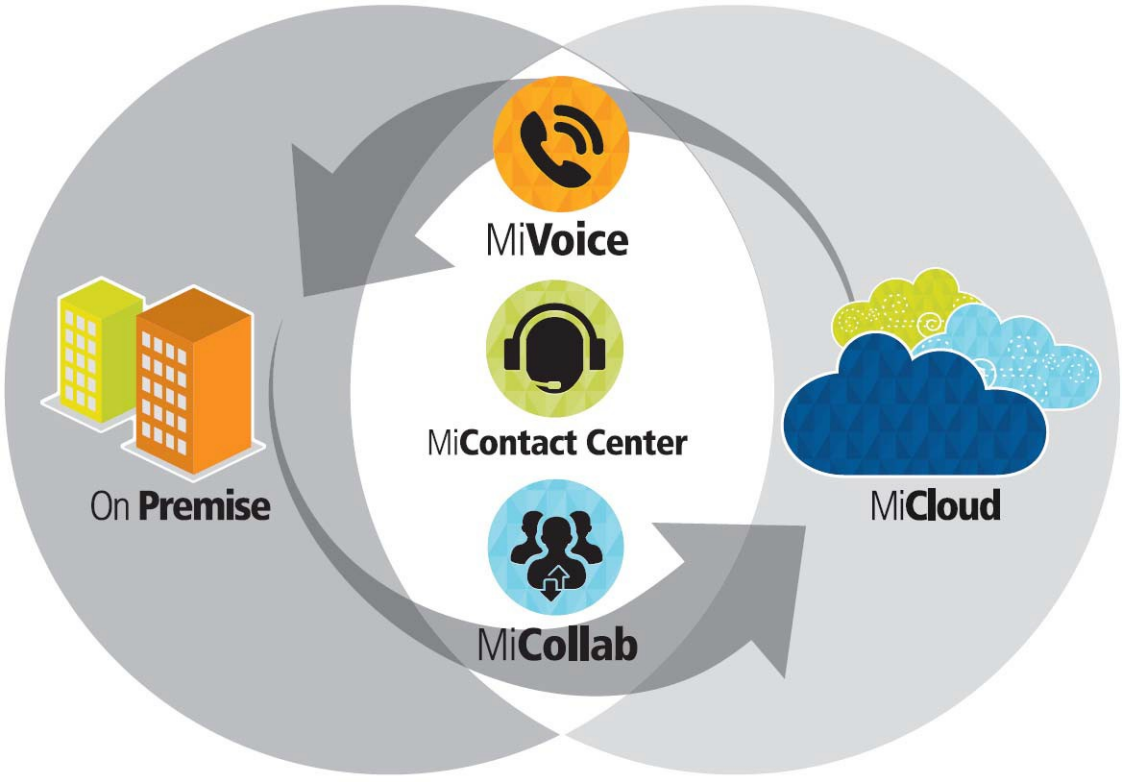
INTRODUCTION

UC Enterprise Solution is a Mitel unified communications (UC) solution built on Mitel's MiCollab and MiVoice Business capabilities. The Mitel UC portfolio includes cloud and premise-based solutions for service providers and enterprises. Mitel UC solutions are easily adapted or scaled to match the changing demands and needs of the hosted market, the enterprise, and the end-user.

Selecting the most appropriate cloud or premise solution requires identifying all of the stakeholders involved in the delivery of the UC solution. A topology can be selected after evaluating each stakeholder's requirements. The Mitel UC solution architecture offers customers the freedom to move between premise-based and cloud strategies with changing business priorities.

Mitel solution architecture encompasses a full suite of Unified Communications and Contact Center solutions. This blueprint focuses on the enterprise deployments of MiVoice Business centric UC solutions. For service providers, MiVoice Business centric UC solutions are covered in the solution guide, *MiCloud Business Solution Blueprint*. Contact Center solutions are covered in the solution guide, *Mitel Contact Center Blueprint*.

Figure 1: Mitel Solution Architecture



UNIFIED COMMUNICATIONS

Unified communications (UC) is a term that implies the real-time integration of voice, data, and video communication. Without UC, a user's voice mail, e-mail, video conferencing, voice

conferencing, text chatting, and desktop sharing applications are independent and require separate interaction.

A rich UC solution delivers a user experience that integrates all the user's communication tools into a unified experience. With a UC solution a user can seamlessly choose the medium they want to use without impacting the medium that other participants are using. For example, users may attend a meeting from different locations using a combination of text, voice, or video technologies without impacting the other attendees. Combined with real-time presence, each participant knows what options they have for communicating with another participant. UC provides a user with a consistent unified experience across multiple devices and media-types.

WHY DEPLOY A UC SOLUTION?

Adopting a unified communications solution improves employee productivity and consolidates infrastructure, but a UC solution is more than a telephony upgrade or a consolidation of applications. UC solutions evolve how, when, where, and even what communication takes place in an organization.

The digital age has created a culture where end-users are constantly 'plugged in', almost regardless of where they are. In a crisis, consumers are connected to multiple resources, requesting help, and monitoring multiple communication channels for responses. Mining for information to solve a problem is not necessarily limited by time of day or location.

UC solutions provide the tools to respond immediately, with the most appropriate content, over the most effective channel. Remote conversations that begin with instant messaging or texting, can switch to voice calls, exchanging electronic files, or even a conference call with other team members using video and voice. Coordinating presence, calendars, and geo-location can result in face-to-face meetings to find a resolution.

UC solutions impact the productivity of teams and employees. For example, UC solutions enable:

- Increased mobility of the workforce, yet with an ability to still work with co-workers when not in the office.
- Bursting capabilities that allow off-site personnel to handle bursts of business traffic without physically being present in the office.
- Working remotely to accommodate travel and personal issues such as school cancellations and home repairs.
- Individually tailored communications environment from any desk at head office, branch offices, or remotely.

UC SOLUTION STAKEHOLDERS

The combination of on premise, virtualized platforms, and hosted service capabilities creates a broad spectrum of stakeholders in the UC marketplace. Mitel's flexible UC solution architecture is an opportunity for organizations to specialize their offers and expertise or widen their business models and operate in multiple capacities as one or more of the following roles.

- Service providers (SPs) either maintain their own data center or purchase resources from a data center to offer hosted services. Service providers manage the applications and images and either engage end-customers directly or wholesale service blocks to virtual

service providers (VSPs). Service providers may also engage value added resellers (VARs) to sell their hosted solutions.

- Enterprise customers define their service requirements and choose between premise-based, private cloud, and shared cloud solutions. Investment mix and the extent the Enterprise can control the system varies with each solution. When using a hosted solution, enterprise customers may perform some application management at their organizational level. Enterprise customers are not resellers of their purchased UC services. Component ownership does not prevent an enterprise from engaging service providers to manage their systems as a professional service.
- Value added resellers (VAR) act as agents to sell solutions bundled with their own value added services. Typically VARs, acting as Mitel agents, engage Enterprise customers who are purchasing their complete solution. Hosted solutions create opportunities for resellers to act as agents for service providers as well.
- Virtual service providers purchase wholesale services from SPs and offer their services to end-customers directly. A VSP manages the solution at the application layer at each customer or VAR instance.
- Users are the UC service consumers. Users may be associated with an enterprise that has a premise-based system or associated with an enterprise that is buying hosted services from a service provider.
- Data centers provide floor space or servers for hosting virtual machines and applications. A data center offers expertise at an operating system level and typically does not manage any features within the applications or images.

Software as a Service

Software as a Services (SaaS) is an industry term for cloud services that offer end-customer applications or functions as a service. The Mitel UC portfolio enables service providers to build SaaS offers spanning voice-centric to UC intensive services.

For example, a SaaS arrangement occurs when an end-customer pays a service provider every month for 30 extensions. Each extension includes voice-mail, presence, and instant messaging. The end-customer does not have any equipment installed at their site except for desk phones that connect into their IP infrastructure. This model is a service provider cloud offering not appropriate for an enterprise deployment.

Platform as a Service

Platform as a Services (PaaS) is an industry term for cloud services offering a complete solution that includes the middleware and operating system layers, and in some cases applications, as well as any additional resources like storage and network devices.

PaaS customers are charged for a complete instance of the solution. The PaaS provider will scale resources to match application demand so that the cloud user does not have to allocate resources manually.

For example, a PaaS arrangement occurs when a service provider offers Mitel UC capabilities based on a private cloud deployment. The end-customer pays the service provider relative to the capacity they are leasing.

Unified Communications as a Service

Unified Communications as a Service (UCaaS) refers to cloud services that offer Unified Communications as an application layer solution built by a service provider and managed by the UCaaS customer, typically another service provider. This is a type of Platform as a Service offering customized for Unified Communications service providers. Mitel offers UCaaS, sometimes referred to as “Mitel built, partner managed”. This offer is targeted to service providers rather than end-customers.

Infrastructure as a Service

Infrastructure as a Services (IaaS) is an industry term for cloud services offering computing resources, using physical or virtual machines. IaaS providers pool data center resources to support large numbers of virtual machines for scaling services up and down according to customers' changing needs. IaaS solutions may offer additional networking and storage resources on-demand.

IaaS customers install and manage their application software on the cloud infrastructure and the IaaS provider patches and maintains the virtualized infrastructure and physical machines.

For example, an IaaS arrangement occurs when an end-customer leases server space from a data center provider for hosting a Mitel UC solution in a private cloud. The end-customer is responsible for managing the UC platforms.

MITEL UC PORTFOLIO OVERVIEW

Determining the best topology to fit your business model starts with looking at Mitel’s UC portfolio relative to three distinct customer markets.

- MiCloud Business enables service providers to offer UC services to a broad range of customers ranging from small businesses to large multi-site enterprises. The topologies are optimized for different market segments characterized by their end-customer line sizes, the richness of the UC feature set, and the capabilities of the service provider's data center.
- UC Enterprise Solution topologies are designed for enterprise customers requiring greater ownership and control of their UC solution. Enterprise UC topologies are on-premise and data center solutions that can include private clouds and shared services.
- Mitel also offers contact center solutions with rich UC capabilities.

Mitel UC solutions include a range of call control platforms and application offers. This document focuses on the MiVoice Business centric solution offer.

BUSINESS CONSIDERATIONS

In addition to technical requirements, many business considerations will have a bearing on the choice of deployment topology. Some aspects to consider include:

- How the topology scales and the impact on ROI.

- The capability of the topology to meet expected service level agreements.
- The training, skills, and staffing needed to support the solution and provide customer support.
- The preferred end device management strategy (purchase, lease, returns) for end-customers.

This is not an exhaustive list but rather a few key aspects. This document focuses on the technical considerations for the choice of topology.

UC SOLUTION DOCUMENTATION

This solution blueprint documents Mitel designed topologies for enterprise UC solutions in the medium to large enterprise market. The topologies are reference designs to address the requirements of typical end-customers. The blueprint describes the architecture, capabilities, and capacities of each topology and is an essential document for anyone who is scoping, comparing, designing, and planning a cloud UC deployment.

The UC Enterprise Solution topologies are designed to successfully address the requirements of most deployments. Mitel Professional Services are available to help engineer the topology details when unique business requirements create a need for a variation to one of the documented topologies.

Blueprint documents do not include deployment instructions, pricing, order codes, or release note details. Mitel documentation is available online from Mitel-On-Line (MOL).

A blueprint document exists for each of the UC solutions.

- *MiCloud Business Solution Blueprint*
- *Enterprise UC Solution Blueprint* (this document)

Deployment guides for selected UC solutions provide high-level requirements, specifications, networking considerations, best practices, and other useful references to plan and implement a successful solution deployment. The following documents exist to support your UC solution.

- *MiCloud Business Solution Small Business Deployment Guide*
- *MiCloud Business Solution Medium Large Business Deployment Guide* (this service provider topology is similar to the Private Cloud topology)
- Product documents are also required for designing and using your UC system. Product specific documents are available from Mitel-On-Line (MOL).

UC ENTERPRISE SOLUTION

UC Enterprise Solution is a Mitel solution for deploying and managing Unified Communications (UC) services for Enterprise customers. Mitel offers UC solutions based on several call control platforms. This blueprint focuses on UC Enterprise Solution topologies built on MiVoice Business platforms with MiCollab, offering UCC services ideal for mid-size and large businesses.

WHO IS THE UC ENTERPRISE SOLUTION CUSTOMER?

UC Enterprise Solution topologies are designed for Enterprise customers that are intent on maintaining and enhancing their competitive edge through capital expenditures on communication solutions.

UC Enterprise Solution customers will realize a fast return on their investment due to the enhanced business communications and collaboration capabilities of the solution, which in turn will allow for increased employee effectiveness and higher levels of customer satisfaction.

UC ENTERPRISE SOLUTION CAPABILITIES

- Predictable service levels and operational expenditure
- The UC Enterprise Solution is built on the solid legacy of Mitel's field proven call control software - MiVoice Business.

MiVoice Business is the foundation that allows for the seamless integration of voice, e-mail, unified messaging, mobility, presence, conferencing, contact center applications, and more – enabling faster, more effective communication.

MiVoice Business is a single software stream that supports a range of deployment models: distributed, centralized, and cloud, or hybrid.

MiVoice Business can be deployed on the hardware platform that best fits the specific requirements: MiVoice Business 3300 Controllers, Industry Standard Servers (ISS), or a virtualized version (MiVoice Business Virtual) that is deployed on a server that is running VMware. If a customer evolves from one deployment model to another, software licenses are portable from one deployment model to another – delivering a strong and future-proof total cost of ownership (TCO).

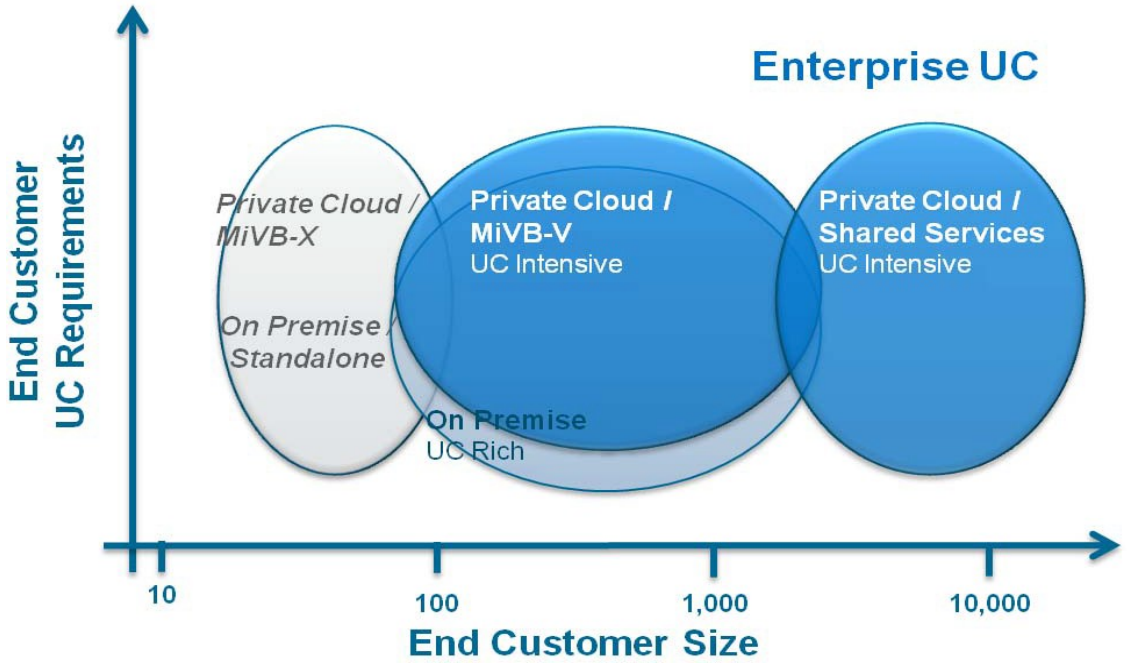
UC Enterprise Solution supports resilient operation of both user controllers and trunking gateways to ensure system availability and business continuity.

The UC Enterprise Solution supports:

- Business ranging in size from 100 users to over 10,000 users
- Single site and multi-site deployments
- On-Premise and Private Cloud deployments
- MiCollab UCC applications
- Mitel MiNet and SIP telephones, including SIP ATA devices
- Generic SIP telephones
- MiVoice Conference Unit
- MiVoice Video Unit

Third-party SIP video end-points and video conferencing services. The figure "UC Enterprise Solution topologies Comparison" on page 9 can be used to determine which UC Enterprise Solution topology is most suitable for a specific customer. The determination should be based on that customer's UC requirements and the number of end-users.

Figure 2: UC Enterprise Solution Topologies



KEY UC ENTERPRISE SOLUTION TOPOLOGIES

UC Enterprise Solution supports a wide range of features and network configurations. It is best to deploy a UC Enterprise Solution using the topology that most appropriately meets the customers's specific requirements. This document focuses on three UC Enterprise Solution topologies:

- On-Premise
- Private Cloud
- Private Cloud, Shared Services

The table "UC Enterprise Solution topologies" on page 9 shows all UC Enterprise Solution MiVoice Business centric topologies. The On-Premise, Private Cloud, and Private Cloud, Shared Services topologies, highlighted in green, are discussed in this document. Refer to the *MiVoice Business Engineering Guidelines* or contact Mitel Professional Services for information regarding the topologies that are not discussed in this document.

Table 1: UC Enterprise Solution topologies

NUMBER OF USERS	ON PREMISE DEPLOYMENTS	DATA CENTER DEPLOYMENTS
Fewer than 100	Standalone controller	MiVoice Business Express
100 to 2500 (centralized deployments)	On-Premise	Private Cloud
100 to 2500 (distributed deployments)	Geographically distributed medium to large	MiVoice Business Multi-Instance-based
2500 to 100000	Geographically distributed very large	Private Cloud, Shared Services

The table "UC Enterprise Solution topologies Comparison" on page 9 compares the three topologies described in this blueprint for several key deployment considerations.

Table 2: UC Enterprise Solution topologies Comparison

UC ENTERPRISE SOLUTION			
TOPOLOGY	**ON-PREMISE**	**PRIVATE CLOUD**	**PRIVATE CLOUD, SHARED SERVICES[1]**
Market segment size	• Typically 100 - 2500 users • Can scale to 3000 users	• Typically 100 - 2500 users • Can scale to 3000 users	• Typically 1000 - 5000 users • Multiple BUs up to 3000 users each • Can scale to 10000+ users
Sites per end-customer	Single	Multiple	Multiple
Services	UCC	UCC	UCC
Business voice platform	• MiVoice Business • MiVoice Business for Industry Standard Servers (ISS) • MiVoice Business Virtual • MiVoice Business Express	• MiVoice Business • MiVoice Business Virtual	MiVoice Business Virtual
UC applications platform	• MiCollab • MiCollab Virtual • MiVoice Business Express	MiCollab Virtual	MiCollab Virtual, per BU
Management platform	Mitel Performance Analytics	Mitel Performance Analytics	Mitel Performance Analytics
Access network	Not applicable	MPLS	MPLS

[1] Requires Mitel Professional Services

ON-PREMISE

The On-Premise topology is intended for applications where there are 100 to 2500 users located at one central site. This topology allows the customer to control their own network from end-to-end. All equipment is physically on site, on the customer's premises, including video and telephony end-points, user controllers, trunking gateways, Mitel MiVoice Border Gateways, business applications, and UC applications.

PRIVATE CLOUD

The Private Cloud topology is intended for applications where there are 100 to 2500 users. End-users could be located at one site or distributed across a few different sites. The Private Cloud topology allows the customer to locate the majority of their equipment in a centralized location such as their data center or in a private cloud. User controllers, trunking gateways, Mitel MiVoice Border Gateways, business applications, and unified communications applications can all be private cloud-based.

Video and telephony end-points are located with employees at the customer's site or sites. Communication between the customer sites and the private cloud is via an MPLS network.

MiVoice Business can be deployed on a Mitel ICP with PSTN connectivity at a customer site. This deployment is capable of local PSTN breakout or local survivability in the event of an MPLS network outage.

PRIVATE CLOUD, SHARED SERVICES

The Private Cloud, Shared Services topology is intended for applications when there are 2500 to over 10,000 end-users, distributed across multiple sites. The Private Cloud, Shared Services topology builds on the Private Cloud topology by deploying voice and UC services in blocks that support up to 2500 users.

This topology allows the customer to locate the majority of their equipment in a centralized location such as their data center or in a private cloud. User controllers, trunking gateways, Mitel MiVoice Border Gateways, business applications, and unified communications applications can all be private cloud-based.

Video and telephony end-points are located with employees at the customer's site or sites. Communication between the customer sites and the private cloud is via an MPLS network.

MiVoice Business can be deployed on a Mitel ICP with PSTN connectivity at a customer site. This deployment is capable of local PSTN breakout or local survivability in the event of an MPLS network outage.

Note: This topology requires engaging Mitel Professional Services to assist with the design and implementation.

Chapter 2

UC ENTERPRISE SOLUTION TOPOLOGIES

UC ENTERPRISE SOLUTION TOPOLOGIES

UC Enterprise Solution topologies are a number of different Mitel Unified Communications reference designs to meet service provider and customer requirements, network connectivity requirements, and system Unified Communications scaling. The solutions cover scaling from a few users up to and beyond 10,000 users. Each user may also be associated with multiple devices.

The topologies also include different virtualization technologies, and in many cases a mix of technologies, to take advantage of different features. The applications and call server platforms range from on-premise servers and appliances, through Mitel optimized virtual call servers, to virtualized application packages running on VMware virtual platforms.

The “Key Topology Components” on page 13 describes the purpose of each technology component that may be used in one or more topologies.

The UC Enterprise Solution topologies are:

- “On-Premise” on page 19
- “Private Cloud” on page 30
- “Private Cloud, Shared Services” on page 42

KEY TOPOLOGY COMPONENTS

The UC Enterprise Solution topologies are based on a common set of solution components. The key components include:

- **MiVoice Business**
  Mitel’s feature-rich communications system providing IP telephony with seamless IP networking and SIP trunking. MiVoice Business offers over 500 telephony features provided to users through easy-to-use phones and web-based user desktop interfaces. MiVoice Business is available on different platforms tailored for different market segments.
- **MiCollab**
  MiCollab unifies Mitel applications into an easy to use, cost effective communications solution. End-users have a single point of access to all their Mitel applications through the My Unified Communications portal, a web-based interface. MiCollab may be deployed with multiple applications per server or with a single application per server when increased capacity is required.
- **MiVoice Border Gateway**
  MiVoice Border Gateway is a specialized application proxy supporting SIP, MiNet, and web protocols. MiVoice Border Gateway may be deployed as a Server-Gateway, in a Demilitarized Zone (DMZ), or within the LAN when used for connection to call recording equipment.
- **Management Applications and Tools**
  Comprehensive solution management includes tools for configuration, maintenance and trouble shooting. Rich administrative interfaces are provided with different capabilities tailored to the service provider, customer administrator and end-user.

- **Mitel End-points**
  Mitel offers a range of desk phones, soft phones, wireless phones and web-based applications to suit user communication preferences.

The solution components are available in several packages and/or configurations optimized for different network and system requirements. These variations are reflected in the component selection and network design for the topologies described in the following sections.

The table "Topology Components" on page 14 describes the components used in the topologies as well as their purpose and functionality. The table may describe a wider range of functionality than is used within any particular topology. Also, some components may not be used in all topologies.

Each topology description provides further details on how each component is used in the context of that topology.

Note: Some infrastructure components, such as Layer 2 switches and routers, are not included or described in the table.

Table 3: Topology Components

COMPONENT	FUNCTION
MiVoice Business 3300	Call control engine on dedicated hardware providing: • Proprietary application platform for running MiVoice Business software • IP to PSTN gateway (analogue and digital/PRI) • Analogue and TDM phone connectivity • Built in applications including voice mail, music on hold, ad-hoc conference, basic call recording • Access to different scaling platforms, with increasing scaling levels of analogue/digital and PSTN connectivity
MiVoice Business EX Gateway	Call control engine on dedicated hardware providing: • Proprietary application platform for running MiVoice Business software • IP to PSTN gateway (analogue and digital/PRI) • Analogue phone connectivity • Built in applications including voice mail, music on hold, ad-hoc conference, basic call recording
MiVoice Business ISS	Call Control engine running on Industry Standard Servers providing: • MiVoice Business call control software and integrated media services that run on an Industry Standard x86 Servers • A rich communications system including access to SIP trunk • Scaling via seamless IP-networking
MiVoice Business Virtual	Call Control engine running in a VMware virtual environment providing: • MiVoice Business call control software and integrated media services that run on an VMware virtualization platforms • A rich communications system with access to SIP-Trunks • Scaling via seamless IP-networking • Scaling through defined deployment configurations

MiVoice Business Multi-Instance	Mitel optimized virtual platform for Call Control instances, providing: • High density of virtualized MiVoice Business • Isolation of individual and multiple MiVoice Business units from neighbors through use of native VLAN configurations. • Associated and individual media services on separate servers

Table 3: Topology Components

COMPONENT	FUNCTION
MiVoice Border Gateway	MiVoice Border Gateway is a specialized application proxy supporting SIP, MiNet, and web protocols. Some of the key functionality provided by MiVoice Border Gateway includes: • Teleworker service for connection to remote SIP and MiNet end-points • SBC functions and SIP trunk proxy for connection to external third-party SIP providers • Web proxy for externally connected devices such as: MiCollab mobile clients and softphones, management access, and access to LAN-based applications. • Use with Secure Recording Connector (SRC) is mutually exclusive with border gateway functions and deployed on a per customer basis. Use with SRC is included in the Contact Center Blueprints.
SBC	This is the access point into the SIP Trunk service provider for network isolation. The MiVoice Border Gateway is used in a similar manner for customer and service provider connections
MiVoice Business Express	This is a combined Unified Communications and Collaboration package that runs in a VMware virtualization environment, providing: • Call Control via MiVoice Business Virtual • Unified Communications and Collaboration in MiCollab • Border gateway via MiVoice Border Gateway • Single OVA package, scalable through pre-defined deployment configuration settings
MiCollab	MiCollab unifies Mitel applications into an easy to use, cost effective communications solution. End-users have a single point of access to all their Mitel applications through the My Unified Communications portal, a web-based interface. MiCollab provides co-residency of applications to support: • MiCollab Client Service • MiCollab Audio, Web, and Video Conferencing • MiVoice Border Gateway • MiCollab Unified Messaging
MiCollab Client Service	MiCollab Client Service is an application within MiCollab that provides Presence information for all UC users as well as providing PC softphone and Mobile softphone clients.
MiCollab Client	The MiCollab Client connects to the MiCollab Client Service, part of the MiCollab server. It provides telephone presence and dialling capabilities for the end-user. The MiCollab Client is used as a separate client with a hard phone, with the PC softphone and also with the mobile softphone. • Static softphones within the customer network must be registered with the MiCollab Client Service directly on the customer LAN • Mobile softphones outside of the customer network must be registered with the MiCollab Client Service via the external teleworker MiVoice Border Gateway • Mobile softphones registered via the MiVoice Border Gateway may continue to consume Internet connection bandwidth when used within the customer premises.

Table 3: Topology Components

COMPONENT	FUNCTION
MiCollab Audio, Web, and Video Conferencing	MiCollab Audio, Web, and Video Conferencing is a Unified Communications Conference Unit within MiCollab that provides the ability to provide internal and external conferences of one to many users for voice, video and presentation.
MiCollab Unified Messaging	MiCollab Unified Messaging is a Unified Communications voice mail application within MiCollab whose features include, but not limited to: • Voice mail • Text to speech when integrated with e-mail • E-mail notification of voice mails • Auto-attendant and voice recognition (available as an add-on feature) • Visual voice mail
MiCollab Speech Auto Attendant	MiCollab Speech Auto Attendant is a feature within MiCollab Unified Messaging to provide automatic routing of calls based on spoken commands or dialled digits. MiCollab Speech Auto Attendant is only available as a stand-alone application, or as an optional add-on when used with MiCollab.
Mitel Open Integration Gateway	Mitel Open Integration Gateway provides a proxy for connection to Customer Relationship Management (CRM) business applications, including integration with: • MiVoice Integration for Salesforce • MiVoice Integration for Google Mitel Open Integration Gateway can also be used by customer specific applications for better integrations of UCC to business operations. (For example, call handling, click to dial, etc.)
Mitel Management Portal	Mitel Management Portal is a tool for provisioning users and settings on MiVoice Business and MiCollab applications. Mitel Management Portal provides capability for: • Service providers to provision customers • Resellers to provision customers from service provider templates • Customer self-service • End-customers can be granted access to specific aspects of their configuration information • End-customers can be granted privileges to customise aspects of their phone service. • Different management levels are provided for end-users and customer administrators The level of provisioning and user capability is defined within Mitel Management Portal templates, from full access to limited and targeted access.
Native Management	This is a direct management interface to the individual products, including: • Individual applications • Network and virtualization infrastructure • Call control engines. These interfaces are used to initially provision and connect applications prior to connection via Mitel Management Portal, e.g. to configure resiliency and single access sign-on.

Table 3: Topology Components

COMPONENT	FUNCTION
Mitel Performance Analytics and MPA Probe	The Mitel Performance Analytics application uses a probe called the MPA Probe, which is a virtual probe that collects fault and performance data for Mitel components and selected network devices. The Mitel MPA Probe reports product integrity and performance, and includes the following: • The MPA Probe is a diagnostic tool deployed at any location in the network where specific monitoring is required • For service providers, a publicly-accessible Mitel Performance Analytics server needs to be deployed for this service. • For on-premise, or Enterprise deployments, the hosted public server portal may be used. • MPA Probe collects call quality information from the individual MiVoice Business and generates alarm indicators when quality falls below specified thresholds. • MPA Probe monitors the activity of the topology components, including network equipment, and provides alarm indications when units are out of service or reaching performance thresholds. • MPA Probe can be deployed within individual customer networks when more specific monitoring is required. • MPA Probe can be deployed in the service provider network to monitor product integrity, performance, and user call quality from individual MiVoice Business • Reports are sent to a central Mitel Performance Analytics cloud server, via the Internet connection, or to a locally provisioned Mitel Performance Analytics server with the service provider. Further details on Mitel Performance Analytics components are available from Mitel Edocs.
Business applications/Virtual business applications	These are customer-specific business applications that the UC system may need to be aware of, or to integrate with. It may include, but not be limited to: • E-mail, and integration with voice mail • Customer Database • Directory Services • Web Services

Table 3: Topology Components

COMPONENT	FUNCTION
Internet	This provides default connections between multiple carriers and networks, and global access to services. The Internet provides a best-effort service level with varying bandwidth connections. Some global connections may offer high bandwidth connections while others may have more restricted options. Also referred to as Over-the-Top (OTT) connections for services that are able to traverse multiple and different carrier networks. Used for: • Public User Gateway access • Management Portal global access • License confirmation • Simple set deployment with Mitel Redirection and Configuration Service server • General Customer Web access, including connections to public services with Mitel Open Integration Gateway
MPLS	This is a dedicated and secured network connection from the hosted site to the customer site. It also provides: • Isolation from the public network • Isolation between different customers • Cross connection for multiple customer sites as a single network • Ability for the Network provider, or carrier, to provide QoS and Service Level Agreements (SLA) on data delivery that could not be guaranteed over the Public Internet
SIP Trunk Provider	The SIP service provider provides IP connected SIP trunks, either for the UC service provider, or for the customer, depending upon configuration of the network. It includes: • DDI/DID numbers that are hosted or assigned by the SIP serviceprovider • SIP to PSTN access • IP Network isolation via an SBC • Billing • E911 location information
Teleworker (Public Network)	This is connectivity for Teleworker phones. This access is typically over the Public Internet connection, or over a publicly-accessible network.
PSTN	The Public Switched Telephony Network is the existing and legacy voice network using time and circuit switched technology.
Mitel Redirection and Configuration Service	Public Internet accessible server that allows simple deployment of phones for Internet/Over-the-Top (OTT) deployments by providing redirection information to the service provider user gateway.

ON-PREMISE

The On-Premise topology is intended for applications where all the users are located at one central site. All equipment and applications are physically located at the customer's premises. This allows the customer to control their own network from end-to-end.

The following sections provide further information for evaluating the On-Premise topology to determine if it is a suitable solution for meeting the customer's needs.

ON-PREMISE TOPOLOGY BUSINESS AND SALES GUIDE

The UCC Enterprise solution, when deployed as per the On-Premise topology is intended for customers that have the following requirements and preferences:

- The customer's business operations are located at a single site
- The customer preference is to have the entire UC solution located at their premises
- The number of users ranges from 100 to 2500
- In addition to basic telephony services, the users require varying levels of Unified Communications and Collaboration services
- The customer requires high service availability for telephony, but not necessarily for applications
- The customer prefers to own the entire UC solution themselves
- This deployment is a CAPEX business model
- The customer would like to either manage the UC solution themselves, or to contract a third-party VAR to manage the UC solution on their behalf

ON-PREMISE TOPOLOGY ARCHITECTURE

The On-Premise topology architecture is based on voice-centric components, and Unified Communications and Collaboration (UCC) components. The main voice component is the Mitel MiVoice Business application, which depending on the number of end-users, could be running

on a 3300 ICP platform, an MiVoice Business-EX gateway, an Industry Standard Server (ISS) or also as a virtualized application in a VMware environment. Unified Communications and Collaboration services are provided by applications running on the MiCollab server.

The table “On-Premise Topology Components” on page 20 explains the context of each component in the “On-Premise Topology Diagram” on page 20.

Figure 3: On-Premise Topology Diagram

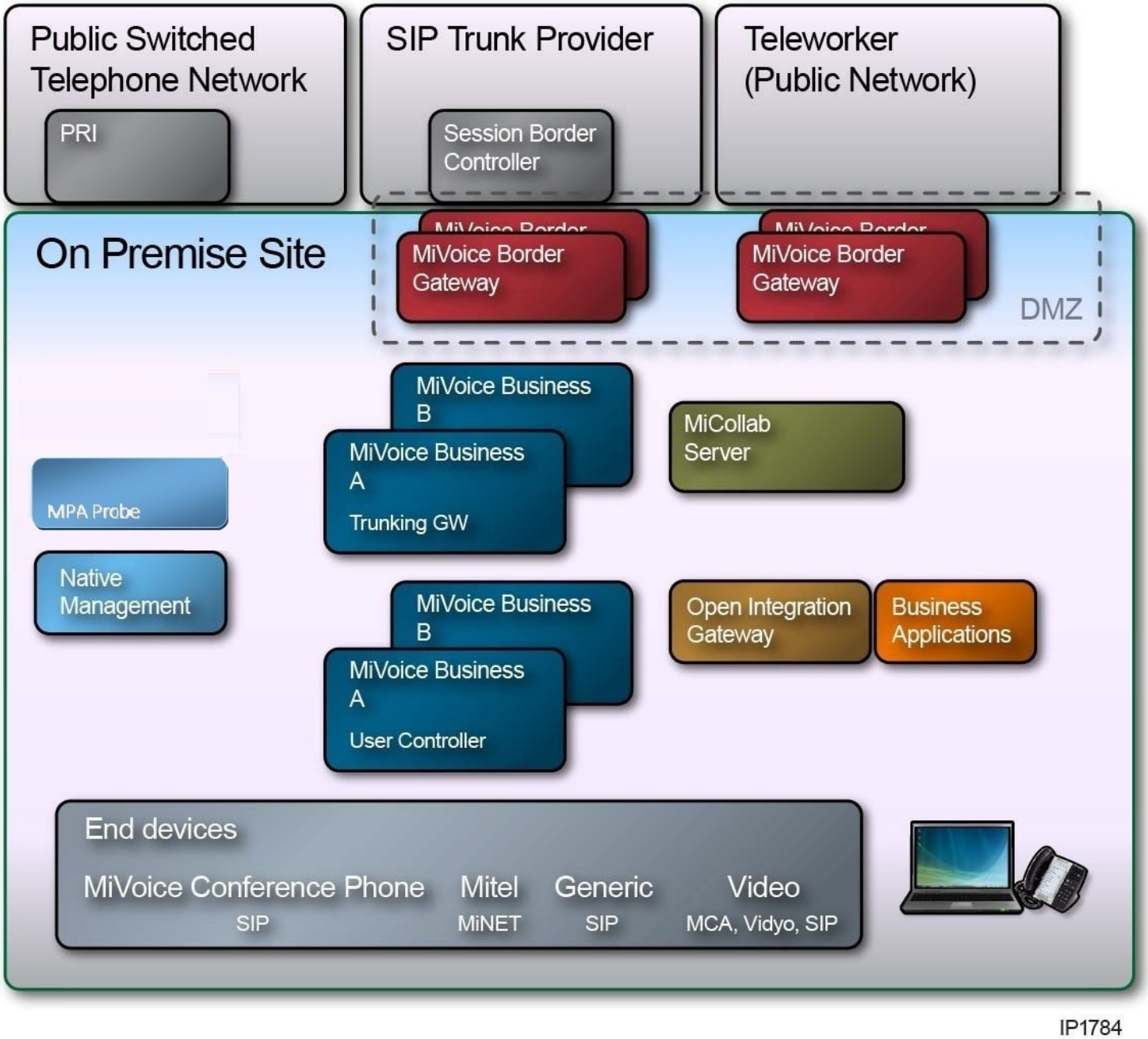


Table 4: On-Premise Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
MiVoice Business - User Controller	The MiVoice Business user controllers perform telephony call control and media handling. • MiVoice Business user controllers are clustered for scaling and resilient operation. • Depending on the scaling requirements, the MiVoice Business software may be installed on a MiVoice Business 3300 ICP or on an ISS/VMware platform.

Table 4: On-Premise Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
MiVoice Business - Trunking Gateway	The MiVoice Business trunking gateway is a 3300 ICP or EX platform running MiVoice Business software. • Multiple MiVoice Business trunking gateways are deployed for scaling purposes and also for resilient operation. • The MiVoice Business trunking gateways provide connectivity to the PSTN - via PRI trunks - and also to the SIP service provider, via the MiVoice Border Gateways and SIP trunks. • The MiVoice Business trunking gateways use ARS programming to determine which trunking connection should be used for a particular call.
MiVoice Border Gateway	The Mitel MiVoice Border Gateway is a specialized application proxy supporting SIP, MiNet, and web protocols. The On-Premise topology uses two groups of MiVoice Border Gateways located in the DMZ. The first group of MiVoice Border Gateways are used to provide connectivity to the SIP trunk service provider. • The MiVoice Border Gateways are deployed at the customer premise network edge, along with fire walls and the SIP trunks connect to an SBC which is located at the SIP trunk provider's facilities. • The MiVoice Border Gateways are deployed in a primary/secondary configuration (1+1) to support resilient MiVoice Border Gateway operation and resilient SIP trunk operation. The second group of MiVoice Border Gateways are used to provide connectivity to an Internet service provider. The MiVoice Border Gateways provide: • Teleworker service for connection to remote SIP and MiNet end-points • Web proxy for externally connected devices such as: MiCollab mobile clients and Softphones, management access, and access to LAN-based applications To support resilient operation for SIP phones, resilient MiVoice Border Gateway operation and resilient Internet connections, the MiVoice Border Gateways are deployed in a primary/secondary configuration (1+1). To support resilient operation for Mitel proprietary hard phones (MiNet phones), resilient MiVoice Border Gateway operation and resilient Internet connections, the MiVoice Border Gateways can be deployed as a N+1 cluster. For example, three MiVoice Border Gateways would be deployed in an N+1 configuration if two MiVoice Border Gateways are needed for the user connections.
MiCollab	The MiCollab server unifies Mitel applications into an easy to use, cost effective communications solution. End-users have a single point of access to all their Mitel applications. MiCollab provides co-residency of applications to support: • MiCollab Client Multi-Tenant Service • MiCollab Audio, Web, and Video Conferencing MiVoice Border Gateway • MiCollab Unified Messaging

Table 4: On-Premise Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
MiCollab Audio, Web, and Video Conferencing	MiCollab Audio, Web, and Video Conferencing is a conferencing and Collaboration application running within MiCollab. MiCollab Audio, Web, and Video Conferencing can be used to provide conferencing support with voice, video and presentation capabilities.
Mitel Performance Analytics and MPA Probe	The Mitel Performance Analytics application uses a probe called the MPA Probe, which is a virtual probe that collects fault and performance data for Mitel components and selected network devices. The MPA Probe transfers the data that it has collected to a Mitel Performance Analytics server. • The MPA Probe may be deployed at any location in the network where monitoring is required. • The MPA Probe collects call voice quality information from the individual MiVoice Business and operational data from network equipment, the data is then transmitted to the Mitel Performance Analytics server, via an Internet connection, or to a locally provisioned Mitel Performance Analytics server on the customer premises. • The Mitel Performance Analytics application analyses the data received from the MPA Probe and provides alarm indications to the Administrator when units are out of service or monitored parameters are reaching pre-specified thresholds. • The use of Mitel Performance Analytics and the MPA Probe is optional.
Native Management Interfaces	These are direct management interfaces to the individual products, including: • Individual applications • Network and virtualization infrastructure • Call control engines
MiCollab Unified Messaging	MiCollab Unified Messaging is a Unified Communications voice mail application within MiCollab, whose features include, but are not limited to: • Voice mail • Text to speech when integrated with e-mail • E-mail notification of voice mails • Auto-attendant and voice recognition (available as an add-on feature) • Visual Voice mail
Mitel Open Integration Gateway	Mitel Open Integration Gateway provides a proxy for connection to Customer Relationship Management (CRM) business applications, including integration with: • MiVoice Integration for Salesforce • MiVoice Integration for Google Mitel Open Integration Gateway can also be used by customer specific applications for better integrations of UCC to business operations. (For example, call handling, click to dial, etc.)

Table 4: On-Premise Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
Business applications	These are customer specific business applications that the UC system may need to be aware of, or to integrate with. It may include, but is not be limited to: • E-mail, and integration with voice mail • Customer Database • Directory Services (Microsoft Active Directory) • Web Services
Teleworker (Public Network)	This network provides connectivity for Teleworker phones. This access is typically over a Public Internet connection, or over a publicly-accessible network.
PSTN	The term Public Switched Telephone Network (PSTN) describes the various equipment and interconnecting facilities that provide phone service to the public. The MiVoice Business trunking gateways connect to the PSTN via PRI trunks.
SIP Trunk Provider	A SIP trunk provider is a service provider that offers customers SIP trunk connectivity, the offering includes: • DDI/DID numbers that are hosted or assigned by the SIP service provider • SIP to PSTN access • IP Network isolation via an SBC • Billing • E911 location information
MiCollab Client Service	MiCollab Client Service is an application within MiCollab that provides Presence information for all UC users as well as providing PC softphone and Mobile softphone clients.
MiCollab Client	The MiCollab Client connects to the MiCollab Client Service, part of the MiCollab server. It provides telephone presence and dialing capabilities for the end-user. The MiCollab Client is used as a separate client with a hard phone, a PC softphone, and also with the mobile softphone. • Static softphones within the customer network must be registered with the MiCollab Client Service directly on the customer LAN • Mobile softphones outside of the customer network must be registered with the MiCollab Client Service via the external teleworker MiVoice Border Gateway • Mobile softphones registered via the MiVoice Border Gateway may continue to consume Internet connection bandwidth when used within the customer premises

ON-PREMISE TOPOLOGY CONSIDERATIONS

The following sections highlight some considerations that apply to the On-Premise topology.

- “On-Premise Supported Phone and End-User Device Types” on page 24
- “On-Premise Quality of Service Considerations” on page 24

ON-PREMISE SUPPORTED PHONE AND END-USER DEVICE TYPES

The On-Premise topology supports the use of Mitel's proprietary MiVoice 53xx and 69xx IP Phones, the MiVoice Business Console, specialty end-points, the MiVoice Video and Conference phones, MiCollab softphones and mobile clients, SIP Analog Terminal Adapters, alarm interfaces and door openers. For a complete list of supported end-points, refer to “End-Users and Devices” on page 63.

ON-PREMISE QUALITY OF SERVICE CONSIDERATIONS

Quality of Service (QoS) needs to be provided throughout the customer premise LAN, across the connection to the SIP trunk service provider.

Service Level Agreements to ensure that priority marked packets are treated in an appropriate manner should be established with the SIP trunk service provider.

The Teleworker connections are made over the public Internet and SLAs and QoS are not typically honoured due to uncertainty of the connection route over different networks. In the absence of SLAs, it is recommended that the customer provide a means of enabling QoS and queuing mechanisms within their own network and within the Teleworker's local network. Traffic shaping units can also be included in the customer connection, either by the Public Network Provider, or installed on the customer site. These effectively throttle unmarked download traffic to provide sufficient bandwidth for voice traffic.

For further details on QoS settings see “Network and Networking Considerations” on page 167.

ON-PREMISE TOPOLOGY SCALING

The On-Premise topology which is suitable for customers that have all of their end-users located at one site, scales from 100 to 2500 end-users.

MIVOICE BUSINESS SCALING

For the Enterprise On-Premise deployment, the deployment size can range from 100 to 2500 users.

More detail on MiVoice Business scaling can be found in “Traffic and Scaling Considerations” on page 95, and also in the *MiVoice Business Engineering Guidelines*.

MIVOICE BORDER GATEWAY SCALING

The Mitel MiVoice Border Gateway supports a number of different logical functions such as SIP Trunking connectivity, Session Border Controller functionality and Teleworker gateway functionality for both SIP and MiNet IP end-points.

For most On-Premise topology deployments one MiVoice Border Gateway can provide connectivity to both the SIP Trunk Service provider and the Teleworker end-points. However, in practice the MiVoice Border Gateways are deployed in resilient pairs to support resilient operation.

Multiple MiVoice Border Gateways are only required for scaling up to support a larger number of users. Should the number of MiVoice Border Gateways need to be scaled to more than one resilient pair, then it is recommended to use one resilient pair of MiVoice Border Gateways for SIP trunking and another pair of resilient MiVoice Border Gateways to support Teleworkers.

Due to the UC licensing model, all Teleworkers need be in the same cluster but MiVoice Border Gateway load sharing can be used to effectively provision resilient SIP users with MiVoice Border Gateways in a 1+1 mode and resilient MiNet users in a N+1 mode.

The number of MiVoice Border Gateways required for SIP trunks is primarily driven by the number of active voice connections, as well as the database redirection entries (example: Which DDI/DIDs are assigned to which MiVoice Business?). Use of common DDI/DID ranges therefore reduces this limitation impact.

Typically the SIP trunk MiVoice Border Gateways are statically assigned to specific MiVoice Business. For resiliency, the MiVoice Border Gateways are deployed on a 1:1 basis. For example, if two MiVoice Border Gateways are needed to handle the media streams, then four MiVoice Border Gateways are deployed. SIP trunk MiVoice Border Gateways are clustered in pairs to share licenses and database information.

The number of device registrations and the number of voice connections influence how many MiVoice Border Gateways are required for user connections. Typically, the number of voice connections for the user and trunk MiVoice Border Gateways will be similar. However, the introduction of EHDU connections may increase the required number of SIP trunk MiVoice Border Gateways.

User MiVoice Border Gateways can be deployed in an N+1 configuration for Mitel proprietary hard phones (MiNet phones). For example, five MiVoice Border Gateways would be deployed in an N+1 configuration if four MiVoice Border Gateways are needed for the user connections. See the *MiVoice Border Gateway Engineering Guidelines* for cluster scaling limits.

MiVoice Border Gateway scaling rules are different for user SIP devices. MiVoice Border Gateways are deployed in resilient pairs (1 +1) for resilient SIP phones using DNS to locate a secondary access point. The access points for SIP and Mitel proprietary phones are separated due to their different scaling requirements.

MiVoice Border Gateways used for UC connections, with UC Clients and softphones, are associated with a single MiCollab server. These MiVoice Border Gateways should be clustered with the internal MiVoice Border Gateway within MiCollab for license sharing and configuration.

Refer to the *MiVoice Border Gateway Engineering Guidelines*, available on Mitel-On-Line (MOL), for registration limit, voice connection and cluster limits for the MiVoice Border Gateway.

ON-PREMISE TOPOLOGY MANAGEMENT CONSIDERATIONS

Management of the On-Premise topology is performed locally, either by the customer or by a third-party that is under contract to the customer via the native management interfaces. For details on the native management interfaces, refer to the appropriate product documentation

or the section “Management Considerations” on page 131.

