MiVoice Business Express Engineering Guidelines

FEBRUARY 2017
RELEASE 7.3

Mitel

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

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

MiVoice Business Express
Engineering Guidelines
Release 7.3

February 2017

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2017 Mitel Networks Corporation
All rights reserved

List of Tables

List of Figures

INTRODUCTION

This document provides guidelines for implementing MiVoice Business Express solutions.

ABOUT THE DOCUMENTATION SET

Documentation for this product is available on the Mitel Customer Documentation web site.

- For a list of documentation assocates with this product refer to the *MiVoice Business Express Deployment Guide*.
- For specific information related to deployments in virtualized environments, see theVirtual Appliance Deployment Guide.

ACCESSING DOCUMENTATION AND SOFTWARE

Documentation

1. Log in to Mitel Connect.
2. Click **Mitel Online**.
3. Point to **Support** and then click **Product Documentation**.
4. In the right panel, select **Product Documentation**.
5. Point to **Applications** and click **MiCollab**.

Knowledge Base Articles

1. Log in to Mitel Connect.
1. Click **Mitel Online**.
2. Point to **Support**, under **Technical Support** click **Mitel Knowledge Base**.
3. In the Product list, select the appropriate product.
4. Under **Article Type**, select the type of article to be viewed.
5. Specify other search parameters to narrow your search and click **Search**.

Product Release Notes

1. Log in to Mitel Connect.
2. Click **Mitel Online**.
3. Point to **Support**, under **Technical Support** click **Mitel Knowledge Base**.
4. At the bottom of the page, click **Search for Release Notes by Product**.
5. Under **Title**, click **Mitel Applications Suite** (MiVoice Business Express).

Product Bulletins

1. Log in to Mitel Connect.
2. Click **Mitel Online**.
3. Log in to Mitel OnLine.

4. Point to **Support** and then click **Bulletins**.
5. Click the link to access a list of recent bulletins.

Software Downloads with MiVoice Business

1. Log in to Mitel Connect.
2. Click **Mitel Online**.
3. Point to **Support** and then click **Software Downloads**.
4. Click **Mitel Applications Suite** (MiVoice Business Express).
5. Click the appropriate MiVoice Business Express Software Download version.
6. Review the Release Notes.
7. Download the ISO files for your deployment by clicking the file links in the table. When you click a link, you are presented with a software **Disclaimer**.
8. Click the "I Agree [Download using Software Download Manager (Recommended)]".
9. If you don’t already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
10. Save the downloaded software ISO images to a network folder.

WHAT'S NEW IN THIS RELEASE

MIVOICE BUSINESS EXPRESS RELEASE 7.3

No new MiVoice Business Express functionality. However, the supported applications are at new releases.

MIVOICE BUSINESS EXPRESS RELEASE 7.2.2

No new MiVoice Business Express functionality. However, the supported applications are at new releases.

MIVOICE BUSINESS EXPRESS RELEASE 7.2

No new MiVoice Business Express functionality. However, the supported applications are at new releases.

MIVOICE BUSINESS EXPRESS RELEASE 7.1

Restore Encrypted Backup: MSL 10.4 and later allows you to create a backup with password encryption. The Configuration Wizard now allows you to restore an encrypted backup in the Configuration Options panel. If the backup file is encrypted, you must enter and confirm the Encryption Password to proceed with the restore. The filename for an encrypted backup ends with ".aes256".

Configure MiVoice Business FQDN: In the Email & Servers page of the Configuration Wizard, you can choose to configure the MiVoice Business with a Fully Qualified Domain Name (FQDN). This functionality supports Reach Through (single sign-on) from the internet to the MiVoice Business.

Points-based Calculation for User Capacity: You can now calculate the user capacity for a system that has a mix of UCC user licenses using a simple points-based calculation up to the supported user capacity. See Table 1 on page 34.

ACD Agents: MiVoice Business Express small business deployments support up to 25 ACD agents; mid market deployments support up to 50 ACD agents.