In cases where there is a requirement to monitor the network from a remote location, Mitel Performance Analytics and the MPA Probe can be used to monitor equipment alarms and voice quality of phone calls.

ON-PREMISE TOPOLOGY ADDRESSING CONSIDERATIONS

The customer's local network uses a private IP addressing scheme. The SIP trunk provider and the Internet service provider use public IP addresses to address the MiVoice Border Gateways. The MiVoice Border Gateways must use statically assigned IP addresses. Teleworker users connect to the Teleworker gateway using their own public IP address provided by the carrier, or a statically assigned IP address at the customer router.

The customer router also provides the network address translation from internal LAN address to external public address. The MiVoice Border Gateway will translate customer public IP addresses to appropriate internal IP addresses.

ON-PREMISE TOPOLOGY BILLING

External calls from the customer to the wider public are made through the SIP trunks of the SIP service provider. Charges may be applied to these connections depending upon the service provider capabilities and charges that they apply.

Calls that terminate or originate on an EHDU device are treated as internal extensions, but rely on the external trunk and cell-phone access connections. Charges may apply to these calls, since these are carried over a different service provider connection, even for calls to other internal extensions.

End-customers are provided with unique DID/DDI numbers. The DID/DDI numbers may be assigned locally, regionally, or represent their calling patterns. For example, a company in the Central United States may have two sets of DID/DDI numbers for calls originating from the east and west portions of the country, even though they are not physically located in either one. Having DID/DDI numbers in the region that corresponds to the client base helps to reduce tariff charges and presents a local number for callers to dial.

ON-PREMISE TOPOLOGY EMERGENCY NUMBERS (E911)

Locating an end-user with emergency location systems, such as E911 is crucial. If the business is small enough, the business location may be identifiable simply from the assigned DID/DDI number. This will be registered with the SIP trunk service provider. However, to locate an individual, especially where the business is physically large, becomes more difficult. To assist in this situation, every user is assigned a DDI/DID number and the location of that individual is maintained in the SIP trunk service provider database and the local PSAP authority’s database.

It is important that the customer understand that if end-users change locations, they must inform the SIP service provider of this change so that the SIP service provider can update their files.

Before installation, it should be verified that the location information stored with the SIP Trunk provider can be forwarded to the appropriate PSAP that would service the customer. With the advent of IP networks, this is becoming easier, but some physical locations may not subscribe to this service, making E911 location services difficult from the SIP trunk provider. This is especially important where the SIP Trunk provider may host a number of DID/DDIs from many locations, but physically connect to the PSTN at a few major points of presence.

The on-premise deployment may also use PRI trunks for emergency calling. The MiVoice Business can include location information to be sent over these trunks. See *MiVoice Business Engineering Guidelines* and on-line help for further details.

ON-PREMISE TOPOLOGY PREMISE, NETWORK, AND SERVICE PROVIDER CONSIDERATIONS

To ensure a successful solution deployment, it is recommended that the following considerations be reviewed. This list of considerations while not exhaustive, is intended to provide guidance for reviewing this topology.

- “End-Customer Considerations” on page 27
- “Network Considerations” on page 27

END-CUSTOMER CONSIDERATIONS

The following items should be considered for end-customers.

- Firewall and NAT capabilities for network security are defined
- Requirements for non-standard interfaces (example: SIP ATA for door openers) have been identified

NETWORK CONSIDERATIONS

The following items should be considered for the network and carrier portions of the solution.

- QoS settings are supported and honoured and different SLAs are defined if necessary.
- The customer network has external access to AMC for license verification
- If management is being contracted out to a third-party, has the third-party identified an e-mail forwarder for alarms and notification
- If a third-party is managing the network, the customer will need to decide if they will allow the third-party to access the network remotely, or if they prefer that the management access will only be local
- SIP Trunk provider interoperability has been reviewed
- SIP device interoperability has been reviewed
- Public DNS registrations for MiVoice Border Gateways are defined
- Backup storage and schedule identified
- Ongoing monitoring and alarm reporting strategy is in place

- MiVoice Border Gateway clustering strategy defined
- The network is redundant at all levels and regularly tested (example: VRRP, HSRP, MSTP, LACP)
- Public IP address requirements are identified (IPv4 is in short supply)
- Internal IP address map is defined

ON-PREMISE TOPOLOGY RELATIVE STRENGTHS AND LIMITATIONS

This section identifies the strengths and limitations of this topology relative to the other UC Enterprise Solution topologies.

- “Topology Strengths” on page 28
- “Topology Limitations” on page 28

TOPOLOGY STRENGTHS

- Depending on the particular requirements, the customer has the flexibility to deploy the MiVoice Business software on 3300 ICP Controllers and/or Industry Standard Servers. MiVoice Business software may also be deployed as a virtualized solution (MiVoice BusinessMiVoice Business) in a VMware environment
- UCC applications are deployed as part of a MiCollab server
- A wide range of Mitel IP telephony end-points, mobile end-points, Teleworker and video end-points are supported
- Both PSTN and SIP trunking are supported
- Integrity of the LAN infrastructure is under the control of the customer
- System availability does not depend on the WAN link or the WAN service provider
- Call control, IP Phones and MiVoice Border Gateways support resilient operation
- The customer has the choice to manage their own UC solution or to contract a VAR to do so on their behalf

TOPOLOGY LIMITATIONS

- A capital expenditure is required to procure the UCC solution
- The customer will be responsible for establishing their own relationship and SLA with both the SIP and PSTN trunk providers
- The customer must bear the ongoing maintenance expenses for the UCC solution and network infrastructure
- Applications resiliency is not normally supported with this topology, but cold standby servers can be used so that service may be recovered in the event of a server hardware failure
- The customer must retain their own technical personnel, either employees or a VAR, for UC solution and network infrastructure maintenance and support

- Some customers may need to ensure that technical staff are available 24/7, this may result in a significant expense for employees who are basically on stand-by
- Should connectivity with a remote office be required, the customer is responsible for establishing their own relationship and an SLA with WAN providers
- The customer must bear the initial cost for procuring the LAN infrastructure and the cost of upgrades when the networking gear reaches end of life
- The customer must ensure that software upgrades are carried out in a timely manner and that Software Assurance and Support payments are current.

PRIVATE CLOUD

The Private Cloud topology allows the majority of the equipment to be located in a centralized location such as an off-premise data center the or in a private cloud. The Private Cloud topology is intended for deployments where the end-users are located at one site or distributed across a few different sites

The Private Cloud topology relies on an Infrastructure as a Service (IaaS) offering, specifically, the majority of the required infrastructure to support the solution is provided to the customer sites as a service. This means that user controllers, trunking gateways, MiVoice Border Gateways, business applications, and unified communications applications are all located in a private cloud or a data centre.

The applications and deployment are all managed by the customer or designated VAR. The data centre infrastructure is managed by the IaaS service provider.

Video and telephony end-points are located with employees at the customer's site or sites, and communication between the customer sites and the private cloud or data centre is via an MPLS network.

MiVoice Business software can be deployed on a Mitel 3300 ICP located at the customer site to provide local PSTN breakout and/or local call control survivability in case of an MPLS network outage.

The following sections provide further information for evaluating the Private Cloud topology to determine if it is a suitable solution for meeting the customer's needs.

PRIVATE CLOUD TOPOLOGY BUSINESS AND SALES GUIDE

The Private Cloud topology relies on an IaaS offering that provides the same end-user functionality as the On-Premise topology, but with the difference that the UCC solution infrastructure is hosted in a private cloud or data centre rather than being physically located at the customer premises.

This topology is intended for customers that have the following requirements:

- The customer may have a single site or multiple sites
- The customer preference is to have their business applications and UC operations located off premise, in a data centre or in a private cloud
- The customer doesn't want to invest heavily in data centre infrastructure, or wishes to amortize infrastructure CAPEX costs into an OPEX cost.
- The number of users ranges from 100 to 2500
- The customer requires a service availability of up to 5-9s for telephony and for UCC applications
- In addition to basic telephony services, users will require varying levels of UC services
- The customer preference is to own the UCC solution
- Ownership of the UCC solution may encompass the hardware platforms and the software applications or in the case where the hardware platforms are rented, the customer preference is to own the software applications
- The customer preference is to manage the UCC solution themselves or to contract a third-party to manage the UCC solution on their behalf

PRIVATE CLOUD TOPOLOGY ARCHITECTURE

The Private Cloud topology architecture is based on voice-centric components and Unified Communications and Collaboration (UCC) components. The main voice component is the Mitel MiVoice Business application, which depending on the number of end-users, could be running on a 3300 ICP platform, an Industry Standard Server (ISS) or as a virtualized application in a VMware environment.

Unified Communications and Collaboration services are provided by the application suite within MiCollab. MiCollab and Business applications are deployed on their own VMware-based servers, and use VMware's High Availability capabilities to support high service availability operation.

The table "Private Cloud Topology Components" on page 32 explains the role and deployment of each component in the "Private Cloud Topology Diagram" on page 32.

Figure 4: Private Cloud Topology Diagram

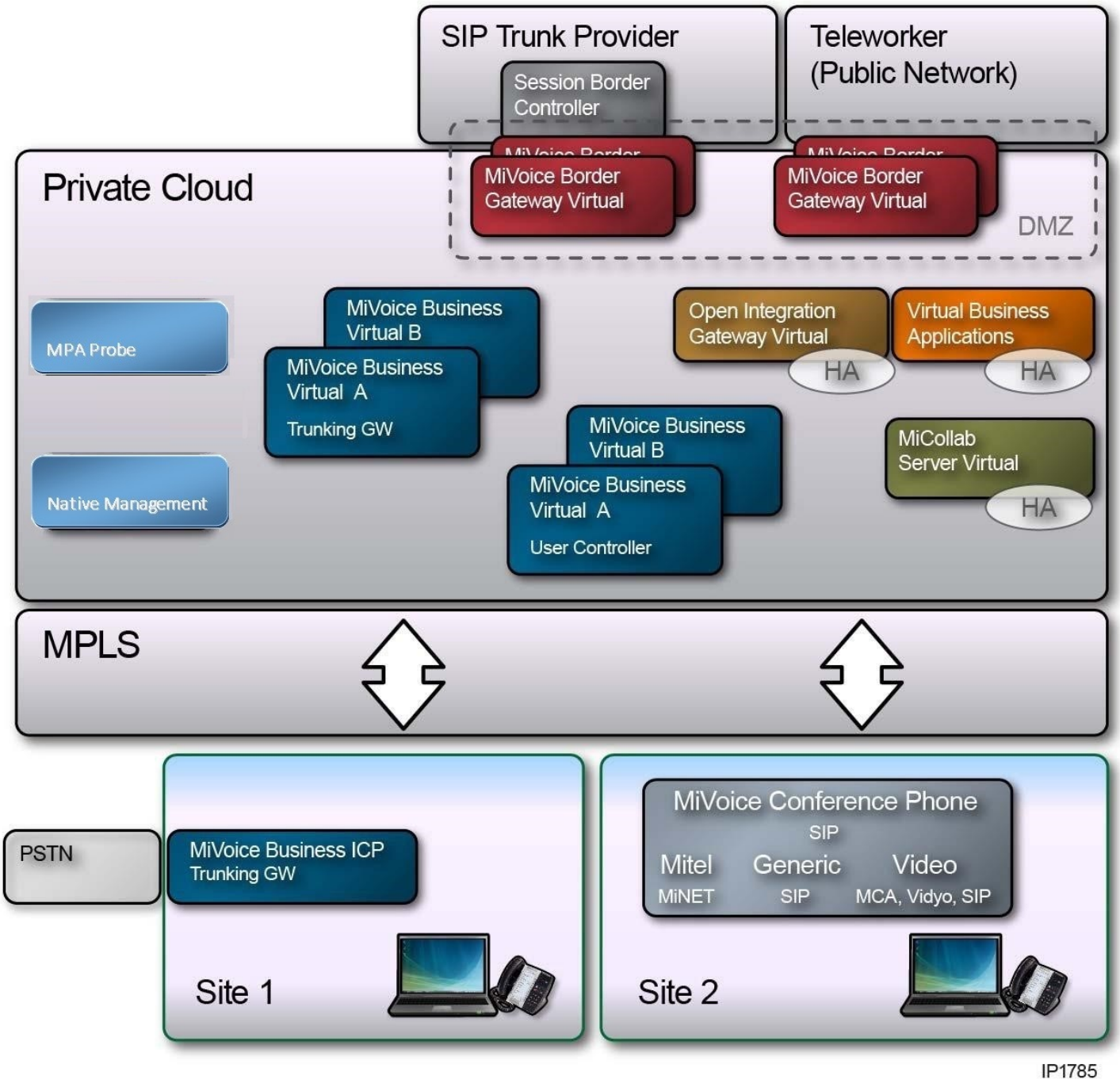


Table 5: Private Cloud Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
MiVoice Business - User Controller	The MiVoice Business user controllers perform telephony call control and media handling. • MiVoice Business user controllers are clustered for scaling and also for resilient operation. • Depending on the scaling requirements, the MiVoice Business software may be installed on a 3300 ICP or on an ISS/VMware platform.
MiVoice Business - Trunking Gateway	The MiVoice Business trunking gateways provide connectivity to the SIP service provider - via the MiVoice Border Gateways and SIP trunks. • Multiple MiVoice Business trunking gateways are deployed for scaling and resilient operation.

Table 5: Private Cloud Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
MiVoice Border Gateway Virtual	The Mitel MiVoice Border Gateway Virtual is a specialized application proxy supporting SIP, MiNet, and web protocols. The Private Cloud topology uses two groups of MiVoice Border Gateways located in the DMZ. The first group of MiVoice Border Gateway Virtuals are used to provide connectivity to the SIP trunk service provider. • The MiVoice Border Gateway Virtuals are deployed at the cloud or data centre network edge, along with fire walls and the SIP trunks connect to an SBC which is located at the SIP trunk provider's facilities • The MiVoice Border Gateway Virtuals are deployed in a primary/secondary configuration (1+1) to support resilient MiVoice Border Gateway Virtual operation and resilient SIP trunk operation The second group of MiVoice Border Gateways are used to provide connectivity to an Internet service provider. The MiVoice Border Gateway Virtuals provide: • Teleworker service for connection to remote SIP and MiNet end-points • Web proxy for externally connected devices such as: MiCollab mobile clients and Softphones, management access, and access to LAN-based applications To support resilient operation for SIP phones, resilient MiVoice Border Gateway Virtual operation and resilient Internet connections, the MiVoice Border Gateway Virtuals are deployed in a primary/secondary configuration (1+1). To support resilient operation for Mitel proprietary hard phones (MiNet phones), resilient MiVoice Border Gateway Virtual operation and resilient Internet connections, the MiVoice Border Gateway Virtuals can be deployed as a N+1 cluster. For example, three MiVoice Border Gateway Virtuals would be deployed in an N+1 configuration if two MiVoice Border Gateway Virtuals are needed for the user connections.
MiCollab	MiCollab unifies Mitel applications into an easy to use, cost effective communications solution. End-users have a single point of access to all their Mitel applications. MiCollab provides co-residency of applications to support: • MiCollab Client ServiceMiCollab Audio, Web, and Video Conferencing MiVoice Border Gateway • MiCollab Unified Messaging

Table 5: Private Cloud Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
Mitel Performance Analytics and MPA Probe	The Mitel Performance Analytics application uses a probe called the MPA Probe, which is a virtual probe that collects fault and performance data for Mitel components and selected network devices. The MPA Probe transfers the data that it has collected to a Mitel Performance Analytics server. • The MPA Probe may be deployed at any location in the network where monitoring is required • The MPA Probe collects call voice quality information from the individual MiVoice Business and operational data from network equipment, the data is then transmitted to the Mitel Performance Analytics server, via an Internet connection, or to a locally provisioned Mitel Performance Analytics server on the customer premises • The Mitel Performance Analytics application analyses the data received from the MPA Probe and provides alarm indications to the Administrator when units are out of service or monitored parameters are reaching pre-specified thresholds • The use of Mitel Performance Analytics and the MPA Probe is optional. • Mitel Performance Analytics and MPA Probe may also be used by the reseller/VAR for remote management access.
Native Management Interfaces	These are direct management interfaces to the individual products, including: • Individual applications • Network and virtualization infrastructure • Call control engines
MiCollab Unified Messaging	MiCollab Unified Messaging is a Unified Communications voice mail application within MiCollab, whose features include, but are not limited to: • Voice mail • Text to speech when integrated with e-mail • E-mail notification of voice mails • Auto-attendant and voice recognition (available as an add-on feature) • Visual Voice Mail
Mitel Open Integration Gateway	Mitel Open Integration Gateway provides a proxy for connection to Customer Relationship Management (CRM) business applications, including integration with: • MiVoice Integration for Salesforce • MiVoice Integration for Google Mitel Open Integration Gateway can also be used by customer specific applications for better integrations of UCC to business operations. (For example, call handling, click to dial, etc.)

Table 5: Private Cloud Topology Components

COMPONENT	CONTEXT AND DEPLOYMENT DETAILS
Virtual business applications	These are customer specific business applications that the UC system may need to be aware of, or to integrate with. It may include, but is not be limited to: • E-mail, and integration with voice mail • Customer Database • Directory Services (Microsoft Active Directory) • Web Services The Private Cloud topology uses virtualized business applications, which are business applications that have been deployed in a VMware environment.
Teleworker (Public Network)	This network provides connectivity for Teleworker phones. This access is typically over a Public Internet connection, or over a publicly-accessible network.
PSTN	The term Public Switched Telephone Network (PSTN) describes the various equipment and interconnecting facilities that provide phone service to the public. 3300 ICP trunking gateways / survivable gateways may be deployed at the customer sites for connecting to the local PSTN.
SIP Trunk Provider	A SIP trunk provider is a service provider that offers customers SIP trunk connectivity, the offering includes: • DDI/DID numbers that are hosted or assigned by the SIP service provider • SIP to PSTN access • IP Network isolation via an SBC • Billing • E911 location information
MiCollab Client Service	MiCollab Client Service is an application within MiCollab that provides presence information for all UC users as well as providing PC softphone and Mobile softphone clients.
MiCollab Client	The MiCollab Client connects to the MiCollab Client Service, part of the MiCollab server. It provides telephone presence and dialing capabilities for the end-user. The MiCollab Client is used as a separate client with a hard phone, a PC softphone, and also with the mobile softphone. • Static softphones within the customer network must be registered with the MiCollab Client Service directly on the customer LAN • Mobile softphones outside of the customer network must be registered with the MiCollab Client Service via the external teleworker MiVoice Border Gateway • Mobile softphones registered via the MiVoice Border Gateway may continue to consume Internet connection bandwidth when used within the customer premises

PRIVATE CLOUD TOPOLOGY CONSIDERATIONS

The following sections highlight some considerations that apply to the Private Cloud topology.

- “Supported Phone and End-User Device Types” on page 36
- “Quality of Service Considerations” on page 36

SUPPORTED PHONE AND END-USER DEVICE TYPES

The Private Cloud topology supports the use of Mitel's proprietary MiVoice 53xx and 69xx IP Phones, the MiVoice Business Console, specialty end-points, the MiVoice Video and Conference phones, MiCollab softphones and mobile clients, SIP Analog Terminal Adapters, alarm interfaces and door openers. For a complete list of supported end-points, refer to “End-Users and Devices” on page 63.

QUALITY OF SERVICE CONSIDERATIONS

Quality of Service (QoS) needs to be provided throughout the LANs on the customer sites, across the MPLS network to the private cloud or data centre, and also across the connection to the SIP trunk service provider.

Service Level Agreements to ensure that priority marked packets are treated in an appropriate manner should be established with the SIP trunk service provider.

Service Level Agreements should be established with the MPLS network provider to ensure that priority marked packets are treated in an appropriate manner and that sufficient bandwidth is always available.

The Teleworker connections are made over the public Internet and SLAs and QoS are not typically honored due to uncertainty of the connection route over different networks. In the absence of SLAs, it is recommended that the customer provide a means of enabling QoS and queuing mechanisms within their the private cloud or data centre network and within the Teleworker's local network. Traffic shaping units can also be included in the customer connection, either by the Public Network Provider, or installed in the Private Cloud. These effectively throttle unmarked download traffic to provide sufficient bandwidth for voice traffic.

For further details on QoS settings, see “Network and Networking Considerations” on page 167.

PRIVATE CLOUD TOPOLOGY SCALING

The Private Cloud topology which is suitable for customers that have from 100 to 3000 end-users.

- “Private Cloud MiVoice Business Virtual Scaling” on page 36
- “Private Cloud MiVoice Border Gateway Virtual Scaling” on page 37

PRIVATE CLOUD MIVOICE BUSINESS VIRTUAL SCALING

For the Private Cloud deployment, MiVoice Business is deployed in a VMware environment (MiVoice Business Virtual) and the deployment size can range from 100 to 3000 users. For resilient operation, the MiVoice Business Virtual are deployed in resilient pairs.

Survivable gateways deployed at customer sites employ MiVoice Business running on 3300 ICPs, these gateways can scale up to 1400 users.

PRIVATE CLOUD MIVOICE BORDER GATEWAY VIRTUAL SCALING

The MiVoice Border Gateway Virtual supports a number of different logical functions such as SIP Trunking connectivity, Session Border Controller functionality and Teleworker gateway functionality for both SIP and MiNet IP end-points.

For small sites (those with up to 150 IP end-points or requiring up to 30 media streams), the MiVoice Border Gateway Virtual Small Business can provide connectivity to both the SIP Trunk Service provider and the Teleworker end-points. However, in practice the Small Business MiVoice Border Gateway Virtuals are deployed in pairs to support resilient operation.

For sites that have more than 150 IP end-points or sites that need to support more than 30 media stream, the MiVoice Border Gateway Virtual Enterprise is used. The MiVoice Border Gateway Virtual Enterprise supports up to 2500 IP end-points and up to 500 media streams.

Multiple MiVoice Border Gateway Virtuals are only required for scaling up to support a larger number of users. Should the number of MiVoice Border Gateway Virtuals need to be scaled to more than one resilient pair, then it is recommended to use one resilient pair of MiVoice Border Gateway Virtuals for SIP trunking and another pair of resilient MiVoice Border Gateway Virtuals to support Teleworkers.

Due to the UC licensing model, all Teleworkers need be in the same cluster but MiVoice Border Gateway Virtual load sharing can be used to effectively provision resilient SIP users with MiVoice Border Gateway Virtual in a 1+1 mode and resilient MiNet users in a N+1 mode.

The number of MiVoice Border Gateway Virtuals required for SIP trunks is primarily driven by the number of active voice connections, as well as the database redirection entries (example: Which DDI/DIDs are assigned to which MiVoice Business?). Use of common DDI/DID ranges therefore reduces this limitation impact.

Typically the SIP trunk MiVoice Border Gateway Virtuals are statically assigned to specific MiVoice Business Virtual. The MiVoice Border Gateway Virtuals are also deployed on a 1:1 basis. For example, if two MiVoice Border Gateways are needed to handle the media streams, then four MiVoice Border Gateways are deployed. SIP trunk MiVoice Border Gateway Virtuals are clustered in pairs to share licenses and database information.

The number of device registrations and the number of voice connections influence how many MiVoice Border Gateway Virtuals are required for user connections. Typically, the number of voice connections for the user and trunk MiVoice Border Gateway Virtuals will be similar. However, the introduction of EHDU connections may increase the required number of SIP trunk MiVoice Border Gateway Virtuals. EDHU connections also impact the number of MiVoice Border Gateway Virtuals needed for UC connectivity.

User MiVoice Border Gateway Virtuals can be deployed as a N+1 cluster for Mitel proprietary hard phones. For example, five MiVoice Border Gateway Virtuals would be deployed in an N+1 configuration if four MiVoice Border Gateway Virtuals are needed for the user connections. See the *MiVoice Border Gateway Virtual Engineering Guidelines* for cluster scaling limits.

MiVoice Border Gateway Virtual scaling rules are different for user SIP devices. MiVoice Border Gateway Virtual is deployed in clustered pairs for resilient SIP phones using DNS to locate a

secondary access point. The access points for SIP and Mitel proprietary phones are separated due to their different scaling requirements.

MiVoice Border Gateways are also associated with a single MiCollab server and should be clustered with the internal MiVoice Border Gateway within MiCollab for license sharing.

Refer to the *MiVoice Border Gateway Engineering Guidelines*, available on Mi-Line (MOL), for registration limit, voice connection and cluster limits for the MiVoice Border Gateway.

PRIVATE CLOUD TOPOLOGY MANAGEMENT CONSIDERATIONS

Management of the Private Cloud topology is performed from within the private cloud or data centre. Survivable gateways that are located at the customer sites are managed from within the customer site. Management is performed either by the customer or by a third-party that is under contract to the customer via the native management interfaces.

For details on the native management interfaces and Enterprise Manager, refer to the appropriate product documentation or the section “Management Considerations” on page 131.

In cases where there is a requirement to monitor the network from a remote location, Mitel Performance Analytics and the MPA Probe can be used to monitor equipment alarms and voice quality of phone calls. Mitel Performance Analytics can also be used to set up a management access tunnel for remote management.

VPNs can be set up for remote management or access by the customer or a designated VAR.

PRIVATE CLOUD TOPOLOGY ADDRESSING CONSIDERATIONS

The customer site local network and the Private Cloud use a private IP addressing scheme. The SIP trunk provider and the Internet service provider use public IP addresses to address the MiVoice Border Gateway Virtuals. Teleworker users connect to the Teleworker gateway using their own public IP address provided by the carrier, or a statically assigned IP address at the customer router.

The Private Cloud router also provides the network address translation from the private LAN address to external public address. The MiVoice Border Gateway Virtual will translate customer public IP addresses to appropriate internal IP addresses.

PRIVATE CLOUD TOPOLOGY BILLING

Outgoing calls from the customer to the wider public are made through the SIP trunks of the SIP service provider. Charges may be applied to these connections depending upon the service provider capabilities and charges that they apply.

Calls that terminate or originate on an EHDU device are treated as internal extensions, but rely on the external trunk and cell-phone access connections. Charges may apply to these calls, since these are carried over a different service provider connection, even for calls to other internal extensions.

End-customers are provided with unique DID/DDI numbers. The DID/DDI numbers may be assigned locally, regionally, or represent their calling patterns. For example, a company in the Central United States may have two sets of DID/DDI numbers for calls originating from the east and west portions of the country, even though they are not physically located in either one. Having DID/DDI numbers in the region that corresponds to the client base helps to reduce tariff charges and presents a local number for callers to dial.

PRIVATE CLOUD TOPOLOGY EMERGENCY NUMBERS (E911)

Locating an end-user with emergency location systems, such as E911 is crucial. If the business is small enough, the business location may be identifiable simply from the assigned DID/DDI number. This will be registered with the SIP trunk service provider. However, to locate an individual, especially where the business is physically large, becomes more difficult. To assist in this situation, every user is assigned a DDI/DID number and the location of that individual is maintained in the SIP trunk service provider database and the local PSAP authority's database.

It is important that the customer understand that if end-users change locations, they must inform the SIP service provider of this change so that the SIP service provider can update their files.

Before installation, it should be verified that the location information stored with the SIP Trunk provider can be forwarded to the appropriate PSAP that would service the customer. With the advent of IP networks, this is becoming easier, but some physical locations may not subscribe to this service, making E911 location services difficult from the SIP trunk provider. This is especially important where the SIP Trunk provider may host a number of DID/DDIs from many locations, but physically connect to the PSTN at a few major points of presence.

Local survivable gateways can also be used for emergency call routing, where appropriate. The phones need to use an emergency route in order to pass the phone location information out the local PRI connections, and the survivable gateway must be part of the overall cluster.

PRIVATE CLOUD TOPOLOGY PREMISE, NETWORK, AND SERVICE PROVIDER CONSIDERATIONS

To ensure a successful deployment, it is recommended that the following considerations be reviewed. This list of considerations while not exhaustive, is intended to provide guidance for reviewing this topology.

END-CUSTOMER CONSIDERATIONS

The following items should be considered for end-customers.

- Firewall and NAT capabilities for network security are defined
- Requirements for non-standard interfaces (example: SIP ATA for door openers) have been identified

NETWORK CONSIDERATIONS

The following items should be considered for the network and carrier portions of the solution:

- QoS settings are supported and honoured and different SLAs are defined if necessary.
- The customer network has external access to AMC for license verification
- If management is being contracted out to a third-party, has the third-party identified an e-mail forwarder for alarms and notification
- If a third-party is managing the network, the customer will need to decide if they will allow the third-party to access the network remotely, or if they prefer that the management access will only be local
- SIP Trunk provider interoperability has been reviewed
- SIP device interoperability has been reviewed
- Public DNS registrations for MiVoice Border Gateways are defined
- Backup storage and schedule identified
- Ongoing monitoring and alarm reporting strategy is in place
- MiVoice Border Gateway Virtual clustering strategy defined
- The network is redundant at all levels and regularly tested (example: VRRP, HSRP, MSTP, LACP)
- Public IP address requirements are identified (IPv4 is in short supply)
- Internal IP address map is defined?

PRIVATE CLOUD TOPOLOGY RELATIVE STRENGTHS AND LIMITATIONS

This section identifies the strengths and limitations of this topology relative to the other UC Enterprise Solution topologies.

- “Topology Strengths” on page 40
- “Topology Limitations” on page 41

TOPOLOGY STRENGTHS

- MiVoice Business, MiVoice Border Gateways, MiCollab and Business applications are all deployed in a VMware environment allowing for enhanced resilient operation through the use of VMware's High Availability feature
- Service availability can reach 5-9s
- Local resiliency - at the customer site - is possible with the use of 3300 ICPs running MiVoice Business
- A wide range of Mitel IP telephony end-points, mobile end-points, Teleworker and video end-points are supported
- SIP trunking is supported

- Integrity of the LAN infrastructure is directly under the control of the customer or indirectly via the customer's VAR
- The customer has the choice to manage their own UC solution or to contract a VAR to do so on their behalf
- Data Centre infrastructure maintenance is outsourced to the IaaS provider.
- On-Premise data centre CAPEX costs are amortized over a longer period and are effectively OPEX costs

TOPOLOGY LIMITATIONS

- A capital expenditure is required to procure the UCC applications and solution
- The customer will be responsible for establishing their own relationship and SLA with both the SIP trunk providers and the MPLS network provider
- The customer must bear the ongoing maintenance expenses for the UCC solution and network infrastructure
- The customer must retain their own technical personnel - either employees or a VAR - for UCC solution and local network infrastructure maintenance and support
- Some customers may need to ensure that technical staff are available 24/7, this may result in a significant expense for employees who are basically on 'stand-by'
- The customer must bear the initial cost for procuring the LAN infrastructure and the cost of upgrades when the networking gear reaches end of life

PRIVATE CLOUD, SHARED SERVICES

An Enterprise business that has a large number of employees that wishes to look at a private cloud or hosted UC Solution would typically use the Enterprise UC Private Cloud, Shared Services topology. This topology is targeted at a single customer, although the customer may have a number of offices that are geographically dispersed. An example would be an Enterprise with corporate headquarters and a number of regional offices. Hosting the services in the Cloud Data Centre and linking the sites with a common network will simplify and reduce costs compared to a multi-site solution.

The Private Cloud, Shared Services topology is a large and complex deployment. This will be managed by an in-house IT staff, and will require training to understand how to achieve this. Management will be from within the customer address space, although external access may be provided for support and reseller access, if needed.

This deployment is based on a building block of up to 3000 UC users. It requires the identification of business units within the Enterprise, limited to 3000 users. Multiple Business Units are then linked together to scale to larger deployment sizes. The linkage requires application and federation connections between UC components across all the business units plus the addition of common functionality, such as centralised Auto-Attendant.

Each deployment will require a level of custom design to meet the customer needs, and although an initial template is envisaged, the end requirements may change that design. Other configurations or solutions may also be included for these larger deployments, especially to link in to existing business processes and equipment, for example e-mail and messaging services.

Details of the topology are not provided within this section, although an example deployment template and diagram is provided below. Further details of possible deployment scenarios to meet the customer requirements can be obtained with Professional Services involvement.

Contact Professional Services when considering a deployment of this size and complexity. This will ensure that the deployment meets the customer requirements, will link in to existing business equipment and will ensure a timely roll-out of the deployment.

PRIVATE CLOUD, SHARED SERVICES TOPOLOGY BUSINESS AND SALES GUIDE

Where used:

- Large corporation or enterprise that wishes to deploy a common hosted data centre
- Large corporation that has a number of regional offices all linked via a common data network

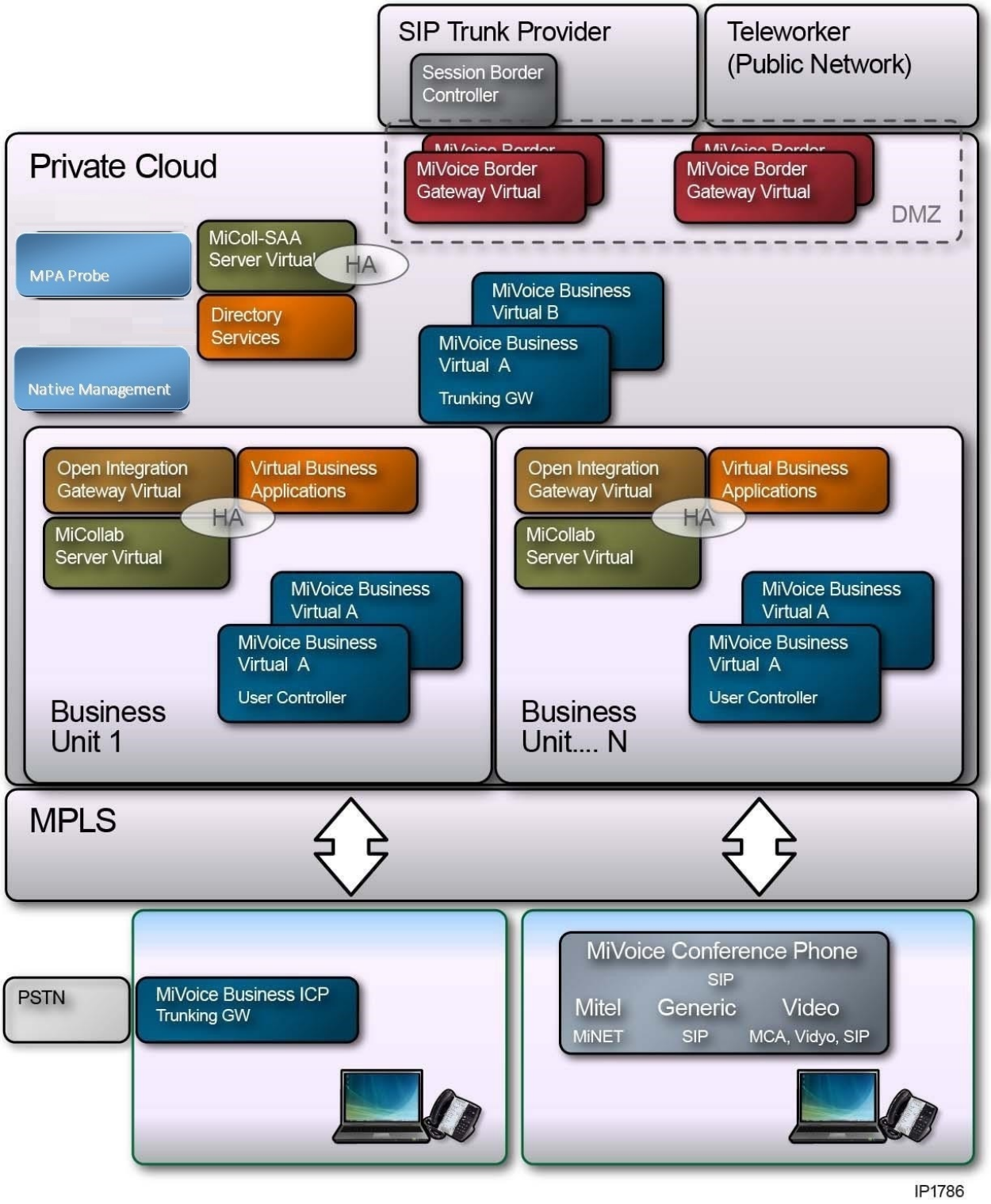
Typical end-customer:

- Large corporation or enterprise
- IT and application knowledgeable staff

PRIVATE CLOUD, SHARED SERVICES TOPOLOGY ARCHITECTURE

"Private Cloud, Shared Services Topology Diagram" on page 43 is provided as an example template for the Private Cloud, Shared Services topology.

Figure 5: Private Cloud, Shared Services Topology Diagram



Chapter 3

APPLICATIONS

APPLICATIONS

Mitel's UC solution is designed to provide a rich feature set encompassing core voice capabilities with an extensive telephony feature set, and a customizable UCC feature set including mobility capabilities. The solution topologies rely on several common product portfolio elements to deliver this functionality, which include:

- MiVoice Business – Mitel's proven call control platform including embedded applications
- MiCollab – an integrated application suite for rich UC capabilities
- Mitel Open Integration Gateway – web server to facilitate integration of the communication systems to third-party applications and Mitel MiVoice Integration applications
- Emergency Response Adviser - an application providing an emergency call display and response console for local security personnel

These application platforms are described in the following sections:

- "MiVoice Business" on page 47
- "MiCollab" on page 49
- "Mitel Open Integration Gateway" on page 56
- "Emergency Response Adviser" on page 58

Application entitlement is built into the UCC User licenses. The capabilities for each level of user license, Basic IPT, Standard IPT, Entry UCC, Standard UCC, and Premium UCC, are described for Enterprises in *MiCollab General Information Guide*, and for service providers in *MiCloud Business Solution for Service Providers Licensing Guide*.

All the topologies described in this blueprint support rich UCC capabilities, with the exception of the Small Business topology designed to provide cost effective light UC services. This Small Business topology includes capabilities supported by MiVoice Business including embedded voice mail and MiCollab Client.

The Emergency Response Adviser is suitable for enterprise on-premise or cloud deployments. It is not supported for service provider deployments.

MIVOICE BUSINESS

MiVoice Business includes an extensive number of applications and system features that support effective and efficient communications, thereby providing significant value to an organization and its employees. These applications enhance communication, productivity, accessibility, mobility, and support the specialized site requirements of businesses and institutions, such as: hotels, hospitals, schools, military sites, and contact centers.

CALL CONTROL

The MiVoice Business call control engine provides sophisticated call management, applications and desktop solutions to businesses.

MiVoice Business is a time proven, highly scalable, resilient, and robust call control engine that fully utilizes the power of IP while fully supporting the traditional TDM-based telephony for legacy devices and PSTN connectivity.

The MiVoice Business architecture uses the IP network to connect IP telephony devices together. If support for TDM telephony is not required, MiVoice Business may be installed on an ISS running Mitel Standard Linux, on an ISS running VMware, or and ISS running Mitel's virtualization platform.

If support for TDM telephony is required, MiVoice Business may be deployed on one of Mitel's 3300 ICP platforms which provide a supplementary TDM subsystem to switch calls between traditional TDM telephone devices.

EMBEDDED VOICE MAIL

MiVoice Business when deployed on a 3300 ICP, an ISS running VMware or Mitel's virtualization platform, includes an integrated fully-featured voice mail system. The number of ports available to support simultaneous voice mail calls and the maximum number of mailboxes supported depends on the platform. For voice mail capacity limits, refer to *MiVoice Business Engineering Guidelines* available on Mitel Edocs.

The voice mail system includes the following features:

- Standard Unified Messaging enables users to forward voice messages, including Record-a-Call messages, to e-mail addresses. Users can manually forward individual voice messages, or automatically forward all voice messages.
- An automated attendant plays different greetings during and following business hours, provides a company directory that uses extension numbers or names as the dialing method, and allows single-digit option selection.
- A Multi-level auto attendant (MLAA) enables a hierarchical menu to be programmed on the auto attendant. This provides callers with self-service options (for example, "Press one for Sales") to reach individuals, departments, or pre-recorded information, or to leave voice messages.
- Personal Contacts enables users to create a customized voice menu so callers can reach users on their cellular phone, or by fax, etc.
- User mailboxes can be password-protected.

For further information refer to the MiVoice Business product documentation available on Mitel Edocs.

FAX

If support for FAX is required, a 3300 ICP may be deployed as a FAX gateway. The 3300 ICP can be configured to allow faxes to be sent over IP trunks between FAX machines that are connected to 3300 ICP systems. A 3300 ICP running MiVoice Business supports the real time transmission of FAX by using G.711 pass-through or by using the T.38 Group 3 FAX protocol. For hosted deployments without 3300 ICP platforms, web fax available from cloud service providers is recommended.

For further information refer to the MiVoice Business product documentation available on Mitel-On-Line (MOL).

COMPONENTS

MiVoice Business call control software is available for deployment on 3300 IP Communications Platforms, Industry Standard Servers, VMware, Hyper-V and custom Mitel virtualization platforms. Further details on the capacity and scaling of MiVoice Business platforms are available in “Traffic and Scaling Considerations” on page 95 and in the product specific engineering guidelines available on Mitel Edocs.

LICENSING

MiVoice Business application licensing is based on user and group licenses. UCC user license bundles embed within the bundle the applicable MiVoice Business licenses related to the features available at different UCC User license levels. When UCC license bundles are added to the ULM, programming within AMC handles allocating the MiVoice Business licenses to the MiVoice Business or Designated License Manager (DLM) within the ULM. These licenses are activated when the MiVoice Business or DLM synchronizes with the AMC, over the Internet or other network connection. Further details are available in “Licensing Considerations” on page 183.

MICOLLAB

MiCollab unifies Mitel applications into an easy to use, cost effective communications solution. The applications co-resident within MiCollab include:

- MiCollab Unified Messaging – provides voice messaging, unified messaging, fax, and paging support
- MiCollab Speech Auto Attendant – provides speech-enabled auto attendant
- MiCollab Client – provides contact management, dynamic status, instant messaging and audio conferencing
- MiCollab Audio, Web, and Video Conferencing – provides web conferencing, supporting audio, video, chat (text) and presentations
- MiVoice Border Gateway – a specialized application proxy supporting SIP, MiNet, and web protocols
- MiCollab Suite Application Services – provides single point user services provisioning, centralized management of shared system resources and license management; also provides the administrator and My Unified Communications portals.

The UCC applications are described in the following sections. MiVoice Border Gateway is described in “External Connectivity” on page 111. MiCollab Suite Application Services is described in“Management Considerations” on page 131.

All of the reference architectures, with the exception of Small Business, support multiple MiCollab applications. The Small Business topology provides cost effective unified communications using a multi-tenanted single application deployment of MiCollab which only includes MiCollab Client.

MICOLLAB UNIFIED MESSAGING

MiCollab Unified Messaging is a powerful, voice processing application that allows users to manage their voice, fax and recorded messages. Unified messaging provides users with the capabilities to:

- send, receive, forward, save, and sort voice and fax messages; fax message support places more stringent requirements on the IP network as discussed below.
- record mailbox greetings
- create and manage personal distribution lists
- play a voice or Record-A-Call (RAC) message over PC speakers or over the phone
- record a phone conversation
- read, print, and send faxes
- reply to a voice, RAC, or fax message with a text message
- forward a message
- call back the sender of the message

With unified messaging, users can access and manage their messages via several interfaces, including:

- Telephone User Interface – MiCollab Unified Messaging plays a menu of options and the user selects the desired option using the telephone key pad
- Visual Voice Mail – allows users to visually interact with their voice mail using their phones' display; available on Mitel 5340 and MiVoice 5360 IP phones with MiCollab Unified Messaging integrated to a MiVoice Business system
- Web View – provides a web-based GUI for managing voice and fax messages
- E-mail – allows users to manage voice and fax messages using an e-mail client; with SMTP, MiCollab Unified Messaging supports sending a WAV file for Voice or TIFF file for Fax; with IMAP or MAPI integrations, messages and Message Waiting Indicators are synchronized between the MiCollab server and e-mail server. MiCollab Unified Messaging also supports an Outlook client plug-in which provides a tool bar to reply to, forward, and manage voice messages, as well as to create and send new voice messages.

MiCollab Unified Messaging Call Director allows users to create an automated attendant application (known as a call flow) to handle incoming calls. Call flows are a collection of call-processing actions such as: play a message, transfer the call to another phone, forward a call to a specified mailbox, send a page or text message or hang up. Call flows may be programmed by the end-user or system administrator.

Text-to-Speech (TTS) may be used to listen to e-mail messages using the MiCollab Unified Messaging voice mail box. Record-A-Call (RAC) allows a user to record both ends of a call and deliver the recording to the user's mailbox. Record-A-Call is only supported with MiVoice Business systems and may only be activated for phones registered to a MiVoice Business connected to the MiCollab Unified Messaging server. Call Detail Recorder creates a record of

each transaction on the MiCollab Unified Messaging server. Compression with G.729a may be enabled for reduced bandwidth costs for a geographically diverse user community.

MiCollab Unified Messaging supports transmitting faxes with both G.711 pass through, where fax data is carried in G.711 voice packets, and T.38 protocol. G.711 Fax pass-through requires that the LAN meet more stringent network parameters than is required for VoIP applications. G.711 Fax pass-through is susceptible to failure if the IP network presents any significant packet loss or jitter. In these cases, T.38 protocol is recommended. T.38 gateway functionality can be integrated into some of the 3300 ICP platforms. T.38 functionality is also supported in some third-party SIP gateways. For further information, refer to the *MiCollab Unified Messaging Engineering Guidelines*. For hosted deployments without 3300 ICP platforms, web fax available from cloud service providers is recommended G.711 pass through is included in the base MiCollab Unified Messaging license. Support for T.38 fax is a separate licensable option.

Speech navigation allows users to perform basic mailbox commands with speech commands. Speech navigation with alternate extension enables hands free access to the MiCollab Unified Messaging mailbox. The speech navigation option is only supported if MiCollab Unified Messaging is the only installed application. This restriction applies to both the MiCollab server and MiCollab Virtual Appliance. With the requirement for MiCollab single application deployment, speech navigation is not supported with UCC licensing.

Networking

MiCollab Unified Messaging requires connection to both the voice network and data network. For UC solutions, voice connectivity for MiCollab Unified Messaging is through one or more MiVoice Businesss. MiCollab Unified Messaging emulates IP sets which register with the MiVoice Business. Each port appears to the MiVoice Business as a 5020 or 5240 IP set and using MiTAI signalling to direct the call handling and manage the Message Waiting Indicators (MWIs). All voice mail and MWI ports must land on a single MiVoice Business and be grouped in a hunt group; this ensures a single hunt group pilot for all users and MWIs. TTS and soft Fax ports are a shared resource with voice mail ports. Non-voice mail ports such as pager ports and RAC ports may be in different hunt groups on different MiVoice Businesss. MiCollab Unified Messaging connects to up to four MiVoice Businesss.

MiCollab Unified Messaging connects to the data network via an e-mail server. For basic or standard UM, where MiCollab Unified Messaging server and e-mail server are managed independently, SMTP Forwarding may be used. MiCollab Unified Messaging can connect to a customer's existing SMTP server. Alternatively, Mitel Standard Linux includes an industry standard SMTP server which can be used for integration to hosted e-mail service platforms such as: Google Mail, Microsoft Office 365 and hosted Microsoft Exchange servers.

With Advanced UM, included in UCC licensing, the MiCollab Unified Messaging system and e-mail server are synchronized so that actions taken on one system will be reflected on the other system. For this two way interaction, MiCollab Unified Messaging supports IMAP and MAPI interfaces. IMAP supports integration to server-based e-mail platforms. Microsoft API (MAPI) Gateway. provides improved access speed and scalability. For further information refer to *MiCollab Unified Messaging Engineering Guidelines*.

MiCollab Unified Messaging supports MiVoice Business resiliency where MiCollab Unified Messaging ports will automatically fail over to the secondary MiVoice Business, maintaining

calls in progress. MiCollab Unified Messaging virtual deployments support VMware HA and SRM features.

MICOLLAB SPEECH AUTO ATTENDANT

MiCollab Speech Auto Attendant allows internal and external callers to place a call by speaking the name, department name, spoken digits or DTMF digits for the extension number. The system supports barge-in allowing a user to interrupt a system prompt with a speech or keystroke command.

Speech recognition matches database names to spoken names and extensions. MiCollab Speech Auto Attendant capacity in terms of the maximum number of names and ports is described in the *MiCollab Unified Messaging Engineering Guidelines*. The speech recognition is customizable for the relative priority of concurrent speech sessions versus accuracy and for the sensitivity of the speech detector.

Networking

MiCollab Speech Auto Attendant connects to a MiVoice Business system in a way similar to that of MiCollab Unified Messaging. Each MiCollab Speech Auto Attendant port appears as a Mitel 5020 or 5240 IP set with call handling via MiTAI. MiCollab Speech Auto Attendant ports are configured in a line group. The MiCollab Speech Auto Attendant ports are managed as a separate resource from the voice mail ports.

MiCollab Speech Auto Attendant is performance intensive and recommended installation is on a stand-alone physical or virtual server with MiCollab single application deployment.

MICOLLAB CLIENT

MiCollab Client provides a single access point for business communication and collaboration. It brings together the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications. Key capabilities include:

- Simplified call management and logging – the server logs all incoming calls for the client and updates the client with all cached call log information; the client also provides access to frequently dialed numbers from a drop-down menu.
- Presence and availability – the server automatically tracks and updates presence information including Dynamic Status, telephony, IM and video presence.
- Dynamic status – provides capabilities to set a status message and optional custom text and manage customized call routing, IM and video presence; status may be changed manually at any time and updated automatically in response to events; calendar integration is supported for Google and Microsoft Outlook calendar information; with mobile clients, users may also define GPS locations to associate with each dynamic status which automatically updates status based on GPS location.
- Corporate Instant Messaging (IM) – allows users to send and receive instant messages and share files; supports multi-party messaging; supports federation with external IM servers using Extensible Messaging and Presence Protocol (XMPP).

- Visual Voice Mail – provides access to the MiCollab Unified Messaging features including capability to receive Message Waiting Indicators, play/view, forward and delete voice and fax messages.
- Contact Management – provides access to corporate and personal contacts; corporate contacts are provided by the MiCollab Client Multi-Tenant Service corporate directory; personal contacts may be imported from a Personal Information Manager (PIM) or created manually. Supported PIMs include Microsoft Outlook, IBM Lotus Notes and Sage Software ACT!
- Knowledge Management – allows users to index files and documents associated with a contact and the client presents this list of associated files in a popup window when the user receives an incoming call.
- RSS Window – the desktop client may be used to display RSS feeds.

MiCollab Client supports several clients that can be integrated with phone capabilities, which include:

- Desktop client – provides access to all MiCollab Client Multi-Tenant Service features and supports integration to a desk phone; this client also includes an embedded PC soft phone which can be configured for either MiNet or SIP protocols; the MiNet version provides extensive telephony features whereas the SIP version supports video calling functionality.
- Web portal – allows web-based access to a subset of MiCollab Client Multi-Tenant Service features; users may change their Dynamic Status, access call history data, view corporate contacts, access voice mail messages, and configure account options; there is no embedded phone capabilities via the web client.
- Mobile clients – provides a user interface designed for mobile devices; the mobile client includes an embedded SIP soft phone; mobile client variants are available for Android™, iOS® on iPad® and iPhone®, and Blackberry®.
- MiCollab Client Console - provides attendants with console features and presence information; supports 60 calls per hour and two simultaneous calls; for higher capacity, the MiVoice Business Console is recommended.

When MiCollab Client is connected to a MiVoice Business network, the desktop client supports handoff of an active call from the associated phone to another device and also pick up of an active call from another device. The mobile client allows a user to push a call to another device within their multi-device user group.

For most UC solutions, MiCollab Client is deployed within a multi-application MiCollab providing a rich suite of UC capabilities. The exception is for the Small Business topology, where MiCollab Client is deployed as a multi-tenanted single application MiCollab configuration, with a reduced feature set.

Networking

MiCollab Client server requires connections to MiVoice Business, using MiTAI for call control and MiXML for configuration changes. MiCollab Client server also requires connection to MiCollab Unified Messaging and MiCollab Audio, Web, and Video Conferencing. For multi-application deployments, these connections are internal to the MiCollab server.

MiCollab Client end-points on the corporate network connect using http to the MiCollab Client Server and MiCollab Unified Messaging server and the embedded soft phones connect with MiNet or SIP to the MiVoice Business; clients on external networks and mobile clients connect via MiVoice Border Gateway using the web proxy for client access and teleworker for the embedded MiNet or SIP phones. MiCollab Clients also require a persistent web socket connection, SSL over TCP, to MiCollab Client server for real-time notifications of missed calls and other events.

MICOLLAB AUDIO, WEB, AND VIDEO CONFERENCING

MiCollab Audio, Web, and Video Conferencing allows users to schedule and hold audio and web conferences. MiCollab Audio, Web, and Video Conferencing supports three types of conferences, which include: Audio and Web, Audio only, and Web only.

Audio conferences allow users to:

- upload documents to present to callers during a conference call
- mute, drop, and add participants, and place individual participants on hold while the call is in progress.

Web conferences allow users to:

- upload documents, transfer files, record the conference, chat online, and broadcast videos
- share applications or desktop and use white board features.

User access and manage their conferences using:

- MiCollab Audio, Web, and Video Conferencing Desktop client – allows users to schedule and join audio and web conferences; the desktop client supports two-way audio participation
- MiCollab Audio, Web, and Video Conferencing Web portal – allows users to schedule and view conferences with listen only audio support; the web-based interface is integrated into MiCollab End-User Portal.

Conferences can be initiated immediately or pre-scheduled. MiCollab Audio, Web, and Video Conferencing may be integrated with corporate directories and personal address books from Microsoft Outlook and Lotus Notes. Optionally, conference accessibility requires personal identification for added security. MiCollab Audio, Web, and Video Conferencing supports recording conference calls and collaborative sessions for later playback. Call Detail Records (CDRs) provide a log of all calls including the dates, times, and call durations for audit and billing purposes.

Networking

MiCollab Audio, Web, and Video Conferencing adds additional IP network configuration requirements. A web browser can request a web page or a Connection Point (file sharing) communication. Both of these web browser requests are made on the standard web port 443. To separate the two types of requests using port 443, the external facing firewall must have two IP addresses for AWV (one IP address for web conferencing, a second IP address for web collaboration client communication to Connection Point). Internal connections separate the traffic based on ports.

COMPONENTS

MiCollab runs on the Mitel Standard Linux operating system. It is supported on Industry Standard Servers and as a virtual appliance on VMware platforms. MiCollab is also available as a server appliance with MiCollab software pre-installed on Mitel supplied server.

MiCollab supports both multi-application deployments and single application deployments. For virtual deployments, although all applications are installed in the MiCollab Virtual Appliance OVA, if licenses are applied for only a single application then it is considered a single application installation.

MiCollab supports the following configurations:

- Small Business multi-application sites up to 250 users
- Mid-Market Business multi-application sites up to 1500 users
- Enterprise multi-application sites up to 3000 users
- Enterprise single-application sites (MiCollab Client or AWV) up to 5000 users; not available as an OVA, refer to *Mitel Virtual Appliance Deployment Solutions Guide* for VMware resources, available on Mitel Edocs.

MiCollab capacity is dependent both on the server specifications and whether MiCollab supports multiple applications or a single application. Further details on capacity are provided in *MiCollab Engineering Guidelines*, available on Mitel Edocs.

MICOLLAB LICENSING

For UC solutions, UCC licensing is only supported on multi-application deployments, with the exception of the UC Light Small Business topology where UCC licensing is supported on MiCollab with MiCollab Client single application deployment.

UCC user licence bundles include MiCollab component licensing with various entitlements based on the number and type of user licenses. For the embedded applications:

- MiCollab Unified Messaging: Entry UCC users and above include Advanced UM and Call Director licenses; add on monthly subscription licenses are available for additional mailboxes, Text-to-Speech and soft Fax ports; CAPEX-based licensing is available for other MiCollab Unified Messaging features such as: Record-A-Call, Call Detail Recorder, G.729, and other custom features.
- MiCollab Speech Auto Attendant: not included in UCC licensing; available through add on monthly subscription licenses for MiCollab Speech Auto Attendant ports.
- MiCollab Client: MiCollab Client client capabilities are included in UCC licensing; add on monthly subscriptions licenses are available to enable the MiCollab Client MiNet or SIP soft phone, MiCollab Client Mobile Client with SIP soft phone, and MiCollab Client Console; for mobile users, Teleworker licenses are included in the Standard and Premium UCC user bundles and also available as add on monthly subscription licenses.
- MiCollab Audio, Web, and Video Conferencing Standard and premium UCC user bundles include a scaled number of MiCollab Audio, Web, and Video Conferencing ports; add on

monthly subscriptions licenses are available for additional MiCollab Audio, Web, and Video Conferencing ports.

Further details about application entitlement are available for Enterprises in *MiCollab General Information Guide* and for service providers in *MiCloud Business Solution for Service Providers Licensing Guide*.

MITEL OPEN INTEGRATION GATEWAY

The Mitel Open Integration Gateway is a web server offering an open, standards-based Web Services applications programming interface (API). Together with the MiVoice Business, the Mitel Open Integration Gateway helps deliver seamless integration of unified communications and third-party business applications, enabling faster, more effective communications for your customers.

Mitel Open Integration Gateway supports three web services:

- Session Management Service – manages the communication session with Mitel Open Integration Gateway for services
- Call Control Service – controls and monitors CTI behavior in connected MiVoice Businesss
- Data Access Service – provides data change notifications and read access to MiVoice Business configuration data.

The Call Control Service is available with two levels:

- Standard Call Control – allows an application to monitor and control the telephony activity of Mitel physical and logical devices (devices programmed or configured in a MiVoice Business) including IP phones, Personal Ring Groups and line appearances on multi-line phones. The Standard Call Control Service allows applications to control and monitor a Mitel desktop phone similar to a user manually controlling the phone.
- Advanced Call Control – includes third-party call control capabilities and offers a full suite of functionality from simple call control to contact center monitoring and control. Advanced Call Control Service provides monitoring and control of MiVoice Business functions, e.g., Hot Desk Agent login (Internal and External), Trunking, Ring Groups, Hunt Groups, ACD2, ACD Express. Control relates to functions not normally associated with a specific desktop phone user. Support for MiVoice Business level monitoring (e.g., all conferences within a MiVoice Business) is included. Setting the phone message waiting lamp and auto answer are also only provided in Advanced Call Control

Mitel Open Integration Gateway offers a single point of access to web services available within a Mitel communication system. An application opens a communication session with a Mitel Open Integration Gateway. When authenticated and authorized, the application can use this communication session to access all Mitel Open Integration Gateway web services that the application is authorized to use. Mitel Open Integration Gateway provides full equivalency to the legacy MiTAI Call Control API, including support for MiVoice Business resiliency.

Available applications include Mitel developed applications, i.e., MiVoice Integration for Salesforce and MiVoice Integration for Google, and applications available from third-party developers who provide horizontal and vertically-focused CRM and ERP integrations, such as

for Oracle, SAP, and Microsoft. Also, Mitel provides comprehensive documentation, training, sample applications and hosted Mitel Open Integration Gateway virtual lab access to allow customers to integrate their business applications with the Mitel Open Integration Gateway API. All applications must be registered with Mitel as either Standard or Advanced applications; advanced applications require a Mitel certificate to use the Mitel Open Integration Gateway Advanced services.

COMPONENTS

Mitel Open Integration Gateway runs on the Mitel Standard Linux and is available for deployment on physical or virtual servers. Mitel Open Integration Gateway does not support co-residency with other applications. Mitel Open Integration Gateway is supported with Mitel Standard Linux in LAN mode; Mitel Standard Linux in network edge mode is not supported. Mitel Open Integration Gateway does not provide firewall protection and should be deployed on a private LAN; it should not be deployed in an enterprise DMZ or on the Internet. MiVoice Border Gateway may be used to provide a secure web proxy for remote applications. In this case both the Mitel Open Integration Gateway and MiVoice Border Gateway servers must be configured with third-party CA certificates.

Mitel offers two MiVoice Integration applications:

1. MiVoice Integration for Salesforce that uses a hosted Salesforce server and the Salesforce AppExchange
2. MiVoice Integration for Google that uses a hosted Google server and the Google Chrome Web Store.

Further information on the MiVoice Integration applications is available in the MiVoice Integration administrator guides and user guides, available on Mitel Edocs.

Information on capacity, including maximum number of applications supported, MiVoice Business connections, events per second, operations per second and MiVoice Business impacts, is available in *Mitel Open Integration Gateway Engineering Guidelines* available on Mitel Edocs.

LICENSING

Mitel Open Integration Gateway must maintain connectivity to the AMC for licensing and the Mitel Certificate Server (MCS) for the current Access Control List (ACL) used to authenticate and authorize application connections. The Mitel Open Integration Gateway server must be configured with a third-party CA certificate when using MiVoice Integrations.

Mitel Open Integration Gateway is licensed as a base package with add-on licenses. The base license includes the Session Management Service and Data Access Service. Additional Call Control licenses may be purchased in increments of one user up to 25,000 users. The Mitel Open Integration Gateway Call Control Service – Std / Adv Server license enables up to 25,000 users, and is more economical for larger numbers of users. Optional add-on licenses are required for MiVoice Integration users. These are available in increments of one or fifty users and Mitel Open Integration Gateway allows a maximum of 500 of these user licenses. With UCC licensing, in the CAPEX model, each premium user license includes one MiVoice

Integration for Salesforce user license and one MiVoice Integration for Google user license. In the OPEX model, UCC licensing activates all Mitel Open Integration Gateway in the ULM for the Mitel Open Integration Gateway maximum of 500 MiVoice Integration user licenses. Monthly license usage reports are automatically submitted to the Mitel Hosted AMC server and the Mitel Open Integration Gateway offers an option to e-mail (to an entered e-mail) a monthly usage report.

Each Mitel Open Integration Gateway user license provides two MiVoice Business monitors. Mitel Open Integration Gateway tracks monitors created by applications, not users in the MiVoice Business system. A particular application may use one or more monitors for each user. Mitel Open Integration Gateway supports MiVoice Business resiliency by creating a monitor on the primary and on the secondary MiVoice Business controllers.

Application developers specify the types and numbers of licenses required for the application. Mitel Open Integration Gateway may have either an Advanced Server license or Standard Server license but not both. Mitel Open Integration Gateway may be licensed with both Advanced and Standard User licenses. User licenses are not available when the corresponding Server license is activated.

Call control licenses are shared by all connected applications and allocated to applications on a first-come-first-served basis. Standard applications consume either Standard or Advanced Call Control Server licenses or Standard Call Control User licenses, but not Advanced Call Control User licenses. Advanced applications consume Advanced Call Control Server or User licenses. Sufficient call control licenses, standard and/or advanced, should be available to accommodate the concurrent user requirements of all applications.

EMERGENCY RESPONSE ADVISER

The Emergency Response Adviser (ER Adviser) is an application providing an emergency call display and response console for local security personnel. The ER Adviser is suitable for enterprise on premise or cloud deployments. Service provider deployment is not supported. The ER Adviser capabilities include:

- a visual and optional audible alert for new emergency calls
- display with the location of the phone used to dial the emergency number, as well as any extra information such as door access codes or user health information
- support for pager messages and e-mail messages to a pre-configured distribution list
- detailed logs of emergency calls and system generated events; logs may be displayed, formatted into text files or exported as XML or CSV files
- generation of a National Emergency Number Association (NENA) standard ALI database update file which can be sent to the PSAP

The ER Adviser provides additional functionality to the emergency service features offered by the MiVoice Business. The MiVoice Business performs the actual routing of emergency calls to the Public Safety Answering Point (PSAP). The public emergency response occurs independent of the ER Adviser, using facilities owned and maintained by the telephone company and PSAP service provider. The ER Adviser is used to alert local security personnel.

With display of the local number, security personnel may join in the call to listen to the conversation.

COMPONENTS

The ER Adviser is a light weight windows application. Supported operating systems and server specifications are available in the *Mitel Emergency Response Adviser Installation and Maintenance Guide*.

ER Adviser works with standard domain-based user group management system, and supports three user groups:

- ER-Administrator – allows access to all features and functionality of the ER Adviser application
- ER-Help desk – allows access to most features except scheduled tasks and database back-up and restores
- ER-User – designed for those responsible for monitoring the ER Adviser for received emergency calls and restricts access to only key operational areas of the application.

The ER Adviser supports the main terminal associated with the application server and remote consoles.

LICENSING

ER Adviser is available for enterprise deployment only. It is not included in the Managed Service Provider Program.

ER Adviser is licensed with a base software package that includes the base software (includes main terminal), pager support, PSAP update, one remote client and 100 station licenses. Additional licenses include station licenses for additional devices and remote terminal licenses for additional remote terminals.

Chapter 4

END-USERS AND DEVICES

END-USERS AND DEVICES

This section discusses end-users, IP desktop devices and applications, IP conference units, and specialty end-points.

For information related to network Quality of Service, end point configuration and infrastructure requirements refer to “Network and Networking Considerations” on page 167.

TYPES OF END-USERS

The Mitel portfolio of devices and applications are designed to meet the communications requirements of a wide range of end-users. When selecting end-points for a UC solution the following types of users, their requirements, and the system design implications should be considered.

Table 6: End-User Types

END-USER TYPE	DESCRIPTION
Public Telephony	Phone deployments that fall into this category are publicly-accessible phones, such as: lobby phones, cafeteria phones, hall way phones and class room phones. These users need to be able to place calls and receive calls and there is no requirement for UC capabilities. The extension number for these phones is cross referenced to a physical location rather than a user.
Basic telephony	Some employees may only require basic telephony services at their desktops or workstations, for example, factory and production workers, cashiers and retail clerks. These users do not usually require UC capabilities, they may, however, require access to voice mail and unlike public phones, the extension number for these phones will be cross referenced to a specific user.
Basic user - desktop and teleworker	This type of user requires basic telephony services and may also require multi-line support and the ability to access basic MiVoice Business UC applications from their desktops. These users would typically be office workers, lab workers, SOHO workers or teleworkers.
Power user - desktop and teleworker	The power user requires basic telephony services, multi-line support and the ability to access more MiVoice Business UC applications from their desktops than the basic user. These users would typically be office managers, administrative staff, SOHO workers or teleworkers.
Executive user	This user requires basic telephony services, multi-line support and the ability to access the full range of MiVoice Business UC applications from their desktops. As the name suggests, these users are typically executives, managers and end-users in supervisory roles.
Executive user (with Internet/Intranet access)	This user has the same requirements as the executive user, but, the ability to access the Internet or Intranet is also required. These users are typically executives and/or users that need the ability to access Web-based information without using a PC.

Different types of end-users will generate different call traffic patterns, these call traffic patterns and the resulting call processing loads need to be taken into account.

For information on call patterns, traffic and MiVoice Business call handling performance refer to the *MiVoice Business Engineering Guidelines* and the *MiVoice Business System Engineering Tool*.

Note: Mitel's UC licensing model uses naming conventions that are similar to the end-user names described above. In most cases, the end-user type fits with the similarly named UC license, however, this is not required. A particular user type may select any of the set types or UC licenses as required for their communication needs, however, there is no correlation between the names used for UC licenses and the names used to describe types of end-users.

MITEL IP DESKTOPS

Mitel has one of the most comprehensive portfolios of IP desktop devices and applications in the industry. These solutions give users easy, intuitive access to the feature-rich telephony and advanced desktop applications enabled by Mitel IP communications platforms

- “MiVoice IP Phones” on page 65
- “SIP Desktop Devices” on page 66
- “Mitel IP Desktop Applications” on page 67

MIVOICE IP PHONES

MiVoice IP Phones address a range of applications, from basic lobby phones to feature-rich executive phones.

The table “Supported Mitel IP Phones” on page 66 provides a basic overview of the available MiVoice IP Phones for the range of UC Enterprise Solution topologies.

For additional information regarding MiVoice IP Phones the reader should refer to the following documents, which can be found on Mitel Edocs:

- MiVoice IP Phones and Peripherals Feature Matrix
- Mitel IP Telephone Data Sheets (specifications and supported standards)
- Mitel IP Desktop FAQ
- Mitel IP Telephone Product Bulletins
- *Mitel IP Sets Engineering Guidelines* (Discusses power requirements, required infra- structure and deployment)

Table 7: Supported Mitel IP Phones

MITEL IP DESK PHONE	TYPICAL PHONE CLASS	APPLICATION	FEATURE PROGRAMMABILITY
MiVoice 6920	Entry Level - business phone	Basic user – desktop and teleworker	Basic – access to MiVoice Business enabled applications
MiVoice 6930	Mainstream – business phone	Executive and supervisory desktops	Full feature and advanced UC capabilities
MiVoice 6940	Premium – business phone	Internet/Intranet appliance for executive and supervisory desktops	Full feature, advanced UC capabilities and Internet/Intranet access
MiVoice 5304	Basic - IP display phone	Public areas (lobbies, guest rooms, classrooms, retail)	Basic - access to MiVoice Business enabled applications
MiVoice 5312	Entry level - key system phone	Basic user - desktop & teleworker	Basic - user programmable access to MiVoice Business enabled applications
MiVoice 5324	Mainstream - key system phone	Power user - desktop & teleworker	Expanded - user programmable access to MiVoice Business enabled applications
MiVoice 5320	Entry - business phone	Basic user - desktop & teleworker	Basic - user programmable access to MiVoice Business enabled applications
MiVoice 5320e	Entry - business phone	Basic user - desktop & teleworker	Basic - user programmable access to MiVoice Business enabled applications
MiVoice 5330e	Mainstream - business phone	Executive & supervisory desktops	Full feature & advanced UC capabilities
MiVoice 5340e	Premium - business phone	Executive & supervisory desktops	Full feature & advanced UC capabilities
MiVoice 5360	Premium - business phone	Internet/Intranet appliance for executive & supervisory desktops	Full feature, advanced UC capabilities & Internet/Intranet Access

SIP DESKTOP DEVICES

Mitel supports a number of third-party SIP telephones that have been verified for interoperability with Mitel products.

The Mitel SIP Centre of Excellence (SIP CoE) performs interoperability testing between third-party devices and Mitel products. The CoE generates documents that cover the results of the interoperability tests and how the devices should be configured for successful inter-operation.

For the complete list of third-party SIP devices that are supported, refer to the Knowledge Base article called *Mitel Technical Reference Guide: Mitel Compatibility and Third-Party Certification*

Reference Guide for Mitel Products, 08-5159-00014.

The reference guide can be found on Mitel On-Line under Support - Technical Support - SIP Centre of Excellence.

A number of Knowledge Base articles exist that are referred to as SIP configuration guides. These guides provide configuration recommendations for SIP servers and SIP end-points.

The *Mitel Technical Reference Guide* lists the available SIP configuration guides and where to find them.

The SIP configuration guides provide the following information:

- Configuration recommendations for SIP phones and the MiVoice Business
- Configuration recommendations for third-party SIP servers and SIP phone
- A list of potential interoperability and/or feature limitations

MITEL IP DESKTOP APPLICATIONS

Mitel offers the following desktop applications; these applications run on IP desktop phones and will improve the user experience and drive employee productivity:

For more information on Mitel IP desktop applications refer to product information on Mitel Edocs.

Live Content Suite

Live Content Suite enables the creation and publishing of dynamic and personalized information to end-users, transforming Mitel MiVoice 5320e, 5330e, 5340e, and 5360 IP Phones into rich media information appliances. Live Content Suite improves employee communications by providing easy access to the information they need, when they need it and where they need it, on their phones.

Live Blogger allows corporate executives to deliver custom content to employee's phones in order to communicate crucial messages through the written medium of communication to the phone.

Another useful function of this application includes the ability to obtain information updates via RSS feeds directly on the desktop phone.

MITEL IP DESK PHONE PERIPHERALS

Desktop functionality can be extended via a range of add-on peripherals and accessories that are designed to provide the end-user with more choice and flexibility.

The following Mitel IP peripherals are available.

Table 8: Mitel IP Peripherals

MITEL IP PERIPHERAL	DESCRIPTION	SUPPORTED PHONES								
		MIVOICE 5324	MIVOICE 5330	MIVOICE 5330E	MIVOICE 5340E	MIVOICE 5360	MIVOICE 5610	MIVOICE 6920	MIVOICE 6930	MIVOICE 6940
Mitel 5610 DECT handset and IP DECT stand	The Mitel 5610 DECT Handset and Mitel IP DECT Stand offer a low cost wireless solution for personal area mobility on IP Phones.						✔			
Mitel Cordless (DECT) Accessories	A cordless (DECT) handset and a cordless (DECT) headset are available for IP Phones		✔	✔	✔	✔			✔	✔
Mitel Bluetooth® Accessories	A Bluetooth® handset is offered that provides corridor mobility for Mitel IP Phones.		✔	✔	✔	✔			✔	✔
Mitel Line Interface Module (LIM)	The LIM integrates with IP Phones and provides a connection to an analog line that is secondary to the IP connection to support Teleworker resiliency and local emergency call support.	✔	✔	✔	✔	✔				
Mitel Programmable Key Modules (PKMs)	Mitel PKMs allow for the addition of 12 or 48 or up to 96 buttons to the existing programmable keys on IP Phones.	✔	✔	✔	✔			✔	✔	✔

For additional information, refer to the product documentation, the *Mitel IP Sets Engineering Guidelines*, and the *MiVoice Business Engineering Guidelines*.

MITEL IP CONSOLES

The following Mitel IP Consoles are intended for use by attendants, receptionists and operators.

For additional information about Mitel's IP Consoles, refer to the Product Documentation on Mitel Edocs.

- “MiVoice Business Console” on page 69
- “Mitel 5540 IP Console” on page 69

MIVOICE BUSINESS CONSOLE

The MiVoice Business Console supersedes the 5550 IP Console which is no longer supported in Release 9.0. Customers that are presently using the 5550 IP Console should upgrade their console.

The MiVoice Business Console is a soft console application with all audio and telephony functions (voice, call announcement and tones) as well as keyboard input integrated into the PC application.

Like its predecessor, the MiVoice Business Console enables operators to handle a large volume of calls. It is targeted at businesses with over 100 users and offers advanced capabilities such as transfer assistant, as well as presence and busy lamp integration.

The MiVoice Business Console can be deployed on the customer's LAN (or via an MPLS connection) with full UC capabilities and resiliency. The UC functions, presence, and chat are not supported when the MiVoice Business Console is used as a Teleworker through the MiVoice Border Gateway. Resiliency to the MiVoice Border Gateway is not supported in release UC Enterprise Release 1.0 when deployed as a Teleworker. The MiVoice Border Gateway supports resiliency to primary and secondary MiVoice Business call controllers.

MITEL 5540 IP CONSOLE

The Mitel 5540 IP Console is the ideal attendant solution for small and medium businesses using the Mitel MiVoice Business solution. The 5540 IP Console can be used as an attendant console, a sub-attendant position for departments or workgroups, or as a back-up answering position. Affordable, simple, with a broad range of standard and specialty functions make the 5540 IP Console the practical choice for small-business or hospitality customers.

SPECIALTY END-POINTS

Mitel's product portfolio contains a number of specialty IP and SIP end-points that are described in the following section. Refer to Product documentation on Mitel-On-Line (MOL) for more information on any of the following specialty end-points.

MIVOICE CONFERENCE PHONE

The MiVoice Conference Phone is an audio conference bridge with in-room collaboration. The MiVoice Conference Phone provides audio conferencing with local presentation capabilities.

MiVoice Conference Phone supports audio conferences with a maximum of four parties natively within the Conference Phone (that is, the Conference Phone plus three external participants) plus the ability to set up an additional consultation call with an external party.

MIVOICE VIDEO PHONE

The MiVoice Video Phone with Remote Collaboration provides the same functionality as the MiVoice Conference Phone with In-room Collaboration while also enabling remote presentation and multi-party video conferencing functionality.

The MiVoice Video Phone supports video conferences with a maximum of four parties natively within the MiVoice Video Phone, for example the MiVoice Video Phone plus three external participants.

Note: One of the external participants could be a link into another video conference bridge.

MIVOICE 5505 GUEST IP PHONE

The MiVoice 5505 Guest IP Phone provides a unique hospitality feature set aimed at meeting the needs of hospitality customers who are looking to deploy IP telephony to the guest room. The 5505 Guest IP Phone base provides the physical features hotel guests have come to expect. The 5505 Cordless Handset provides industry-leading features by virtue of its built-in, two-line backlit display. With an operating range of up to 50 meters (150 feet) from the phone base, the 5505 Cordless Handset is ideal as a second phone for a guest room or a suite of rooms.

THIRD-PARTY END-POINTS

Mitel supports a number of third-party end-points such as: SIP-based Analog Terminal Adapters (ATA), alarm interfaces and door openers. Refer to the Mitel SIP Centre of Excellence for a list of devices that have been tested for interoperability, additional information may be obtained through Mitel Professional Services.

MICOLLAB DESKTOP CLIENT AND MICOLLAB MOBILE CLIENTS

This section describes Mitel's portfolio of MiCollab Client end-points.

MICOLLAB DESKTOP CLIENT

The MiCollab Desktop Client is an application that is installed on the user's Windows desk top computer, or Microsoft Surface Pro tablet. The MiCollab Desktop Client allows users to control their IP desk phone and associated devices from their computer or Microsoft Surface Pro tablet. The MiCollab Desktop Client includes an embedded softphone, providing users with two devices, if both are configured on the PBX. The softphone requires a separate license.

The MiCollab Desktop Client allows users to search their corporate directory, check visual voice mail, and automatically update their presence status and call routing preferences based on their location or time of day.

For additional information about MiCollab and MiCollab Desktop Client, refer to the product documentation on Mitel Edocs.

MICOLLAB MOBILE CLIENT

MiCollab Mobile Client is a suite of Unified Communication applications; the mobile client can be installed on supported BlackBerry®, Android™, and iPhone® / iPad®devices and extends key MiCollab Client capabilities to mobile users.

For Android, and iOS devices, an integrated SIP softphone allows calling over Wi-Fi or 3G/4G data networks.

The available MiCollab Mobile Clients are shown in the table “MiCollab Mobile Clients” on page 71.

Table 9: MiCollab Mobile Clients

MOBILE CLIENT	DESCRIPTION
MiCollab Mobile Client for BlackBerry	MiCollab Mobile Client for BlackBerry is a stand-alone client that users install on their BlackBerry mobile device. The client provides automatic dynamic status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, corporate contacts, and OfficeLink calling capabilities.
MiCollab Mobile Client for Android	MiCollab Mobile Client for Android is a stand-alone client that users install on their Android mobile device. The client provides automatic dynamic status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, corporate contacts, a softphone and OfficeLink calling capabilities.
MiCollab Mobile Client for iPhone	MiCollab Mobile Client for iPhone is a stand-alone client that users install on their iPhone mobile device. The client provides automatic dynamic status updates based on the user's current location. In addition, the client provides access to call logs, messages, corporate contacts and softphone calling capabilities.
MiCollab Mobile Client for iPad	MiCollab Mobile Client for iPad is a stand-alone client that users install on their iPad mobile device. The client provides automatic dynamic status updates based on the user's current location. In addition, the client provides access to call logs, messages, corporate contacts and softphone calling capabilities.

For additional information about MiCollab and MiCollab Mobile Clients, refer to the product documentation on Mitel-On-Line (MOL).

OTHER MICOLLAB CLIENTS

MiCollab Client Web Portal: The MiCollab Client Web Portal provides an intuitive tabbed interface for remote access to MiCollab Client features from a supported Web browser on your computer.

Refer to the *MiCollab Engineering Guidelines*, for detailed information pertaining to MiCollab connections to the MiVoice Border Gateway and security certificates.

Chapter 5

AVAILABILITY AND RESILIENCY

AVAILABILITY AND RESILIENCY

System reliability, redundancy, and resiliency are all inter-related and have a direct influence on the availability of services. A non-redundant, non-resilient system will provide users with a high level of availability, however, a higher level of service availability can be achieved when redundant and resilient design techniques are employed.

The term “resiliency”, describes the ability of a network, an application or a service to adjust to and recover from a failure. The failure might be a network failure, a power failure, a server failure, or a software application failure.

Using self-correction techniques that take advantage of the IP-network characteristics of location independence and network element distribution, resiliency is an improvement over the more costly and less flexible redundancy solution.

Resilient systems provide higher levels of service availability than non-resilient systems by providing continued availability, even when a system component failure occurs.

Different businesses will have different availability requirements, Mitel's Unified Communication solutions can be tailored to provide the varying degrees of overall service availability needed to meet the requirements of a particular business.

To determine the system availability requirements for a particular business, the following business requirements need to be determined:

- What level of availability is required for the different services? A business will have certain availability requirements for basic telephone operation but the same business may have different availability requirements for the voice mail system or for advanced telephony features.
- What level of service outage is acceptable? For each customer, the business continuity or availability requirements need to be understood so that an acceptable level of service outage can be defined. For example, a business that needs phones operational from nine to five, five days a week will accept a different level of system outage than a business that needs phones operational twenty-four hours a day, seven days a week.

Additional information pertaining to meeting a customer's availability requirements and network design for availability can be found in a suite of Mitel white papers, for details refer to the Mitel document called List of Telephone System Availability Document, available on Mitel-On-Line (MOL) under the Business Continuity section. Further details on MiVoice Business and IP telephone resiliency can be found in the *MiVoice Business Resiliency Engineering Guidelines*.

The next sections of this chapter discuss the availability and resiliency mechanisms as they relate to the various components, applications and services that are used to build the overall UC solution.

MITEL IP DESK PHONES

Prior to deploying the UC solution it will need to be determined if there are specific users and devices that require resilient operation.

If required, the MiVoice Business solution allows individual IP phones to be configured and licensed for resilient operation to meet the needs of users that require high availability telephony service.

The Administrator may choose to make all users and devices resilient, or only those required for critical services. The Administrator will also need to determine which MiVoice Business system each user and device will fail over to in the event that the primary MiVoice Business fails.

When a resilient IP phone is on an active call with another IP phone and its primary MiVoice Business system or the link between the phone and the MiVoice Business system fails, the phone will operate in the following way:

- The current phone call survives, provided the network media path remains operational.
- The IP phone fails over to its secondary MiVoice Business system when the current phone call terminates.
- When the primary MiVoice Business returns to service, the IP phone will fail back to the primary MiVoice Business.

Information on planning for resilient operation, network design and configuring users for resilient operation can be found in the *MiVoice Business Engineering Guidelines* and the *MiVoice Business Resiliency Engineering Guidelines*, available on Mitel-On-Line (MOL).

MIVOICE BUSINESS CONSOLE

The MiVoice Business Console is an IP console that supports resilient operation.

- Like other resilient IP phones, if a resilient IP Console is hosting an active call stream when its primary MiVoice Business system or the link between the console and the MiVoice Business system fails, then the console experiences call resiliency; that is, the call survives.
- The console does not fail over to its secondary MiVoice Business system until the call has ended and the console is in the idle state.
- When the primary MiVoice Business returns to service, the IP Console fails back to the primary MiVoice Business.

At MiVoice Business Release 7.0, when an IP console is connecting to the primary and the secondary MiVoice Business controllers/servers through an MiVoice Border Gateway connection, should the MiVoice Border Gateway itself fail, the console will not failover to the secondary MiVoice Border Gateway.

However, if the communication link between the MiVoice Border Gateway and the primary MiVoice Business fails, or the primary MiVoice Business fails, the MiVoice Border Gateway will failover to the secondary MiVoice Business, which in turn allows the IP console to communicate with the secondary MiVoice Business.

MIVOICE 5540 IP CONSOLE

The MiVoice 5540 IP Console is an IP console that supports resilient operation. Like other resilient IP phones, if a resilient MiVoice 5540 IP Console is hosting an active call stream when

its primary MiVoice Business system or the link between the console and the MiVoice Business system fails, then the console experiences call resiliency, that is, the call survives.

The console does not fail over to its secondary MiVoice Business system until the call has ended and the console is in the idle state.

When the primary MiVoice Business returns to service, the IP Console will fail back to the primary MiVoice Business.

The MiVoice 5540 IP Console supports Power over Ethernet (IEEE 802.3af) operation, which allows the console to be remotely powered from a PoE capable L2 switch, for enhanced availability the L2 switch itself could be powered via a UPS.

MIVOICE BUSINESS - HARDWARE PLATFORMS

The MiVoice Business call control software may be installed on a number of different hardware platforms, including MiVoice Business 3300 ICPs, Industry Standard Servers running Mitel Standard Linux (MSL) or Industry Standard Servers running VMware. For information beyond what is provided here, refer to the Mitel MiVoice Business product documentation.

MIVOICE BUSINESS 3300 ICP AND EX

The MiVoice Business 3300 ICP and EX platforms are Mitel proprietary hardware platforms used for running the MiVoice Business software. There are three MiVoice Business platforms available to meet different user scaling and analog/digital PSTN connectivity requirements, the CX II, the MXe III, and the EX (together referred to as MiVoice Business Appliances). These platforms can also provide the following functionality:

- IP to PSTN gateway (analog and digital/PRI)
- Analog and TDM phone connectivity
- Voice mail
- Music on Hold
- Ad-hoc conferencing
- Basic call recording

INDUSTRY STANDARD SERVERS (ISS)

MiVoice Business can be installed on a number of Mitel approved Industry Standard Servers (ISS). ISS platforms offer higher call processing performance and faster fault recovery times than the MiVoice Business 3300 ICP platforms.

When compared to MiVoice Business 3300 ICP platforms, ISS platforms can offer improved availability of hardware components that are typically known to exhibit higher levels of reliability. These include use of multiple power supplies, multiple hard disk drives with RAID configurations, RAM with parity and error correction mechanisms, multiple redundant cooling fans.

For large service provider deployments, there are additional improvements that can be achieved through the use of chassis-based technologies rather than traditional “rack and stack” ISS

platforms. Improvements include advanced integrated management which provides advance warning of a pending failure and hot swap capabilities for power supplies, fans and hard drives, which allows a component change to be performed without taking the server out of service.

Chassis-based technologies may support some resilient networking and switching functions, and may also include link aggregation capabilities, multiple redundant switching backplanes, and multiple external connections, which can simply the deployment of systems that need to be resilient.

To determine if a particular server is supported for a given application, refer to the Mitel Qualified Hardware List.

MIVOICE BUSINESS RESILIENCY

While failures and outages in any complex system are unavoidable, the MiVoice Business call control resiliency solution provides the ability to preserve telephony service in the event that a MiVoice Business is out of service or network connectivity to the MiVoice Business has failed.

The MiVoice Business resiliency capability is available on all MiVoice Business hardware platforms.

Additional information related to resilient operation can be found in the *MiVoice Business Engineering Guidelines*, the *MiVoice Business Resiliency Engineering Guidelines* and the *Mitel Virtual Appliance Deployment Solutions Guide*, available on Mitel-On-Line (MOL).

RESILIENT OPERATION - DESCRIPTION

Resilient call routing handles cases in which a phone is in service on its secondary MiVoice Business system or in transition between MiVoice Business systems. When configured in a resilient cluster, all MiVoice Business systems are aware of the primary and secondary systems associated with each IP phone and are able to route calls to these phones when they are in service on either their primary or secondary systems.

Call Survival

Call survival is the process of keeping active calls alive when a device involved in an active call loses contact with its MiVoice Business system. An IP phone does not have to be resilient to experience call survival because maintaining a previously established voice path between two IP phones is not dependant on the availability of the MiVoice Business system. Once a call that was in survival mode has ended; a non-resilient device will go out of service because it can't reach its MiVoice Business system, but a resilient device will fail over to its secondary MiVoice Business system.

During a MiVoice Business system or network failure, both non-resilient and resilient devices (that are currently in talk state), experience call survival, but because they will have lost the link to their MiVoice Business they cannot access phone features or dialing functionality.

Only calls in talk state are capable of call survival in a failure situation. Calls that are in the process of being set up or are in feature transition, for example, do not experience call survival.

Resilient Call Control Features

While in service on a secondary MiVoice Business , an IP phone will retain basic call service. Most call features are available while a phone is in service on a secondary system, some with possible behavior differences. For details refer to the *MiVoice Business Resiliency Engineering Guidelines*, specifically, the chapter on feature resiliency.

MIVOICE BUSINESS - SURVIVABLE GATEWAY

In some cases, the customer may require the ability to access the local PSTN from the customer premises if there has been a service interruption related to the WAN connectivity between the customer site and the data centre. PSTN access may be also required for legacy business purposes and also for emergency services. These requirements can be satisfied by deploying a MiVoice Business 3300 ICP platform or a MiVoice Business EX at the customer site. The MiVoice Business Appliances can provide trunking capabilities to connect to the local PSTN, and process incoming and outgoing calls.

More information on using a MiVoice Business 3300 ICP as a survivable gateway can be found in “External Connectivity” on page 111, the MiVoice Business product documentation, and the *Mitel Survivability of Remote Branch Offices Solutions Guide*.

MIVOICE BUSINESS FOR INDUSTRY STANDARD SERVERS (ISS)

MiVoice Business for ISS offers the same resiliency capabilities as MiVoice Business 3300 ICP. However, when compared to MiVoice Business 3300 ICP platforms, ISS platforms offer improved availability of hardware components that are typically known to exhibit higher levels of reliability.

MiVoice Business for ISS works with SIP trunks and can handle multiple routes which offers improved trunking availability compared to a MiVoice Business 3300 ICP. For instance, if a MiVoice Business 3300 ICP loses a physical trunk connection, it may result in the loss of an external trunk connection, but with MiVoice Business on ISS, SIP trunks can be routed to alternative paths.

Further information is provided in the section “Industry Standard Servers (ISS)” on page 77.

MIVOICE BUSINESS MULTI-INSTANCE

MiVoice Business Multi-Instance is a product that allows numerous instances of MiVoice Business to be run on a single ISS, the ISS has the same hardware availability characteristics as MiVoice Business on ISS. Each MiVoice Business instance on a MiVoice Business Multi-Instance supports the same resiliency capabilities as MiVoice Business.

When deploying a resilient MiVoice Business Multi-Instance solution, the IP sets are configured with a primary MiVoice Business running on one physical server, and a secondary MiVoice Business running on a different physical server.

MiVoice Business Multi-Instance allows individual instances of MiVoice Business to be run, a tenanted model is not supported. This improves service availability since it is possible to reset

a single instance of MiVoice Business without impacting the other MiVoice Business instances running on the same server platform.

MIVOICE BUSINESS VIRTUAL

The MiVoice Business Virtual offering is a version of the MiVoice Business software that is packaged in Open Virtualization Archive (OVA) format for deployment into a VMware environment.

MiVoice Business Virtual offers the same resiliency capabilities as MiVoice Business, specifically, primary node failure detection and automated failover to a secondary node.

In addition to the resilient operation capabilities of MiVoice Business, VMware can offer additional resiliency capabilities, this is accomplished with VMware's High Availability (HA) solution in conjunction with VMware's vCloud Center for automated operation.

HA is a service that automatically detects a physical server failure or a virtual machine failure, and restarts virtual machines on alternative servers when a failure is detected. In the case of MiVoice Business Virtual, VMware HA will detect a failure on the server that is hosting the MiVoice Business Virtual or the failure of the virtual machine containing MiVoice Business. Upon host failure, VMware HA will restart a new instance of the MiVoice Business Virtual on an alternate server host. Upon a Virtual machine failure, VMware HA will restart a new instance of MiVoice Business Virtual.

When combined together, the resiliency capabilities of MiVoice Business Virtual and VMware's HA capabilities provide a solution that offers very high service availability. For example, should the server that is hosting the primary MiVoice Business Virtual experience a failure, the phones will failover to the secondary MiVoice Business Virtual and service will be maintained. Meanwhile, HA will have detected that the primary MiVoice Business Virtual has failed and will restart the primary MiVoice Business Virtual on an operational server. Once the primary MiVoice Business Virtual is back in service, the phones will recover (return) to the primary MiVoice Business Virtual.

Without HA, the system would have been operating in a non-resilient mode until action was taken to repair the primary MiVoice Business Virtual and restore it to service.

The major benefit provided by HA is that HA reduces the recovery time of a failed unit, and automates the recovery process. This greatly reduces the Mean Time To Recovery time, which would normally involve a technician call-out and possible travel time.

Certain policies must be adhered to when using the resiliency capabilities of MiVoice Business Virtual. For instance, anti-affinity rules should be established to ensure that the primary MiVoice Business Virtual and secondary MiVoice Business Virtual are never deployed on the same physical host server within a VMware cluster.

Additional information related to MiVoice Business resiliency can be found in the *MiVoice Business Resiliency Engineering Guidelines*. Information related to VMware and its capabilities can be found in the *Mitel Virtual Appliance Deployment Solutions Guide*.

APPLICATIONS

This section discusses the resiliency capabilities of the various applications that are available as part of the Unified Communications solution.

For additional information refer to the specific product's documentation and the following sections:

- “Applications” on page 47
- “End-Users and Devices” on page 63
- “External Connectivity” on page 111

For information on VMware, see “VMware and Service Reliability” on page 89 and the *Mitel Virtual Appliance Deployment Solutions Guide*.

MICOLLAB UNIFIED MESSAGING - VOICE MAIL

The MiCollab Unified Messaging is an e-mail application that is a feature of MiCollab. MiCollab Unified Messaging offers users the ability to manage their voice mail, e-mail, and fax messages from their PCs or telephones. MiCollab Unified Messaging also allows inbound callers to an organization to quickly find the person they need to talk with, using a speech-enabled auto attendant and call routing functionality.

Like an IP set, the MiCollab Unified Messaging application supports MiVoice Business resilient operation. Specifically, the MiCollab Unified Messaging system has the ability to fail over to a secondary MiVoice Business when the primary MiVoice Business is non-operational or unreachable, and then to recover to the primary MiVoice Business when it returns to service.

The MiCollab Unified Messaging application does not natively support resiliency of the application itself. When higher levels of service availability are required:

- The use of MiCollab Virtual, which runs in a VMware environment should be considered. MiCollab Virtual, can take advantage of the additional resiliency capabilities provided by VMware's HA.
- MiCollab Unified Messaging storage should be located on a different server than the Mi-Collab server, typically storage will be located in a SAN and access to the SAN will be via redundant connections.

For information about resiliency, programming for resilient operation and SAN technology, refer to the following documents, which are available on Mitel-On-Line (MOL).

- *MiCollab Unified Messaging Technician’s Handbook*
- *MiVoice Business Resiliency Engineering Guidelines*
- MiVoice Business System Administration ToolHelp.
- *Mitel Virtual Appliance Deployment Solutions Guide*

MICOLLAB

MiCollab is a comprehensive, integrated solution that unifies business communications applications, MiCollab supports any combination of the following applications.

- MiCollab Unified Messaging
- MiCollab Client Service
- MiCollab Audio, Web, and Video Conferencing
- MiVoice Border Gateway

MiCollab is available on the following hardware platforms:

- Industry Standard Server (Non- Resilient)
- Virtual Appliance (Resilient Capable)

Higher service availability is supported when MiCollab is deployed as a virtual appliance within the VMware vSphere Cloud Operating System, this product offering is called MiCollab Virtual.

For information on VMware, see “VMware and Service Reliability” on page 89 and the *Mitel Virtual Appliance Deployment Solutions Guide*.

MiCollab Client Multi-Tenant Service

MiCollab Client Multi-Tenant Service is a product that combines the call control capabilities of Mitel communications platforms with contact management, dynamic Status, and presence information to simplify and enhance communications. MiCollab Client Multi-Tenant Service is available as a component of MiCollab.

If the PC softphone is deployed on a desktop or workstation it can connect to the MiCollab Client Multi-Tenant server directly via the LAN. If, however, this is installed on a laptop or a tablet that may go outside of the range of the business network (Wi-Fi or LAN), then the PC softphone should always register via the MiVoice Border Gateway, even when on the local network. Registering with the MiVoice Border Gateway allows for hand-over when switching between business and external networks, for improved network connectivity and availability.

The Mobile softphone should always connect to the external MiVoice Border Gateway, even if it uses the internal business network to reach the business Internet Gateway.

MiCollab Client Multi-Tenant Service Availability

The MiCollab Client Multi-Tenant server must be operational for the MiCollab Clients to be able to place calls. The MiCollab Client Multi-Tenant server itself is not resilient, which means that should the MiCollab Client Multi-Tenant server fail, then any device that connects to the MiCollab Client Multi-Tenant server, such as mobile phones and PC Softphones will lose telephony connectivity.