MIVOICE BUSINESS EXPRESS RELEASE 7.0

Separate Engineering Guidelines: In previous releases the MiCollab with Voice engineering guidelines were included in the MiCollab Engineering Guidelines. Engineering guidelines for MiVoice Business Express are now covered in this guide.

Product Name Change: MiCollab with Voice has been rebranded in this release as MiVoice Business Express.

Flow Through Provisioning: Flow Through Provisioning allows you to perform user and service provisioning for the MiVoice Business from the MiCollab User and Services application. This feature synchronizes updates made to the following data between the MiCollab and MiVoice Business databases using System Data Synchronization (SDS):

- User and Services Data
- Network Elements
- Departments
- Locations
- Roles
- Templates, and

- Phones

The Single Point Provisioning (SPP) functionality supported in MiVoice Business Express Release 6.0 SP2 and earlier is not supported in MiVoice Business Express Release 7.0 and later. It used MiXML to apply MiCollab updates to MiVoice Business systems. SPP has been replaced with Flow Through Provisioning in this release.

Reach-Through: This feature allows you to access the MiVoice Business system administration tool forms from links or drop-down menus within specific User and Services administration pages. Because you have logged into the MiCollab server manager, you are allowed direct access and do not have to log in separately to the MiVoice Business. This functionality reduces the amount of time it takes to perform programming tasks that require configuration on the MiVoice Business, such as modifying a user's MiVoice Business phone and group settings.

MiVoice Business systems also support Reach Through to MiCollab. Administrators can link directly to certain MiCollab USP forms from specific MiVoice Business system administration tool forms

Microsoft Hyper-V Support: MiVoice Business Express is now supported in Microsoft Hyper-V virtual environments. Refer to the Virtual Appliance Deployment Guide for the virtual resource requirements. See the *MiVoice Business Express Deployment Guide* for installation instructions.

Unified Communication and Collaboration (UCC) V4.x User Licensing: MiVoice Business Express Release 7.0 supports V4.0 Enterprise UCC User Licenses only. UCC Business licenses are no longer available for UCC V4.0 licensing. After an upgrade to MiCollab Release 7.0, V3.x Enterprise licenses are automatically converted to V4.0 Enterprise licenses.

Browser Support: MiCollab supports the following internet browsers for the server manager interface, application administration interfaces, end user portal interface, and all web-based end-user client interfaces:

- Internet Explorer 9, 10, and 11
- Mozilla® Firefox® 33 and higher
- Google Chrome (version 38 and higher)

Note that Flow Through Provisioning and Reach Through are only supported in Internet Explorer or FireFox browsers.

Additional Languages: Support has been added to the MiCollab application end-user interfaces for three additional Nordic languages: Finnish, Swedish, and Norwegian.

Support for Additional NuPoint Prompt Languages: If the NuPoint Unified Messenger application is installed, you can set up to five languages for the NuPoint system prompts. Users who call into the NuPoint auto attendant can choose to hear prompts in one of the supported languages for the duration of their call. In previous releases, only three languages were supported.

MiCollab Client Deployment: MiCollab Client 7.0 introduces a new blade (MiCollab Client Deployment) which allows for the simplified deployment of the MiCollab for Mobile application. This solution is supported in integrated and co-located MiCollab Client deployments. Refer to MiCollab Administrator help for details.

Note: If you wish to use the existing MiCollab UC-Client (previously known as MiCollab Mobile) application and do not wish to deploy the new MiCollab for Mobile application, you must select Do Not Deploy in the Deployment Profile in template information when adding new users.

Resilient Configurations: The following resilient configurations are supported:

- MiVB-X Voice Resiliency
- MiVB-X behind an MiVB ACD agent gateway
- MiVB-X behind an MiVB Trunk Gateway

Custom OVA Template Restore Option: If you are deploying on vCenter, a Customize Template screen is presented during the deployment wizard. This screen allows you to configure the MSL operating system parameters. A new check box has been added to this screen that allows you to specify that you want to restore a database from the MSL server console.