For mobile users that require higher levels of availability it is recommend that both a mobile softphone and EHDU are installed on the smart phone device, and the users should be deployed with EHDU within the UCC profile. This will provide a secondary and alternative carrier

connection back to the system, and it will also allow mobility outside the office across different networks.

MiCollab Audio, Web, and Video Conferencing

MiCollab Audio, Web, and Video Conferencing is a comprehensive audio conferencing and web collaboration application that improves collaboration and information sharing among employees and with customers, partners, and suppliers. MiCollab Audio, Web, and Video Conferencing is available as a core component of MiCollab. MiCollab Audio, Web, and Video Conferencing provides no native application resiliency; MiCollab Audio, Web, and Video Conferencing relies on MiCollab service availability.

MiVoice Border Gateway

The MiVoice Border Gateway is a highly scalable solution that ensures the deployment of secure internal and external work spaces, enabling remote workers, road warriors, and day-extenders seamless access to the voice and data capabilities of the office, wherever they are.

MiVoice Border Gateways can be clustered for license sharing and load balancing for devices that support the MiNet protocol. For SIP device connectivity and SIP-Trunk connectivity MiVoice Border Gateways are typically clustered as primary/secondary pairs.

Supported MiNet sets can hold IP addresses for two MiVoice Border Gateways. If a set loses its connection to the MiVoice Border Gateway and it cannot re-establish the connection, it will try the second IP address on its list. When MiNet sets are configured for persistent resiliency lists, this resiliency list is remembered through a power cycle.

If MiVoice Border Gateway high availability service is required, the MiVoice Border Gateway Virtual offering which runs in a VMware environment should be considered.

The VMware High Availability (HA) solution is used to provide application level resiliency. HA is the recommended deployment mode when used with UC in order to provide a common IP address that the UC clients can register with. Additional information can be found in the MiVoice Border Gateway product documentation.

MiCollab includes MiVoice Border Gateway within the application suite. For UC solutions, the MiVoice Border Gateway within MiCollab is configured as the master instance of the MiVoice Border Gateway cluster. In the case of MiCollab failure, the remaining units within the MiVoice Border Gateway cluster will continue to function while the master MiVoice Border Gateway recovers.

MITEL OPEN INTEGRATION GATEWAY

The Mitel Open Integration Gateway is a software solution that executes on an industry standard server. Mitel Open Integration Gateway offers web services to applications and also integration with web-based services such as Google and Salesforce. Detailed information about services and how an application communicates with a Mitel Open Integration Gateway is discussed in the Mitel Open Integration Gateway developer guides.

At the time of writing, an Mitel Open Integration Gateway resiliency mechanism that employs a primary and secondary Mitel Open Integration Gateway sever is not supported, however, Mitel Open Integration Gateway does support inter-operation with MiVoice Business systems that are configured for resilient operation. For instance, if a Mitel Open Integration Gateway system is configured to operate with a resilient pair of MiVoice Business systems, and the primary MiVoice Business fails or becomes unreachable, the IP phones that were homed to the primary MiVoice Business will failover to the secondary MiVoice Business and the Mitel Open Integration Gateway will now provide services to these IP phones via the secondary MiVoice Business.

If Mitel Open Integration Gateway application resiliency is required, the Mitel Open Integration Gateway Virtual offering which runs in a VMware environment should be considered. VMware offers a High Availability (HA) solution which will provide Mitel Open Integration Gateway with enhanced system availability.

MIVOICE BUSINESS EXPRESS

The MiVoice Business Express provides a complete communications solution for small to medium businesses. MiVoice Business Express runs as virtual appliance on a VMware vSphere infrastructure.

The MiVoice Business Express consists of the following components:

- MiVoice Business
- MiCollab: provides the following applications:
  - MiCollab Unified Messaging
  - MiCollab Client Service
  - MiCollab Audio, Web, and Video Conferencing
  - MiVoice Border Gateway

For information on VMware, see “VMware and Service Reliability” on page 89 and the *Mitel Virtual Appliance Deployment Solutions Guide*.

NETWORKING AND AVAILABILITY

Network connectivity, between the customer premises and the data centre, and within the customer premises is often the weakest link in a UC deployment. Secondary connections and dual routers should be considered for deployments that are sensitive to service outage time. Service Level Agreements (SLA) should also be considered when signing with a carrier, because the network link from the customer premise to the data centre is critical to the business. Such links are not easily achieved over the Internet, so the carrier should be selected with care, and it should line up with connectivity from the hosted data center.

There are many factors related to network design that must be planned to ensure that the UC solution components can reliably communicate with each other in the event that a network-related failure occurs. This section discusses these factors.

TRUNKING CONSIDERATIONS

IP Trunks are used to connect multiple MiVoice Business controllers together. SIP trunks may be used to connect the customer premises to the data centre and also to a service provider who, in turn, passes connections on to the PSTN. TDM trunks may be used to connect MiVoice Business controllers to the PSTN, or to connect multiple MiVoice Business controllers together.

IP trunking, ARS, and Hunt Groups

A well-designed IP network will be partially meshed, meaning that there is always more than one IP path between IP networking devices. An IP network that offers multiple connection paths is inherently resilient.

When MiVoice Business controllers are introduced into a partially-meshed IP network, it follows that IP trunks within the network are resilient at the physical level. Additional trunk resiliency can be provided by TDM trunks. Use ARS and secondary routing to configure alternative paths through the network to minimize a single point of connection failure.

SIP Trunking

Service providers offer SIP trunks that provide flexible and cost-effective solutions for connecting the customer premises to the data centre. SIP trunking can be used to connect the customer premises to multiple service providers, and the SIP trunking solution can be used to provide trunking resiliency.

For SIP Trunks, a gateway unit or Session Border Controller (SBC) function, is required to isolate the customer network from the carrier network. The MiVoice Border Gateway provides this gateway functionality, along with a number of SIP SBC functions. The MiVoice Border Gateway function can be deployed in pairs for redundant operation.

Primary and secondary SIP trunk registration with primary and secondary SBCs can be used to a common service provider and provide 100% failover in the event of a lost SIP trunking gateway or connection.

TDM Trunking

In non-IP networks, it is standard practice to use alternate TDM trunk routes to provide trunk resiliency. This practice remains valid in IP/TDM-based networks, and the level of network resiliency increases if these TDM paths are employed as back-up paths for IP trunks.

WAN AND OTT CONSIDERATIONS

Compared to all of the other components that comprise the UC solution, the external network connections are typically more likely to fail. Keeping this in mind, the availability of all WAN links and Over-the-Top (OTT) connections must be taken into account.

The availability of WAN connections can be improved by:

- Choosing a service level agreement (SLA) that meets the availability requirements.
- Using dual WAN connections to provide WAN redundancy.

- Using routers to implement WAN connections so that routing protocols such as HSRP or VRRP can be employed to detect faults and switch to alternate paths.
- When using dual connections, ensuring that the cabling for the two connections is not sharing the same physical route, to eliminate the risk of both links being accidentally severed at the same time.
- When using dual connections, use two different carriers in two different geographic locations, for carrier resiliency.
- Consider using an OTT connection as a back up to the WAN connections

For high service availability, consider the installation of additional network connections at the customer premises. For some network deployments, those that do not employ OTT connections, the addition of a survivable gateway may be an alternative option.

Remote Site Survivability

There are varying degrees of functionality that might be required at a customer premise site or at a remote site in the event that the connection to the data centre fails. Some customer sites may require that certain applications or functions be fully operational, even if the communication path to the head office fails, If this is the case consider:

- Physically locating application infrastructure and application servers at the customer site so that these applications can operate independently of the data centre, (DHCP server, for example).
- Locating a MiVoice Business appliance on site to serve as a survivable PSTN gateway.
- Providing local connectivity to external networks such as the PSTN and the Internet, so that these networks can be accessed independently from the customer premise location.
- Consider providing back-up power to critical pieces of equipment at the customer premises.

Direct connections to the PSTN network can be realized with MiVoice Business appliance platforms. The preferred MiVoice Business platforms are:

- MXe III
- CX II
- EX

As a minimum, even in cases where remote site survivability is not a requirement, ensure that support for emergency calls is provided using local connections to the PSTN.

For more detailed information, refer to the *Mitel Survivability of Remote Branch Offices Solutions Guide*, available on Mitel Edocs.

LAN CONSIDERATIONS

If a high availability UC solution is required, then it is critical that the LAN be designed to be resilient. LAN resiliency ensures that traffic can be redirected to the desired destination, if a networking switch or router fails. The LAN must also be designed so that sufficient bandwidth is always available, even during network equipment failures.

Quality of Service (QoS) mechanisms must be employed when designing the network so that different types of traffic are treated with the appropriate priorities across the network.

For additional information related to network design for high availability, refer to the following documents which are available on Mitel-On-Line (MOL):

- Mitel White Paper: *Network Design for Availability*
- *MiVoice Business Engineering Guidelines*
- *MiVoice Business Resiliency Engineering Guidelines*

LAN Topology

There are a number of LAN topologies that may be employed when designing a LAN; however, it is highly recommended that the LAN be based on a hierarchical design.

Hierarchical networks are typically designed with three layers; the core, distribution, and access layers.

- The core equipment is located in a server room or data center room. The core connects distribution groups to each other, and it also provides connectivity to servers and gateways.
- The distribution layer equipment is located in wiring/telecommunications closets, and connects to the core and access layer equipment through high-speed links.
- The access layer is located either in the wiring closets or physically close to the work groups that require connectivity. The access layer connects end-user devices to the distribution layer.

Note: Connections from the access layer to the end-customer, or end point are not redundant. However, in critical situations, such as an emergency call centre, it is possible agents may have dual phones, as well as dual connections to different physical access layer switches.

Hierarchical networks allow similar users and their resources to be grouped together into specific work groups.

This allows:

- A work group's traffic to be contained in a local area and to be connected to a common Layer 2 network.
- Resources that are dedicated to a particular work group, such as printers, to be connected to the Layer 2 access switch for the work group.
- Containment of work group traffic and resources to each work group allows key work groups to be provisioned with a higher level of availability than other, less critical, work groups, which allows for cost savings where higher availability is not required.

Hierarchical network designs easily overlay onto structured building wiring plants. This allows for:

- Less costly installations due to minimal re-wiring requirements.
- Easier moves, adds, and changes, and more efficient network maintenance.

- Easier scalability, when it is necessary to expand the call center size.
- Faster troubleshooting of network faults.
- Prevention of wide-spread network disruptions when a network fault occurs, by containing the disruption to a localized area.

In some cases the UC solution may have different availability requirements at different levels in the network hierarchy. A hierarchical network allows the network designer to tailor the level of availability to meet these different requirements.

Redundancy Mechanisms in LANs

Some specific examples of redundancy mechanisms that can be used when designing a high availability contact center LAN are:

- Use of Layer 2 and Layer 3 networking equipment that supports full redundancy.
- Duplication of Layer 2 switches and Layer 3 networking devices throughout the LAN.
- Duplication of transmission paths using partial mesh networking to support redundant communication paths.
- Use of Layer 2 protocols that enable the use of duplicate network paths as back-up paths, specifically; STP, RSTP, and MSTP.
- Use of two DHCP servers
- Duplication of storage devices; SAN, NAS, and RAID arrays, for example.
- Use of resilient topologies, (implies hierarchical network design).
- Use of Layer 3 protocols that enable the use of duplicate network paths as back-up paths; specifically, OSPF, VRRP, or Cisco HSRP.
- Multiple NICs on servers and use of LACP (IEEE 802.3ad).

Ideally, a network that has been designed for high availability does not contain any single points of failure, and when a failure is encountered, the network re-establishes functionality as quickly as possible.

Network Power Provisioning

The critical elements of the UC solution should retain power in the event that the mains power feed fails. This can be achieved through an alternative power source such as a secondary mains supply, local UPS, or local generator.

Primary network devices (MiVoice Business controllers, Layer 2 switches, and servers) should be powered from different branch circuits than the circuits used for powering the secondary network devices.

Critical phones should also be provided with back-up power. If the phones are powered locally, then this is required at each phone. It might be prudent, therefore, to use a Layer 2 switch that has Power over Ethernet (PoE) capabilities. The PoE capable Layer 2 switch could then be powered with a common back-up power mechanism such as a UPS, in the event of a power outage.

For additional information related to PoE planning, IP phone power provisioning and network power provisioning, refer to the following documents which are available on Mitel-On-Line (MOL):

- *MiVoice Business Engineering Guidelines*
- *MiVoice Business System Engineering Tool* (SET) - This tool has an embedded IP phone power calculator.
- Mitel Data Sheets for MiVoice Business 3300 platforms and associated hardware
- *Mitel 3300 ICP Hardware Technical Reference Manual*
- Manufacturer’s data sheets for third-party servers, Layer 2 switches and routers

VMWARE AND SERVICE RELIABILITY

VMware offers an extensive suite of software solutions that allow customers to create a virtual IT infrastructure. Mitel's virtual products are intended to run on VMware's virtual infrastructure and leverage the capabilities that VMware provides, which includes the ability to provide application level resiliency for customers that require high service availability.

VMware High Availability (HA) and VMware Site Recovery Manager (SRM) are two VMware features that are designed to increase the availability of systems running in a VMware environment.

If a Mitel virtual application has no native resiliency capabilities, HA and SRM may be used to provide a higher level of system availability.

In cases where a Mitel application does offer native resiliency capabilities, HA and SRM work with the application's resiliency capabilities to further increase system availability.

Information about deploying in a VMware environment can be found in the *Mitel Virtual Appliance Deployment Solutions Guide*, available on Mitel-On-Line (MOL).

HA (High Availability) is a failover protection mechanism that is used to recover a virtualized application's availability during hardware or operating system failures. With HA, the servers are geographically co-located; switching time between servers is approximately 15 minutes. HA provides the following capabilities:

- HA detects operating system and hardware failures
- HA restarts the virtualized application on another physical server in the resource pool without manual intervention when a server failure or operating system failure is detected.

SRM (Site Recovery Manager) offers customers a disaster recovery mechanism that can also be used for planned migrations. SRM can manage failover from production data centers to disaster recovery sites which are based in a geographically different location. When used to perform a complete data center recovery, SRM can provide RPOs (Recovery Point Objectives) of several hours to several days.

Refer to the *Mitel Virtual Appliance Deployment Solutions Guide*, available on Mitel-On-Line (MOL), for further details,

The following Mitel virtual appliances are SRM-compatible:

- MiCollab Virtual
- MiVoice Border Gateway Virtual
- MiCollab Client Virtual
- MiCollab Unified Messaging Virtual
- MiVoice Business Virtual

Note: To deploy the Site Recovery Manager capability with Mitel virtual applications, Mitel Professional Services must be purchased. Request a quotation for SRM support from Services Solutions at the following URL:

http://domino1.mitel.com/mol/servsol.nsf/ServSolApp?OpenForm

You must be logged in to Mitel OnLine to use this request form.

For more information about VMware and its products, visit the VMware web site:

http://www.vmware.com/ and http://www.vmware.com/products/vcenter-server

DETERMINING SYSTEM AVAILABILITY

It is a common practice within the telecommunications industry to refer to the reliability level of a product, or a system, as 5-9s or 5 x 9. What is actually being referred to, however, is the availability of a service expressed as a percentage for a particular product or system. When a product has an availability of 5-9s it is available 99.999% of the time.

Determining the availability of a particular UC solution is a complicated task. Hardware products such as a server can achieve better than 5-9s of availability. But it must be remembered that the overall system availability is defined by the weakest link in the chain.

When determining overall system availability, Mitel uses a seven-layer business continuity model. This business continuity model takes into account all of the factors that could have an influence on system availability.

The seven layer business continuity model is comprised of the following components:

- Server hardware – The server hardware forms the foundation of the business continuity model.
- Server software – This is software that runs on the server hardware (e.g., the operating system, call control software, application software). It can have a major impact on system availability.
- Data Network – The data network includes the data networking hardware and related protocols (e.g., Layer 2 switches, routers, networking protocols). Overall system availability is dependent on the data network availability.
- Power Distribution – This fundamental requirement needs to be taken into consideration so that if required, equipment can continue to be powered even under fault conditions (e.g., uninterruptible power systems, generators).

- Geography – System availability can be enhanced when the network design takes geographical distribution of equipment and personnel into account, particularly when the business is dispersed across multiple locations and / or cities.
- Process – Company processes related to maintenance and repair need to be considered, since these processes can have a direct effect on availability.
- People – The availability of maintenance and repair personnel and their impact on system availability needs to be considered, i.e., whether or not repair and maintenance personnel are located on site or off site.

Mitel's white papers about telephone system availability (available on Mitel-On-Line (MOL) under Business Continuity) outline the steps that must be taken to determine the availability of a particular UC solution. Performing such an availability analysis is beyond the scope of this document, it is recommended that Mitel Professional Services be contacted to assist with an availability analysis.

Chapter 6

TRAFFIC AND SCALING CONSIDERATIONS

TRAFFIC AND SCALING CONSIDERATIONS

Traffic on the system determines how many resources are used including bandwidth, trunks and voice mail. UC deployments must also consider the types and number of devices that are assigned to each user UC profile.

Note: This section is relevant to topologies of both the Enterprise UC Solution Blueprint and the MiCloud Business Solution Blueprint. This section may refer to specific topologies covered in the other associated document.

This document uses some base assumptions in order to calculate the traffic and scaling limits for each topology.

Note: Customers wishing to use different traffic rates, or assumptions, are advised to contact Mitel Professional Services to confirm any different scaling and quantity of unit calculations are correct.

UC PROFILES

The number of devices assigned to a user is an important factor for considering performance and configuration limits. Users, including the devices they use, are classified into five profiles shown in the table "User and UC Profiles" on page 95. Three of the profiles are considered UC specific.

Table 10: User and UC Profiles

USER AND UC PROFILE	EXAMPLES
Base IPT	A physically fixed phone with no voice mail. Typically used in lobbies, conference rooms, or work stations.
Standard IPT	A typical office desk phone assigned to a user or hot-desk. Extension includes voice mail for the user
Entry UCC	An extension on the standard IPT with inclusion of an EHDU or forwarding of calls to a specific PSTN number. This is the first multi-device user level, up to two devices assigned to the user **Note:** With the SB topology the Entry SB UCC license will be used, but is still considered Entry UCC for the scaling calculations
Standard UCC	Extends the Entry UCC profile with the addition of PC softphone and teleworker capability. Up to three devices are assigned to the user
Premium UCC	Extends the Standard UCC profile with the addition of a mobile phone softphone and an additional teleworker. Up to four devices assigned to the user

Further details on licensing can be found under “Licensing Considerations” on page 183.

Traffic and scaling calculations in this document employ an average number of devices per user to consider the different profile mixes for the overall deployment.

The table “Average Devices per User Target Scenarios” on page 96 describes the expected and typical UC profiles for standard deployments and corresponds to the average devices per user profiles in the table “Typical UC Profiles for Standard Deployments” on page 97.

Note: Customers wishing to use different traffic rates, or assumptions, are advised to contact Mitel Professional Services to confirm any different scaling and quantity of unit calculations are correct.

Table 11: Average Devices per User Target Scenarios

KEY TARGETS	DESCRIPTION
2.75 Devices Target UC (red)	This is the target UC deployment scenario using the standard templates provide with MiCollab.
1.5 Devices Special (yellow)	This is a special condition for the SB topology solution where extended mobility with PC softphones may be used instead of EHDU or simple twinning. This is a non-standard template. It requires UC licensing, with an addition a-la-carte mobility license.
1.5 Devices Target UC (blue)	This is the target UC deployment for the SB topology solution. This is a reduced UC deployment with only Entry UC
1.0 Devices Standard (green)	This is the standard non-UC deployment with a mix of fixed and hot desk phones.

Note: The key target deployments shown in Red (2.75), Blue (1.5) and Green (1), are also highlighted in subsequent scaling tables for ease of cross comparison

A customer may wish to use different target profiles, or devices per user, from that shown above. These target profiles are expected to fit most UCC deployments.

It is possible to increase, or decrease, the number of devices per UCC profile. The table “Typical UC Profiles for Standard Deployments” on page 97 provides some examples.

Table 12: Typical UC Profiles for Standard Deployments

DEVICES PER USER	PHONE		UCC		
	BASIC IPT	STANDARD IPT	ENTRY	STANDARD	PREMIUM
4	0%	0%	0%	0%	Internal HD device PC softphone (TW) Mobile softphone (TW) EHDU 100%
3.75	0%	0%	0%	Internal HD device PC softphone (TW) EHDU 25%	Internal HD device PC softphone (TW) Mobile softphone (TW) EHDU 75%
3.5	0%	0%	0%	Internal HD device PC softphone (TW) EHDU 50%	Internal HD device PC softphone (TW) Mobile softphone (TW) EHDU 50%
3.25	0%	0%	Internal HD device EHDU 25%	Internal HD device PC softphone (TW) EHDU 25%	Internal HD device PC softphone (TW) Mobile softphone (TW) EHDU 50%
3	0%	0%	Internal HD device EHDU 25%	Internal HD device PC softphone (TW) EHDU 50%	Internal HD device PC softphone (TW) Mobile softphone (TW) EHDU 25%
2.75 Target UC	0%	0%	Internal HD device EHDU 25%	Internal HD device PC softphone (TW) EHDU 50%	Internal HD device Mobile softphone (TW) EHDU 25%
2.5	0%	0%	Internal HD device EHDU 50%	Internal HD device PC softphone (TW) EHDU 50%	0%
2.25	0%	Internal HD device 25%	Internal HD device EHDU 25%	Internal HD device PC softphone (TW) EHDU 50%	0%
2	0%	Internal HD device 25%	Internal HD device EHDU 50%	Internal HD device PC softphone (TW) EHDU 25%	0%
1.75	0%	Internal HD device 25%	Internal HD device EHDU 75%	0%	0%
1.5 Special case Hosted MiCloud Business	0%	Internal HD device 50%	Mobile Softphone (TW) EHDU 50%	0%	0%

Table 12: Typical UC Profiles for Standard Deployments

DEVICES PER USER	PHONE		UCC		
	BASIC IPT	STANDARD IPT	ENTRY	STANDARD	PREMIUM
1.5 Target MiCloud Business UC Hosted MiCloud Business	0%	Internal HD device 50%	Internal HD device EHDU %	0%	0%
1.25	0%	Internal HD device 75%	Internal HD device EHDU %	0%	0%
1 Standard deployment	Internal device 25%	Internal HD device 75%	0%	0%	0%

USER TRAFFIC LEVELS

User traffic levels are typically defined as “Standard Office” and are defined as:

- Typically six Calls Per Hour (6 CPH)
- Hold times of between 100 to 120 seconds per call

Other traffic levels can also be used, such as lower values for hospitality deployments or increased levels that might be used for a distribution type of business.

Note: Customers wishing to use different traffic rates, or assumptions, are advised to contact Mitel Professional Services to confirm any different scaling and quantity of unit calculations are correct.

Traffic blocking is based on Erlang B calculation and uses the following standard blocking levels:

- P.01 for external trunks
- P.001 for internal traffic

Erlang B is used to estimate peak traffic conditions and resources required to meet that peak demand using the blocking ratios above. The peak period is considered for key hours during the day, typically in the morning and early afternoon. Traffic and resource occupance can be expressed in Erlangs or Centum Call Seconds:

- 1 e (Erlang) = 100% occupancy = 3600 CS (Call seconds) = 36 CCS (Centum Call Seconds)
- 36 CCS = 36 calls of 100 seconds duration

Other traffic factors to consider include where the traffic originates or terminates. It is assumed, on average, that calls are answered across all devices in an even fashion for UC users. Changes to this could influence use of certain resources, e.g. trunks.

MIVOICE BUSINESS SCALING

MiVoice Business scaling is important for UC deployments requiring a solution composed of individual components. MiVoice Business scaling is especially important for larger deployments where self contained units, such as those used for the SMB, cannot be deployed.

See the section “Small Medium Business Scaling” on page 101 for the self-contained UC deployment solution.

There are a number of limits, internal and external to MiVoice Business, that need to be considered for the UC deployments on the MiVoice Business, including, but not limited to:

- Performance
- Registered devices
- Monitors
- Application attachment

Each of these factors is considered along with the number of, and type of, devices per user. From this a scaling value can be obtained, and this will determine the number of MiVoice Business that are required for the solution. The platform type may provide additional influence, especially when considering virtual MiVoice Business controllers that have potentially reduced capabilities, such as user and traffic limits, compared to other MiVoice Business controllers.

For non-UC deployments, each user has one device for receiving all calls. Users can have multiple devices in a UCC deployment. All of a user’s devices receive incoming calls, except when presence settings are configured for an alternative. One device is used to answer the call, but multiple ringing connections are established and torn down. The scaling calculations consider this process for determining the available system performance.

Further details on how monitors and HCI are used along with working limits are include in the *MiVoice Business Engineering Guidelines*.

- “MiVoice Business Building Blocks” on page 99
- “MiVoice Business Scaling Table” on page 100

MIVOICE BUSINESS BUILDING BLOCKS

For larger deployments that use virtual MiVoice Business, it has been determined that the MiVoice Business Virtual 2500 has sufficient capacity to handle the defined number of UC users as well as the required media resources.

For the standard MiVoice Business deployments, the MiVoice Business for Industry Standard Servers (ISS) and MiVoice Business Multi-Instance platforms have sufficient capacity to handle the UC deployments. When using MiVoice Business Multi-Instance, it is strongly advised that the individual MiVoice Business are performance checked with the System Engineering Tool (SET) and also the MiVoice Business Multi-Instance Engineering Tool (MET), both available in the Technician's Toolbox under Technical Training on Mitel MiAccess.

MiVoice Business building blocks:

- MiVoice Business Virtual 2500 for virtual deployments

- MiVoice Business for Industry Standard Servers (ISS) for on premise deployment
- MiVoice Business Multi-Instance for service provider and on-premise deployment

Note: Although the MiVoice Business Virtual 5000 can offer more capacity in certain areas, this is not applicable for the defined UC deployments. The MiVoice Business Virtual 5000 can handle more users, but the total device limit is the same as for the MiVoice Business Virtual 2500, with an increased OVA reservation requirement. For a UC deployment, there is no benefit, and a potential cost disadvantage in using the MiVoice Business Virtual 5000. The MiVoice Business Virtual 2500 is therefore used as the virtual UCC building block.

MIVOICE BUSINESS SCALING TABLE

For the three MiVoice Business Building Blocks the same UC limits apply. The table “MiVoice Business Scaling” on page 100 shows the number of MiVoice Business required when the number of users, including UC, is compared to different devices per user, as defined in ““UC Profiles” on page 95” on page 95, for MiVoice Business Release 7.0.

The row headings that show the target deployments are also color highlighted to match with the key target UCC deployments.

The table“MiVoice Business Scaling” on page 100 shows the number of MiVoice Business units needed for an operational UCC configuration. Where primary and secondary resilient MiVoice Business units are required, double these numbers. Where VMware HA is being used instead of application resiliency these numbers can be used directly.

The special mobility case for the SB topology does not impact the predicted number of required MiVoice Business, since the number of users is typically less than 50 users and less than 100 devices per MiVoice Business.

Note: Contact Mitel Professional Services to calculate MiVoice Business scaling if there are more than 50 users and 100 devices per MiVoice Business planned for a SB topology deployment.

Table 13: MiVoice Business Scaling

# OF USERS	DEVICES PER USER												
	1	1.25	1.5	1.75	2	2.25	2.5	2.75	3	3.25	3.5	3.75	4
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1 to 100	1	1	1	1	1	1	1	1	1	1	1	1	1
101 to 200	1	1	1	1	1	1	1	1	1	1	1	1	1
201 to 300	1	1	1	1	1	1	1	1	1	1	1	1	1
301 to 400	1	1	1	1	1	1	1	1	1	1	1	1	1
401 to 500	1	1	1	1	1	1	1	1	1	1	1	1	1
501 to 600	1	1	1	1	1	1	1	1	1	1	1	1	1
601 to 700	1	1	1	1	1	1	1	1	1	1	1	1	1
701 to 800	1	1	1	1	1	1	1	1	1	1	1	1	1

Note: The boxes marked “1/2*” represent a minor variation between vMiVoice Business2500 using the standard OVA settings and MiVoice Business for Industry Standard Servers (ISS). Use the higher number of vMiVoice Business2500, the lower for MiVoice Business for Industry Standard Servers (ISS).

Table 13: MiVoice Business Scaling

# OF USERS	DEVICES PER USER												
	1	1.25	1.5	1.75	2	2.25	2.5	2.75	3	3.25	3.5	3.75	4
801 to 900	1	1	1	1	1	1	1	1	1	1	1	1	1
901 to 1000	1	1	1	1	1	1	1	1	1	1	1	1	1
1001 to 1100	1	1	1	1	1	1	1	1	1	1	1	1	2
1101 to 1200	1	1	1	1	1	1	1	1	1	1	2	2	2
1201 to 1300	1	1	1	1	1	1	1	1	1	2	2	2	2
1301 to 1400	1	1	1	1	1	1	1	1	2	2	2	2	2
1401 to 1500	1	1	1	1	1	1	1	2	2	2	2	2	2
1501 to 1600	1	1	1	1	1	1	2	2	2	2	2	2	2
1601 to 1700	1	1	1	1	1	2	2	2	2	2	2	2	2
1701 to 1800	1	1	1	1	2	2	2	2	2	2	2	2	2
1801 to 1900	1	1	1	2	2	2	2	2	2	2	2	2	2
1901 to 2000	1	1	1	2	2	2	2	2	2	2	2	2	2
2001 to 2100	1	1	2	2	2	2	2	2	2	2	2	2	2
2101 to 2200	1	1	2	2	2	2	2	2	2	2	2	2	3
2201 to 2300	1	2	2	2	2	2	2	2	2	2	2	3	3
2301 to 2400	1	2	2	2	2	2	2	2	2	2	3	3	3
2401 to 2500	1	2	2	2	2	2	2	2	2	2	3	3	3
2501 to 2600	1/2*	2	2	2	2	2	2	2	2	3	3	3	3
2601 to 2700	1/2*	2	2	2	2	2	2	2	3	3	3	3	3
2701 to 2800	1/2*	2	2	2	2	2	2	2	3	3	3	3	3
2801 to 2900	2	2	2	2	2	2	2	3	3	3	3	3	3
2901 to 3000	2	2	2	2	2	2	2	3	3	3	3	3	3

Note: The boxes marked "1/2*" represent a minor variation between vMiVoice Business2500 using the standard OVA settings and MiVoice Business for Industry Standard Servers (ISS). Use the higher number of vMiVoice Business2500, the lower for MiVoice Business for Industry Standard Servers (ISS).

SMALL MEDIUM BUSINESS SCALING

The SMB deployment is a self contained virtualized OVA intended for UC attachment and for deployment in virtualized data centres. The scaling of the components within the OVA are already predefined to work correctly with the target UC profile of 2.75 devices up to 500 users.

Since the deployment will not need to consider additional external units or connections, from a performance and scaling view, this solution is complete. It does not need to consider additional scaling factors for MiVoice Business and MiVoice Border Gateway, as these are already included and scaled for this deployment

MIVOICE BORDER GATEWAY VIRTUAL SCALING

MiVoice Border Gateway scaling in a virtual environment is important for UC deployments requiring a solution composed of individual components. MiVoice Border Gateway Virtual scaling is especially important for larger deployments where self contained units, such as those used for the SMB, cannot be deployed.

There are a number of internal limits that need to be considered for the UC deployments on the MiVoice Border Gateway Virtual, including, but not limited to:

- Performance
- Number of concurrent media and UC connections through the MiVoice Border Gateway
- Number of registered users.

Typically the MiVoice Border Gateway Virtual will be used for two functions. These are:

- SIP Trunk Gateway
- Teleworker Gateway

By combining these functions to a group of MiVoice Border Gateways it is possible to consolidate the number of instances that need to be created. The table “MiVoice Border Gateway Virtual Scaling with Resiliency” on page 103 considers this consolidated case. Should it be necessary to split MiVoice Border Gateway Virtuals into separate functions, then add two additional units for deployments up to 2500 users and a further two units up to 5000 users.

Included in the requirement is the possibility that the PC softphone is deployed on a laptop or tablet, and may therefore require to be mobile outside of the normal office environment. As such, this device will need to connect into the deployment as an external Teleworker, rather than an internal LAN connected device.

The scaling for the MiVoice Border Gateway Virtual is based on the registration and streaming limits in the *MiVoice Border Gateway Virtual Engineering Guidelines* at MiVoice Border Gateway Release 8.1.

The row headings that show the target deployments are also color highlighted.

The quantity of MiVoice Border Gateway Virtual units is shown for a normal deployment. If VMware HA is used for resiliency, or resiliency is not required, then use these numbers directly. If the MiVoice Border Gateways are clustered for resiliency, then increase the unit quantities by the resiliency configuration, i.e. double for a primary/secondary combination and plus one for an N+1 configuration.

The special mobility case for the SB topology does not impact the required number of MiVoice Border Gateway Virtuals, since the number of users is typically less than 50 users and less than 100 devices per MiVoice Business.

MIVOICE BORDER GATEWAY SCALING

Note: Contact Mitel Professional Services to calculate MiVoice Border Gateway Virtual scaling if there are more than 50 users and 100 devices per MiVoice Business planned for a SB topology deployment.

Table 14: MiVoice Border Gateway Virtual Scaling with Resiliency

# OF USERS	DEVICES PER USER												
	1	1.25	1.5	1.75	2	2.25	2.5	2.75	3	3.25	3.5	3.75	4
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1 to 100	1	1	1	1	1	1	1	1	1	1	1	1	1
101 to 200	1	1	1	1	1	1	1	1	1	1	1	1	1
201 to 300	1	1	1	1	1	1	1	1	1	1	1	1	1
301 to 400	1	1	1	1	1	1	1	1	1	1	1	1	1
401 to 500	1	1	1	1	1	1	1	1	1	1	1	1	1
501 to 600	1	1	1	1	1	1	1	1	1	1	1	1	1
601 to 700	1	1	1	1	1	1	1	1	1	1	1	1	1
701 to 800	1	1	1	1	1	1	1	1	1	1	1	1	1
801 to 900	1	1	1	1	1	1	1	1	1	1	1	1	1
901 to 1000	1	1	1	1	1	1	1	1	1	1	1	1	1
1001 to 1100	1	1	1	1	1	1	1	1	1	1	1	1	1
1101 to 1200	1	1	1	1	1	1	1	1	1	1	1	1	1
1201 to 1300	1	1	1	1	1	1	1	1	1	1	1	1	2
1301 to 1400	1	1	1	1	1	1	1	1	1	1	1	1	2
1401 to 1500	1	1	1	1	1	1	1	1	1	1	1	2	2
1501 to 1600	1	1	1	1	1	1	1	1	1	1	1	2	2
1601 to 1700	1	1	1	1	1	1	1	1	1	1	2	2	2
1701 to 1800	1	1	1	1	1	1	1	1	1	1	2	2	2
1801 to 1900	1	1	1	1	1	1	1	1	1	1	2	2	2
1901 to 2000	1	1	1	1	1	1	1	1	1	2	2	2	2
2001 to 2100	1	1	1	1	1	1	1	1	2	2	2	2	2
2101 to 2200	1	1	1	1	1	1	2	2	2	2	2	2	2
2201 to 2300	1	1	1	1	1	1	2	2	2	2	2	2	2
2301 to 2400	1	1	1	1	1	1	2	2	2	2	2	2	2
2401 to 2500	1	1	1	1	1	1	2	2	2	2	2	2	2
2501 to 2600	1	1	1	1	1	2	2	2	2	2	2	2	3
2601 to 2700	1	1	1	1	2	2	2	2	2	2	2	2	3
2701 to 2800	1	1	1	2	2	2	2	2	2	2	2	2	3
2801 to 2900	1	1	1	2	2	2	2	2	2	2	2	3	3
2901 to 3000	1	1	1	2	2	2	2	2	2	2	2	3	3

Scaling of the MiVoice Border Gateway is important for UC deployments that require the solution to be composed of individual components, typically on-premise. This is especially important for larger deployments where self contained units, such as used for SMB, cannot be deployed.

There are a number of internal limits that need to be considered for the UC deployments on the MiVoice Border Gateway, including, but not limited to:

- Performance
- Number of concurrent media and UC connections through the MiVoice Border Gateway
- Number of registered users

Typically the MiVoice Border Gateway will be used for two functions. These are:

- SIP Trunk Gateway

- Teleworker Gateway

By combining these functions to a group of MiVoice Border Gateways it is possible to consolidate the number of instances that need to be created. The table “MiVoice Border Gateway Scaling” on page 104 considers this consolidated case. Should it be necessary to split MiVoice Border Gateways into separate functions, then add two additional units for deployments up to 5000 users.

Included in scaling calculations is the possibility that the PC softphone is deployed on a laptop or tablet, and may therefore require to be mobile outside of the normal office environment. As such, this device will need to connect into the deployment as an external Teleworker, rather than an internal LAN connected device.

The scaling for the MiVoice Border Gateway is based on the registration and streaming limits in the *MiVoice Border Gateway Engineering Guidelines* at MiVoice Business Gateway Release 8.1.

Note: The MiVoice Border Gateway can only be associated with a single MiCollab deployment. The MiVoice Border Gateways should be scaled according to this single associated MiCollab unit. Where multiple MiCollab units exist, multiple groupings of MiVoice Border Gateways are required.

The row headings that show the target deployments are also color highlighted.

The quantity of MiVoice Border Gateway units is shown for a normal deployment. If resiliency is not required then use these numbers directly. If the MiVoice Border Gateways are clustered for resiliency, then increase the unit quantities by the resiliency configuration, i.e. double for a primary/secondary combination and plus one for an N+1 configuration.

The special mobility case for the SB topology does not impact the required number of MiVoice Border Gateways, since the number of users are typically less than 50 users and less than 100 devices per MiVoice Business.

Note: Contact Mitel Professional Services to calculate MiVoice Border Gateway scaling if there are more than 50 users and 100 devices per MiVoice Business planned for a SB topology deployment.

Table 15: MiVoice Border Gateway Scaling

# OF USERS	DEVICES PER USER												
	1	1.25	1.5	1.75	2	2.25	2.5	2.75	3	3.25	3.5	3.75	4
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1 to 100	1	1	1	1	1	1	1	1	1	1	1	1	1
101 to 200	1	1	1	1	1	1	1	1	1	1	1	1	1
201 to 300	1	1	1	1	1	1	1	1	1	1	1	1	1
301 to 400	1	1	1	1	1	1	1	1	1	1	1	1	1
401 to 500	1	1	1	1	1	1	1	1	1	1	1	1	1
501 to 600	1	1	1	1	1	1	1	1	1	1	1	1	1
601 to 700	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 15: MiVoice Border Gateway Scaling

# OF USERS	DEVICES PER USER												
	1	1.25	1.5	1.75	2	2.25	2.5	2.75	3	3.25	3.5	3.75	4
701 to 800	1	1	1	1	1	1	1	1	1	1	1	1	1
801 to 900	1	1	1	1	1	1	1	1	1	1	1	1	1
901 to 1000	1	1	1	1	1	1	1	1	1	1	1	1	1
1001 to 1100	1	1	1	1	1	1	1	1	1	1	1	1	1
1101 to 1200	1	1	1	1	1	1	1	1	1	1	1	1	1
1201 to 1300	1	1	1	1	1	1	1	1	1	1	1	1	1
1301 to 1400	1	1	1	1	1	1	1	1	1	1	1	1	1
1401 to 1500	1	1	1	1	1	1	1	1	1	1	1	1	1
1501 to 1600	1	1	1	1	1	1	1	1	1	1	1	1	1
1601 to 1700	1	1	1	1	1	1	1	1	1	1	1	1	1
1701 to 1800	1	1	1	1	1	1	1	1	1	1	1	1	1
1801 to 1900	1	1	1	1	1	1	1	1	1	1	1	1	1
1901 to 2000	1	1	1	1	1	1	1	1	1	1	1	1	1
2001 to 2100	1	1	1	1	1	1	1	1	1	1	1	1	1
2101 to 2200	1	1	1	1	1	1	1	1	1	1	1	1	1
2201 to 2300	1	1	1	1	1	1	1	1	1	1	1	1	1
2301 to 2400	1	1	1	1	1	1	1	1	1	1	1	1	1
2401 to 2500	1	11	1	1	1	1	1	1	1	1	1	1	1
2501 to 2600	1	1	1	1	1	1	1	1	1	1	1	1	2
2601 to 2700	1	1	1	1	1	1	1	1	1	1	1	1	2
2701 to 2800	1	1	1	1	1	1	1	1	1	1	1	1	2
2801 to 2900	1	1	1	1	1	1	1	1	1	1	1	2	2
2901 to 3000	1	1	1	1	1	1	1	1	1	1	1	2	2

MICOLLAB SCALING

The MiCollab platform is a collection of UCC applications. This is a multi-application deployment for a single customer and may be realized with a dedicated server for on-premise deployment or as a virtual application for both private and public Cloud deployments.

This is not the MiCollab Client Multi-Tenant UC solution. See the section on MiCollab Client Multi-Tenant for this single application.

The MiCollab application can scale up to 3000 users based on 2.75 devices per user, as a single deployment

The MiCollab may be associated with multiple MiVoice Business units. Multiple MiVoice Border Gateways can be associated with a single MiCollab unit. MiVoice Border Gateways cannot be associated with multiple MiCollab units.

MICOLLAB CLIENT MULTI-TENANT SCALING

The MiCollab Client Multi-Tenant Service is a specific configuration of a single UC deployment using the MiCollab UCC platform. This is a single application and can be used across multiple customers to provide UC functionality (telephony presence).

This is not the multi-function MiCollab UCC solution, but a special deployment of one application. See the section on MiCollab Scaling for the richer UCC solution.

The MiCollab Client Multi-Tenant can scale to the following limits:

- 250 tenants on a single platform
- A single tenant is typically based on 50 users (12500 users total), scalable to 5000 users
- Per tenant at two devices per user (25000 devices total)
- One client per user (12500 clients total)

The MiCollab Client Multi-Tenant will be associated with multiple MiVoice Business units. There will also be a multiple MiVoice Border Gateway associated with this single MiCollab Client Multi-Tenant unit. Where multiple MiCollab Client Multi-Tenant units exist in a server provider environment, a similar number of MiVoice Border Gateway groups are also needed.

MITEL OPEN INTEGRATION GATEWAY PLATFORM

The Mitel Open Integration Gateway will allow applications to access the UCC solution components as well as providing connections to Google and Salesforce integrations.

Finer details of the limits for Mitel Open Integration Gateway can be found in the *Mitel Open Integration Gateway Engineering Guidelines*, available on Mitel-On-Line (MOL).

Some key limits to consider with a UCC deployment include:

- Total number of monitors: 50,000
- Maximum MiVoice Business, or UC application connections (outgoing): 250
- Maximum number of user connected applications (incoming): 500
- Deployed to a single customer

The following considerations need to be taken into account, due to these limits.

For the MiCollab Client Multi-Tenant solution, the Mitel Open Integration Gateway must be deployed per customer, or two per customer if resiliency is required without HA. If used via a MiVoice Border Gateway, the same MiVoice Border Gateway should be used for Mitel Open Integration Gateway as for the MiCollab Client Multi-Tenant connections to simplify tenant connections and IP address usage.

Each MiVoice Integration for Google, or for Salesforce, counts as an individual application attachment. A single Mitel Open Integration Gateway is limited to 500 application attachments. Therefore only 500 MiVoice Integrations can be connected to a single Mitel Open Integration Gateway. The number of Mitel Open Integration Gateway will need to be scaled accordingly, i.e. 3000 users on MiVoice Integration for Salesforce would require six Mitel Open Integration Gateway platforms.

Note: If multiple Mitel Open Integration Gateways connect to the same MiVoice Business and they monitor the same device, this will add a multiplier to the HCI count within the MiVoice Business.

Mitel Open Integration Gateways can be deployed as virtual instances alongside existing virtual deployments, or can be combined onto a single physical server for improved customer to server density. See *Mitel Open Integration Gateway Engineering Guidelines* for further details on OVA and reservation settings.

Chapter 7

EXTERNAL CONNECTIVITY

EXTERNAL CONNECTIVITY

This section discusses the various components, protocols and communication paths that are required to support connectivity between the UC solution and external networks, and also between UC components located in a data centre or service provider cloud and components located at the customer site or teleworker site.

While a number of external communication paths are discussed in this section, a specific topology may not require all of the paths discussed here. At a minimum, all topologies will require external connectivity to support IP telephony and management. More generally, external connectivity is required for voice communications and related applications, such as:

- Telephony signalling and related audio streams
- UC applications and related video and data streams
- Business applications
- Network management
- Troubleshooting
- Product licensing and license renewal
- Software maintenance

In a typical deployment, the call control engine and applications servers are deployed within a private network with a limited number of secure gateways to other networks. The end-points, both UC clients and management clients, are deployed at the customer site and other remote locations. Gateways are required to connect UC servers to clients and UC servers to other service providers. These external facing gateways must support signalling, audio, video and data traffic connecting over public or private networks.

In general terms, a gateway is a component that interconnects two different types of networks, both physically and logically; the gateway may also serve as a protocol converter between the two networks. The Unified Communications topologies rely on several gateways for connections to external networks, which include:

- MiVoice Business 3300 ICP or EX for PSTN connectivity
- MiVoice Border Gateway (MiVoice Border Gateway) for public data network connectivity including SIP trunks
- Third-party IP router and firewall for public IP-based data network connectivity
- Third-party label switch router for MPLS-based data network connectivity

Further details on MiVoice Business 3300 ICP working capacity and using a MiVoice Business 3300 ICP for local breakout can be obtained from *MiVoice Business Engineering Guidelines*, available on Mitel-On-Line (MOL).

Additional information on MiVoice Border Gateway, including clustering, resiliency and bandwidth requirements, is provided in *MiVoice Border Gateway Engineering Guidelines*, available on Mitel-On-Line (MOL). Details on configuring the MiVoice Border Gateway to

support Teleworker services and/or Web proxy are found in *MiVoice Border Gateway Installation and Maintenance Guide*, available on Mitel-On-Line (MOL).

SERVICE PROVIDER GATEWAYS

Depending on a particular topology's external connectivity requirements, the following service provider gateways may be required.

To connect to the PSTN:

- A PSTN gateway and the associated trunk connections to a Telco; and
- A SIP Aware Proxy and the associated IP-based trunks to a SIP service provider; typically, the SIP service provider offers connectivity through to the PSTN and to other SIP service providers.

To connect to cloud-based data services:

- A web proxy for Mitel Open Integration Gateway-based and other web services and associated public data network connections; and
- A router with firewall for UC applications' client and management traffic and other services and associated private or public data network connections.

These gateways will be co-located with the UC servers, typically within a data center.

PSTN CONNECTIVITY (CENTRAL AND REMOTE)

Mitel's MiVoice Business running on a MiVoice Business appliance can serve as a PSTN gateway and provide direct trunk connections to the PSTN. The preferred MiVoice Business 3300 ICP platforms are:

- MXe III
- CXi II
- EX

The main factor that limits the number of PSTN connections is the number of physical connections available on the MiVoice Business 3300 ICP gateway. The physical interface limit is eight T1 or E1 circuits allowing 192 or 240 channels respectively. The MXe III and CX II may be further limited based on the number of Ethernet to TDM conversion channels. The deployment of PSTN gateways should also take into consideration the calls per hour capacity of the gateway.

In some cases remote survivability and local PSTN break out may be required at a customer site or at a remote site; a MiVoice Business appliance can fulfill this requirement.

SIP CONNECTIVITY

SIP trunks are provided by Internet Telephony service providers to connect communication platforms to other SIP switches and to the traditional PSTN. SIP trunks offer several benefits relative to traditional PSTN connections such as: local phone numbers from any location; increased resiliency for disaster recovery; and typically less expensive toll-free service and overall cost savings.