SYSTEM OVERVIEW

MiVoice Business Express provides a complete communications solution for small to medium businesses. It runs as virtual appliance on a VMware vSphere or Microsoft Hyper-V infrastructure. This solution is well-adapted to the following deployment models:

- **Unified Communications as a Service (UCaaS)**: Service Providers host the MiVoice Business Express solution as a software application within a virtualized infrastructure and offer it to customers as a service.
- **Infrastructure as a Service (IaaS)**: Infrastructure providers rent out the resources (for example: vCPU, GHz, RAM, HDD, ports and so forth) required to host the MiVoice Business Express solution on their vSphere or Microsoft Hyper-V shared infrastructure.
- **Customer Premise Equipment**: Mitel certified dealers install and configure MiVoice Business Express in the VMware or Hyper-V environment on the customer's premise.

MiVoice Business Express can be deployed in either Network Edge (server-gateway) mode or LAN (server only) mode with or without an optional third LAN.

For MiVoice Business Express installation and configuration instructions, see the *MiVoice Business Express Deployment Guide*.

CONSTRAINTS

- MiVoice Business IP trunking is not supported in the mainstream release; however, it is supported as a "Technical Preview Only" feature. Contact your local Mitel Sales Representative for information.
- An existing MiVoice Business or MiCollab database cannot be migrated (restored) directly to a MiVoice Business Express deployment from a backup file.
- MiCollab Client is supported only in Integrated Mode.
- Multi-MiCollab is not supported with MiVoice Business Express.
- Applications that require the installation of additional software (for example, NuPoint Speech Auto Attendant) are not supported.

SUPPORTED APPLICATIONS

The MiVoice Business Express solution supports co-residency of the following applications:

- Mitel Standard Linux (MSL) Release 10.5 (64-bit only) operating system
- MiVoice Business Release 8.0.x (without embedded voicemail)
- MiCollab Release 7.3 which includes the following application versions:
  - Suite Application Services (SAS) Release 7.3
  - MiCollab Client Release 7.3
  - MiCollab Client Deployment Release 7.3
  - AWV Release 6.3
  - NuPoint Unified Messenger (NP-UM) Release 8.3
  - MiVoice Border Gateway (MBG) Release 9.4
- Microsoft Office 365 (up to 500 users)
- Gmail (up to 2500 users)

Note: The MiCollab Speech Auto Attendant (SAA), Text-to-Speech (TTS), and Speech Navigation, applications are not supported by MiVoice Business Express.

VIRTUAL INFRASTRUCTURE AND RESOURCE REQUIREMENTS

Refer to the Virtual Appliance Deployment Guide.

CONNECTIVITY MODELS

The following connectivity models are supported:

- MiVoice Business Express Hosting Remote Office via MLPS Router
- MiVoice Business Express Hosting Remote Office using Teleworker Service.
- MiVB-X on Customer Premise connected to an External Firewall

The first two connectivity models in the above list are applicable to both SaaS and IaaS deployments.

Note: Refer to the MiCollab Client Deployment online help for the deployment topologies required to support MiCollab for Mobile Client deployment.

HOSTING REMOTE OFFICE VIA MLPS ROUTER

In this configuration, the UCC virtual machine connects to the remote office using an MPLS router. This configuration extends the customer's network infrastructure into the service provider data center. The IP phones connect to the LAN side of the network infrastructure. Note that this configuration requires the deployment of an optional vMBG for Secure Call Recording (SRC). For call recording, it is recommended that you deploy the vMBG on the LAN, preferably on the same LAN segment as the MiVoice Business Express.

You must configure the WAN interface with an external IP address to support SIP trunking. When deploying MiVoice Business Express on the network edge, you may need to deploy MiVoice Business Express behind a firewall in order to meet your IT network security requirements. For a description on how to set-up the external firewall for use with MiVoice Business Express, refer to Figure 6 on page 12.

MiCollab mobile clients can be used in the remote office because they route to the Internet via a separate router (not the MPLS router).

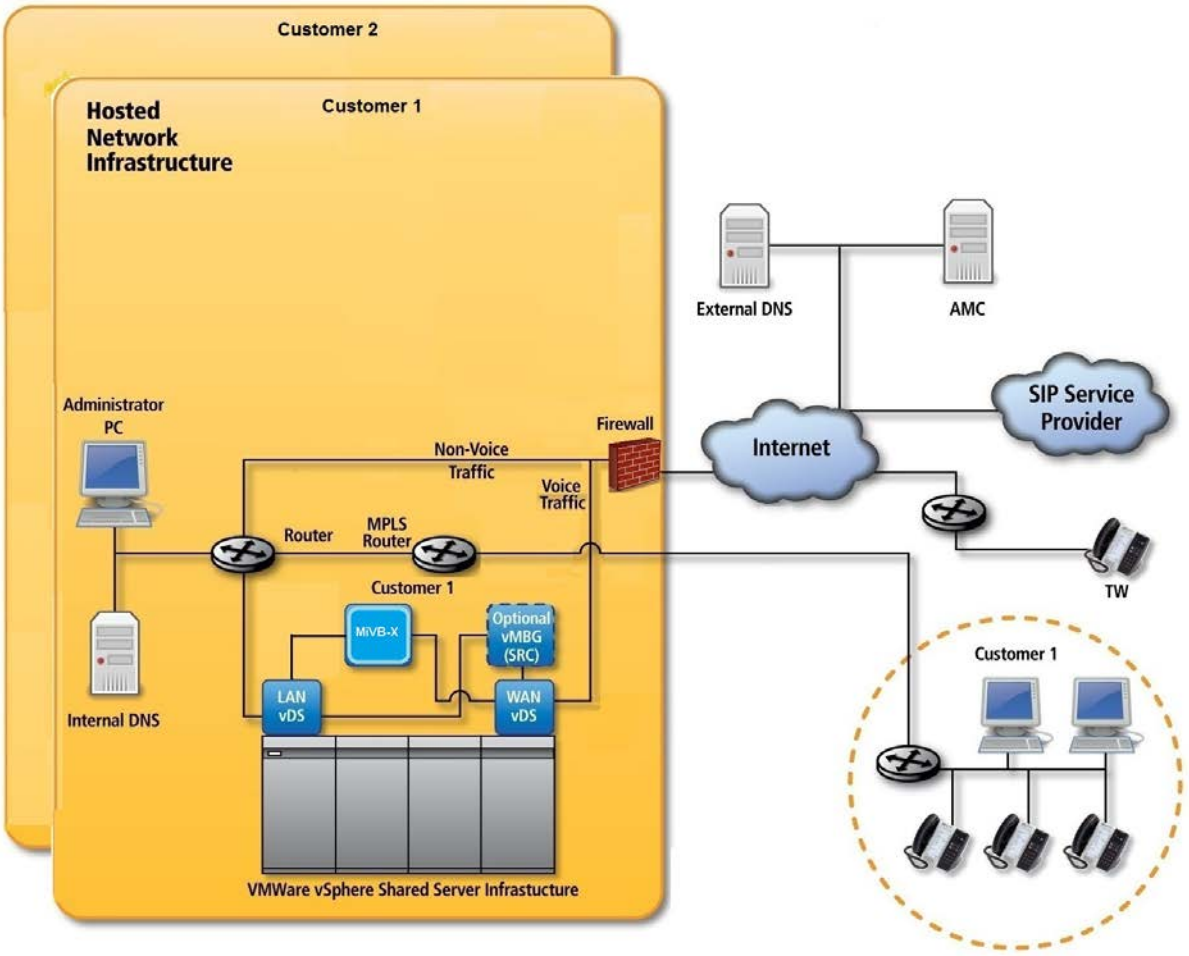

Figure 1: Hosting Remote Office via MPLS (Network Edge)

HOSTING REMOTE OFFICE USING TELEWORKER SERVICE

Figure 2 shows a typical deployment configuration in which MiVoice Business Express hosts Teleworker sets that are deployed in a remote office. In this model, the internal vMBG service of MiVoice Business Express must have direct Internet access. Note that you can also host the customer's Active Directory and mail server along with the MiVoice Business Express. MiVoice Business Express is configured with two network adapters. You configure one as LAN for connection to the local network virtual distributed switch, and the other as "WAN" for connection to the Internet virtual distributed switch. The WAN network adapter has a publicly-routable IP address.