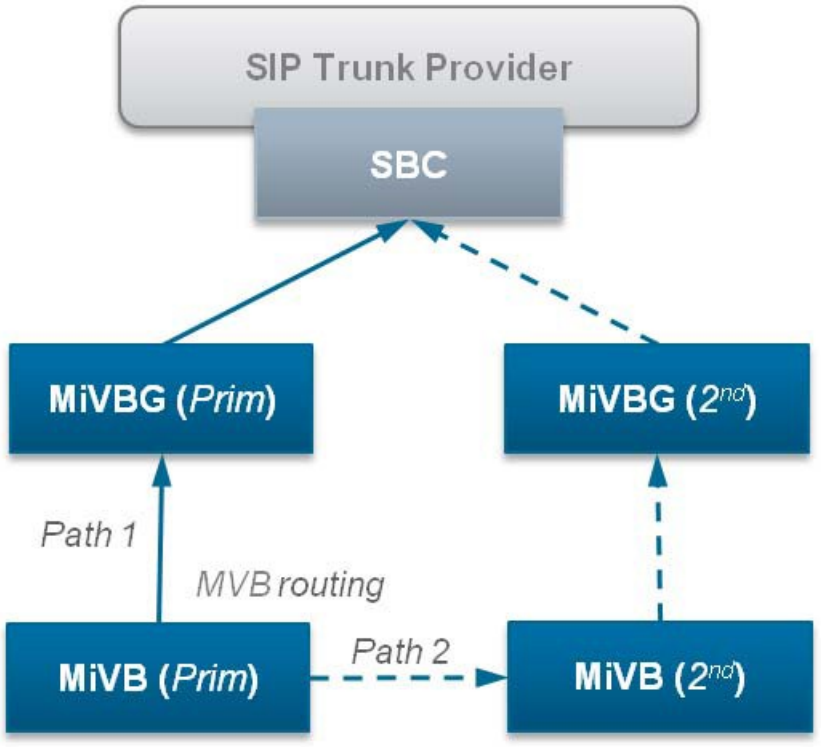
SIP trunks are established from the MiVoice Business to the SIP trunk provider using MiVoice Border Gateway as a SIP-aware firewall and proxy. The MiVoice Border Gateway SIP proxy implements a full back-to-back User Agent. The MiVoice Border Gateway SIP trunk service provides:

- NAT traversal of media and signalling;
- Media anchoring for the remote provider;
- SIP adaptation and normalization to improve interoperability;
- DTMF detection as per RFC 4733, re-ordering of RTP streams, and KPML notifications to support EHDUs; and
- Protection from malformed and malicious requests, request flooding and various other types of attacks.

A “SIP trunk” in the context of an MiVoice Border Gateway is a pair of end-points defined by their IP addresses and signaling ports. One endpoint is typically the call control engine (MiVoice Business) and the other endpoint is the SIP trunk provider’s firewall or SBC. A trunk can have any number of “channels” each of which corresponds to an active bi-directional media stream.

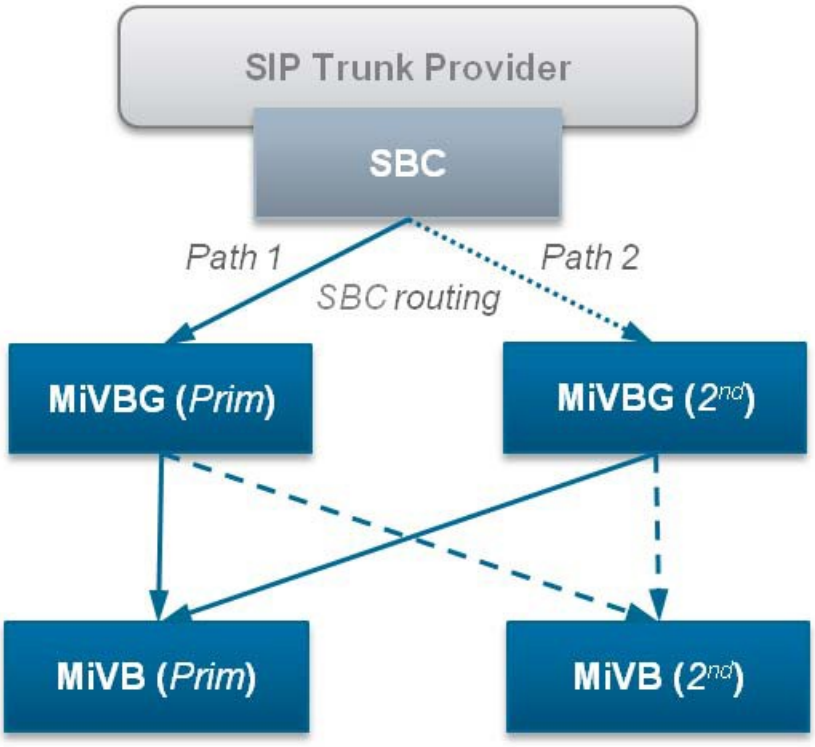
Outgoing SIP call routing is configured with the MiVoice Business using one or more Automatic Route Selection (ARS) rules. The SIP trunk service provider is configured as a Peer Profile, specifying the MiVoice Border Gateway as the related SIP proxy. Routing rules support specifying the minimum and maximum channels, i.e. active calls, per trunk. Multiple routing rules to different SIP Trunk providers are supported. MiVoice Business will detect trunk failures and set all trunks to the same peer out of service for both incoming and outgoing calls. In the case of outages causing missing keep alive messages, the MiVoice Business sets the trunks out of service to prevent instability in trunk status. For resilient operation for outgoing calls, routing rules must include a route to an alternate peer. “SIP Trunk routing - Outgoing Calls” on page 114 is an example where the resilient paths for the primary controller are configured with path1: MiVoice Business-primary to MiVoice Border Gateway-primary and path2: MiVoice Business-primary to MiVoice Business-secondary (different peer) to MiVoice Border Gateway-secondary and similarly for the secondary controller.

Figure 6: SIP Trunk routing - Outgoing Calls



Incoming SIP call routing is determined by the SIP Trunk Service provider routing to MiVoice Border Gateways and by MiVoice Border Gateways routing to MiVoice Business. Typically, third-party SBCs will support primary and secondary routes; the SBC will automatically detect trunk failures and re-route over the secondary path. The MiVoice Border Gateway SIP trunk proxy supports routing rules with match criteria mapped to all or part of the SIP URI within the SIP header Request, From, or To fields, effectively providing routing based on called party, calling party and original called party. Routing rules can designate both the primary and secondary controller for the route. An MiVoice Border Gateway will automatically detect trunk failures and route to the secondary controller. An example for MiVoice Border Gateway routing is shown in the figure “SIP Trunk Routing - Incoming Calls” on page 115.

Figure 7: SIP Trunk Routing - Incoming Calls



For smaller sites with shared trunking, one MiVoice Border Gateway can act as proxy for multiple MiVoice Business, up to the active trunk capacity limit. For larger sites, multiple MiVoice Border Gateways and MiVoice Business can be deployed for increased capacity. MiVoice Border Gateways support clustering up to five units with license sharing among cluster members. When dedicated to SIP trunking, MiVoice Border Gateway clustering beyond the resilient pair provides no advantage for resiliency or capacity as trunk traffic is determined by routing rules while clustering incurs the cost of increased synchronization communications. As such, MiVoice Border Gateways dedicated to SIP trunking should be deployed in a two member cluster containing the resilient pair and allowing license sharing between the pair.

For smaller deployments, a resilient pair of MiVoice Border Gateways may have sufficient capacity to act as both the SIP trunk gateway and access gateway for teleworkers and web proxy provided both are reachable with a public address. In the case that SIP trunks are carried over a private network, separate resilient pairs of MiVoice Border Gateways are required, with the SIP trunk gateway configured with a carrier-specific non-public IP address and the access gateway configured with a public IP address.

The MiVoice Border Gateway SIP trunk service is an edge or gateway type of service, supported by the MiVoice Border Gateway in either DMZ mode or Server-Gateway mode. These two modes are shown in the later section, Deployment Considerations. Gateway services are not supported when the MiVoice Border Gateway is deployed on an internal LAN configured for LAN mode operations, such as used for Secure Recording Connector services. Similar considerations apply when the MiVoice Border Gateway is integrated with other applications. MiCollab with Voice, deployed with MiVoice Border Gateway in Server Gateway mode, supports SIP trunk services, whereas MiCollab deployed on an internal LAN, with MiVoice Border

Gateway in LAN mode, does not support SIP trunk services. When deployed in server gateway mode, SIP Service providers connect through the external facing router to the MiVoice Border Gateway's WAN facing interface.

An MiVoice Border Gateway SIP Trunking Channel license is required for each active channel. MiVoice Border Gateway SIP trunk licenses are for concurrent use. So, for the MiVoice Border Gateway, the maximum number of active SIP trunk calls equals the number of configured MiVoice Border Gateway SIP trunk licenses, up to the MiVoice Border Gateway capacity limit. With UCC licensing, MiVoice Business SIP-enabled trunks are open licensed providing sufficient capacity for the licensed users. With a la carte licensing, MiVoice Business SIP trunk licenses are for concurrent use. For an MiVoice Business, the maximum number of active SIP trunk calls equals the number of configured MiVoice Business SIP trunk licenses, up to the MiVoice Business capacity limit. Both the MiVoice Border Gateway and MiVoice Business support clustering with license sharing among cluster members. This allows the available licenses to be shared across individual MiVoice Border Gateways or MiVoice Business respectively. The total number of licenses required will depend on busy hour traffic patterns.

DATA SERVICES CONNECTIVITY

Several cloud-based services may augment the UC solution. For example,

- Mitel's Application Management Center (AMC) provides software downloads and licensing for Mitel applications. Mitel applications must maintain data connectivity to the AMC to avoid entering license violation mode;
- Mitel Performance Analytics supports remote performance monitoring and management for Unified Communications systems and the associated networking infrastructure; Mitel Performance Analytics is available both as a cloud service and as an application deployed within the customer network;
- Integration with Salesforce.com provides full phone set management features within the hosted Salesforce.com user interface without the need for a locally installed client; and
- Integration of MiVoice Business with remotely hosted business applications incorporates voice communications, conferencing, and collaboration capabilities into popular business applications such as: personal information managers (PIMs), Microsoft Internet Explorer®, and Microsoft Office.

Integration of telephony features with applications is accomplished by interworking with Mitel Open Integration Gateway connected to a MiVoice Business system. The Mitel Open Integration Gateway offers a web service, WSDL messages over SOAP, which may be accessed locally or remotely with typical web traffic networking configurations. A brief description of the Mitel Open Integration Gateway capabilities and requirements is provided in the earlier chapter on Applications. Mitel continues to support the legacy MiTAI interface on the MiVoice Business system, providing a Mitel enhanced TAPI interface. However, it is recommended that all new implementations be based on Mitel Open Integration Gateway.

These data services require connectivity from the UC systems to cloud-based servers. Such connectivity is implemented using a router with integral or in-line firewall. The MiVoice Border Gateway in server gateway mode provides static routing and basic firewall capabilities. Alternatively, a third-party router with firewall protection may be used. Firewall protocol/port

configuration rules for many Mitel applications and services may be found in *MiVoice Border Gateway Engineering Guidelines* and *Mitel Open Integration Gateway Engineering Guidelines*, available on Mitel Edocs.

For web-based services, the MiVoice Border Gateway implements a web proxy to secure access between UC servers and other cloud service providers. This is recommended for connections from Mitel Open Integration Gateway to hosted business applications. MiVoice Border Gateway as web proxy is discussed further below.

ACCESS GATEWAYS

Depending on a particular topology's external connectivity requirements, the following access gateways may be required.

To connect to remote workers, home-based, mobile or anywhere off-site:

- A PSTN gateway or SIP aware proxy providing PSTN connectivity for access by digital and cellular phones as EHDU devices;
- A MiVoice Border Gateway (MiVoice Border Gateway) providing Teleworker service for access by remote MiNet and SIP end-points, including hard and soft phones;
- A web proxy for access by MiCollab and MiCollab Audio, Web, and Video Conferencing clients and management clients; and
- An IP router with firewall for data traffic such as associated media streams.

To connect to UC clients co-located at a customer site:

- An MPLS Edge Router or other LAN extension technology to extend the private LAN between the hosted UC server site and the customer site for LAN-based access by IP phones and other UC application and management clients; and
- An IP router for Internet-based access by UC application and management clients; the customer edge router uses Network Address translation (NAT) capabilities to uniquely identify individual end-points.

For remote workers, access gateways will be co-located with the UC servers, typically within a data center. For customer sites, access gateways will be required both at the data center edge and the customer LAN edge.

PSTN CONNECTIVITY (EHDU)

Remote users may connect to UC services using digital or analogue phones, with tone dialing, over the PSTN access network or cell phones over the public cellular wireless voice networks, all of which will connect through to the UC servers over PSTN or SIP trunks. The ubiquity of these devices and access networks provides a reliable means of connection from nearly any location.

For connection through the PSTN or cellular networks, the user dials a designated access number and then logs in for service as an External Hot Desk User (EHDU). The MiVoice Business may be configured with trusted trunks for EHDUs with Call Recognition Service

enabled, which recognizes the Calling Line ID and automatically log in the user. In other cases, the user will need to log in with their hot desk directory number and Personal Identification Number (PIN). Once logged in, the external user is seen by the system as a local user and has access to extension dialling, voice mail, and other phone system resources. Call handling and call features are available through simple keypad commands.

The PSTN or SIP trunk connections to the MiVoice Business appear similarly to other incoming trunks except in respect of the need for in-band DTMF detection for call handling. For PSTN connections, an MiVoice Business running on a MiVoice Business 3300 ICP platform can serve as a PSTN gateway, as described above. For SIP trunks, an MiVoice Border Gateway can serve as SIP trunk proxy, also described above. For SIP trunks, the SIP Trunk provider should transmit in-band DTMF tones with RTP packets compliant to RFC 4733, or the earlier RFC 2833. The MiVoice Business uses KPML subscription to the SIP trunk proxy to be notified of key press events used to manage call handling and call features. Termination of SIP trunks for EHDUs is not supported on the MiVoice Business as it does not support detection of in-band DTMF tones. Termination of SIP trunks on third-party SBCs requires interoperability testing to ensure compliance. Use of the MiVoice Border Gateway for SIP trunk termination is recommended.

When determining the required capacity of the PSTN or SIP trunk gateways, the EHDUs' traffic needs to be considered in the calculations. A trunk connection is required for every active EHDU connection for the communication path between the MiVoice Business and the external EHDU device. This is in addition to any trunk requirements for routing the call between the MiVoice Business and the other party in the call.

Call recording for EHDU calls cannot be done with the typical implementation which taps the LAN accessible line-side connection triggering recording based on a calling/called number identifier. EHDU calls connect via SIP trunks to the MiVoice Business, and for external calls, all call legs are carried on SIP trunks. As such, these trunk connections do not expose the line identifier to manage recording. For recording EHDU devices, the Call Recording Equipment (CRE) must establish a MiTAI monitor on either the EHDU device or SIP trunk and correlate the MiTAI event field for Call Leg Call ID with the similar information added to the SIP header within the SIP trunk. For trunk recording, the MiVoice Border Gateway gateway acting as SRC forwards the SIP signalling and media streams to the CRE.

SIP CONNECTIVITY (TELEWORKER)

Remote users may connect to UC services using IP phones over public or private data networks through the MiVoice Border Gateway Teleworker service. This service implements a SIP back-to-back user agent (B2BUA) or MiNet proxy to connect the remote IP phone to the MiVoice Business IP phone system. The Teleworker phone is registered as a standard extension of the office phone system, providing full access to voice mail, collaboration tools and all features of the system. Most Mitel IP phones, SIP and MiNet hard desk phones and soft phones, may be configured for Teleworker or normal mode of operation.

An interesting use case is the cellular phone with mobile SIP client which may access the UC services in two modes, namely as an EHDU device connecting via the mobile phone over the cellular wireless voice network and as a Teleworker device connecting via the mobile SIP client over an available wireless data network. The choice of EHDU or Teleworker depends largely

on the availability and cost for the access network. When using the MiCollab Mobile Client with Premium UC license, the Teleworker mode offers the advantage of handing off between the cellular wireless data network and local Wi-Fi networks. On the mobile client, wireless network availability and signal strength changes trigger enabling the command to hand off between networks.

When using the MiVoice Border Gateway Teleworker service with a Mitel IP phone, the following capabilities are provided:

- Encryption to improve voice path security;
- Adaptive jitter buffering and other enhancements to improve voice quality; and
- G.729 compression to reduce bandwidth requirements

For larger deployments, MiVoice Border Gateways may be clustered to support larger numbers of Teleworker users. Dynamic load balancing across cluster members is supported when both MiVoice Border Gateway and the device supports redirection. MiVoice Border Gateway supports redirection of MiNet devices; most MiNet desk phones support redirection. SIP devices and MiNet softphones must be manually load balanced by configuring the device to connect to a specific MiVoice Border Gateway node.

Resiliency available for teleworker devices depends on the capabilities of MiVoice Business, MiVoice Border Gateway and the device. For MiNet devices, MiVoice Border Gateway maintains a list of available PBX platforms. On failure of the primary PBX, all sets will disconnect and attempt to re-register. For MiNet devices that support redirection, when the devices re-connect the MiVoice Border Gateway will redirect the device to an available PBX. SIP devices and devices that do not support redirection will not be able to use this mechanism. For devices that support multiple registration configurations, resiliency is provided through manually configuring multiple MiVoice Border Gateway addresses or via FQDN and DNS redirection. On failure of the path through the primary MiVoice Border Gateway to primary MiVoice Business, the device will attempt to register with a secondary MiVoice Border Gateway. If the device does not support either redirection or multiple registration capability, the device will be unable to make calls until the primary MiVoice Border Gateway and/or primary PBX returns to service.

For recording Teleworker devices, the gateway MiVoice Border Gateway is configured to route calls to a second LAN-based MiVoice Border Gateway serving as the SRC which further connects to the MiVoice Business.

The MiVoice Border Gateway Teleworker service is an edge or gateway type of service, supported by the MiVoice Border Gateway in either DMZ mode or Server-Gateway mode. These two modes are shown in the later section, Deployment Considerations. Teleworker service is not supported when the MiVoice Border Gateway is deployed on an internal LAN configured for LAN mode operations. Similar considerations apply when the MiVoice Border Gateway is integrated with other applications. MiCollab with Voice, deployed with MiVoice Border Gateway in Server Gateway mode, supports Teleworker services, whereas MiCollab deployed on an internal LAN, with MiVoice Border Gateway in LAN mode, does not support Teleworker services.

MiVoice Border Gateway Teleworker service is licensed per device. If multiple MiVoice Border Gateways are deployed, the licenses may be shared across clustered nodes to support dynamic load balancing of MiNet devices. With UCC licensing, MiVoice Border Gateway Teleworker

licenses are included within the Standard and Premium User licenses and also are available as a la carte add-on option.

DATA CONNECTIVITY (WEB CLIENT)

The MiVoice Border Gateway Web proxy implements a reverse proxy with URL mapping. The proxy provides a secure method for end-user desktop and web clients to connect with LAN-based applications. The web proxy restricts access to only those URLs that belong to the end-user web interfaces for the recognized applications. The current release supports MiCollab and MiCollab Audio, Web, and Video Conferencing desktop and web clients.

The MiVoice Border Gateway web proxy also supports remote access to native management web pages for both MiVoice Business and MiCollab. For MiVoice Business management access, MiVoice Border Gateway adds additional access control security by requiring user name and password; also management access may be restricted to listed client IP addresses.

To provide a resilient web proxy service, redundant MiVoice Border Gateway servers may be deployed. The client applications can be configured to access these redundant MiVoice Border Gateways either directly or via multiple DNS entries. For MiCollab Clients, the connection through MiVoice Border Gateway to the MiCollab server is not resilient. Application layer resiliency may be achieved through deploying MiVoice Border Gateway and MiCollab on virtual servers configured with high availability.

The reverse proxy acts between an Internet accessible server and Internet-protected LAN server. It is not required if the application server is deployed in Network Edge mode with direct Internet access or if the web client has direct LAN access to the application server.

MiVoice Border Gateway web proxy is included in the MiVoice Border Gateway base software license. No separate license is required.

DATA CONNECTIVITY (LAN EXTENSION)

For UC communications, a commonly encountered scenario is multiple end-points connected on a common voice LAN within the customer's site and MiVoice Business servers on a LAN within a remote data center. Geographically extending the Layer 2 network between these sites allows the UC clients to connect directly to the UC servers without the need to deploy and provision proxies and fire walls. Typically these LAN extension connections will provide higher QoS, based on SLAs and/or the underlying transport mechanism.

There are a number of technologies and commercial offers available to provide LAN extension such as dedicated VPNs or MPLS connections. The choice is based on availability, service level agreements and cost. Typically, the addressing scheme and required networking equipment will be determined by the choice of carrier.

Within the UC solution, these remote end-points appear as local and are accessible via Layer 2 addressing schemes. UC design considerations include ensuring sufficient bandwidth and QoS mechanisms are available to support the expected traffic patterns.

When LAN access is available, this is the preferred method of connection between fixed UC clients and servers. For mobile clients, there are two possible configurations – normal mode

directly accessing the call control engine or teleworker mode accessing the set-side of the Teleworker gateway. For most Mitel IP phones, changing between normal and teleworker mode requires manual configuration of the mode, and for MiCollab Mobile Client requires changing the IP address used for registration (MiCollab Client supports only a single IP address). Dual mode hand-off between Wi-Fi and LTE/4G networks, available for premium UC users, requires that the active call be anchored at the MiVoice Border Gateway, as SIP redirection between MiVoice Business and MiVoice Border Gateway is not supported. So, for ease of use avoiding these manual steps, and dual-mode handoff, it is recommended that all mobile clients be configured for Teleworker mode both within the LAN and externally.

Within the customer site, routing rule exceptions may be used to route teleworker connections over the QoS enabled LAN extension path. Teleworker devices must connect to the set-side of the MiVoice Border Gateway, which may be either an Internet accessible WAN address or a DMZ address behind a fire wall with NAT. In either case, sets register to a public WAN address. Standard routing would direct these connections to the customer's Internet access gateway for connection across the public Internet. To avoid this path, manually configured rules may be added to the routing tables within the customer site and data center to ensure this traffic is directed to the MPLS egress devices such that the MiVoice Border Gateway WAN address routes via the QoS enabled path.

DATA CONNECTIVITY (OTHER)

UC communications requires access connectivity for various other types of traffic, not described above, such as the TCP connections for presence and collaboration features. Also, the access network requires connectivity for non-UC traffic such as hosted business applications. External facing fire walls and routers must be configured to allow this UC and application traffic, both at the data center and the customer site.

For Mitel application clients, the MiVoice Border Gateway includes templates and forms that simplify configuration when used in Server-Gateway mode. When the MiVoice Border Gateway is deployed in the DMZ or in-line with third-party fire walls, communication paths must be manually provisioned through external facing fire walls and routers.

Most Mitel management clients will gain access via the MiVoice Border Gateway web proxy described above. In a service provider data center, manual provisioning is required for the scenario where Mitel Management Portal is deployed in the service provider domain and used to manage UC components in the customer domain. Specifically, Mitel Management Portal requires 1:1 NAT mapping between virtual addresses in the service provider address space for these managed components, which include: MiVoice Business, MiCollab and MiVoice Border Gateways, and the component addresses in the customer space and configuration to allow both web services and THRIFT protocol connections between Mitel Management Portal and UC components. Mitel Management Portal networking is discussed further in the chapter Networking and network considerations. Client access to the Mitel Management Portal is via web proxy through an MiVoice Border Gateway or a third-party proxy.

MPA Probe is a data collection agent for Mitel Performance Analytics, available as software or custom appliance. It may be installed in the data center or customer's site to monitor device and network performance. MPA Probe connects to the Mitel Performance Analytics server using HTTP secured with SSL. MPA Probe always initiates IP connections with Mitel Performance Analytics and this outbound connection

will pass most firewall rules without specific configuration. Client access to Mitel Performance Analytics portal is via a third-party proxy or firewall.

At the data center, any firewall in-line with the MiVoice Border Gateway in Server-gateway mode should not implement NAT. At the customer site, the firewall is expected to implement NAT providing a unique port for identifying individual end-points.

Firewall protocol/port configuration rules for many Mitel applications may be found in *MiVoice Border Gateway Engineering Guidelines*. Also, protocol/port requirements are included in product-specific engineering guidelines.

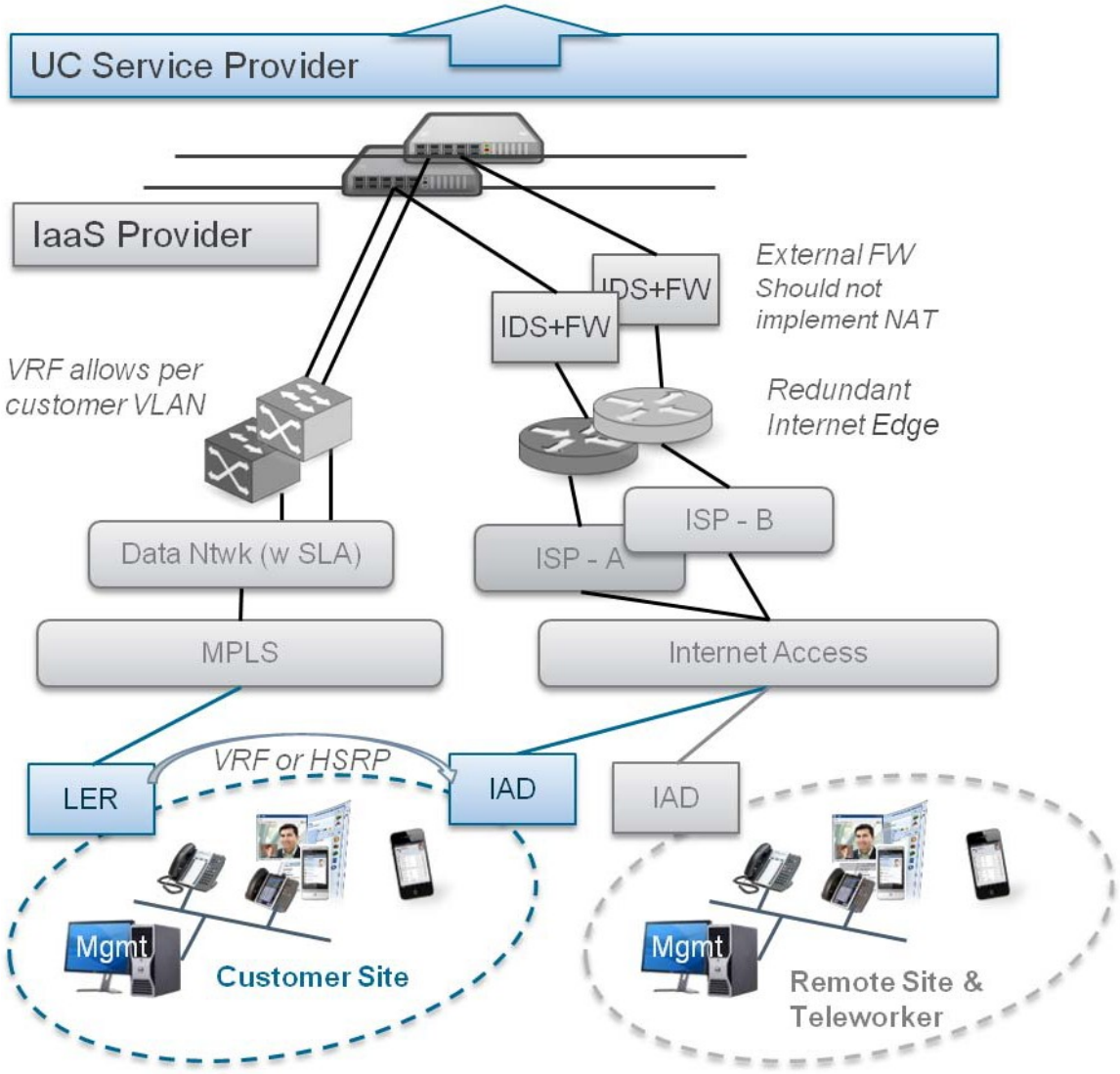
DEPLOYMENT CONSIDERATIONS

Network design for UC components within the data center and customer site has many options depending in part on the type of access network being used, the service provider peering network and the network capabilities available from an IaaS provider. This discusses a few design considerations specific to UC components but is not intended as a comprehensive network analysis.

ACCESS NETWORKS

Access between UC clients and UC servers located in the data centre typically requires WAN connections. These connections may be over the PSTN, the Internet or private data paths. Figure “UC Access Networking” on page 123 shows a high level view of possible access networks.

Figure 8: UC Access Networking



Customer sites will connect over MPLS or other LAN extension technologies, depicted with the Label Edge Router (LER), or over public data networks, depicted with the Integrated Access Device (IAD). Resilient access networking may be achieved with dual connections and redundant networking equipment. In the case that the primary path is via an MPLS connection with backup via the Internet, some means is required to trigger re-establishing connectivity through the back up path. Two possible implementations are a multi-service edge router supporting both MPLS and IP networking which will automatically manage the link states, or implementing Hot Standby Routing Protocol between the access gateways to manage the network re-routing. Using redundant edge routers provides improved resiliency, particularly for the multi-service router scenario.

As discussed above, customer site networking equipment will require a routing exception to route teleworker devices via the LER rather than the IAD. Routing over either device will work; the LER is expected to provide higher QoS than the IAD.

For the data center, there may be an in-line firewall outside the control of the UC service provider. It is recommended that this external firewall not implement NAT. Network design and configuration is simplified if the externally visible IP addresses are configurable by the UC service provider.

The MiVoice Border Gateway provides basic firewall capabilities such as port blocking/forwarding based on Mitel Standard Linux static routing tables. The services implemented effectively provide application layer protection from D/DoS attacks. Acting as a firewall, MiVoice Border Gateway processing speed is sufficient for most sites as traffic will be limited by the WAN pipe. An in-line third-party firewall provides additional protection including Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) with signature based updating, UDP flooding protection, advanced port blocking/forwarding capabilities and advanced reporting. An in-line IDS/IPS system can provide a measure of network layer D/DoS protection. Any in-line firewall should disable SIP adaptation as it conflicts with MiVoice Border Gateway SIP handling. Also as mentioned above, any external firewall on the data center edge should not implement NAT.

DATA CENTER EDGE

The principal external gateways for UC systems are the MiVoice Business 3300 ICP PSTN gateway and the MiVoice Border Gateway. The ICP 3300 is the service provider gateway for TDM trunks. The MiVoice Border Gateway provides both the service provider gateway for SIP trunks and the access gateway for application and management end-points.

The ICP 3300 provides both the PSTN gateway and call control engine. For smaller sites, both functions may be implemented with a resilient pair whereas for larger sites the roles may be divided between user controllers and trunking gateways. MiVoice Border Gateway supports two deployment modes, Server-Gateway and Demilitarized Zone (DMZ). For a typical mid-size hosted UC deployment, example network deployments are shown below. Figure 9 shows a private hosted network with ICP 3300 gateways and MiVoice Border Gateway Virtuals in DMZ mode. Figure “Service Provider Medium Large Business External Networking” on page 126 shows a service provider network with MiVoice Border Gateway Virtuals and MiVoice Border Gateway Virtuals in Server-Gateway mode.

Figure 9: Enterprise Private Cloud External Networking

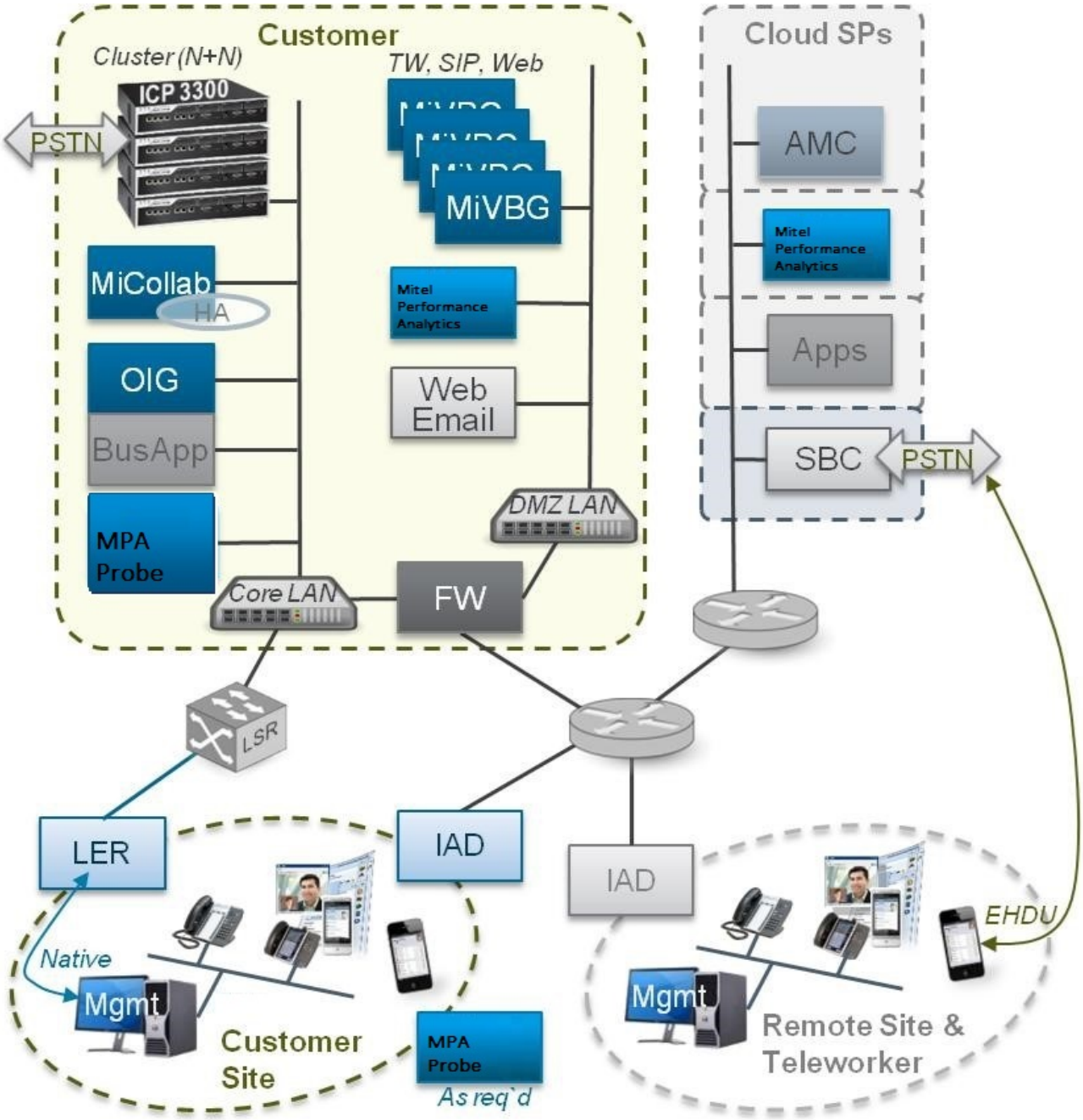
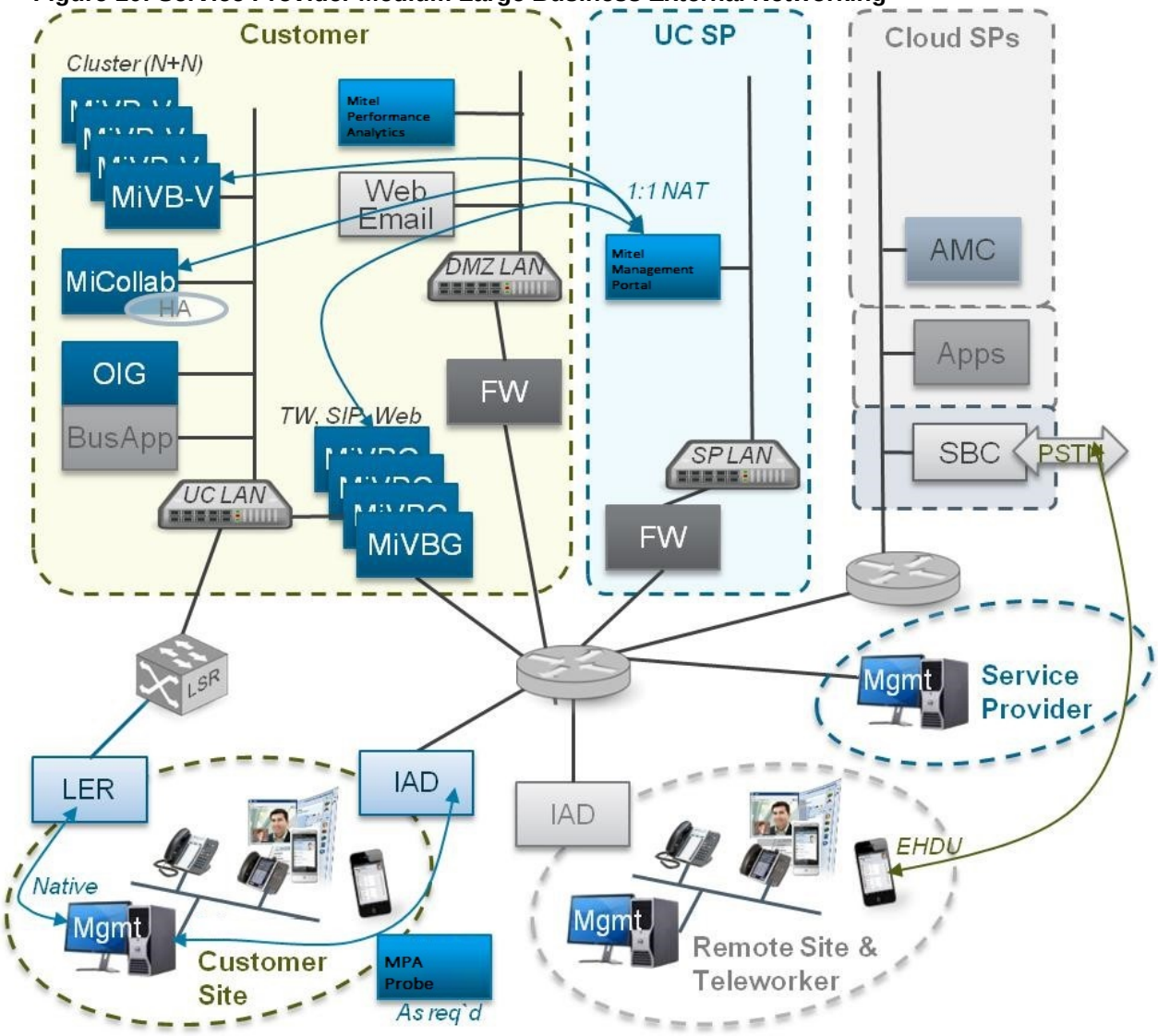


Figure 10: Service Provider Medium Large Business External Networking



Also shown in the service provider diagram is the Mitel Management Portal routing constraint where Mitel Management Portal requires 1:1 NAT access to the managed UC components. For Enterprise deployments, Mitel Performance Analytics server is optionally deployed within the customer's network or accessed as a cloud service. Within the Managed Service Provider Program, Mitel Performance Analytics is optionally deployed per customer; Mitel Performance Analytics cloud-based services are not supported. Mitel Performance Analytics server may be deployed in the DMZ or core LAN with web proxy via a third-party firewall. MPA Probe is deployed wherever network health and monitoring is required, typically the customer site and core UC service provider network.

The PSTN is effectively a private network with well controlled access. Networking for PSTN access to the ICP 3300 is based on dedicated connections – typically PRI or T1. The decision to deploy TDM gateways is largely based on considerations for resiliency, available service provider agreements and existing equipment. For more information on PSTN networking and ICP 3300 as trunking gateway, refer to ICP 3300 document suite available on Mitel-On-Line (MOL).

In both examples shown, MiVoice Border Gateway provides a SIP trunk proxy, Teleworker service and web proxy. When deployed as Server-Gateway, it is also implementing firewall and static routing capabilities. In Server-Gateway mode, the MiVoice Border Gateway is shown in parallel with a third-party firewall. The MiVoice Border Gateway provides access to the UC components and a third-party firewall provides access to other business applications. This is the recommended deployment for Server-Gateway mode for large sites. For smaller sites, MiVoice Border Gateway may act as the firewall for all of the core LAN servers. External addresses are required for each MiVoice Border Gateway, either with NAT to the DMZ address of the MiVoice Border Gateway or directly accessible on the MiVoice Border Gateway WAN interface.

The two major factors in choosing the MiVoice Border Gateway deployment mode are:

- the existing IT networking and security policies; and
- the existing network infrastructure.

Other factors to consider include:

- Security zones increase overall security of the network by confining attacks and breaches within a zone; the DMZ provides a security zone as does separating the UCaaS servers from the other business servers in the Server-Gateway mode;
- The firewall port blocking/forwarding is necessarily similar for DMZ or Server-Gateway modes as firewall rules are required to pass the UC traffic; whether ports are opened in the firewall managing the DMZ or the same ports are allowed in the MiVoice Border Gateway in Server-Gateway mode has limited impact on overall security;
- Networking equipment costs between the two options depend on the existing infrastructure; DMZ mode requires equipment to implement the DMZ; Server-Gateway in parallel with the business firewall requires networking equipment from the Internet access drop to the MiVoice Border Gateway; DMZ mode deployed into an existing DMZ is the most cost effective;
- Configuration and management, particularly trouble shooting, is simpler with Server-Gateway mode; MiVoice Border Gateway provides built in templates for Mitel products; in Server-Gateway mode, MiVoice Border Gateway owns the WAN address, avoiding unexpected routing to reach a firewall owned address; Server-Gateway mode avoids firewall configuration issues such as UDP port mismatch; and
- Visibility and control, both monitoring and reporting, is typically more comprehensive with DMZ mode.

The two modes of operation, Server-Gateway and DMZ affect MiVoice Border Gateway addressing and SIP conversion. Beyond these modes, MiVoice Border Gateway also offers various customization parameters to adapt to non-standard configurations. A custom profile may be used to override the default streaming addresses. Also IP translation tables may be used to translate IP addresses in call setup, particularly useful for streaming between MiVoice Border Gateways on the same LAN.

Chapter 8

MANAGEMENT CONSIDERATIONS

MANAGEMENT CONSIDERATIONS

Management of the UC solution can be divided into a few major aspects:

- System configuration – managing installs and updates, and setting system wide configuration parameters; typically undertaken by a system administrator with access to management applications and embedded system management tools.
- User and service configuration – managing re-usable roles and templates for different types of users and services. For a managed service, these templates would typically be defined by the service provider or reseller. For an enterprise, these templates would be managed by the user or group administrator.
- User and service provisioning – adding, updating and deleting users and their related devices and services, typically undertaken by the end-customer administrator using an admin portal.
- User administration – management and administration for individual end-user services; typically undertaken by the end-user using a user-facing portal.
- Technical support – manages the underlying network and server infrastructure and performs alarm management and troubleshooting of UC systems, typically undertaken by technical staff and IT support staff.
- Customer support - provides technical and administrative support to end-user administrators, typically undertaken by customer support staff within the service provider or reseller.

Mitel provides a comprehensive suite of management tools to support Mitel applications. These management tools are designed to provide different levels of access with varying scopes as appropriate for the different management roles.

“Management Applications” on page 131 provides an overview of Mitel management applications. This is followed by descriptions of the “Embedded Management Tools” on page 144 as well as various system capabilities that simplify provisioning. Following these overviews, the recommended approach for managing different UC topologies is discussed in “Topology-Specific Considerations” on page 162. “Installation Summary” on page 163 provides a brief summary of the major installation steps.

MANAGEMENT APPLICATIONS

Mitel provides several management applications designed for specific scenarios, which include:

- “MiCloud Management Portal” on page 132 – used by service providers to manage multiple customer systems
- “Mitel Performance Analytics” on page 138 – used by both service providers and enterprises for enhanced fault and performance management
- “Mitel Configuration Wizard” on page 141– used to simplify initial system configuration
- “MiVoice Business Migration Tool” on page 142 – required to upgrade any MiVoice Business system to release 9.0 from an earlier version

- “Mitel Redirection and Configuration Service” on page 142 – used to auto-configure Mitel IP phones.

This section provides a brief overview of these stand-alone applications. Embedded management applications are described in “Embedded Management Tools” on page 144.

MITEL MANAGEMENT PORTAL

Mitel Management Portal is a customer provisioning application allowing service providers to deliver multi-customer communications services. Mitel Management Portal is not available for enterprise deployments. Mitel Management Portal major capabilities include:

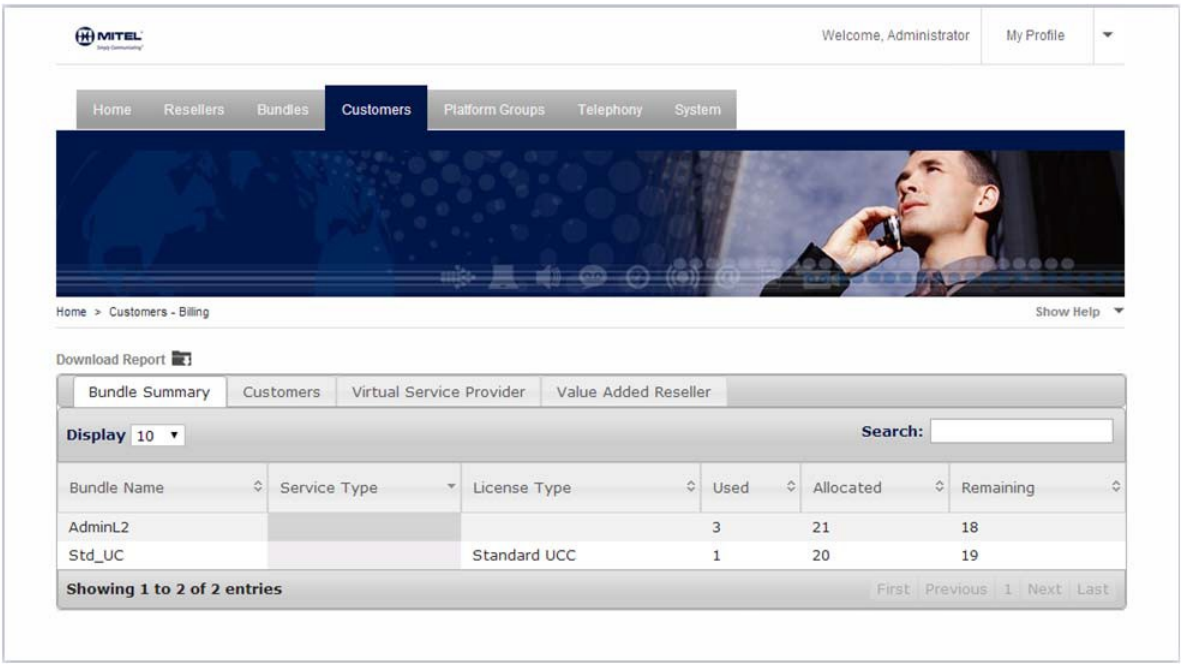
- Services provisioning process - supports registering MiVoice Business, MiCollab, and MiVoice Border Gateway instances to customers and defining service bundles.
- Customer Self Service - allows customer administrators to directly manage users and modify service options; allows end-users to directly manage enabled phone features.
- Customer and User Information aggregation - captures information from multiple MiVoice Business instances and aggregates into a single point of access.
- Billing /Operations integration - collects all information on new or modified user bundles which may be easily viewed and exported to a billing system and/or operations support system; provides a standards-based web service interface for integration.
- User Profiles - supports unique profiles for personnel to customize access to sensitive information and capabilities.
- Branding - customizable UI elements within the portal interface allows increased brand awareness including complimentary banner advertisements.

With simplified deployment of services and self-service portals, Mitel Management Portal enables service providers and resellers to cost effectively deliver communications services to many small and medium businesses through a direct or indirect sales channel.

Components

Mitel Management Portal is a server application typically hosted in a data center. Mitel Management Portal offers either a web portal for administrator and end-user interactions or a set of web service APIs for service provider BSS/OSS integration. The Administrator portal is shown in the figure “Mitel Management Portal, Administrator View” on page 133.

Figure 11: Mitel Management Portal, Administrator View



Mitel Management Portal runs on Mitel Standard Linux and may be installed on a standalone server or as a virtual appliance on a VMware virtual machine. Installing Mitel Management Portal as a virtual appliance has certain advantages for maintenance and resiliency as it enables access to the underlying virtualization platform deployment services and high availability features. Mitel Professional Services are required for Mitel Management Portal installation.

Mitel Management Portal provides a secure web portal for interactions with service providers, resellers, customer administrators and end-users. The web portal supports standard web browsers including Mozilla Firefox, Microsoft Internet Explorer, and Google Chrome. Supported software versions are detailed in *Mitel Management Portal Engineering Guidelines*, available on Mitel Edocs.

Mitel Management Portal offers several profiles that enable a service provider to provide and/or restrict access to data and functions. The default profiles as well as typical allowed actions for the profile are listed below.

- Service provider - full system access, for example system setup and configuration, registering and assigning MiCollab servers and MiVoice Business, DID Management, dial plans, billing and licensing, service definition and bundling
- Virtual service provider - similar to service provider except lacking the ability to assign further virtual service providers.
- Value Added Reseller - limited system access, supporting basic customer management and branding
- Customer Administrator - access to customer-specific data and features; for example, manage users, assign DIDs, define call groups, ACD, and configure user's voice mail

- End-User - access to user-specific data and functions; allowed to view and modify phone and feature control such as: speed dial lists and programmable keys, edit personal profile, reset password, and view call history.

Mitel Management Portal allows service providers to provide a differentiated service offering for each reseller and/or customer.

Mitel Management Portal provides web service interfaces for integration to other BSS/OSS systems. The web services provide data encapsulation using Mitel custom XML (MiXML). Additional capabilities include generation of license usage reports for managed components, producing an XML file with details about bundles and licenses that are in use. The license usage must be entered into a report spreadsheet for compliance with Mitel AMC license usage reporting requirements.

Mitel Management Portal is used to manage Mitel applications required for UC solutions. The managed systems and related communication interfaces between Mitel Management Portal and the managed system include:

- all MiVoice Business platforms (MiVoice Business 3300 ICP, MiVoice Business on ISS, MiVoice Business Virtual and MiVoice Business-MI) offer a web service using MiXML over SOAP (http and https); Mitel Management Portal also relies on MiCollab SPP to provision user data to the related MiVoice Business
- MiCollab, within Suite Application Services (SAS) component, offers a THRIFT interface
- MiCollab Client offers a SOAP web service (http, https)
- MiVoice Border Gateway offers a REST web service (http, https).

In all of the above, the managed component offers the services interface and Mitel Management Portal acts as the client. Port usage is described in the related engineering guidelines.

Mitel Management Portal acts as a mediation layer for managing multiple UC solutions. Mitel Management Portal offers a web portal and web service interface for management activities and handles translating the management information to the underlying managed UC platforms.

Licensing

For service providers, Mitel Management Portal is included in the commercial licenses for MiCloud Voice and MiCloud UC, and is a required component that must be deployed as part of the UC Enterprise Solution. Mitel Management Portal license costs are built into the UCC licensing models.

Currently, Mitel Management Portal is not available through the partner channel for enterprise deployments.

Scalability

Minimum hardware requirements for a standalone server installation or for a virtual server installation are available in the *Mitel Management Portal Engineering Guidelines*. With the recommended server specifications, Mitel Management Portal supports up to 1000 Customers with up to 100,000 end-users.

Networking

Mitel Management Portal networking requirements can be divided into two major aspects, which include: access to the Mitel Management Portal itself via the web portal and web service interfaces, and access between Mitel Management Portal and the managed systems.

The web portal and web service interfaces are standards-based interfaces. The web portal server should be assigned a static IP address to avoid issues with DNS updates when dynamic addresses change. Remote access is available using the MiVoice Border Gateway web proxy service, in which case, Mitel Management Portal re-uses the available proxy selection for MiVoice Business connections.

Mitel Management Portal access to the managed systems depends on the deployment topology. In the case that Mitel Management Portal is located within the same local area network as the managed systems, straight-forward local networking can be applied. In the more typical case for service provider deployments, Mitel Management Portal is deployed within the service provider network while managing systems within the customer network. Mitel Management Portal communicates with managed systems using a variety of protocols for which application layer proxies are not readily available. As such, special networking is required for Mitel Management Portal to communicate with managed systems.

For all but MiVoice Business Multi-Instance, 1:1 NAT connections must be established between Mitel Management Portal and each managed system; the NAT link must support bidirectional path initiation, i.e. for Mitel Management Portal to initiate a connection to a managed system and for the managed system to initiate a connection to Mitel Management Portal. This requirement for 1:1 NAT may be implemented with VMware networking or third-party routers. Mitel Management Portal addresses the managed UCC components using fully qualified domain names and split DNS is used to resolve these domain names based on the local address space. Further information on the recommended network deployment is available in “Network and Networking Considerations” on page 167 and the *MiCloud Business Solution Medium Large Business Deployment Guide*.

For MiVoice Business Multi-Instance deployments, MiVoice Business-MI provides management access independent of the control and signalling access. In this case, the management port may be provisioned within the service provider address space where as the control and signalling port is provisioned in the customer address space. 1:1 NAT is no longer required for MiVoice Business Multi-Instance as both Mitel Management Portal and MiVoice Business Multi-Instance management are in the same service provider network.

In cases where Mitel Management Portal is remote from the managed system, a VPN tunnel is required for secure WAN traffic. This is required for remote access between Mitel Management Portal and any managed system, including MiVoice Business Multi-Instance.

MITEL PERFORMANCE ANALYTICS

Mitel Performance Analytics provides remote fault and performance monitoring and management for UC systems and the associated networking infrastructure. Continuous monitoring allows early identification of problems, reduced downtime, and reduced on-site visits. Key capabilities include:

- Comprehensive health monitoring - monitors, tracks and analyzes the status of network infrastructure and systems with particular focus for UC systems on VoIP quality, IP QoS, IP Service Level Agreement (SLA) monitoring; provides real-time and historical data to diagnose and resolve performance issues; provides visibility of IP set inventory with set status; enables collection and storage of SMDR records.
- Fault Management - manages system alarms and configurable threshold alarms; threshold alarms are customizable and can be created to monitor memory utilization, voice quality, device availability and reach-ability, interface availability, and license status; provides notifications by e-mail, SMS and Twitter.
- Secure remote access - provides on-demand connection to a remote LAN without the need of a VPN; includes remote network diagnostic tools such as: remote DNS, Ping, Trace route, and SNMP browser as well as an integrated web proxy for high performance access to MiVoice Business management tools.

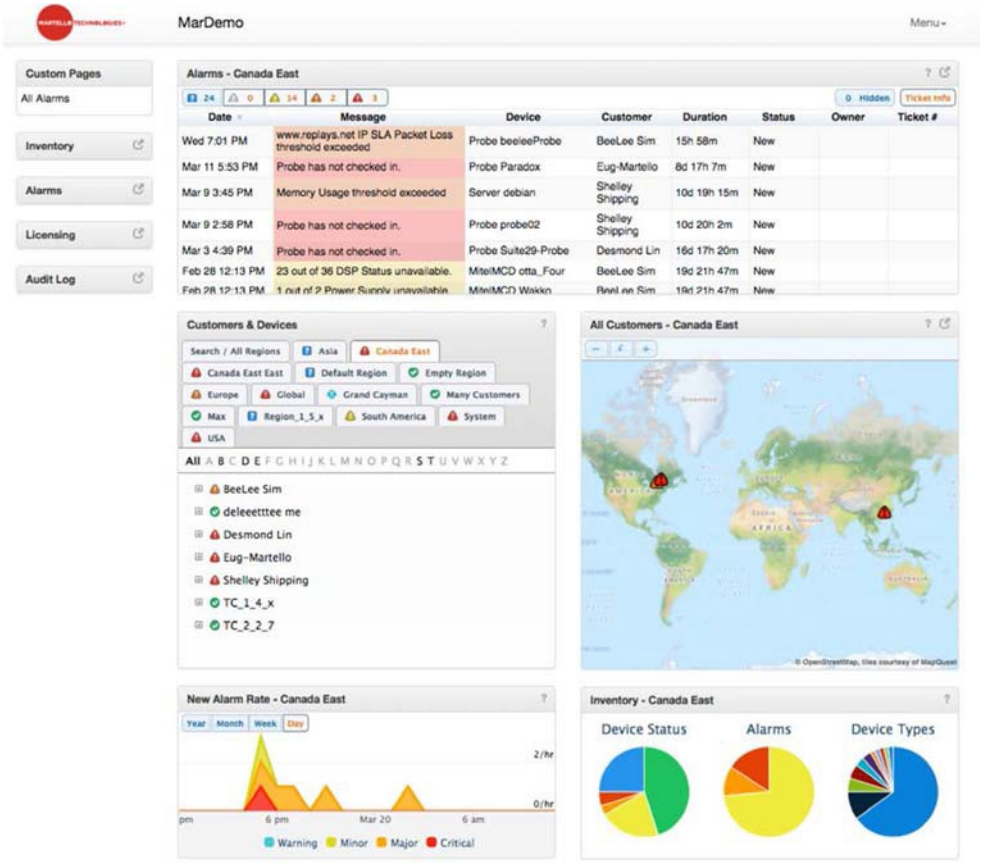
- Off-site backup services for MiVoice Business - supports scheduled and on-demand back-ups for MiVoice Business including the database with optional voice mail and call history; provides secure off-site cloud-based backup storage with downloadable file for restoring.
- Monthly and on-demand reporting - key performance metrics are available to assist with planning and forecasting, assurance for SLAs and ongoing maintenance.
- Enhanced user interface with customizable dashboard - displays alarms with color-coded locations and status with both historical and current views; supports ticket management display and export of alarms to ticketing system; provides a brand-able and customizable layout; supports three user profiles for administrator, limited access used for VARs, and customer.

Mitel Performance Analytics supports a wide range of Mitel platforms and third-party networking products. For a UC solution, Mitel Performance Analytics supports all variants of MiVoice Business, MiCollab, and MiVoice Border Gateway, as well as third-party managed Ethernet switches, routers and servers. For supported versions on SNMP refer to Martello guidelines available on
Mitel-On-Line (MOL). Also, further information on supported third-party products is available on the Martello Technologies web site.

Components

Mitel Performance Analytics is a server application that works in conjunction with MPA Probe deployed on the monitored LAN. A sample view of the “Mitel Performance Analytics Dashboard View” on page 140 is shown below.

Figure 14: Mitel Performance Analytics Dashboard View



For on site server deployments, Mitel Performance Analytics server is available as an OVA for a VMware virtual server in three package sizes, which include: a small, medium and large image. It is recommended to consult Mitel Corporate Sales Engineering to determine the required size for a particular network and topology.

User access to Mitel Performance Analytics requires a web browser with JavaScript and Adobe Flash supported. Mitel Performance Analytics should work with any standards compliant browser; refer to Mitel Performance Analytics guidelines for details of specifically tested browsers.

Licensing

For enterprises, Mitel Performance Analytics is available both as a managed service and as a server-based deployment, specifically

- Remote Monitoring and Access Service (RMAS) is a subscription-based service with Mitel technical staff providing pro-active network and performance monitoring.
- Mitel Performance Analytics is a server application for deployment by service providers, resellers and enterprises. Mitel Performance Analytics licensing covers devices, capacities and services. Depending on Mitel Performance Analytics system licensing, every device may require a license and support additional optional licensable capabilities. Mitel Performance Analytics license entitlement is included in Mitel Premium Software Assurance & Support subscriptions.

Within the Managed Service Provider Program, only the Mitel Performance Analytics server deployment is offered; the managed service is not available. In both cases, MPA Probe must be deployed in the monitored network.

MPA Probe

MPA Probe is the data collection agent for Mitel Performance Analytics. MPA Probe monitors devices on the LAN and transmits reports to the Mitel Performance Analytics server.

MPA Probe may be deployed on a server running

- Windows (runs as a Windows service)
- Red Hat Linux, CentOS (runs as Linux daemon)
- Mitel Standard Linux - deployed as a blade

MPA Probe supports virtual deployment on VMware.

MPA Probe is a lightweight application with minimum system requirements scaled with the number of devices monitored. Server specifications are provided in MPA Engineering guidelines, available on Mitel-On-Line (MOL). Also, MPA Probe is available on a dedicated server called the MPA Probe appliance. This is a small form factor server with MPA Probe software pre-installed running on Debian Linux operating system.

Connectivity requirements include:

- Continuous network access to monitored devices
- HTTP/SSL, access to Mitel Performance Analytics server for remote monitoring
- Optional - FTP, FTPS Implicit, SFTP, or FTPS Explicit, access to a customer defined File Server for SMDR file transfer
- Optional – SSH, to Mitel Performance Analytics server for remote access to monitored network.

MPA Probe always initiates connections; fire walls must allow outbound traffic from the monitored network. For further details on port requirements refer to Martello guidelines, available on Mitel-On-Line (MOL).

MITEL CONFIGURATION WIZARD

The Mitel Configuration Wizard (MiCW) facilitates initial system setup and commissioning for MiVoice Business and MiCollab systems for enterprise installations. The wizard is a user interface that presents a sequence of dialog boxes to walk through typical configuration tasks, and that includes pre-configured defaults and templates. MiCW produces a CSV file that contains data generated by the wizard as well as factory defaults. This file can be applied to program the MiVoice Business or MiCollab system. Also the file may be re-used as a base configuration template for installation of multiple similar systems.

MiCW supports the provisioning of users via import of a CSV file with several major restrictions. For UCC licensing, MiCW user provisioning is not supported. With UCC licensing, user provisioning must be handled using MiCollab User and Services application.

The MiCW is a software tool that runs on the Microsoft Windows Operating System from Windows XP through Windows 8. The tool can be run with the computer connected or disconnected from the MiVoice Business and MiCollab systems.

The MiCW is not used by service providers. Mitel Management Portal provides capabilities to manage the installation and configuration of new systems.

MIVOICE BUSINESS MIGRATION TOOL

The MiVoice Business Migration Tool expedites the distribution of software and supports automatically installing and upgrading software on multiple MiVoice Business systems simultaneously. The MiVoice Business Migration Tool supports the following capabilities:

- Upgrade or install MiVoice Business software on up to ten controllers simultaneously (up to ten instances of the Migration Tool may be launched from the parent window)
- Migrate a database from any release between MiVB 6.0 and 8.0 SP3 to release 9.0 or later
- Backup and restore databases
- Specify a location to install Help files for MiVoice Business System Administration Tool
- License a new system and subsequently change License and Option Selection (LOS) information
- Program the system as the Designated License Manager (DLM) for an application group

For MiVoice Business for Industry Standard Servers (ISS), MiVoice Business Virtual, and MiVoice Business Multi-Instance, the migration tool can only be used for upgrades; full installations are not supported. Full installs and upgrades can also be done using the Scheduler in the System Administration Tool.

The MiVoice Business Migration Tool is a stand-alone tool that runs on the Microsoft Windows Operating System, from Windows 2000 to Windows 7. The installer may be run on a computer local or remote to the MiVoice Business system.

MITEL REDIRECTION AND CONFIGURATION SERVICE

The Mitel Redirection and Configuration Service provides redirection to configuration information and firmware control for Mitel IP phones, facilitating phone deployment for service providers and large geographically distributed enterprises. The Mitel Redirection and Configuration Service provides a plug-and-play provisioning capability for supported phones.

The core feature of Mitel Redirection and Configuration Service is to redirect unconfigured phones to configuration servers that in turn will provide configuration information for the phone. When the phone is plugged in and boots for the first time, the phone will attempt to find its configuration server address from, in order of precedence, static programming, DHCP and finally factory defaults, i.e. Mitel Redirection and Configuration Service. For supported phones, the factory defaults include the URL for the Mitel managed Mitel Redirection and Configuration Service. When using factory defaults, the phone will connect to the Mitel Redirection and Configuration Service, obtain the configuration server address and store these in static settings. For MiNet mode, this server address will be stored in the Teleworker Gateway static setting and the same will be used for the TFTP Server setting if this setting is not configured statically.

For SIP mode, this server address will be stored in the Provisioning Server static setting. The phone will not contact Mitel Redirection and Configuration Service again unless this setting is deleted by the user or a factory reset is performed. The configuration server is typically the MiVoice Border Gateway Teleworker gateway used for connection with mobile or external phones. For LAN-based phones, the configuration server is the MiVoice Business Call Server, although this would typically be discovered via DHCP rather than contacting Mitel Redirection and Configuration Service.

Mitel Redirection and Configuration Service also supports the capability to provide firmware upgrades. When a phone boots up, if it connects to Mitel Redirection and Configuration Service, the phone checks the firmware revision and when required Mitel Redirection and Configuration Service downloads any firmware files specified under the phone's MAC address. Phone firmware may be upgraded or downgraded directly from Mitel Redirection and Configuration Service or from a configuration server, such as the MiVoice Border Gateway or MiVoice Business. The precedence order for upgrading firmware is static programming for TFTP server, Mitel Redirection and Configuration Service, and then DHCP. It should be noted this precedence differs from the ordering for the configuration server, which is static, DHCP, then Mitel Redirection and Configuration Service.

The Mitel Redirection and Configuration Service server URL is pre-configured in the factory default settings for MiVoice 53xx IP Phones.

The Mitel Redirection and Configuration Service is most useful for service provider deployments removing the need for static programming of the configuration server address for mobile or teleworker sets. It may also be useful for large geographically dispersed enterprises with multiple MiVoice Border Gateway gateways.

Components

The Mitel Redirection and Configuration Service is a web server application providing an administrator portal and web services for phone configuration. Mitel Redirection and Configuration Service is available from Mitel as a managed service.

The administrator portal is a web-based interface for entering account information, configuration server parameters, and phone parameters. The portal supports two levels of access, which include:

- Users - Full access to the account. However, a User cannot add, change, or delete accounts for other Users or Super Users.
- Super Users - Full access to the account including adding, changing, and deleting accounts for Users and Super Users.

Users manage a list of configuration server names and addresses. Phones are identified based on MAC address and assigned to a configuration server and firmware version. The phone MAC address may be entered directly or multiple addresses may be uploaded using a CSV file.
Phones must be entered in the Mitel Redirection and Configuration Service server prior to the phones attempt to connect to the service.

Licensing

Mitel managed Mitel Redirection and Configuration Service is available for Hosted service providers as part of UC Enterprise Solution licensing. There is no incremental license fee attached to the service.

For enterprises, contact Mitel Sales for further information and account set up.

EMBEDDED MANAGEMENT TOOLS

All Mitel applications provide embedded management tools that support configuration of the features, users and groups for the specific instance of the application. Some of the embedded tools also support management for clustered instances of the same application. This section describes these embedded system managers.

MITEL STANDARD LINUX

Mitel Standard Linux server offers two management interfaces, the choice depending on the activity. Possibilities include:

- Server Manager: a web-based control panel for performing tasks such as: installing applications, configuring the server and its optional features, and managing available services
- Server Console: a text-based control panel built into the Mitel Standard Linux server and used for performing functions like reconfiguring network parameters such as: changing server configuration, testing Internet access, and managing disk redundancy.

Server Manager is accessed by a standard web browser, e.g. Google Chrome, Microsoft Internet Explorer or Firefox. By default, the server manager is accessible only from the local network. While physically connected to the local network, remote access to the server manager may be configured using the remote management feature or local networks feature.

The server console provides basic, direct access to the server. Most server console operations are also available from the server manager. Also the server console provides a text-based browser view of server manager, which provides access to the server manager capabilities, although typically not the application-specific panels.

Mitel Standard Linux Server Manager is shown in the figure “MSL Server Manager Blades Panel” on page 145.

Figure 15: MSL Server Manager Blades Panel

Selected management capabilities include:

- Blades panel – supports installing, upgrading or removing application software blades. Typically, each software blade modifies the server manager navigation menu to allow access to application configuration pages. Some applications, notably MiCollab, modify the Server Manager only to display information, with functionality to install and upgrade available only through Server Console.
- Service Link Status panel – supports Mitel application license management including displaying AMC status and activation and deactivation of licenses.
- Alarms and Logs Viewers – show application status and support troubleshooting.
- Security panels – allow configuring remote access, granting local network privileges, modifying the firewall and port forwarding rules and managing security certificates.
- Configuration panels – support configuring DHCP and DNS servers, SNMP support and Network Interface Cards.
- Virtualization Panel – allows running diagnostics on the VMware environment.

Mitel Standard Linux server management capabilities, including added application configuration pages, are typically used only by the server administrator, enterprise or service provider. There are no management features or access portals for end-customers or end-users.

MIVOICE BUSINESS MULTI-INSTANCE

Note: This variant is Not Supported in MiVB 9.0, but will be supported in a later release.

MiVoice Business Multi-Instance includes several components with their own management interfaces. The components include:

- Mitel Standard Linux – the base operating system on which all other applications reside; managed as described above.
- MiVoice Business Multi-Instance Server Manager – installed as a software blade and pro-

viding an administrative interface for managing the MiVoice Business instances.

- Related MiVoice Business instances.
- MiVoice Business Media Server Manager – installed as a software blade and providing the administrative interface for managing the media servers.
- Related MiVoice Business Media Servers – one media server is required for each MiVoice Business instance.

MiVoice Business Multi-Instance does not contain any MiVoice Business software loads. One or more software loads must be placed into the inventory managed by MiVoice Business Multi-Instance. The inventory contains "master" or "golden" copies of MiVoice Business software loads. The inventory copies are used as the MiVoice Business software image source when creating or upgrading MiVoice Business instances. The software inventory can support multiple versions of MiVoice Business software.

The MiVoice Business Media Server provides Music On Hold, Group Page, Conference Calling and Embedded Voice Mail for the corresponding MiVoice Business instance. A media server instance is required for each MiVoice Business instance. Media Server instances on a single Media Server may connect to MiVoice Business instances on different MiVoice Business Multi-Instance servers.

The MiVoice Business Media Server must be installed on a separate server with no other software co-located. So, the minimum deployment for MiVoice Business Multi-Instance is two servers. Further details on capacity limits are described in *MiVoice Business Multi-Instance Engineering Guidelines* available on Mitel-On-Line (MOL).

One important consideration when deploying MiVoice Business Multi-Instance is the required IP address allocation. MiVoice Business Multi-Instance provides two addressing modes.

- "Non VLAN Mode" on page 146
- "VLAN Mode" on page 147

For Enterprise deployments, MiVoice Business Multi-Instance supports Enterprise Manager for virtual call server SNMP discovery and inventory, fault management, system management reach-through, moves/adds/changes, and voice quality reporting. A north-bound interface that supports these management capabilities is provided for integration to a Network Management System (NMS).

For hosted deployments, MiVoice Business Multi-Instance Server supports customer self-management at the customer premises with a restricted System Administration Tool interface within the MiVoice Business Embedded System Management (ESM) tools. This interface permits simple configuration changes such as user moves/adds/changes. For service provider deployments, the customer administrator portal of Mitel Management Portal offers similar customer self-management options.

Non VLAN Mode

In this mode, the MiVoice Business Multi-Instance server and all associated MiVoice Business instances reside in the same subnet with the same default gateway. Each MiVoice Business instance consumes a contiguous block of four IP addresses aligned with a /30 (255.255.255.252) boundary within the MiVoice Business Multi-Instance server subnet. MiVoice

Business Multi-Instance and Media Server each consume a single IP address. The Media Server need not be in the same subnet, although using the same subnet will provide fast Layer 2 access. This mode is suitable for enterprise deployments on a single network. It is also appropriate for hosted deployments where all MiVoice Business instances reside in the service provider's address space and customers access the MiVoice Business over public networks via a common MiVoice Border Gateway, such as described for the SB topology.

VLAN Mode

Each MiVoice Business instance is accessible via one of two IP addresses

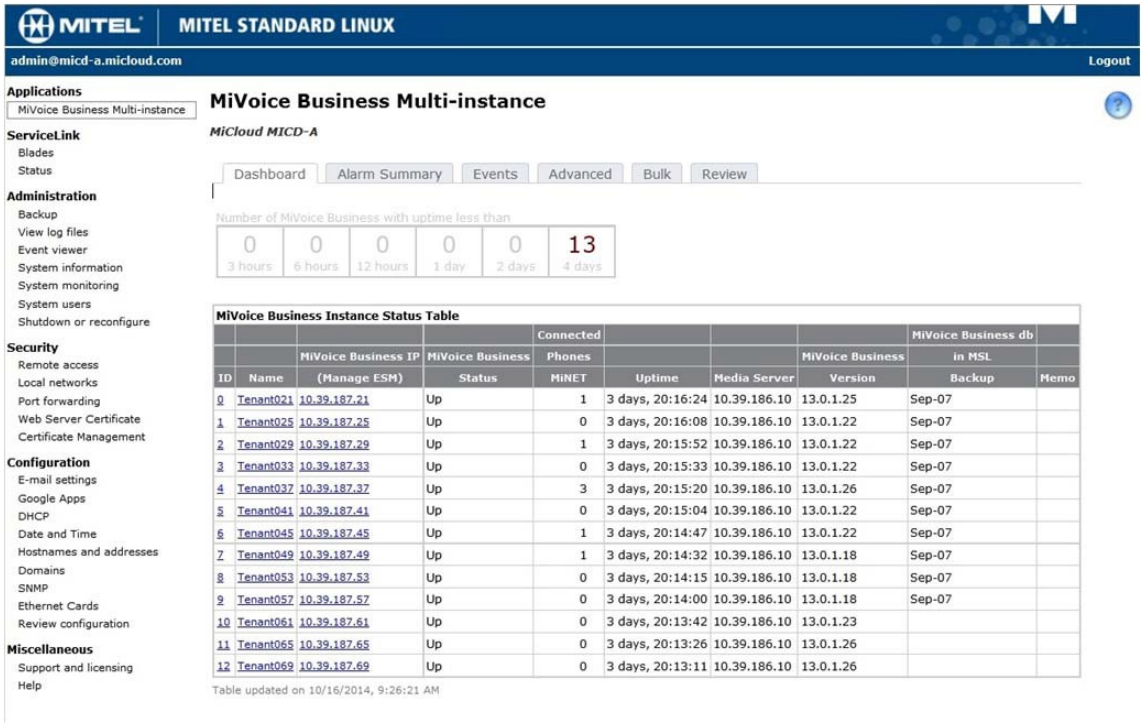
- MiVoice Business Management IP address is in the same subnet as the related MiVoice Business Multi-Instance server and is used for management access to the MiVoice Business instance. Often this subnet is referred to as the management network.
- MiVoice Business System IP address must be associated with a specific VLAN and is used for connections to the media server, phones and other end-points. This VLAN is associated with a specific customer and the assigned IP address fits into the customer's network plan. MiVoice Business instances do not require a specific address within a /30 address field. Multiple MiVoice Business instances may exist within a specific customer's VLAN.

In VLAN mode, the management network must be untagged, sometimes referred to as the native VLAN. Mitel Standard Linux Server Manager Local Networks feature may be used to add other subnets to this management network. MiVoice Business Multi-Instance Server and Media Server are assigned addresses within the management network. Media Server instances must be assigned addresses and appropriate VLAN ID within the customer's network for connection to the MiVoice Business instance and end-points. This mode is suitable for networks which require multiple address spaces with overlapping IP addresses. This mode is used for hosted deployments where customers access the MiVoice Business over private networks, such as described in the SMB topology.

MiVoice Business Multi-Instance Server Manager

MiVoice Business Multi-Instance Server management is based on adding specific panels to the Mitel Standard Linux Server Manager. Multi-Instance Server Manager is accessible under the Applications menu on Mitel Standard Linux Server Manager. The administration web interface is used to manage the life cycle of multiple MiVoice Business instances residing on the MiVoice Business Multi-Instance server, including creating, modifying, starting, stopping and deleting instances. A sample view is shown below.

Figure 16: MiVoice Business Multi-Instance Manager, Dashboard View



The Multi-Instance Server Manager administration interface is organized with five tabs:

- Dashboard - provides a summary of all Instances; also used to modify, start, stop, backup and restore a single MiVoice Business instance and access it's System Administration Tool.
- Alarm Summary - provides a summary and details of any Instances that may be in an alarm state.
- Events - provides a list of resulting actions from all starts, stops, and button presses for all Instances.
- Advanced - used for managing software inventories, enabling VLAN mode and trouble-shooting logs.
- Bulk - provides the capability to perform operations on multiple instances at the same time, such as: modifying, adding, backing up, and restoring a range of instances; also used to create instances.
- Review - contains a table listing all instances and their current MiVoice Business Multi-Instance configuration settings.

MiVoice Business Multi-Instance Server Manager is used for managing MiVoice Business instances. It includes embedded versions of the MiVoice Business Software Installer tool and Mitel Configuration Wizard which are used to simplify the process for creating new instances. After MiVoice Business instances are created, additional MiVoice Business configuration is performed using the MiVoice Business System Administration Tool accessible from the Dashboard tab.

MiVoice Business instances may also be upgraded using the stand alone MiVoice Business Software Installer tool. In this case, the computer where the tool is running must be included as part of the Mitel Standard Linux Local Networks and Mitel Standard Linux must be configured to allow Secure Shell access. When upgrading software using the stand alone tool, the software version should also be added to the MiVoice Business Multi-Instance inventory to enable embedded Software Installer tool operations for backup, restore and upgrade.

Media Server Manager

Media Server management is based on adding specific panels to the Mitel Standard Linux Server Manager. Media Server Manager is accessible under the Applications menu on Mitel Standard Linux Server Manager. The administration web interface is used to configure and manage the media server instances associated with MiVoice Business instances. The interface is organized with four tabs:

- Dashboard - provides a summary of all Media Servers and their corresponding MiVoice Business instances; also used to start, stop or modify a single Media Server instance.
- Events - provides a list of resulting actions from all starts, stops, and button presses for all Media Servers.
- Advanced - used for creating and managing one or more Media Server instances; also used to enable VLAN mode and download troubleshooting logs.
- Metrics - displays real-time and historical data about the Media Server Manager including audio channels in use, disk usage, network traffic, average loading and memory usage.

When Media Server instances are created, it is required to specify the IP address of the corresponding MiVoice Business instance. Media Server Manager retrieves and starts the Media Server executable from the MiVoice Business instance, ensuring the versions of the Media Server and MiVoice Business instances remain synchronized.

MIVOICE BUSINESS

MiVoice Business is available on two platforms, Mitel Standard Linux for x86 based processors and VXLinux for Power PC processors used for the ICP 3300.

- For MiVoice Business-ISS, MiVoice Business Virtual and MiVoice Business Multi-Instance platforms, the application typically installs as a blade on Mitel Standard Linux. Mitel Standard Linux Server Manager is used for software installation, upgrading and licensing. Mitel Standard Linux Server Manager is also used for server configuration such as setting the server IP address and local networks and server maintenance activities such as network backups. Once installed, MiVoice Business management is handled by embedded management tools.
- For ICP 3300 platforms, MiVoice Business is pre-installed with a default factory load. Software upgrades are performed by downloading the upgrade to a separate partition and then restarting on the upgraded version. The default factory load includes default parameters for the network configuration such as the IP address. These settings are changed from the factory defaults using the System Administration Tool within Embedded System Management, described below.

The principal component used for managing MiVoice Business is the Embedded System Management (ESM), which consists of three tools adapted for different users, specifically:

- System Administration Tool - for technicians to program the system
- Group Administration Tool - for administrators to make changes to selected system parameters and user and group information
- Desktop Tool - for IP display phone users to program their phones.

The System Administration Tool, Group Administration Tool and Desktop Tool are web-based tools accessed with a web browser; supported browsers include Internet Explorer and Mozilla Firefox.

MiVoice Business includes several other management tools designed for specific applications, such as the Line Measure Tool, IP Phone Analyzer, among others.

As well as the embedded tools, the MiVoice Business provides several capabilities to simplify management and provisioning, including:

- System Data Synchronization – a data sharing technology that allows a network of MiVoice Business to share system and user data
- Integrated Directory Services (IDS) Integration – Lightweight Directory Access Protocol (LDAP) interface to support user provisioning with Microsoft Active Directory.

These tools and capabilities are described in the following sections.

Multiple MiVoice Business may be grouped for management and data sharing; MiVoice Business management groups include:

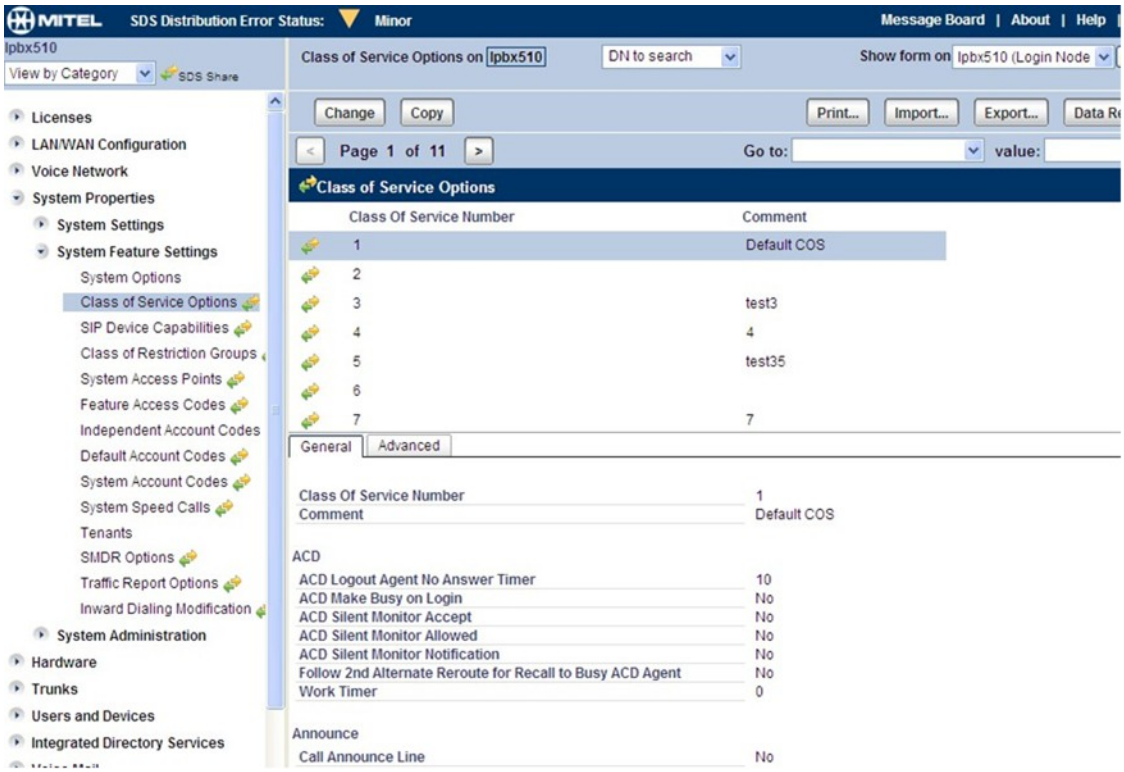
- Network – all MiVoice Business in the data sharing network
- Cluster – up to 999 MiVoice Business, with a uniform numbering plan for extension dialling, common directory, and support for hot desking between nodes
- Administrative Group – a logical grouping of up to 20 MiVoice Business, administered using multi-node management for reach through to remote nodes; administrative groups may be configured independent of clusters
- Resilient Pair – two MiVoice Business, within a single cluster, designated as primary and secondary controllers; multiple resilient pairs are supported within a cluster.

MiVoice Business embedded tools provide sufficient capabilities to manage multi-node networks, typically up to 20 nodes. For Enterprises, Mitel Performance Analytics is recommended for deployments with more than 20 nodes or more complicated distributed solutions. For service providers, Mitel Management Portal provides consolidated management capabilities.

ESM, System Administration Tool

The System Administration Tool is a web-based interface that enables trained technicians and system administrators to program system-wide settings, voice settings (lines, extensions, management parameters, system directories, and voice mail) and IP network features. A sample view is shown below in “MiVoice Business System Administration Tool” on page 151.

Figure 17: MiVoice Business System Administration Tool



Selected tool capabilities include:

- System Options Form – allows configuration of any system option to customize for different network requirements
- User roles and templates – user roles with associated system templates reduce per user provisioning data and simplify bulk data import and automation
- Alarm Banner – shows alarms, license status and SDS status with hyperlinks to the appropriate maintenance window
- Scheduler – automates running system events such as night service, backups, file transfers and IDS synchronization
- Audit Trails – provides a historical record of changes made to the system to assist troubleshooting and security
- Multi-node management – supports reach through from a session on any member element to the System Administration Tool on any remote member element within the same administrative group; allows programming remote elements from a single user interface.

The SAT user interface includes specifically designed forms organized by function. For ease of use, an alarm banner across the top shows the system status, a navigation tree allows ready access to specific forms, and tool tips provide context sensitive feature information within the management window.

For multi-node management, reach through to a remote element is implemented using http re-direct, including pre-authentication with user name and password. For this redirection, the administrator's computer must be authorized to access the remote network. Mitel Standard Linux Server Manager on the remote system may be used to configure remote access permissions.

The MiVoice Business system supports five concurrent sessions of the System Administration Tool or Group Administration Tool or any combination of the two.

ESM, Group Administration Tool

The Group Administration Tool is web-based interface that enables administrators to configure and manage the following basic IP phone settings for group members:

- Basic system parameters
- System phone directory
- Extension and group parameters
- Voice mailboxes
- Group membership (add, edit, or delete users from the system directory)
- Users' personal keys.

For ease of use, the tool is organized based on administrative tasks. Selecting an item provides a customized view with task-specific commands and data entry form. The interface also provides a context sensitive description of the related feature and data fields.

The group administration tool allows configuration of MiVoice Business within an administrative group.

The MiVoice Business system supports five concurrent sessions of the System Administration Tool or Group Administration Tool or any combination of the two.

ESM, Desktop Tool

The Desktop tool is a web-based interface that enables end-users with display IP phones to manage their phone features. The tool allows end-users to:

- Assign features and speed dials to programmable keys
- Manage personal contact lists
- Add and delete Internet bookmarks.

For ease of use, the tool is organized with a searchable list of task-based instructions. Selecting an item from the search results provides both a description of the feature and customized user input screen.

The MiVoice Business system supports ten concurrent Desktop Tool sessions.

For UC solutions, several tools offer similar capabilities for end-user configuration of phone features, including the MiCollab End-User Portal and End-User portal of Mitel Management Portal. Typically the MiVoice Business Desktop tool is used only when these other more

comprehensive tools are not available.

ISDN Maintenance and Administration Tool

The ISDN Maintenance and Administration Tool (IMAT) provides the programming interface for PRI and R2 protocols delivered via a Network Service Unit or Digital Service Unit. Embedded PRI via the Dual T1/E1 Framer is programmed though the ESM, System Administration Tool.

IMAT runs on the Windows O/S and may be installed on a maintenance PC with other management tools.

Line Measure Tool

The Line Measure Tool (LMT) allows technicians to determine the line settings for Loop Start (LS) trunks that are connected to the AX Controller Card Chassis, Analog Main Board, Analog Option Board, or ASU II. The Line Quality test allows technicians to obtain the optimum Balance Network Setting and Trunk Category for each LS trunk, based on the signals received from the CO. These settings are then programmed into the Analog Trunks form of the LS trunk to reduce the possibility of echo and audio level issues between the trunks and IP phones.

The Line Measure Tool is accessed from the ESM, System Administration Tool menu.

IP Phone Analyzer

IP Phone Analyzer collects performance information about the IP devices connected to the MiVoice Business 3300 ICP. It is used to monitor the debug and status information of IP phones.

IP Phone Analyzer runs on the Windows O/S and may be installed on a maintenance PC with other management tools. The maintenance PC must be connected to the network via a Layer 2 switch port on the controller.

System Data Synchronization

The System Data Synchronization (SDS) capability is a data-sharing technology that allows a network of MiVoice Business systems to automatically share system and user data, reducing the time to provision and manage changes for multiple MiVoice Business network elements.

MiVoice Business is programmed using specifically-designed forms in the System Administration Tool. These forms are organized by function; examples of forms include the Network Elements Form, System Options form, and Telephone Directory form. System data can be shared form by form at a sharing scope; examples of sharing scope are All Network Elements, All Cluster Members, Resilient Pair, Admin Group Members and None (no form data is distributed). The sharing scope for each form is pre-set and these default sharing scopes work well for most deployments. The sharing scope may be viewed, and for some forms edited, in the SDS Form Sharing form.

It should be noted that not all form data need or should be shared. For example, form data for physical trunks should not generally be shared as the data applies only to the physical attributes of one MiVoice Business 3300 ICP.

SDS sharing operates in two modes:

- Synchronization - When elements are initially deployed or following major changes, SDS Sync operation is used to synchronize all the data at once. During synchronization, data from the selected forms will be shared with all other network elements in the sharing scope relevant for the change.
- Change Propagation - Whenever a change is made on a shared form on a network element, the change is propagated automatically to all other network elements set up for sharing with this element. SDS change propagation affects only the database records that were changed.

SDS monitors and displays the performance of data sharing, allowing an administrator to resolve any distribution errors and keep the network elements synchronized.

When network controllers are configured for SDS, changes to network data are propagated consistently and accurately across the network, significantly reducing time and management costs, while simplifying network deployment and day-to-day management.

Integrated Directory Services Integration

Integration to Directory Services may be used to reduce data entry required for user provisioning. MiVoice Business provides a flexible solution for integration to Directory Services. MiVoice Business user attributes may be pointed to Microsoft Active Directory (AD) attributes such that integration requires no AD schema changes or snap-ins. Using AD integration combined with user roles and templates, a user can be almost completely configured for MiVoice Business services without manual provisioning on an MiVoice Business system.

Devices and users in the MiVoice Business solution are classified as IDS managed or not. If IDS managed, changes in AD will be replicated in MiVoice Business. IDS synchronization is scheduled through the MiVoice Business SAT scheduler; MiVoice Business will distribute user data changes to clustered nodes with SDS.

MiVoice Business supports LDAP v3 using TLS or SSL. Currently, the supported directory is Microsoft Active Directory. A single MiVoice Business can connect to multiple AD domains within a single AD Forest. For multiple AD Forests, multiple MiVoice Business connection points are required.

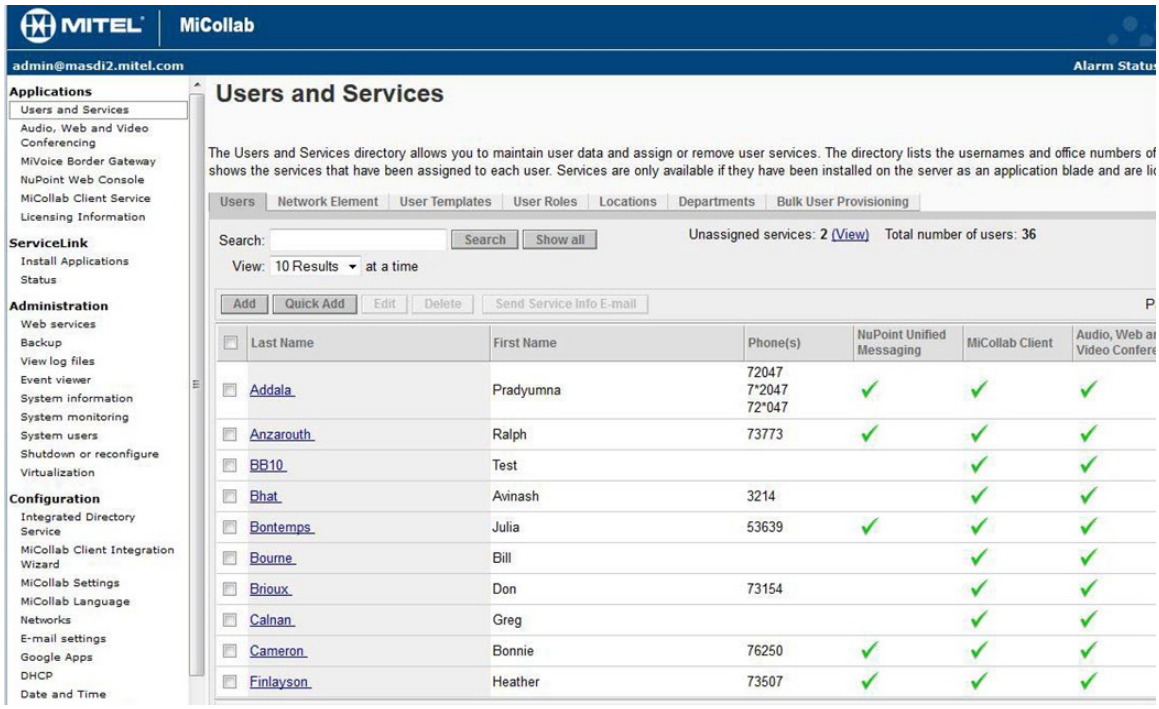
Each MiVoice Business system that is a Microsoft Active Directory connection point requires an MiVoice Business IDS License.

For UC solutions, users and services are typically provisioned via the MiCollab application. MiCollab also supports IDS integration and with Single Point Provisioning enabled, user data is passed through to the MiVoice Business systems. This is described further below.

MICOLLAB

MiCollab offers a web-based administrator portal for managing MiCollab services as well as the embedded applications. MiCollab also adds MiCollab-specific panels to the Mitel Standard Linux Server Manager which may be used for displaying MiCollab information.

Figure 18: MiCollab Administrator Portal, Users and Services Panel



Selected management capabilities include:

- MiCollab Configuration panels – allows managing MiCollab system options such as: welcome e-mails, logs, setting networking information such as E-mail configurations and SNMP support.
- Users and Services panel – provides tabs for managing users, templates, roles, network elements as well as managing bulk provisioning
- MiCollab Unified Messaging Web panel – links to the MiCollab Unified Messaging administrative interface for configuring MiCollab Unified Messaging
- MiCollab Client – allows configuring MiCollab Client server, checking status, managing client software and running diagnostics
- MiCollab Audio, Web, and Video Conferencing – links to the MiCollab Audio, Web, and Video Conferencing administrative page with capabilities to manage the server, such as configure ports and set system options, as well as monitoring and reporting services
- MiVoice Border Gateway – allows configuring supported MiVoice Border Gateway services such as Secure Recording Connector, Teleworker and SIP trunking

For the embedded applications, the application management panels are similar to those offered by the stand-alone applications. The MiCollab administrator portal offers a single user interface for entering configuration and administrative settings for all the applications. Common data elements are shared among the applications, reducing both the need for duplicate entry and the possibility for error.

Within MiCollab, Suite Application Services (SAS) offers several capabilities to facilitate suite management including:

- MiCollab Administrator portal – manages the MiCollab system resource panels within Mitel Standard Linux Server Manager, described above
- User and Services Provisioning (USP) – tool used to provision users and their services
- Single Point Provisioning (SPP) – allows an administrator to provision MiVoice Business through the USP interface
- My Unified Communications portal – end-user facing portal for updating user-configurable information, described below
- Management API – offers management services using a THRIFT interface.

These capabilities are further described in the following sections.

User and Services Provisioning (USP)

The User and Service Provisioning tool provides capabilities to manage users and services provisioned on the embedded applications. It provides a single interface to add, edit, or delete users and their phone and application services on the MiCollab system.

In most cases, the USP tool may be used to manage all MiCollab embedded applications. However, MiCollab Client provides two modes for managing users and services, which include:

- Integrated Mode – in this mode, the MiCollab Users and Services database and MiCollab Client database are synchronized to behave as a single database. This mode supports Single Point Provisioning of MiCollab Client services on the associated MiVoice Business platforms.
- Co-located Mode – in this mode, the MiCollab Users and Services database and MiCollab Client database are maintained as independent databases on the MiCollab server. MiCollab Client services must be provisioned directly with the MiCollab Client interface. This mode is required to support MiCollab Client multi-tenant deployments.

By default, MiCollab Client is in co-located mode. *MiCollab Engineering Guidelines*, available on Mitel-On-Line (MOL) provide details on configuration constraints required for integrated mode. MiCollab Client integration wizard is used to integrate the MiCollab Client application database with the MiCollab USP application database. For upgrades of existing installation, the wizard manages importing users from both MiCollab Client and MiVoice Business databases, and provides instructions for resolving any configuration issues or database conflicts.

For the UC solutions described here, MiCollab Client should be configured for integrated mode, except in the case of the SB topology. The SB topology includes MiCollab Client multi-tenant and so MiCollab Client must remain in co-located mode. For this topology, Mitel Management Portal is used for User and Service provisioning and manages the required interfaces to provision both MiCollab and MiCollab Client.