Figure 2 illustrates the preferred deployment with MiVoice Business Express on the Network Edge. MiVoice Business Express is typically deployed behind a third-party firewall that controls business data traffic. This deployment configuration uses an optional separate vMBG, also deployed behind the firewall, which aggregates SIP trunking resources for several customers. Refer to Figure 6 for a description on how to set-up the external firewall for use with MiVoice Business Express. Internal and external DNS servers are also needed for hostname resolution (see for DNS Configuration for the Web Proxy on page 14 for more details). An internal DNS server is optional in this configuration. It is only required for internal hostname resolution. If the application, such as MiCollab AWV, is deployed on the internet, the management is performed remotely and an internal DNS server is not required.

MiCollab mobile clients users are supported on the WAN and on the customer premise. MiCollab mobile clients should always be set in Teleworker mode and routed through the vMBG.

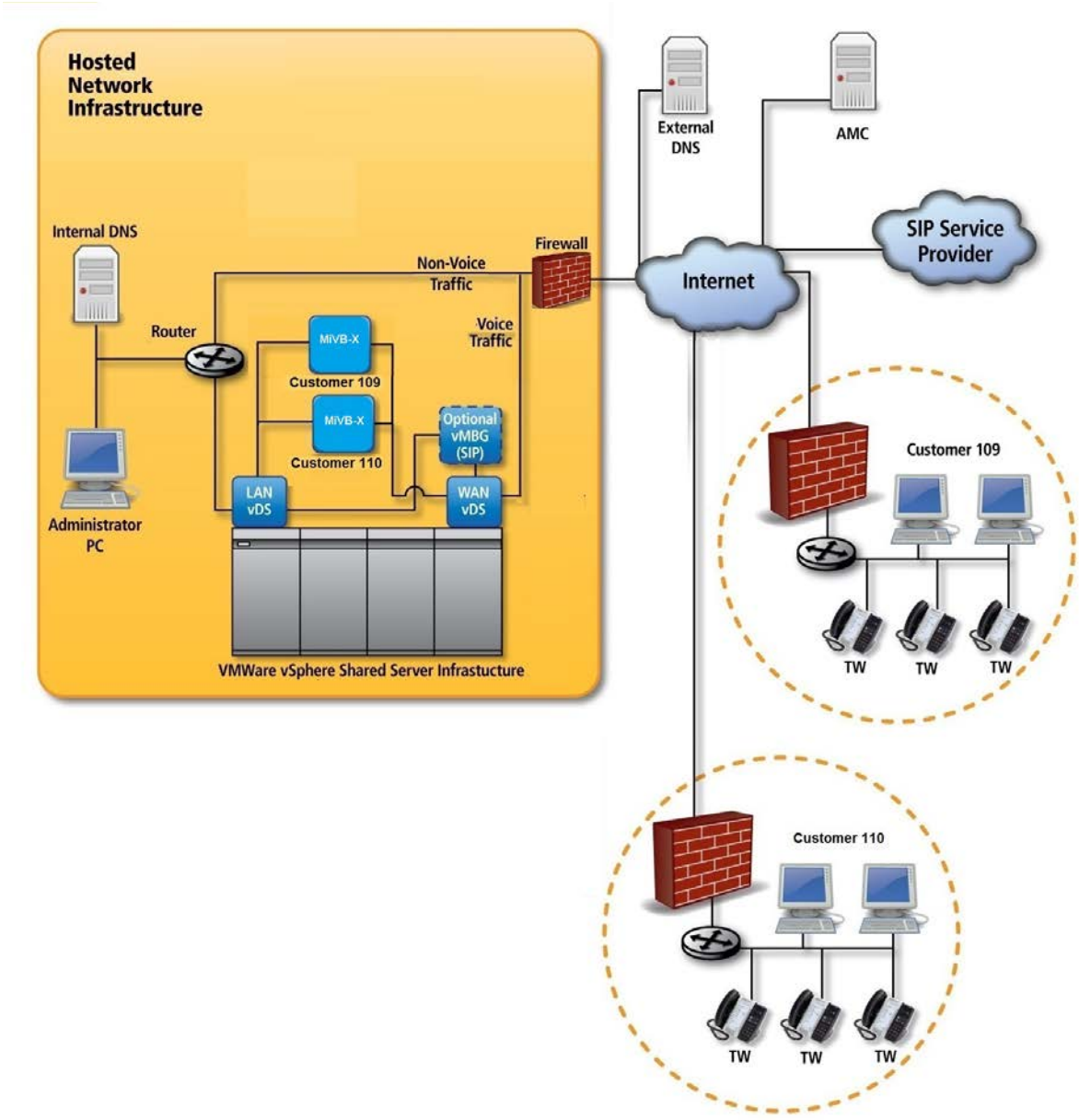

Figure 2: Hosting Remote Office Teleworker Sets (Network Edge)

CUSTOMER PREMISE CONNECTED TO AN EXTERNAL FIREWALL

Refer to the MiCollab Engineering Guidelines for information on how to deploy MiCollab on the Network Edge. MiVoice Business Express in the same manner.

SIP TRUNKING

SIP TRUNK AGGREGATION

If a hosted infrastructure has multiple MiVoice Business Express systems, it is possible to reduce SIP trunking costs by purchasing the trunks in bulk and then aggregating (consolidating) the trunks on a separate standalone vMBG. The SIP trunks can then be distributed among the MiVoice Business

Express systems via the vMBG SIP Trunking web proxy services. See *SIP Trunk Aggregation* in the *MiVoice Business Express Deployment Guide* for details.

CONFIGURATION OF SIP PROVIDER PROXY

During the Initial Configuration Wizard in the SIP Provider Proxy page, the installer is prompted to select one of the following SIP Trunk Proxy configurations

- Internal SIP Proxy
- External SIP Proxy
- None (no SIP Proxy)

See Figure 3, Figure 4, and Figure 5 for diagrams of these configurations.