The USP tool includes several additional capabilities to facilitate provisioning, which include:

- Roles and templates – Roles define the task, position, or responsibilities for a type of user; templates define the common phone and application service settings; users are categorized with roles and roles associated with templates to allow common configuration data to be applied across multiple user entries. This approach greatly reduces the amount of time that it takes to enter user data.
- Bulk User Provisioning – MiCollab supports the import a CSV or LDIF file of user entries including specification of user roles.
- IDS Provisioning – MiCollab may be integrated with a directory server, with a directory service attribute mapped to a MiCollab role. When a user is provisioned in the directory service and synchronized with the MiCollab database, the associated template data is applied to the user entry that is created in the MiCollab database. With IDS integration, user data updates should be implemented in IDS; changes implemented directly in MiCollab are not synchronized with IDS and many fields within the USP form are disabled to prevent data conflicts.
- Service (Welcome) E-mails – MiCollab supports automatically sending an e-mail to new users that contains the user's communications settings, such as: login ID, password, primary e-mail address, phone type, and number.

For Enterprise deployments, MiCollab USP is the primary tool used to provision users and services. For service provider deployments, Mitel Management Portal is the primary tool used by administrators. Mitel Management Portal interfaces the MiCollab USP tool to perform the provisioning.

MiCollab Single Point Provisioning (SPP)

MiCollab Single Point Provisioning (SPP) refers to the embedded capability to push new configuration data, such as phone and mailbox creation, COS option setup, Call Forwarding, and Desktop Monitor setup, from MiCollab to the associated MiVoice Business programming database. These changes will then be synchronized to all relevant MiVoice Business systems in the SDS network.

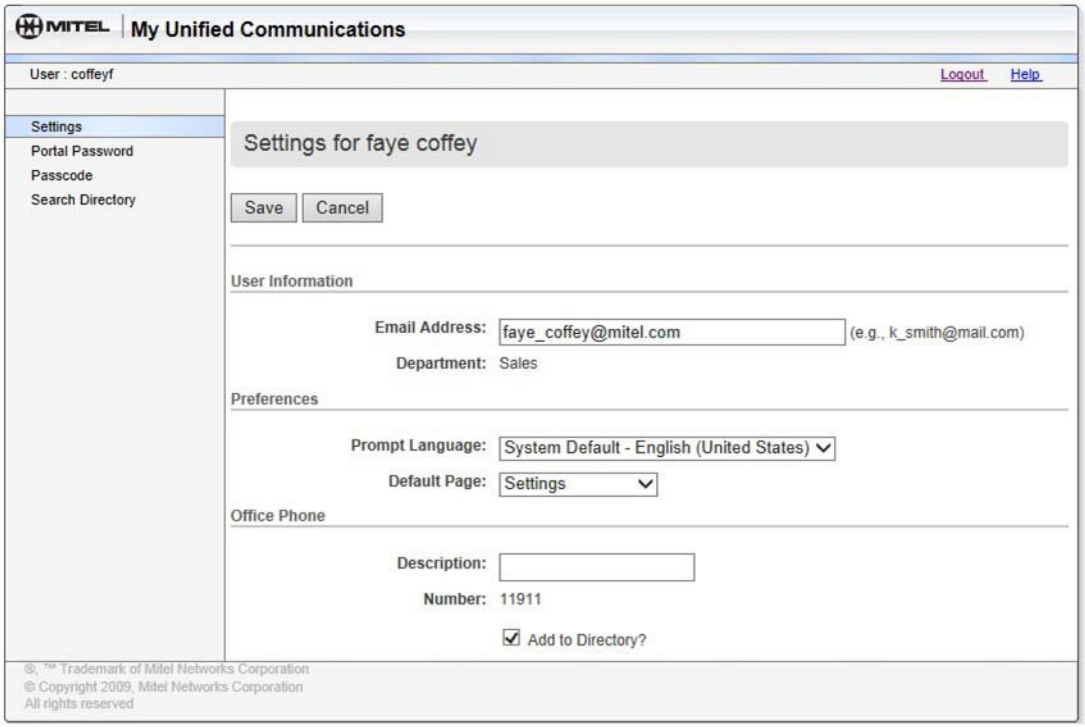
Single Point Provisioning is only supported for MiCollab Client operating in integrated mode with this option enabled. When initializing this mode, MiCollab Client Integration wizard will import existing MiVoice Business user data. However after this initial integration, Single Point Provisioning operates as a one way synchronization from MiCollab to MiVoice Business. Changes directly entered on MiVoice Business systems will not be synchronized with MiCollab.

For service providers, Mitel Management Portal provides similar capabilities for "Single Point Provisioning" and manages updating the related UC system databases.

MiCollab End-User Portal

MiCollab End-User Portal provides a single URL for users to manage their application settings and access application features. The end-user portal is shown in the figure "MiCollab End-User Portal" on page 158.

Figure 19: MiCollab End-User Portal



The end-user portal may be used to update general settings such as e-mail address, login password and language of the telephone user interfaces. The MiCollab Unified Messaging component allows users to access and manage voice, fax and recorded messages. The MiCollab Audio, Web, and Video Conferencing component allows users to schedule and manage conferences. The portal may be accessed from a PC on the corporate LAN or from the Internet through the MiVoice Border Gateway web proxy.

With MiCollab Client in integrated mode with SPP enabled, changes to user phone parameters are automatically updated in the related MiVoice Business database.

Management API

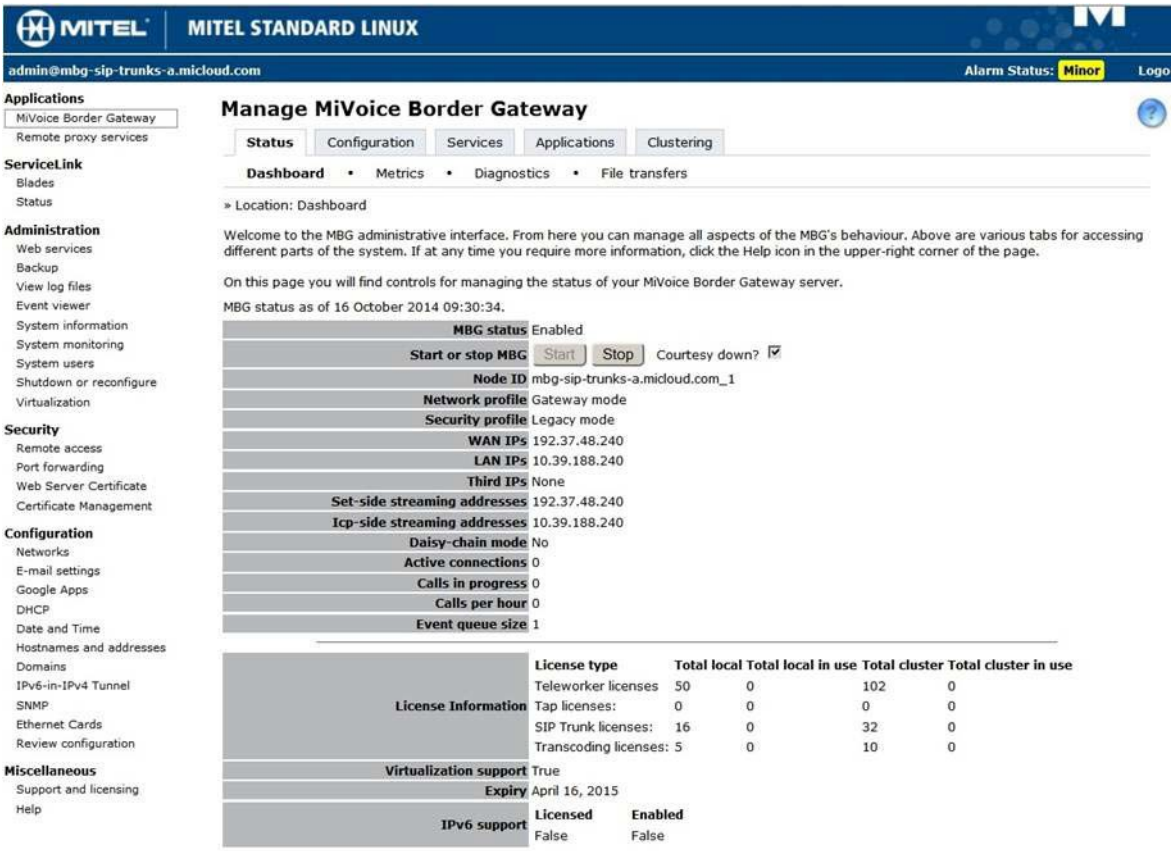
MiCollab offers a management API using the THRIFT protocol. THRIFT is an interface definition language and binary communication protocol used for remote procedure calls. The THRIFT service runs on the MiCollab server and is accessed by THRIFT clients. This API is used by Mitel Management Portal to manage MiCollab provisioning.

In some cases, Mitel Management Portal will also reach directly to the management interfaces offered by the embedded applications. In particular, Mitel Management Portal manages multi-tenanted MiCollab Client applications directly via the MiCollab Client management interface.

MIVOICE BORDER GATEWAY

MiVoice Border Gateway management is based on adding MiVoice Border Gateway-specific panels to the Mitel Standard Linux Server Manager. The MiVoice Border Gateway-specific panel is shown in the figure “MiVoice Border Gateway Panel, Dashboard Tab” on page 159.

Figure 20: MiVoice Border Gateway Panel, Dashboard Tab



Selected MiVoice Border Gateway management capabilities include:

- Dashboard and Metrics – provides system, status and license information and metrics such as calls per hour and active calls; the dashboard also allows enabling and disabling the application
- Configurations – allows editing system parameters, setting the network profile, setting up the interacting nodes and setting alarm thresholds
- Services – allows adding and editing MiNet and SIP devices that connect to the server, configuring SIP trunk details and status of call recording equipment and taps
- Applications – supports configuring MiNet and SIP connections as well as application connections
- Clustering – supports configuring resiliency, load balancing, clusters and zones.

MiVoice Border Gateway supports the Web Services framework. MiVoice Border Gateway provides a Representational state transfer (REST) API that enables management integration

through the provisioning portal of the Mitel Management Portal. This feature is configured in Mitel Standard Linux Server Manager.

MiVoice Border Gateway Remote Proxy Services

MiVoice Border Gateway provides remote proxy services to offer a secure interface between applications on the LAN and remote clients. Several components may be configured to support administrative interfaces.

The web proxy component may be used for secure access to both end-user and administrative interfaces of supported applications, including MiVoice Business, MiCollab, Mitel Open Integration Gateway and generic Mitel Standard Linux. Administrative access may be enabled or disabled; when enabled, administrative access may be restricted to one or more specific network addresses.

The remote management component provides administrative-level access control with password authentication. Currently supported permissions include administrative access to the MiVoice Business and MiCollab management web interfaces. User name and password are required to authenticate access via the MiVoice Border Gateway, in addition to authentication required by the application.

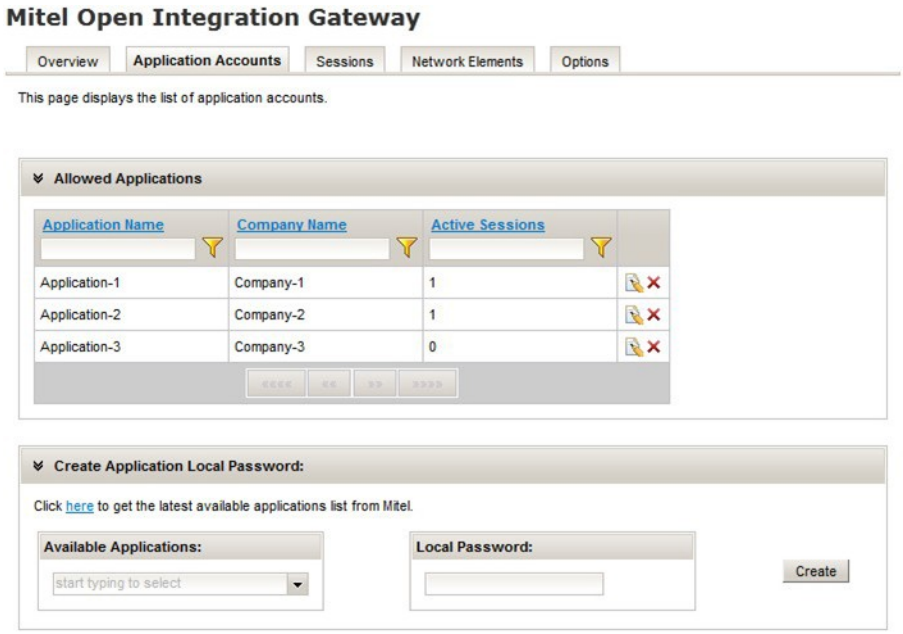
Remote Proxy services also provide a password protected FTP server for MiVoice Business software loads and backup files.

Remote Proxy services are included in the MiVoice Border Gateway base application license; no additional license is required.

MITEL OPEN INTEGRATION GATEWAY

Mitel Open Integration Gateway management is based on adding Mitel Open Integration Gateway-specific panels to the Mitel Standard Linux Server Manager. The Mitel Open Integration Gateway-specific panel is shown in the figure “Open Integration Gateway, Application Accounts Tab” on page 161.

Figure 21: Open Integration Gateway, Application Accounts Tab



The Mitel Open Integration Gateway administrator panel provides the following tabs:

- Overview: Displays current status and licensing information
- Application Accounts: Displays list of application accounts with local passwords
- Sessions: Displays list of current active communication sessions from applications
- Network Elements: Displays a list of connected MiVoice Business
- Options: Displays system options; currently sets logging level, and admin e-mail for log reports.

The only Mitel Open Integration Gateway configuration action is to define a local password for each application that will connect to the Mitel Open Integration Gateway. If the Mitel Open Integration Gateway, connected MiVoice Business and applications are not located on the same subnet, these other networks must be classified as “Local Networks” with appropriate configuration within the Mitel Standard Linux Server Manager.

IP PHONES

All MiVoice 53xx and 69xx IP Phones include embedded management capabilities, accessible via the phone user interface. The management interface allows reviewing and changing network configuration, adjusting phone parameters, and running diagnostic tests.

Typically, phones are assigned addresses using DHCP. DHCP options include configuration information for the related MiVoice Business address, default gateway, and QoS settings. Configuring options in the DHCP server is typically preferred to configuring individual phones.

The phone management capabilities are particularly useful for troubleshooting phone connectivity and audio quality issues.

TOPOLOGY-SPECIFIC CONSIDERATIONS

Managing the UC solution has many similarities across all topologies. Considering a broad brush view of management tasks,

- System configuration – typically undertaken by a system administrator
  - Mitel Standard Linux Server Manager is used to set up networking, server parameters and remote access; also used to manage installs and updates of the application software.
  - Embedded management tools such as MiVoice Business ESM, MiCollab administrator portal, are used to configure the system parameters.
- User and service configuration – undertaken by an enterprise group administrator or service provider administrator
  - For Enterprises, MiCollab USP within MiCollab administrator portal is used to define re-usable roles and templates.
  - For service providers, Mitel Management Portal is used to define service bundles including roles and templates.
- User and service provisioning – typically undertaken by the end-customer administrator
  - For Enterprises, MiCollab USP is used to add, update and delete users; USP bulk provisioning tool or IDS integration may be also be used; MiCollab SPP capability should be enabled to flow through user data changes to the related MiVoice Business cluster.
  - For service providers, Mitel Management Portal customer administrator portal is used to add, update and delete users. Mitel Management Portal also provides capabilities for bulk import. Mitel Management Portal manages updating user data in the related UC systems.
- User administration – typically undertaken by end-users
  - For Enterprises, My Unified Communications portal allows users to manage their settings; SPP and SDS synchronization ensure changes are updated on related MiVoice Business systems.
  - For service providers, End-User portal of Mitel Management Portal allows users to manage their settings; Mitel Management Portal manages updating the related UC systems.
- Technical Support - typically undertaken by technical staff and IT support staff
  - Most embedded management tools include support for alarm monitoring, log viewing and diagnostics.
  - Mitel Performance Analytics and many third-party tools are available for network and server trouble shooting; Mitel Technical Training and/or Mitel Professional Services should be con- sulted for recommendations on third-party diagnostic tools.
- Customer Support - typically undertaken by technical and customer support staff
  - For Enterprises, embedded management tools provide access to system wide, group and user settings.

- For service providers, Administrator portal of Mitel Management Portal allows access to group and user set- tings; embedded management tools are also used to adjust system wide settings.

For Enterprise deployments, additional management tools to be considered include:

- Mitel Configuration Wizard – for facilitating installation, Mitel Configuration Wizard steps through typical configuration tasks with pre-configured defaults.

For service providers, Mitel Management Portal automates much of the provisioning process and allows re-use of configuration parameters across multiple customers. Mitel Management Portal is a required component for UC Enterprise Solution deployments and provides a similar consolidated view of the network and systems.

For all topologies, Mitel Performance Analytics is recommended for improved fault and performance management. Smaller enterprises may prefer to take advantage of Mitel's managed service, Remote Monitoring and Access Service. Larger enterprises and service providers would typically choose the on premise solution, Mitel Performance Analytics.

Further details on management capabilities are available in the solution deployment guides, product-specific installation and maintenance guides, and online help systems.

INSTALLATION SUMMARY

This section provides a high level summary of how the various management tools are used during deployment.

Note: Technicians and system administrators are referred to the specific topology deployment guides and product-specific installation and maintenance guides for detailed instructions to successfully deploy the different Solution topologies.

The major steps for deploying a UC solution include:

- Identify the network and system requirements; define the topology; determine the required systems; design the required networking in terms of IP addressing and sub networks.
- Purchase the required licenses and set up the system within AMC with the appropriate G-ARIDs and ARIDS.
- Deploy the servers or virtual machines; install Mitel Standard Linux and set up IP networking, such as: defining local networks, setting up DNS, DHCP, etc.
- Deploy management applications:
  - For service providers, install and configure Mitel Management Portal; create UC service bundles.
- Install the applications and perform initial configuration for clustering:
  - Install MiCollab; cluster the internal MiCollab-MiVoice Border Gateway with any external MiVoice Border Gateways.

- Install any external MiVoice Border Gateways and set up MiVoice Border Gateway clusters.
- Install MiVoice Business and set up SDS networking; configure MiVoice Business trunking.

- Perform initial provisioning
  - For service providers, configure Mitel Management Portal for customer management
    - Register the deployed systems, MiVoice Business, MiCollab, etc., with Mitel Management Portal.
    - Create and configure customer accounts; assign service bundles.
    - Use Mitel Management Portal to configure users and services.
  - For enterprises,
    - Run MiCW to perform initial system configuration; MiCW includes capability to apply a default database
    - Use MiCollab USP application to define user roles, create device and service templates, and associate templates with roles.
    - Use MiCollab USP application to complete end-user provisioning.
    - Use embedded management tools to complete any remaining system, user and service provisioning.

For the enterprise, MiCW and the MiCollab USP application are used to facilitate installation and provisioning. For service providers, Mitel Management Portal provides re-usable templates and processes for efficiently deploying many customer instances.

Chapter 9

NETWORK AND NETWORKING CONSIDERATIONS

NETWORK AND NETWORKING CONSIDERATIONS

This chapter addresses a number of networking requirements that need to be taken into consideration prior to deploying a UC solution. The networking requirements discussed here are relevant to service providers providing hosted solutions, data centre operators, and also to those that are responsible for the installation and operation of any equipment located on customer premises.

Note: The subject matter discussed in this chapter is covered in greater detail within the *MiVoice Business Engineering Guidelines*.

QOS, NETWORK ASSESSMENT AND END-POINT CONFIGURATION

This section covers network Quality of Service (QoS), network assessment for supporting voice and video, and end point configuration to support QoS.

QOS OVERVIEW

Network congestion due to high traffic levels can slow the speed with which packets are transmitted and cause the reception of the packets to be delayed. As network congestion increases, network switches and routers will often be forced to discard packets rather than forwarding the packets to the recipient. Packets are discarded when the network equipment cannot receive, process and forward the incoming packets quickly enough, in some cases packets may be discarded if they have been marked as low priority packets and processing precedence is being given to higher priority packets.

When packets belonging to a real time voice or video stream are discarded by a switch or router, the audio quality or video quality experienced by the receiving end will be negatively affected. When packets are discarded, a telephone call may break up to such a degree that the conversation becomes unintelligible and participants in a video conference may receive an image stream that is delayed and possibly heavily pixilated.

L2 and L3 QoS mechanisms are used to mark transmitted packets with a priority level. The priority level, or QoS setting, is used by network switches and routers to give packets with a higher QoS setting precedence over packets with a lower QoS setting or no QoS setting.

Network priority, or QoS settings, are required to ensure the timely delivery of packets carrying data for real time voice and real time video over LANs and WANs. Usage of the correct QoS settings on end-points, switches and routers will help to ensure that users receive high quality voice and video services.

NETWORK ASSESSMENT

An assessment of the LAN should be conducted prior to installation of VoIP or IP video equipment. It is essential to assess, and if necessary configure the network to maintain good voice quality, video quality, and product functionality for the user.

Depending on the results of the network assessment, the existing network may need to be modified, or equipment with QoS capabilities may need to be installed.

The network should be re-assessed if there have been any major changes to the network design or if there has been a significant increase in the number of users.

The main network issues affecting voice and video quality are:

- delay
- jitter
- packet loss

Use the network limits shown in the following table to evaluate the results from a network assessment. For ideal voice and video packet transmission the LAN or WAN should comply with the values shown in the 'Go!' row.

Table 16: Network Limits

STATUS	PACKET LOSS	JITTER	END-TO-END DELAY	PING DELAY
GO!	<0.5%	<20ms	<50ms	<100ms
Caution	<2%	<60ms	<80ms	<160ms
STOP!	>2%	>60ms	>80ms	>160ms

Additional information on network assessment for ensuring voice and video quality can be found in:

- *MiVoice Business Conference Phone/Video Phone Engineering Guidelines*
- *MiVoice Business Troubleshooting Guide*
- *MiVoice Business Voice Quality Troubleshooting Guide*

L2 AND L3 PRIORITY MECHANISMS

There are two areas where priority mechanisms can operate in the network to ensure that specific types of traffic will be treated with higher priority than other types of traffic:

- Layer 2 in the LAN through use of VLANs and packet tagging
- Layer 3 at network routers and for WAN connections using Differentiated Services Code Point (DSCP) values

The following table shows the recommended L2 and L3 QoS settings for various traffic or service classes.

Table 17: Mitel Recommended Network QoS Settings

SERVICE CLASS	RECOMMENDED L2 VALUE	RECOMMENDED L3 VALUE
Telephony (voice)	6	46 (EF)
Signaling	3	24 (CS3)
Multimedia conferencing	4	34 (AF41)
Real-time interactive	4	32 (CS4)

Table 17: Mitel Recommended Network QoS Settings

SERVICE CLASS	RECOMMENDED L2 VALUE	RECOMMENDED L3 VALUE
Standard	0	0 (DF) (BE)

For additional information related to:

- QoS settings for a particular application, end point or product: refer to the appropriate product documentation found on Mitel-On-Line (MOL).
- Troubleshooting voice quality, video quality and network QoS issues: refer to the *MiVoice Business Voice Quality Troubleshooting Guide*, found on Mitel-On-Line (MOL).
- Network QoS settings for third-party networking gear: refer to the manufacturer's documentation.

OBTAINING NETWORK PARAMETERS

Installing IP phones requires programming each phone's networking parameters, including QoS settings.

Mitel IP phones, consoles, and conference units have a number of different methods that they can use to obtain networking parameters such as VLAN and QoS information. Each network parameter source is assigned a priority level. An IP phone seeking network parameters starts with the priority level five method. which has the highest priority, If all of the necessary parameters are not available from this source, the phone uses each decreasing priority level until all the required parameters are found.

Table “Networking Parameters and Priority Level” on page 169 lists the various sources of networking parameters and the priority level.

Table 18: Networking Parameters and Priority Level

SOURCE OF NETWORK PARAMETERS	PRIORITY LEVEL	NOTES
Manual entry (static)	5	Network parameters may be manually programmed by an installer via the Set’s UI
LLDP-MED	4	The IP phone's network parameters are obtained from an LLDP-MED compliant L2 switch
CDP	3	CDP can provide VLAN information to the IP phone and QoS values that are compliant with Cisco equipment can be inferred by the IP phone based on the fact that Cisco gear is present on the LAN
DHCP	2	A DHCP server can provide the IP phone with network parameters
Factory default values	1	The IP phone contains factory default networking parameters

Teleworker Phones - Obtaining a Call Server IP Address

When an IP phone is first powered on in teleworker mode it will attempt to find the IP address of the call server, in the case of a teleworker phone the call server is a MiVoice Border Gateway.

The teleworker phone has three different sources that it can use to obtain the call server IP address, these sources in descending order of precedence are:

- 3: Manual (static) programming (via the IP phone's UI)
- 2: DHCP server
- 1: Mitel Redirection and Configuration Service server

Use of the Mitel Redirection and Configuration Service server is discussed in further detail in “Mitel Redirection and Configuration Service” on page 142.

WI-FI NETWORKS

When Wi-Fi networks are being used to provide connectivity to IP phones and/or IP video devices, the wireless network will need to be carefully evaluated to ensure that it can support good audio and video quality.

The QoS standard for Wi-Fi networks is called WMM (Wi-Fi Multimedia).

Along with geographical coverage and bandwidth considerations the Wi-Fi network evaluation also needs to ensure that WMM is employed and that the WMM setting are correctly mapped to L2 or L3 QoS settings. The following table shows the recommended mapping of values.

Table 19: L2, L3, and WMM QOS Mappings

SERVICE CLASS	L2 PRIORITY	L3 PRIORITY	WMM ACCESS CATEGORY	WMM CATEGORY
Telephony (voice)	6	46	AC_VO	Voice
Signaling	3	24	AC_BE	Best effort
Multimedia conferencing	4	34	AC_VI	Video
Standard	0	0	AC_BK	Background

For additional information refer to the Wi-Fi access point product documentation.

WIDE AREA NETWORKS - QOS AND SLAS

The UC solution uses Wide Area Network connections to:

- Connect remote office networks to the headquarters network
- Connect end-user IP devices located on the customer's premises, to a private cloud or data centre
- Connect end-user IP devices located on the customer's premises to a Hosted service provider

To ensure good voice and video quality, L3 QoS (DSCP) must be employed, and a Service Level Agreement (SLA) should be in place to ensure that the QoS requirements are honored by the WAN provider.

In some situations there might be more than one network provider involved in establishing an end-to-end WAN connection between two particular locations. To ensure that QoS markings are honored end-to end across a WAN connection, it is imperative that the SLAs with all of the network providers involved be correctly defined and use the same definitions, and that all BGP routers be configured according to the SLAs.

Sites requiring a high level of availability require both a primary and a secondary WAN link to provide a level of connection resiliency.

- For some customers the same level of service will be required on both of the WAN links. If this is the case, then both the primary and secondary links need to have similar characteristics and the same SLA must be in place for both connections.
- Customers not requiring the same level of service on both of the WAN links may be willing to accept a lower level of service in return for a cost savings by using a lower grade link as the secondary connection. In this situation, the customer may use an MPLS connection with an appropriate SLA as their primary WAN link and the secondary link could be made over the public Internet where an SLA may or may not be available.

For VoIP engineering guidelines information, refer to the *MiVoice Business Engineering Guidelines*.

For information related to video conferencing over a WAN, refer to the *MiVoice Business Conference Phone/Video Phone Engineering Guidelines*.

NETWORK INFRASTRUCTURE FOR IP PHONES

IP phones require basic networking infrastructure so that they may obtain firmware loads and networking parameters. Additional networking infrastructure is required to provide connectivity between the phones and the MiVoice Business. In some cases network infrastructure may also be used to provide power to the phones over the LAN cabling.

The following sections discuss the components that form the network infrastructure.

It is necessary to consider where the network infrastructure is physically located. For instance, some components, such as TFTP and DHCP servers, may be physically located on the customer premises or they may be located off site in a cloud or data center.

When deciding where to locate the TFTP and DHCP servers consider if there are requirements for local survivability. For example, if the WAN link is down and the servers are located off site, then the phones will not be able to communicate with the TFTP and DHCP servers.

TFTP SERVER

MiVoice Business has an integral TFTP server which may be used to provide IP phones that are located on the same LAN with their application software. External TFTP servers may also be used, but to ensure that the phone software is at the correct revision for a given version of MiVoice Business software it is recommended that the MiVoice Business integral TFTP server be used.

When remote or Teleworker phones are part of the UC solution, the MiVoice Border Gateway, which will have a copy of the current phone application software, will provide the Teleworker phones with their application software. If the phone application software held by the MiVoice Border Gateway is out of date, the MiVoice Border Gateway will obtain the latest phone software load from MiVoice Business.

For more information, refer to the MiVoice Business product documentation, the *MiVoice Business Engineering Guidelines* and the *MiVoice Border Gateway Engineering Guidelines*.

DHCP SERVER

DHCP is one of the methods IP phones can use to obtain their networking parameters such as: IP addresses, L2 priority settings, L3 priority settings, and VLAN information.

The following MiVoice Business products support integral DHCP servers.

- MiVoice Business on a 3300 ICP platform
- MiVoice Business Multi-Instance (See Note)
- MiVoice Business for Industry Standard Servers (ISS)(MSL-based DHCP server)
- MiVoice Business Virtual (MSL-based DHCP server)

Note: When MiVoice Business Multi-Instance is used in hosted site deployments that support multiple customers, the integral DHCP server should not be used because a single DHCP server cannot be shared amongst multiple customers. Such a deployment will need to use multiple third-party DHCP servers.

For more information, refer to MiVoice Business product documentation and the MiVoice Business System Administration Help.

L2 AND L3 NETWORKING EQUIPMENT

To ensure good voice and video quality, L2 and L3 networking equipment must support QoS mechanisms, and the switches and routers should be configured as per the recommendations shown in the Network Assessment section.

To increase system availability, L2 and L3 redundancy and resiliency mechanisms, and networking protocols should be employed.

Some specific examples of redundancy mechanisms that can be used in network design are:

- Usage of fully redundant L2 and L3 networking equipment
- Duplication of L2 switches and L3 networking devices
- Duplication of stored data, i.e. duplication of DHCP servers
- Duplication of storage devices, e.g. SAN, NAS, and RAID
- Duplication of transmission paths via partial mesh networking to support redundant communication paths
- Resilient topologies, i.e. hierarchical network design

- Networking protocols, for example Spanning Tree, Open Shortest Path First, VRRP, or Cisco HSRP

The *MiVoice Business Resiliency Engineering Guidelines* discuss network design for resiliency and L2 and L3 resiliency/redundancy protocols.

The *MiVoice Business Engineering Guidelines* discusses network design practices for network maintainability and scalability.

The Mitel white paper called Network Design for Availability provides a detailed discussion on network design practices for achieving higher availability.

Configuration information for specific models of switches and routers will be covered in the product vendor's documentation.

Mitel's portfolio of IP phones are LLDP-MED compliant. If LLDP-MED compliant L2 switches are deployed the IP phones will be able to take advantage of the LLDP-MED protocol for obtaining networking parameters. LLDP-MED is also useful or providing phone physical location information for E911 purposes.

POWER CONSIDERATIONS

Consider the entire voice path from one device to another when distributing power. Consider especially which devices need to maintain power during a general power outage. End devices, such as phones, and the underlying network infrastructure will continue to need power f phone service is to be maintained.

Networking infrastructure will require UPS systems so that power can be maintained. Refer to the manufacturer's data sheets for each product's power requirements.

L2 switches that support PoE and are compliant with IEEE 802.2af and/or IEEE 802.2at should be considered for use as access layer switches to provide connectivity and power over ethernet cabling to the IP phones.

PoE L2 switches allow the IP phones to be powered and managed from a common location. Additionally, a UPS system can be co-located with the L2 PoE switches so that L2 switch power and IP phone power can be maintained from a centralized location during a mains power outage.

Additional information can be found in the *MiVoice Business Engineering Guidelines* and the L2 switch and router product documentation.

CABLING INFRASTRUCTURE

LAN cabling should at a minimum be Category 5 compliant end-to-end. For information on LAN cabling refer to the *MiVoice Business Engineering Guidelines*.

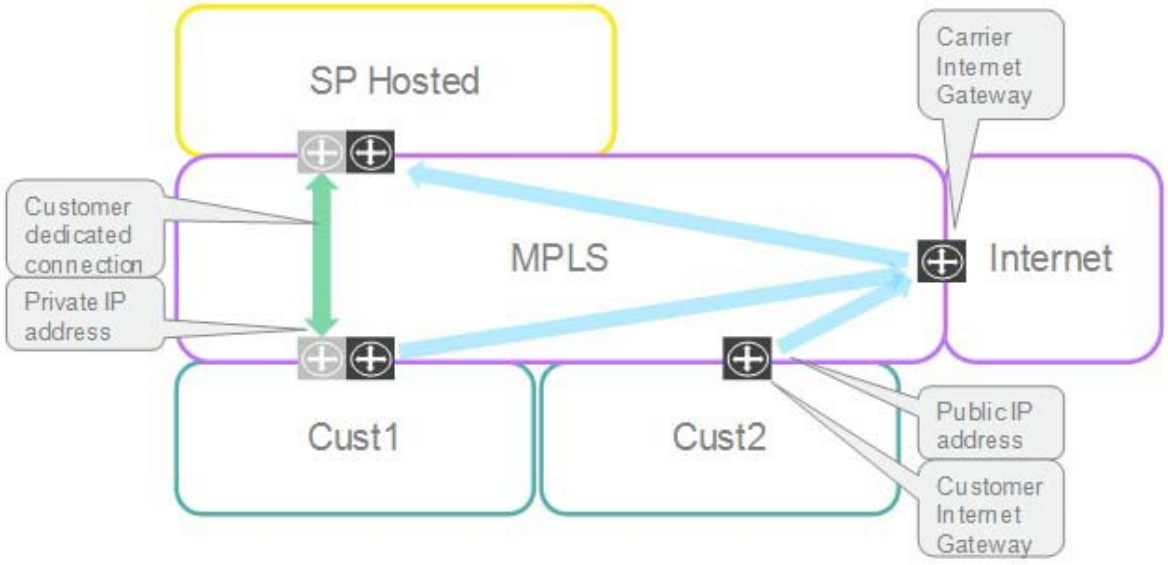
For installations where the LAN cabling is Category 3 and there are circumstances that prevent the customer from upgrading the wiring plant, the StreamLine L2 switch can provide both power and connectivity to the IP phones. For additional information refer to product documentation on Mitel-On-Line (MOL).

PUBLIC NETWORK VS. MPLS

The question is less about Public Network versus MPLS, but rather how a carrier uses MPLS to provide a network infrastructure that is both publicly-accessible while providing private connections for customers when required.

There are a number of ways that an MPLS network can be deployed, whether for private use only, for public use, or a mix of these requirements. “Network with Public and MPLS Connections” on page 174 highlights a typical configuration that deploys both private and public connections:

Figure 22: Network with Public and MPLS Connections



For a public MPLS connection, each of the end-customers and any service providers have a router that has access to a unique public IP address. The IP addresses are provided by the carrier. Typically the carrier then directs any public IP traffic to the carrier’s Internet gateway. Connections to public IP addresses within the carrier network are internally routed. Other public IP addresses are routed externally. The advantage for the hosted service provider is that the public IP address can be reached from any network globally. Service Level Agreements can be applied to end-customers and service providers that share a common carrier/MPLS provider. One disadvantage is that all traffic must go through the common carrier Internet gateway. The carrier may be able to overcome this disadvantage by providing public routing within the network, but this also incurs management overhead of the end devices and programming of routes, which the carrier may be less willing to do on a public connection.

For a private MPLS connection, the end-customer and hosted service provider share the same carrier network. The carrier network may use public IP addresses that are restricted from going out the carrier Internet gateway by the router's access control list, or may opt to use private IP addresses that are not Internet routable. The routers at the customer and service provider are provisioned with dedicated routing rules and connections. In effect the two end connections and networks are provided with a transparent tunnel across the MPLS network. Advantages

include security and also the ability to provision Service Level Agreements with dedicated bandwidths, which may not be available via the carrier's Internet gateway.

MPLS carriers that wish to remain totally private simply have no Internet Gateway provisioned. All connections therefore are private within the carrier space, and each connection has to be uniquely provisioned.

MITEL MANAGEMENT PORTAL ACCESS TO CUSTOMER SITES - USING SPLIT DNS AND NAT

Figure "Split DNS and NAT" on page 177 shows the service provider's network, the end-customer's network and the NAT router that allows the two separate networks to communicate with each other.

The service provider's network uses private IP addresses in the 10.0.100.0/24 range, and the end-customer's LAN uses private IP addresses in the 192.0.101.0/24 range.

The Mitel Management Portal Application resides in the service provider's network and needs to be able communicate with the applications that reside in the end-customer's LAN.

Since the service provider's LAN and the end-customer's LAN are using different IP address ranges, and Mitel Management Portal does not know the IP addressing schema within the end-customer's LAN, a 1:1 NAT router is needed to connect from the SP network into the customer network. Use of FQDN to identify the customer hosts, along with split DNS is also a requirement. Split DNS will allow Mitel Management Portal to identify the management portal on the router, and allow the customer hosts to communicate with each other in the customer network.

During the initial network configuration, IP addressing relationships need to be established. Using figure "Split DNS and NAT" on page 177 as an example, the service provider and end-customer DNS machines would be programmed with the values in the table "Service Provider and End-Customer DNS Entries" on page 175 and the NAT Router would be programmed with the IP address mappings in the table "NAT Router Configuration" on page 176.

Table 20: Service Provider and End-Customer DNS Entries

DNS CONFIGURATION	FQDN	IP ADDRESS
Service provider	Customer_1_MiCollab	10.0.100.2
	Customer_1_MiVoice_Business_A	10.0.100.3
	Customer_1_MiVoice_Business_B	10.0.100.4
	Customer_1_MiVoice_Border_Gateway	10.0.100.5
End-customer	Customer_1_MiCollab	192.0.101.20
	Customer_1_MiVoice_Business_A	192.0.101.30
	Customer_1_MiVoice_Business_B	192.0.101.40
	Customer_1_MiVoice_Border_Gateway	192.0.101.50

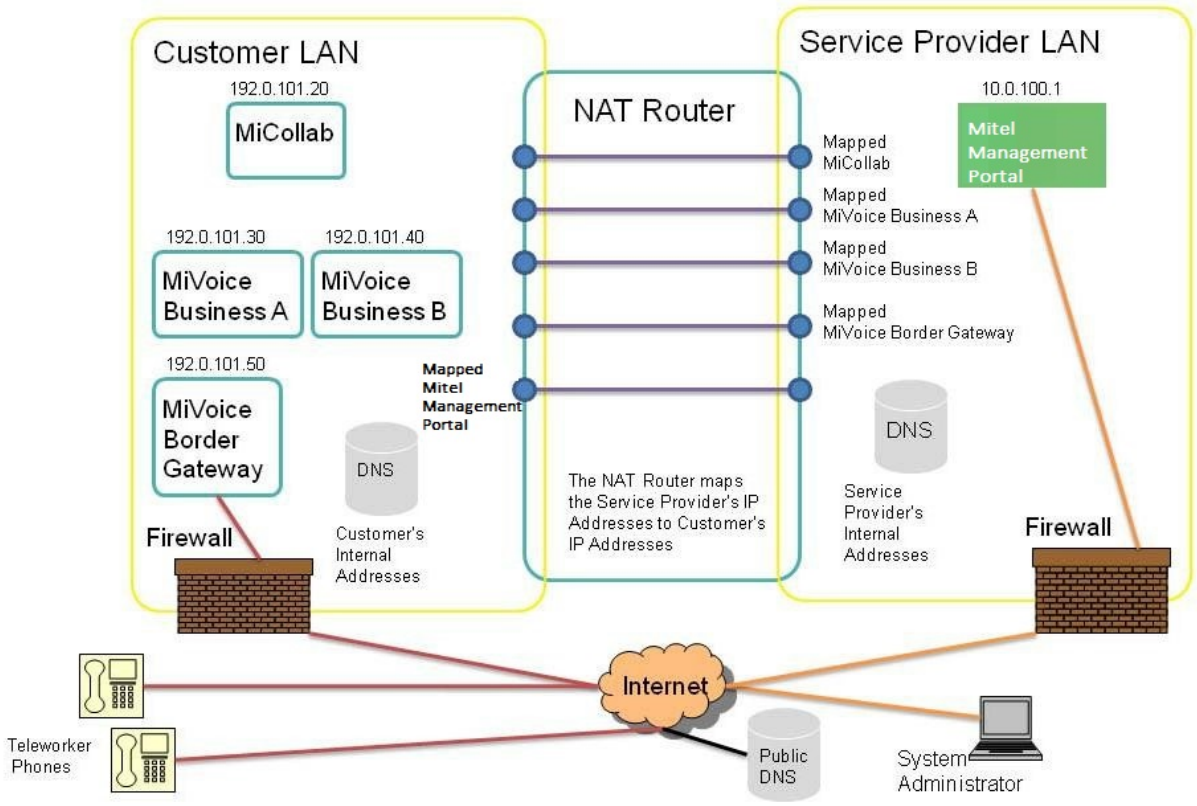
Table 21: NAT Router Configuration

END-CUSTOMER IP ADDRESS	SERVICE PROVIDER IP ADDRESS
192.0.101.20	10.0.100.2
192.0.101.30	10.0.100.3
192.0.101.40	10.0.100.4
192.0.101.50	10.0.100.5

While referring to Figure “Split DNS and NAT” on page 177, the following describes how Mitel Management Portal and the Applications that are in the Customer's network communicate with each other.

- Mitel Management Portal uses an FQDN (or Hostname) to address the customer's MiCollab, the FQDN for the Customer's MiCollab will be Customer_1_MiCollab.
- The DNS server in the service provider space will resolve the FQDN (Customer_1_MiCollab) to an IP address, the IP address provided by the service provider DNS will be, 10.0.100.2.
- The IP address 10.0.100.2 is mapped to a port on the service provider's side of the NAT Router, the NAT router will translate or remap this port to the address 192.0.101.20, which is the IP address of the Customer's MiCollab within the Customer LAN.
- Once a communication path has been established between Mitel Management Portal and the Customer's Mi- Collab, Mitel Management Portal will send messages to MiCollab that contain FQDNs for the primary MiVoice Business, the secondary MiVoice Business and the MiVoice Border Gateway.
- The Customer's DNS will resolve the various FQDNs to the actual IP addresses for the primary MiVoice Business, the secondary MiVoice Business and the MiVoice Border Gateway.
- Mitel Management Portal may also communicate with the Customer's application directly by using the ports on the service provider's side of that NAT router that the Customer's applications are mapped to.
- Applications residing in the customer LAN communicate with Mitel Management Portal by addressing the port on the NAT Router that is mapped to IP address of Mitel Management Portal. The NAT Router will translate this port to the IP address of Mitel Management Portal, which is IP address 10.0.100.1.
- Teleworker phones will have been programmed to seek out a host with the FQDN Customer_1_MiVoice_Border_Gateway_Public. The Public DNS will resolve the FQDN Customer_1_MiVoice_Border_Gateway_Public to the Public IP address that is used to address the Customer's MiVoice Border Gateway.
- The System Administrator's computer will have been programmed to seek out a host with the FQDN Service_Provider_1_ Mitel Management Portal _Portal. The Public DNS will resolve this FQDN to the Public IP address that is used to address the Mitel Management Portal Application.

Figure 23: Split DNS and NAT



BANDWIDTH CONSIDERATIONS

Even when QoS mechanisms are employed in the network so that video and voice packets are handled with the requested priority by L2 switches and routers, it does not alleviate the requirement to verify that there is sufficient network bandwidth to carry all of the expected traffic.

QoS mechanisms are designed to ensure specific classes of traffic receive consistent treatment from networking equipment, but with insufficient bandwidth, QoS cannot guarantee performance for the high priority traffic such as video, nor does QoS ensure that low priority traffic will not be completely blocked by higher priority traffic such as video.

If a network interface does not provide enough bandwidth, or a network router is unable to process the volume of packets it is receiving fast enough, then the packets will be at risk of being corrupted, delayed or completely lost, regardless of the QoS setting applied to the packets.

BANDWIDTH CONSUMPTION

Before determining the bandwidth requirements for a particular communication link, it is important to consider the traffic flow and where devices are located relative to their controllers. The use of compression zones and IP networking may also have a bearing on traffic flow in parts of the network.

To determine what the total bandwidth consumption will be for a particular link, the following must be accounted for:

- Call traffic patterns
- Number of voice calls and whether or not they will compressed
- Number of video calls and which CODEC will be used
- Number of video conferences and which CODEC will be used
- Data traffic, regular business traffic and traffic patterns
- Maintenance traffic, file backup processes and when they run

Information on how to calculate voice media bandwidth, the effect on bandwidth when using different CODECs and IP trunking are discussed in the *MiVoice Business Engineering Guidelines*.

Bandwidth consumption for video conferences using the MiVoice Video Unit is covered in that product's engineering guidelines. For information on the bandwidth required for MiCollab, see the *MiCollab Engineering Guidelines*.

The bandwidth required for third-party applications should be covered in the vendor's documentation. If bandwidth utilization information is not available, network monitoring tools can be used to determine total bandwidth and peak bandwidth requirements, network monitors can be run over a period of time to determine patterns.

Another option for determining bandwidth utilization could be through the use of tools embedded in networking gear. Many routers provide embedded tools that can be used for measuring bandwidth consumption.

COMPRESSION ZONES AND BANDWIDTH MANAGEMENT

CODECs are devices or programs that encode or decode a signal into a digital format, the payload might be voice, video or Fax data. Different CODECs can provide different sized payloads given the same input information. A reduction in payload is often referred to as compression.

IP phone calls that typically require compression are those where the call traverses an IP trunk or a WAN connection with limited bandwidth. Compression zones are used to define where compression will be used, the decision on whether or not to use compression for a call will be based on how compression zones have been configured on MiVoice Business and the zone with which a particular phone is associated.

Establishing compression zones defines where compression will be used for a voice call, but there is nothing limiting the number of calls that can be placed across a connection. In fact, it is possible to oversubscribe a link by placing too many calls across the link. There is a potential for all calls on the link to suffer transmission impairments when a link is oversubscribed.

To monitor the communication links' usage and determine if a call should proceed or not proceed across the communication link based on whether or not the link has reached its maximum capacity requires the use of bandwidth management and Call Admission Control.

The terms “Bandwidth Management” and “Call Admission Control” are often used interchangeably to describe the management, and potential re-routing, of calls across an IP network between end devices. In reality these are two separate concepts. Bandwidth management gathers information about the availability and use of bandwidth on particular connections and links. Call Admission Control uses this information to decide whether a call should be completed or not.

Although the IP network is often considered as a “cloud,” it is actually made up of many parts, including LANs, MANs and WANs. There are constraints on the amounts of data that can be handled at the transitions between the different networks, and often within the networks themselves.

If a link is bandwidth limited, it is desirable to be able to determine the available bandwidth across the link and manage it to ensure that it is available for voice use. Once the bandwidth is known, it is possible to determine how many virtual channels can be established and to admit, redirect or reject calls based on current available resources, that is, bandwidth. The latter is the task of Call Admission Control between end nodes.

The *MiVoice Business Engineering Guidelines* and the MiVoice Business System Administration Help files provide detailed information on establishing compression zones and how to use Bandwidth Management to prevent oversubscription on a connection.

Chapter 10

LICENSING CONSIDERATIONS

LICENSING CONSIDERATIONS

The following section provides an overview of licensing for UCC deployments with Public Cloud, Private Cloud and Enterprise solutions. This section provides an overview of UCC deployments using the UCC v3 licensing constructs within AMC. Further details of the v3 licensing can also be found in the *MiCloud Business Solution for Service Providers Licensing Guide*. The guide can be obtained from your local Mitel sales representative.

This section will include information with respect to:

- “Licensing Terms and Descriptions” on page 183
- “CAPEX and OPEX Licensing Models” on page 184 (Capital Expenditure or Capital Purchase / Operational Expenditure or subscription-based)
- “End-User UCC Licensing Profiles” on page 185
- “Overview of AMC and How UCC Licenses are Organized” on page 188
- “Sample Configurations and Descriptions for Different Topologies” on page 191

LICENSING TERMS AND DESCRIPTIONS

The table “License Terms” on page 183 describes some of the licensing terms and descriptions that are used in this section and also when deploying and configuring licenses within the solution:

Table 22: License Terms

LICENSE TERM	DESCRIPTION
Device	This is a specific end device, or phone, that the user will use. For example this could be a dedicated desk phone, or a PC softphone, or a mobile client, or simply a contact-able number such as a home phone. Devices are associated with user licenses.
User	End-User of UC and phone equipment. A User may be assigned multiple phone devices to provide wider UC access. A UC user has a single prime contact number, typically associated with multiple devices. A non-UC user is typically associated with a single device.
AMC	Application Management Centre: This is the on-line license centre where product licenses are obtained and held within Application Records at the AMC data centre. These records are then accessed remotely by applications to determine the user operations and features that are allowed.
ARID	Application Record Identification (ARID): This is a record identifier that allows Mitel Applications and products to obtain licenses from the AMC and refers to a unique product instance deployed in the field.
MDUG	Multi-Device User Group (MDUG): This is a grouping of devices that can be made to ring when the user is contacted. The MDUG used the single MDUL floating license across all devices. Once one device in the group is busy, all devices are marked busy. A second incoming call will revert to Voice Mail, if available, rather than ringing other group phones. Up to eight members are allowed in a group. Some deployments may restrict to less.

Table 22: License Terms

LICENSE TERM	DESCRIPTION
DLM	Designated License Manager (DLM): This is a single MiVoice Business that is identified as the recipient of the license information identified by the GARID. This is an additional ARID that is assigned to this designated MiVoice Business. This unit then shares licenses and license bundles with other MiVoice Business within the same cluster. The DLM requires a Group Application Record ID (GARID) with Enterprise License Sharing enabled.
GARID	Group Application Record Identification (GARID): This allows a number of ARIDs to be grouped together under a common Group ID where the product instances are clustered and can share data. In the case of an MiVoice Business cluster, one MiVoice Business is designated as the DLM and assigned the GARID number. It will then share data with other MiVoice Business in the cluster. A MiVoice Business Express cannot be a DLM. A GARID is also applied to a ULM, but is a construct number, rather than a product assignable number.
IPT	IP Telephony: IP phone service without attached applications or UC support.
MDUL	Multi-Device User License (MDUL): This is the floating license which is used to activate a Multi-Device User Group (MDUG) within Call Control.
SWAS	Software Assurance and Support (SWAS): This license allows access to the technical support teams, access to documentation as well as downloads of latest software releases and patches. Two levels of support are provided, Standard and Premium.
UC	Unified Communications (UC): This is a general term used to identify a combination of communication technologies used by users to reach each other. It includes real time communication including Chat, Presence, Telephony, Video and Speech Recognition as well messaging services such as: Voice Mail, E-mail, SMS, etc.
UCC	Unified Communications and Collaboration (UCC): This is UC with increased emphasis on collaboration tools, including whiteboard and file sharing, as well as integration with 3rd party products such as social media, Google and Salesforce.
ULM	UCC License Manager (ULM): This is a grouping of applications and products that work together to provide the end-user with a UC experience. The ULM simplifies the licensing of many parts with a single blanket number for a number of underlying services. Rules around use and content of a ULM are covered in later sections.

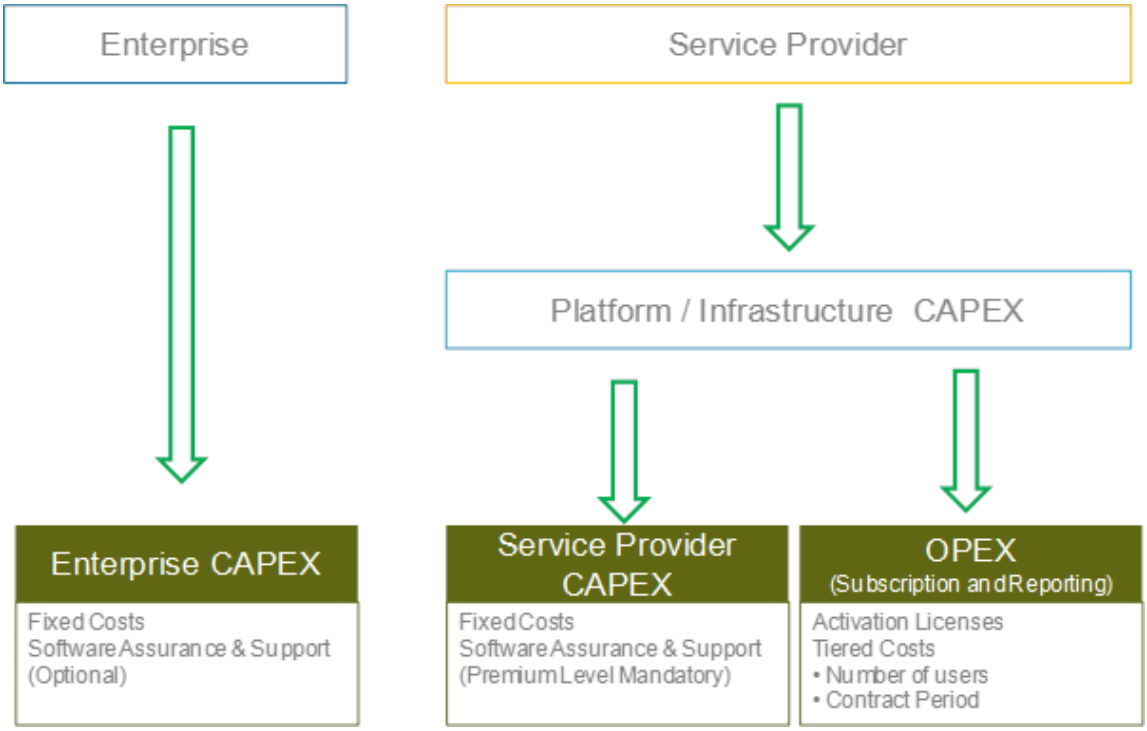
CAPEX AND OPEX LICENSING MODELS

There are two pricing and licensing models that can apply to MiCloud service providers and one model for Enterprise UC. The licensing falls into either the CAPEX (Capital expenditure) or the OPEX (Operational Expenditure) models for the service providers. On-Premise, or Private Cloud Enterprise UC users follow a separate CAPEX only model. The different models are shown in the diagram below. For Enterprise/On-Premise deployments and service providers following the CAPEX model, Software assurance is a separately licensed item. Service providers following the CAPEX model must purchase the premium level of Software Assurance. For service providers following the OPEX model, Software Assurance is included with the monthly subscription.

A service provider must follow the Service Provider Licensing Model, which includes certain qualification agreements as well as specific sales targets. Details on the Terms and conditions for service providers can be found in the Managed Service Provider Addendum to the Mitel Authorized Partner Agreement. Furtherlicense details are found in the *MiCloud Business*

Solution for Service Providers Licensing Guide, available from a local Mitel Sales Representative.

Table 23: Licensing Models



END-USER UCC LICENSING PROFILES

There are a number of pre-bundled user profiles that are used for UCC deployments both Enterprise UC and also MiCloud deployments. The table “UCC User Profiles” on page 185 highlights the different user profiles:

Table 24: UCC User Profiles

USER PROFILE	LICENSED	BASE FUNCTIONS	ADDED FUNCTIONS	ADDED FUNCTIONS
Basic IPT *see notes	UCC Bundle (with ULM)	Base phone		
Standard IPT	Individual licenses	• Base phone • EMEM V.mail		

Table 24: UCC User Profiles

USER PROFILE		LICENSED	BASE FUNCTIONS	ADDED FUNCTIONS	ADDED FUNCTIONS
Entry UCC	Entry SB UCC	UCC Bundle (with ULM)	• Base phone • EMEM V.mail • EHDU (total two devices)		
	Entry UCC	UCC Bundle (with ULM)	• MDUL • EHDU • MiCollab Unified Messaging (total two devices)		
Standard UCC		UCC Bundle (with ULM)	• MDUL • EHDU • MiCollab Unified Messaging (multi-device)	• UC Softphone • Teleworker • UC Client • UC Collaboration	
Premium UCC		UCC Bundle (with ULM)	• MDUL • EHDU • MiCollab Unified Messaging (multi-device)	• UC Softphone • Teleworker • UC Client • UC Collaboration	• UC Mobility • Teleworker

All of the user Profiles that are UC-based are bundled license packages, i.e. these functions are all contained under a single part number. The Standard IPT Profile does not exist as a bundle and must be created from individual licenses, typically the Basic IPT and additional voice mail licenses.

For On-Premise deployments the Standard IPT construct can be associated with a MiCollab Unified Messaging, if available, rather than EMEM.

For On-Premise deployments with UCC, the Basic IPT is replaced with the Basic UCC profile.

The Entry UCC profile is split into two distinct user profiles of EntrySB UCC and Entry UCC. The appropriate profile to use is based on deployment topology, as shown below:

- Use the Entry SB UCC User profile for all Deployments without MiCollab.
- Use the EntrySB UCC User profile for a MiCloud Business deployment, with MiCloud Business SB topology using MiVoice Business Multi-Instance, with MiCollab Client Multi-Tenant.
- Use the Entry UCC User profile when deployed with a full UCC capable MiCollab.

Additional UCC license details can also be found in the *MiCollab Installation and Maintenance Guide*.

The Mitel Management Portal management application can identify the underlying infrastructure and programme the appropriate Entry UC profile.

The table "User Profiles and Topologies" on page 187 highlights where the different user profiles are applied to different topologies:

Table 25: User Profiles and Topologies

USER PROFILE	MICLOUD BUSINESS SB (MIVOICE BUSINESS MULTI-INSTANCE WITH MICOLLAB MULTI-TENANT)	MICLOUD BUSINESS SMB-LD (MIVOICE BUSINESS MULTI-INSTANCE WITHOUT MICOLLAB)	MICLOUD BUSINESS SMB-LD (MIVOICE BUSINESS MULTI-INSTANCE WITH MICOLLAB)	ENTERPRISE UC AND MICLOUD BUSINESS WITH MICOLLAB (NOT MULTI-TENANT)
Basic IPT	Available	Available	Available	Available
Standard IPT	Available	Available	Not Available	Not Available
Entry SB UCC	Available	Available	Not Available	Not Available
Entry UCC	Not Available	Not Available	Available	Available
Standard UCC	Not Available	Not Available	Available	Available
Premium UCC	Not Available	Not Available	Available	Available

The User Profile options that are available are dependent upon whether MiCollab UC capability is present, and also the level of UC capability, such as with full UCC with a per-customer MiCollab, or UC capability with a MiCollab Client Multi-Tenant configuration.

The per-customer MiCollab deployments will make use of the integrated UM-based voice-mail. The MiCollab Client Multi-Tenant, or lack of MiCollab will require either an external voice mail, or use of the Embedded voice mail within the MiVoice Business instance or controller.

The EntrySB UCC and Entry UCC Profiles are limited to two devices whereas the Standard and Premium UCC profiles allow the maximum of eight devices to be associated with a user. Practically the upper quantity of devices is not expected to exceed four devices.

Note: A combination such as EHDU and Mobile softphone will represent two devices, and two different call paths, to the call control, even if they are both deployed on the same physical smart phone.

The Standard IPT profile is normally a construct of separate licenses for most deployments. An activation license bundle does exist for Standard IPT, but may only be used with the following configurations:

- Use with the SB topology with, or without, MiCollab Multi-Tenant with the service provider OPEX model
- Use with SMB-LD topology without MiCollab with the service provider OPEX model

For all other topologies and configurations, the Standard IPT is either replaced with Entry UCC, or is built from component licenses as a construct.

OVERVIEW OF AMC AND HOW UCC LICENSES ARE ORGANIZED

The AMC is a common license repository for customer configuration and deployments. The AMC maintains records of purchased and configured licenses against specific Customer ID. Within this Customer ID record, specific products are assigned licenses against unique Application Records IDs (ARIDs). The ARIDs are then loaded onto the end products, which then use this information to remotely access the AMC and cross verify the licenses.

Using the AMC allows any changes, or updates, to be quickly applied and for the product platforms to pick this up automatically. The AMC also allows licenses to be moved within a customer ID record, for example with adds-moves-changes.

User licenses are grouped and distributed within ULM and DLM constructs. A ULM is required in order to use UCC licenses. Use of a DLM is recommended as a single point of user license distribution within a defined cluster of MiVoice Business platforms.

Licenses from one end-customer can be moved to another end-customer, to the same platform type, within the same Customer ID record. Licenses cannot be moved between Customer ID records. The definition and use of a customer ID is therefore important. For Enterprise UC, On-Premise or for Private Cloud deployments, the customer is unique and is assigned their own Customer ID. For a service provider, there may be multiple end-customers, but only one product or service deployment customer. In this case the Customer ID is assigned to the service provider. Licenses can be moved between end-customers, as needed, within the same service provider Customer ID record. Service providers need to be qualified before using the service provider license model.

For service providers using the OPEX model, two important license types to consider are the activation licenses and monthly subscription licenses. Typically the activation licenses are minimal cost and allow the infrastructure to be put into place ahead of end-customer roll-out. As end-customers come on-board, services are assigned to the end-user through Mitel Management Portal. Each month, the service provider reports back to Mitel which licenses are being consumed from the monthly subscription licenses.

The licenses are constructed in AMC in a hierarchical fashion, starting with the Customer ID record and going down to the level of an individual product and users. The following is an example of the hierarchy that might be encountered under a Customer ID record:

Customer ID Record

- MiVB 1
- MiVBG 1
- ULM 1
  - MiCollab 1
  - MiVBG 2
  - OIG 1
  - GARID 1
    - MiVB (and DLM) 2
    - MiVB 3
    - MiVB 4

The table “License Hierarchy” on page 189 describes this hierarchy.:

Table 26: License Hierarchy

LICENSED DEVICE	DESCRIPTION	ADDITIONAL NOTES AND USAGE
MiVB 1	MiVB 1 is common to all end-customers, or is a unique unit not associated with a ULM	Licenses are manually provisioned. Usage Example: Common SIP or PRI trunk routing
MiVBG 1	MiVBG 1 is common to all end-customers, or is a unique unit not associated with a ULM	Licenses are manually provisioned. Usage Example: Common SIP Trunk gateway to SIP Trunk SP
ULM 1	ULM 1 is a Group ARID to identify a unified solution grouping. The ULM GARID number is not applied directly to an end device or application	This is grouping construct, but not used directly on any applications. See additional notes, below table. Usage Example: Needed to include MiCollab and pool UCC licenses
MiCollab 1	MiCollab 1 is the unified communications application package.	The MiCollab includes an MiVBG which must be clustered to any other MiVBGs in the ULM in order to share licenses. MiCollab does not share licenses with MiVB and DLM, but is aware of the allocation. Usage Example: UCC deployment
Mitel Open Integration Gateway 1	Mitel Open Integration Gateway 1 provides application attachment to MiVB and allows external CRM connections.	Mitel Open Integration Gateway licenses are manually provisioned. Usage Example: Used to provide MiVoice Integrated connections to external 3rd parties such as Google and Salesforce

Table 26: License Hierarchy

LICENSED DEVICE	DESCRIPTION	ADDITIONAL NOTES AND USAGE
GARID 1	GARID 1 is a grouping of MiVB ARIDs. This number identifies the group	The GARID must be applied to one of the MiVB within the GARID grouping. This MiVB will have both ARID and the DLM GARID. Usage Example: Allows licenses to be shared within a cluster of MiVB.
MiVB 2 (and DLM)	MiVB 2 is grouped under the ULM and linked to the MiCollab 1. This unit is also the DLM for a wider number of MiVoice Business	Usage Example: The DLM allows license sharing between MiVB within the same MiVoice Business cluster. This is to allow Single Point of User Provisioning from the MiCollab 1 unit.
MiVB 3	MiVB3 is an MiVB unit linked to the MiVB2 DLM unit	Usage Example: A resilient MiVB to MiVB2, or an additional unit for more users and devices
MiVB 4	MiVB4 is an MiVB unit linked to the MiVB2 DLM unit	Usage Example: The MiVB4 is configured within the same MiVB cluster as MiVoice Business 2 (DLM) for increased scaling of users and devices

Additional restrictions apply to the number of MiCollab and MiVoice Business units that can be in the same ULM. This may result in MiVoice Business being configured outside of the ULM, but linked back via a common DLM, or treated as a separate unit. Following the rules below, should minimise such configuration exceptions.

The ULM can contain the following units and configurations:

- Allowance for multiple MiCollab, but only a single DLM or MiVoice Business
- Allowance for a single MiCollab and multiple DLM or MiVoice Business
- Allowance for multiple MiVoice Border Gateway. These may be clustered back to the MiCollab for license sharing, or treated as standalone units or clusters. MiVoice Border Gateway cluster limits may apply
- Allowance for multiple Mitel Open Integration Gateway (manually provisioned)
- A ULM cannot contain multiple MiCollab AND (multiple DLM OR multiple MiVoice Business)

Some specific platform caveats also apply:

- MiVoice Business Express cannot become a DLM and only the one MiVoice Business within MiVoice Business Express is allowed in the ULM
- MiCollab Client Multi-Tenant is considered a single MiCollab unit, even though many customers may connect via this single unit. Multiple DLM and MiVoice Business for different customers are therefore allowed.

CREATION OF DLM AND ULM WITHIN AMC

The DLM and ULM constructs allow a number of products to be grouped under a common Group ARID (GARID). Although these are used as a top-down grouping, they are created from a bottom-up approach. See the previous section “Overview of AMC and How UCC Licenses are Organized” on page 188 for an example of GARID groupings.

Both ULM and DLM creation is associated with a MiVoice Business. Once an initial MiVoice Business ARID has been created, additional options to create a DLM and ULM exist. The exception to this is the MiVoice Business Express, which is an existing grouping of components. The MiVoice Business Express does not allow the creation of a DLM, but does allow the creation of a ULM.

The DLM is a grouping of ARIDs under a common GARID. This GARID must be associated with a MiVoice Business, and must be programmed into the Designated License Manager unit.

The ULM is a grouping construct. It is used to group ARIDs under a common GARID, but is not programmed into any particular unit. However, by convention a ULM is logically associated with a MiCollab unit, or group of units.

A ULM is required to use UCC licensing. A DLM is recommended to provide a single point of distribution of user licenses within a defined cluster of MiVoice Business platforms.

For service provider deployments that are voice-centric, the use of a ULM is required. This will ensure consistency of deployment and will simplify deployment should UC or UCC functionality be added at a later date. For Enterprise deployments, use of ULM is also recommended for UCC deployments.

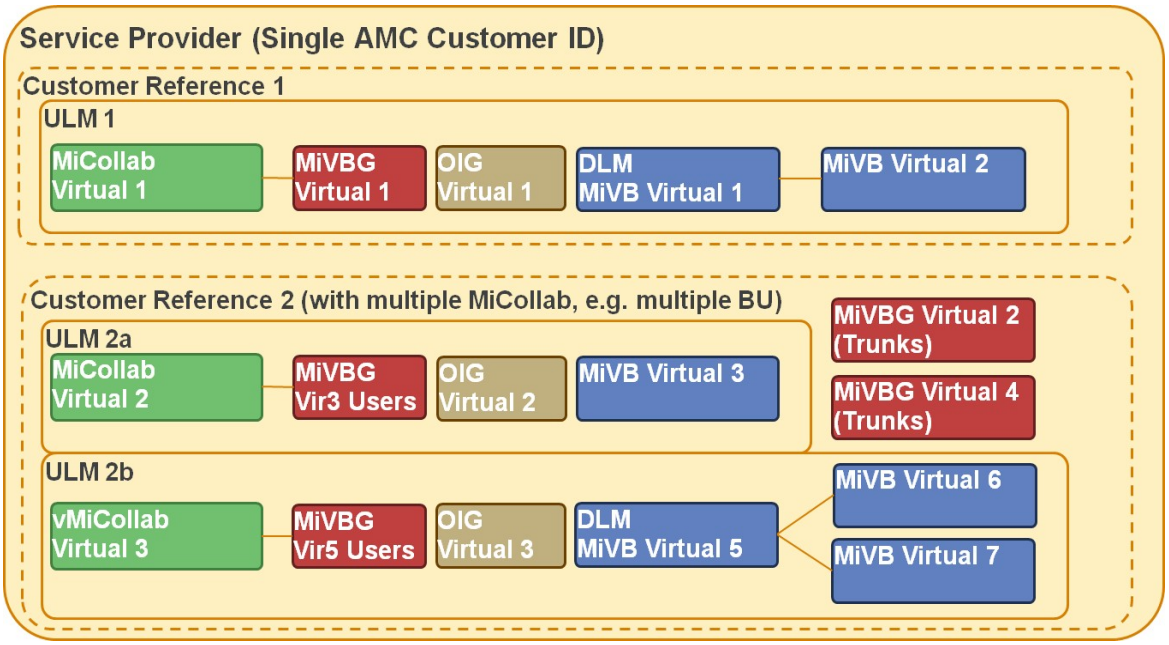
SAMPLE CONFIGURATIONS AND DESCRIPTIONS FOR DIFFERENT TOPOLOGIES

Most of the topologies that are covered within this Solutions Blueprint document can be described within a simple standard AMC license structure. This standard structure is described in the section below. There are some variations on the standard license structure for the MiCloud Business SB and MiVoice Business Express topologies, and these are covered in later sections.

STANDARD UCC AMC HIERARCHY AND LICENSE STRUCTURE

“Service Provider License Hierarchy for Multiple End-Customers” on page 192 shows two examples of a license hierarchy and structure for a service provider where there are multiple end-customers, with segregated deployments, i.e. the MiCollab, MiVoice Border Gateway and MiVoice Business are deployed on a per end-customer basis. This would be the structure for On-Premise, Private Cloudand service providers where customers are assigned their own instances, or private network.

Figure 24: Service Provider License Hierarchy for Multiple End-Customers



In the diagram, the Customer ID is associated with the service provider.

For an On-Premise deployment, or Private Cloud deployment the Customer ID is associated with the end-customer, not the service provider.

In the diagram, two customer references are highlighted, bounded by dashed lines. The Customer Reference does not exist in the AMC, but are used in the diagram to highlight the logical boundaries between customers. Typically a service provider would identify which components would be associated with an end-customer and this would identify the customer reference boundary.

Customer Reference 1 is a typical deployment. The ULM is centred around a single MiCollab. The customer requires an additional MiVoice Border Gateway for trunks and Teleworker and this clustered with the MiVoice Border Gateway that is associated with MiCollab. This customer also requires a MiVoice Integration application. The customer has two MiVoice Business deployed. If these are Primary/Secondary units, the DLM is not needed, but if these are load sharing, or there are more than one MiVoice Business with registered users in the deployment, then a common DLM is required to link these units together. Multiple MiVoice Business can be used, but the common DLM simplifies the configuration and on-going management of licenses with moves/adds/changes.

Although the customer reference would typically line up with a ULM boundary, this may not always be the case. In the ‘Customer Reference 2’ diagram, there are multiple ULMs associated with this customer, and also some additional MiVoice Business and MiVoice Border Gateway units that are common to this customer deployment, independent from the ULM configurations.

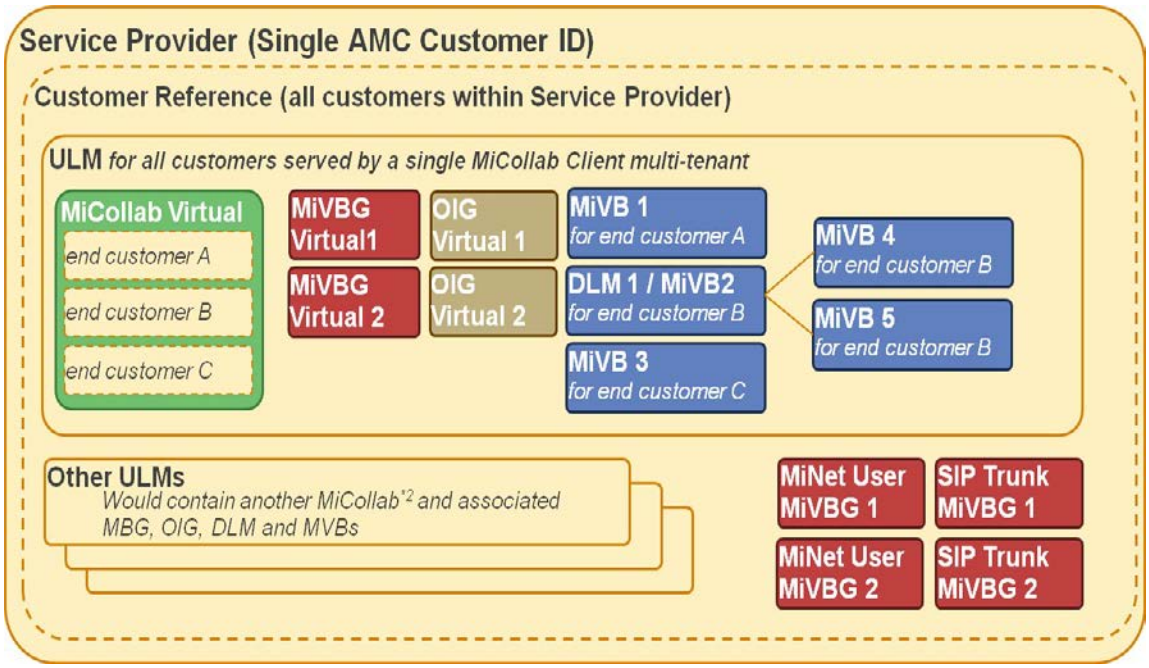
The ‘Customer Reference 2’ is a larger deployment. The customer requires two MiCollab units, and these are split into two ULMs. It is possible to have multiple MiCollab in a single ULM, but

then only one DLM and no MiVoice Business would be allowed inside the DLM. Either of the configurations will work, but including the MiVoice Business with the DLM in the ULM makes it easier to manage license sharing as well as identification of the units that are associated with a particular customer. The recommendation is therefore to deploy one ULM associated with one MiCollab.

UCC AMC HIERARCHY AND LICENSE STRUCTURE FOR MICLOUD BUSINESS SB TOPOLOGY

The MiCloud Business SB Topology uses a common address space to deal with multiple customers, rather than a unique address space per customer. This means that the UC components are more associated with the service provider than with individual customers. The SB topology also makes use of the MiCollab Client Multi-Tenant, which handles multiple end-customers in a single MiCollab unit.

Figure 25: Service Provider Licensing for SB Topology



Although a Customer Reference boundary is shown in “Service Provider Licensing for SB Topology” on page 193, this is really associated with the service provider, not the individual end-customers.

If the capacity of the MiCollab Client Multi-Tenant is exceeded and additional MiCollab Client Multi-Tenant servers are needed, then additional ULMs must be created to match, as indicated by ‘Other ULMs’ in the diagram.

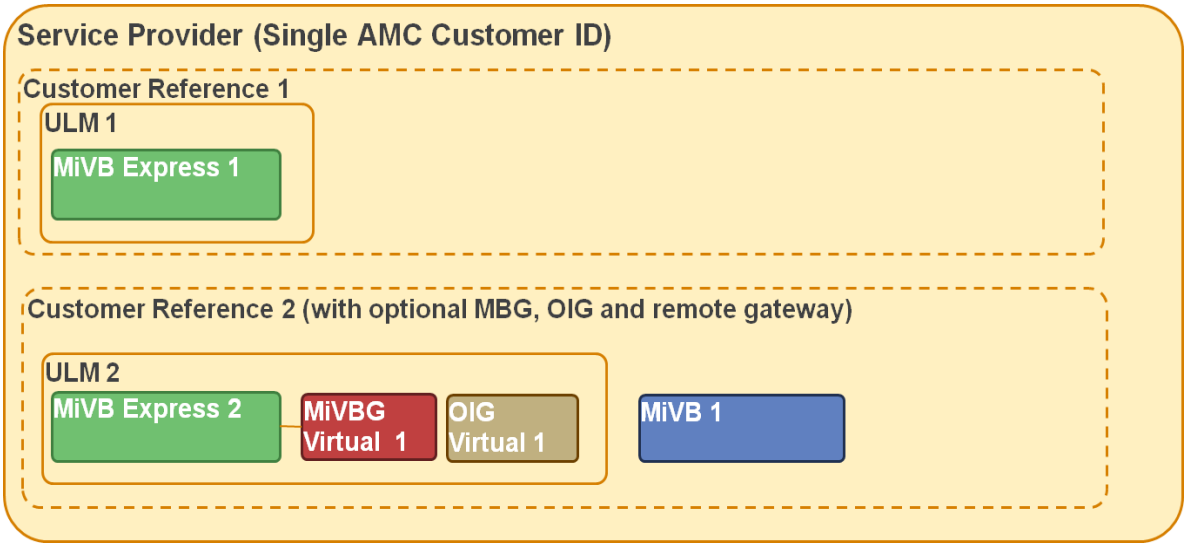
The SB topology includes a number of gateways and portals that are associated with common access into and out of the network. These are for common SIP trunks and also common phone access, as Teleworkers. These common components are highlighted as MiVoice Border Gateways one and two (SIP Trunk and MiNet User) and are independent from any ULM. The licenses for these units are provisioned manually.

ULMs are associated with a single MiCollab Client Multi-Tenant. This shared MiCollab Client Multi-Tenant, at the ULM level, contains all the UCC license requirements across all the tenants. Within this ULM it is possible to assign multiple MiVoice Business and DLMs to associate with each of the end-customers on the MiCollab. Multiple MiVoice Integration can also be deployed within the ULM for customers that require application attachment. Licenses for MiVoice Integration need to be provisioned manually from within the ULM. The MiVoice Border Gateway units, within the ULM, are associated with common UCC functions and service access to the MiCollab Client Multi-Tenant, not to individual customers. These MiVoice Border Gateways can be clustered for resiliency and scaling. This may result in multiple MiVoice Border Gateway clusters. The MiVoice Border Gateway clusters are not associated with the single MiVoice Border Gateway that is associated with the MiCollab, and to have their licenses provisioned manually. The licenses for MiVoice Business and DLM are provisioned manually, and not via MiCollab. The user programming is configured through MiCollab.

UCC AMC HIERARCHY AND LICENSE STRUCTURE FOR MIVOICE BUSINESS EXPRESS (SMB) TOPOLOGY

The MiVoice Business Express with VMware topology uses a dedicated solution package that contains many of the key functions that are needed to deploy this unit. Because the key components are all available in a single package, expansion capabilities for the ULM are limited.

Figure 26: Service Provider Licensing for MiVoice Business Express



The diagram "Service Provider Licensing for MiVoice Business Express" on page 194 highlights two different customer configurations each using a separate MiVoice Business Express package. Customer one uses the standard deployment, whereas Customer two has some expansion options included.

For Customer Reference 1 this customer has deployed a single MiVoice Business Express virtual package. The call control, UCC capabilities and external gateways are all contained within this package.

For Customer Reference 2 some additions have been included along with the MiVoice Business Express. An additional MiVoice Border Gateway has been included. This could be for additional trunks, maybe to an alternative service provider, or for additional Teleworker and UC users. This MiVoice Border Gateway is clustered back to the MiVoice Border Gateway that is part of the MiVoice Business Express in order to share licenses. A MiVoice Integration has been included for additional application attachment. The MiVoice Integration licenses must be provisioned manually.

For Customer Reference 2, an additional on-premise MiVoice Business gateway is also included. This can be clustered with the MiVoice Business Virtual within the MiVoice Business Express. However, since the MiVoice Business Virtual within MiVoice Business Express cannot act as a DLM, licenses cannot be shared between these MiVoice Business. The on-premise MiVoice Business must therefore have licenses provisioned manually. A ULM that contains a MiVoice Business Express cannot contain additional MiVoice Business or DLM, so the on-premise MiVoice Business is licensed outside of the DLM. This adds some overhead if licenses need to be moved, since these would need to be transferred from the on-premise MiVoice Business to the ULM, or vice versa. Due to added complexity of license management, it is recommended that the on-premise MiVoice Business only provide secondary resiliency for users, or have devices that don't typically change, such as paging units and door openers. This reduces license provisioning and complexity due to possible user moves/adds/changes.

Appendix A

GLOSSARY

GLOSSARY

TERM	DESCRIPTION
ACD	Automatic Call Distribution. A package of advanced call processing features, relating to groups of agents who handle calls and agent supervisors.
AMC	Applications Management Center. Used to activate new hardware and software licenses for Mitel products.
ARP	ARP – Address Resolution Protocol. Used to identify a MAC address against an IP address.
ARS	ARS – Automatic Route Selection. This is a method whereby call control can best determine the path from one controller to another and provide a seamless connection to the user.
ASU	ASU – Analog Services Unit. This unit provides a combination of analog ONS interfaces for phones and/or LS trunks.
BRI	BRI – Basic Rate Interface. Digital ISDN connection to PSTN or local digital phone. This is the smallest quantity of digital channels that can be delivered, and consists of two digital channels for voice and data. Variants include the U interface for North America and S0 in Europe.
Call Control	Software to create connections and paths between end-user devices.
CAT 3	Category 3 Cable. A type of UTP cable for use in a LAN, capable of 16 Mbps. Typically used for voice and data on 10BASE-T Ethernet.
CAT 5	Category 5 Cable. A type of UTP cable for use in a LAN, capable of 100 Mbps.
CCS	Centum Call Second. A measure of call traffic. One call lasting 100 seconds is referred to as 1 CCS.
CDE	Customer Data Entry. A command line interface used to configure the Mitel 3300 ICP.
CDP	Cisco Discovery Protocol. A Cisco proprietary protocol that allows IP devices and L2 switches to communicate with each other for configuration purposes.
CEID	Cluster Element ID. A means of identifying different system units to maintain a consistent number plan.
CESID	Customer Emergency Services Identifier. A means of correlating a user and a directory number to information stored in a physical location database.
CIM	Copper Interface Module. A TDM interface module used to connect the ICP to various peripherals via CAT 5 UTP.
CIR	Committed Information Rate. A means to identify how much information MUST be carried in a connection, e.g. CIR = 64 Kbps for voice.
CODEC	COder and DECoder. Coder and decoder commonly used as a single function. A means to convert analog speech into digital PCM and vice versa.
Controller	Control element of ICP (see also RTC).
COS	Class of Service. This refers to the priority value in the Layer 2 part of an IP packet when IEEE 802.1p is used.
CPH	Calls Per Hour. For example, six CPH means six calls per hour.

TERM	DESCRIPTION
CSM	Customer Service Manager. Former name for MiContact Center Office, an entry level contact center solution hosted on MiCollab for basic contact centers or workgroups with up to 100 agents.
CSMA/CD	Carrier Sense Multiple Access Collision Detect. The mechanism used on shared Ethernet connections to ensure that devices are not sending at the same time, and if they are, to initiate a back-off and retry algorithm.
CTI	Computer Telephony Integration. Means of combining computer functions to control operation of telephony equipment.
Datagram	A logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms “frame”, “message” and “packet” are also used to describe a datagram.
DECT	Digital Enhanced Cordless Telephony. Originally this was a European standard for digital cordless phones. This is now a worldwide standard, hence, the name change to Enhanced. Standard DECT phones are not available in North America.
DHCP	Dynamic Host Configuration Protocol. A means of passing out IP addresses in a controlled manner from a central point/server.
DiffServ	Differentiated Services. DiffServ is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence. For example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in WAN connections. This uses the Type of Service field at Layer 3 in an IP packet. See also DSCP.
DN	Directory Number. A telephone or extension number.
DNIC	Digital Network Interface Circuit. A chip used as the basis for several sets which handle both voice and data.
DNS	Domain Name Server. A means of translating between typed names and actual IP addresses, e.g. microsoft.com = 207.46.134.222
DPNSS	Digital Private Network Signalling System. A British common channel signalling protocol for requesting or providing services from/to another PBX.
DSCP	Differentiated Services Code Point. This is a value that is assigned to the Type of Service byte in each outgoing packet. The value can be in the range of 0 to 63 and allows routers at Layer 3 to direct the data to an appropriate queue. Value 46 is recommended for voice and will use the Expedited Forwarding queue or Class of Service.
DSP	Digital Signal Processor. This is a programmable device that can manipulate signals, such as audio, to generate and detect a range of signals, e.g. DTMF signalling.
DSU	Digital Service Unit. A peripheral which provides digital ports for the ICP.
DTMF	Dual Tone Multi-Frequency. In-voice-band tones used by telephones to signal a particular dialed digit. Also known as touch tone.
E	Erlang. A measure of usage of a resource, e.g. 0.75 e = 75%. 1 e = 36 CCS.
E1	Primary Rate running at 2.048 Mbps providing 30 channels of voice of PCM.
E2T	Ethernet to TDM. This is the conversion of voice streaming between TDM and IP.
E911	Enhanced 911 (Emergency Services). Also 999 (UK) and 112 (International).

TERM	DESCRIPTION
eMOH	Embedded Music On Hold.
ESM	Embedded System Management. Means to program a system from the System Administration Tool, Group Administration Tool, or Desktop Tool.
FAX	A means of transmitting printed text or picture information with acoustic tones.
FIM	Fiber Interface Module. A fibre optic TDM interface module used to connect the ICP to various peripherals.
FQDN	Fully Qualified Domain Name. The complete domain name for a specific computer, host, or IP end-point. The FQDN consists of two parts: the host name and the domain name. For example, an FQDN for a hypothetical server might be MyServer.Business.com. The host name is MyServer, and this host is located within the domain called Business.com. A Domain Name Server (DNS) is used to resolve the FQDN to an actual IP address.
FTP	File Transfer Protocol. An electronic method to transfer file information.
G.711	G.711 – PCM Voice Streaming. ITU standard for conversion of voice-streaming to digital PCM (64 kbps).
G.729	Voice Streaming CODEC. Reduced bit rate from G.711 (8 kbit/s)
Group Controller	The call control of the ICP is in control of a number of units, where the functions are more dedicated, e.g. to a separate gateway
GRP	Gateway Routing Protocol. A generic term which refers to routing protocols.
HSRP	Hot Standby Routing Protocol. A Cisco proprietary protocol used to increase availability of default gateways used by end hosts.
ICMP	Internet Control Message Protocol. Messages to help identify when devices are present and create warnings when they fail.
ICP	IP Communications Platform. Includes gateway function, call control, plus a number of other features, such as voice mail.
IP Address	Internet protocol address. A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork.
IP	Internet Protocol. An encapsulation protocol that allows data to be passed from one end-user to another. Typically this was over the Internet, but the same protocol is now used within businesses.
IRDP	ICMP Router Discovery Protocol. An extension to the ICMP protocol that provides a method for hosts to discover routers and a method for routers to advertise their existence to hosts.
ISDN	Integrated Services Digital Network. The digital PSTN network. Integrated because this network carries both voice and data and provides direct digital connectivity to the user via BRI or PRI connections.
ISL	Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.
L2	Layer 2. The second layer of encapsulation of data to be transferred. Typically with TCP/IP this includes the MAC layer.

TERM	DESCRIPTION
L3	Layer 3. The third layer of encapsulation of data to be transferred. Typically with TCP/IP this includes the IP address.
LAN	Local Area Network. This is a network within a local area, typically within a radius of 100 m. The transmission protocol is typically Ethernet II.
Leased IP	An IP address that has been assigned through DHCP and is valid only for the duration of the agreed lease time.
LLDP	Link Layer Discovery Protocol. A low level protocol used to pass information about the connection configuration between two end devices, for example VLAN. Typically this would be between an end device such as a PC or IP phone and the network access port on the Layer 2 switch.
LLDP-MED	Link Layer Discovery Protocol - Media End-point Discovery. LLDP-MED is an extension of LLDP that provides auto-configuration and exchange of media-related information such as Voice VLAN and QoS. It is designed to provide enhanced VoIP deployment and management.
LS	Loop Start – This is a particular analog trunk protocol for signalling incoming and outgoing calls.
MAC	Media Access Controller. This is the hardware interface that data (media) travels through. Typically this will be assigned a world-wide unique address.
MAN	Metropolitan Area Network. This is a larger network that may connect a number of LANs within a business, as well as a number of businesses. Typically, this would cover a city area, and use fibre optics to get maximum bandwidth.
Mbps	MegaBits Per Second. Million bits per second is a measure of bandwidth on a telecommunications medium. May also be written as Mbits/s or Mb/s. Mbps is not to be confused with MBps (megabytes per second).
MFRD	Mitel Feature Resources Dimensions. This is a definition of the number of features that can be used on a particular unit.
MHz	Megahertz. Frequency measurement.
MiCW	Mitel Configuration Wizard
MiNet	Mitel Network Protocol. This is Mitel's proprietary stimulus-based protocol that is used to signal between phones and controllers, for example key and display information.
MiTAI	Mitel Telephony Application Interface. This Mitel implementation of TAPI is used to connect to external applications, e.g. ACD controllers.
Mitel OIG	Mitel Open Integration Gateway
MLB	MiCloud Business Solution Medium Large Business Topology
Modem	MOdulator-DEModulator. Device that converts digital and analog signals. At the source, a modem converts digital signals to a form suitable for transmission over analog communication facilities. At the destination, the analog signals are returned to their digital form. Modems allow data to be transmitted over voice-grade telephone lines.
MOH	Music on Hold
MTBF	Mean Time Between Failures. The statistical time between expected component failures.

TERM	DESCRIPTION
MTU	Maximum Transmission Unit. An MTU is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network, such as the Internet.
MWI	Message Waiting Indicator. A visual indicator in a telephone that indicates to the user that a message is waiting.
NAT	Network Address Translation. A means of translating internal IP addresses to a defined limited range of Internet IP addresses. The benefit is the ability to use a limited range of Internet addresses and map these to a much larger internal range.
NIC	Network Interface Card. Physical connection to the network. In a PC, this is often a plug-in card.
NSU	Network Services Unit. This interface connects between the PSTN Primary Rate trunks and the ICP.
On-Premise	UC Enterprise Solution Solution On-Premise Topology
ONS	On-Premise Line. This is a two-wire analog telephony interface, within an office environment, and not passed outside.
OPS	Off-Premise Line. This is a two-wire analog telephony interface, typically installed external to a building, e.g. external shed or guard house.
OSPF	Open Shortest Path First. A link-state routing protocol used for routing IP traffic over the most cost-efficient route.
PC	Personal Computer
PCM	Pulse Code Modulation. The digital representation of analog signals.
PDA	Personal Digital Assistant. A handheld personal organizer that can interface to a PC or a Mitel PDA Phone.
Permanent IP	An IP address that has been leased (from DHCP) on a permanent basis.
PI	Performance Index. A calculation of the performance limits of a system. Different weighting values are assigned to various types of calls. Based on the expected calls per hour (CPH) of all of the user ports on the system, a system performance index (PI) can be calculated. The system PI is used as an indication of how much traffic the MiVoice Business MiVoice Business 3300 ICP can handle at any one time.
Ping	This is a means of sending a test message and waiting for a reply to determine if a network device is reachable. On a PC, this is invoked with the command ping.
PPM	Parts Per Million. This is a measurement of accuracy, or the expected error in one million events. Therefore one PPM means that 999,999 to 1,000,0001 events occurred when 1,000,000 were expected. This is 0.0001% error. For example, a household clock that is one second accurate per day is 11.5 ppm, or would need to be 0.086 seconds incorrect per day to be one ppm.
PRI	Primary Rate Interface. This is a connection to the PSTN where a number of trunk channels are multiplexed onto a common connection. Both T1 and E1 variants are available.
Private Cloud	UC Enterprise Solution Private Cloud Topology
Private Cloud, Shared Services	UC Enterprise Solution Solution Private Cloud, Shared Services Topology
PSTN	Public Switched Telephone Network. The telephone network that provides local

and long distance connections, e.g. Bell, AT&T, British Telecom.

TERM	DESCRIPTION
PTT	Poste Telefonie Telegrafie. PSTN services. Some countries combine postal services and telephony under a common service provider, e.g. the government.
RAD	Recorded Announcement Device.
RAID	Redundant Array of Independent Disks. Array of hard drives on which the information is duplicated. A controller manages the disks, switching automatically from the primary to the secondary in the event of the failure of the primary hard drive.
RDN	Remote Directory Number. The Remote DN Table is used to identify alternate ICPs to check for availability of devices, and to determine if a device is located on the Primary or Secondary ICP.
RFC	Request For Comments. A document that is created, maintained and distributed by the Internet Engineering Task Force. An RFC is the vehicle that is used to discuss and evolve a networking related protocol. RFCs usually get approved and issued as standards.
RFP	Radio Fixed Parts. The Radio Fixed Parts (RFPs) connect to the MiVoice Business 3300 ICP through the LAN. The wireless phones communicate with the RFPs using standard Digital Enhanced Cordless Telecommunications (DECT) protocol.
RGP	Router Gateway Protocol. A means whereby routers on a common subnet can communicate with and identify each other. Useful when ICMP Re-direct is needed to identify an alternative path.
RIP	Routing Information Protocol. A networking protocol that maintains a database of network hosts and routers and exchanges information about the topology of the network.
RSTP	Rapid Spanning Tree Protocol. A version of STP that will converge networks more rapidly than STP (see STP).
RTC	Real Time Complex. This is the control block within an ICP. This includes Call Control and internal controls for the unit.
RTP	Real Time Protocol. Protocol used to identify sequence of voice packets with timing information before being sent to a user via UDP.
SAC	Switch Application Communications
SB topology	MiCloud Business Solution Small Business Topology
Scalable	MiCloud Business Solution Scalable Topology
SET	System Engineering Tool. Used for calculating system parameters, limits and allowable additions.
SIP	Session Initiation Protocol. An IETF standard for signalling over IP.
SMB	MiCloud Business Solution Small Medium Business Topology
SMB-LD	MiCloud Business Solution Small Medium Business, Low Density UCC Topology
Static IP	An IP address that has been manually assigned and fixed. Typically, static addresses are exceptions within DHCP.
STP	Spanning Tree Protocol. A means whereby the network can determine multiple paths between two points and disconnect them to leave a single path, removing broadcast issues.
Subnet	A subnet (short for “subnetwork”) is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN).

TERM	DESCRIPTION
SWB	Mitel Sales WorkBench
T.37	Internet Protocol for FAX (Store and Forward). A means of taking a TDM FAX, converting it to data, passing it via IP and reconverting it back to TDM.
T.38	Internet Protocol for FAX (Real Time). Similar to T.37 in function, but carried out in real time, i.e. with minimum delay.
T1	Primary Rate. Provides 23 or 24 channels of trunks per connection.
TAPI	Telephony Applications Programming Interface. TAPI is a standard programming interface that lets you and your computer communicate over telephones or video phones to end-users or phone-connected resources.
TAR	Tape Archive and Retrieval. A file transfer utility.
TCP	Transmission Control Protocol. The methods of transmitting data between two end-points using IP with acknowledgement.
TDM	Time Division Multiplex. A means of combining a number of digitally encoded data or voice channels onto a common digital stream, e.g. T1.
TFTP	Trivial File Transfer Protocol. A simplified version of FTP used to transfer data with minimal overhead.
TOS	Type of Service. A field within the Layer 3 (IP) encapsulation layer to identify some properties relating to service parameters; in this case, delay and priority of handling.
UDP	User Datagram Protocol. A layer 4 protocol with minimal handshaking and overhead. Used to stream voice. Considered connection-less.
Unicast	A process of transmitting messages from one source to one destination, as opposed to a broadcast or multicast.
UPS	Uninterruptible Power Supply. A unit capable of providing output power for a period of time when the local mains supply fails. Usually relies on storage devices such as batteries.
UTP	Unshielded Twisted Pair. Cable that reduces emissions and maintains an impedance match through the twists per metre in the cable without resorting to shielding.
VLAN	Virtual LAN. A means of providing virtual LANs on a network using common physical components. Such VLANs are logically unconnected except through some Layer 3 device.
WAN	Wide Area Network. A network connection to a network that could be global, e.g. via Frame Relay.
Wi-Fi	Wi-Fi Alliance technology for Wireless LAN based on IEEE 802.11.
WLAN	Wireless LAN
WAV	WAVe file. WAV is an audio file format, created by Microsoft, that has become a standard PC audio file format for everything from system and game sounds to CD-quality audio. A Wave file is identified by a file name extension of .wav.