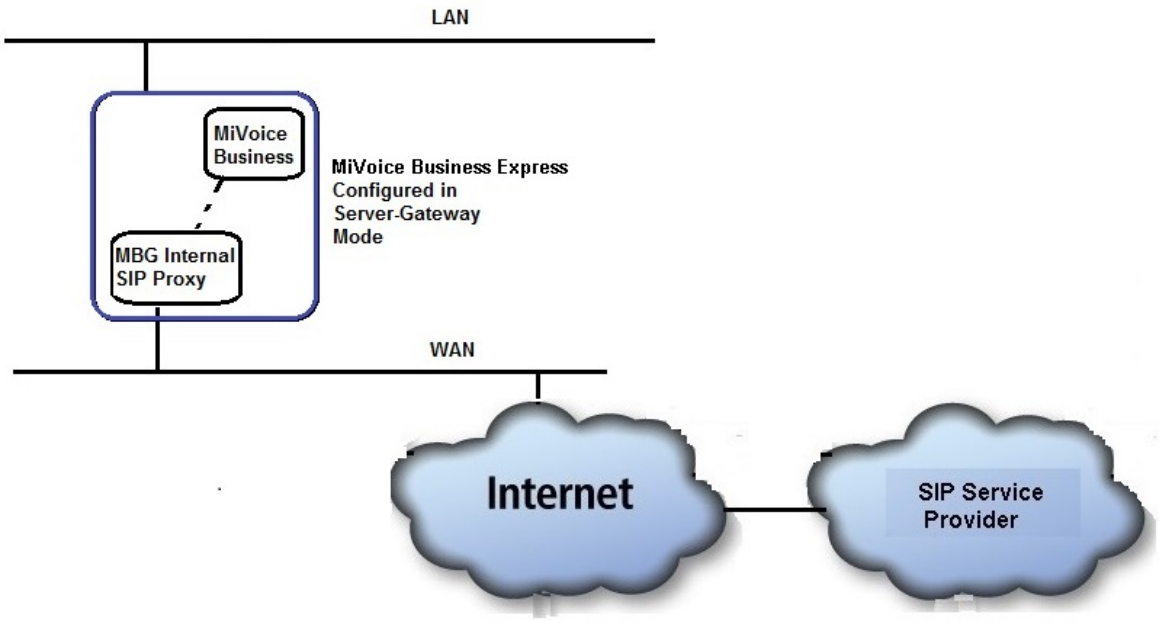

Figure 3: Internal SIP Proxy

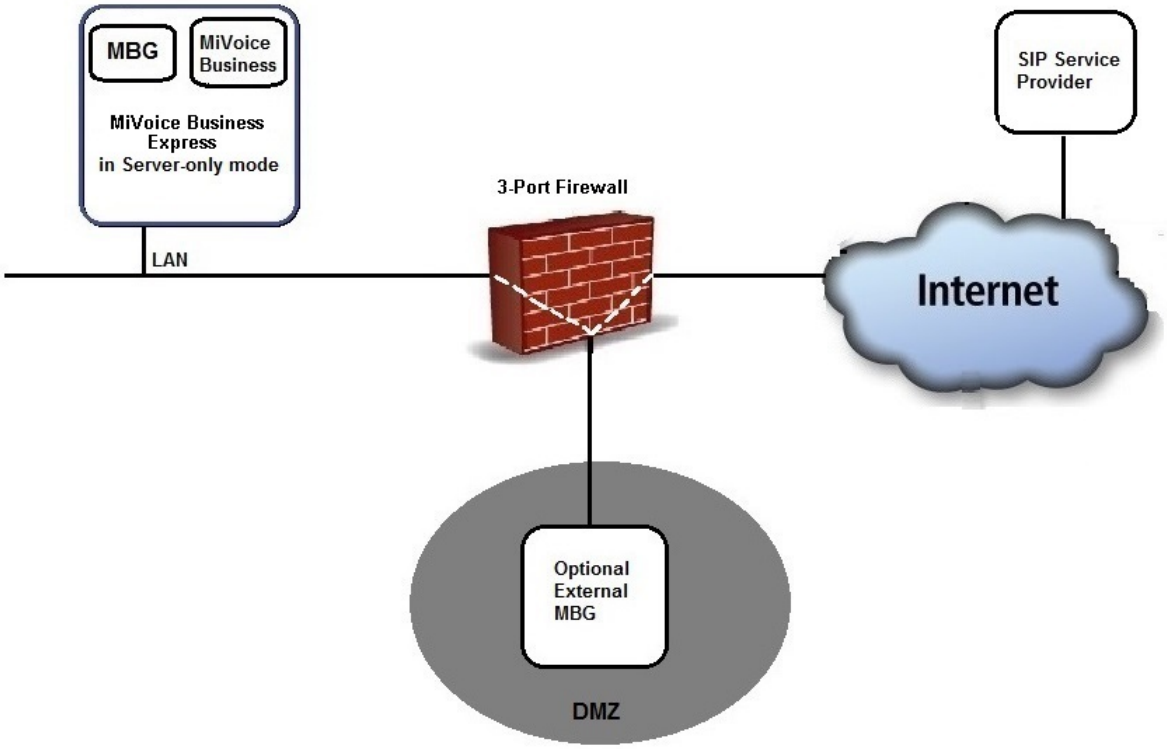

Figure 4: External SIP Proxy

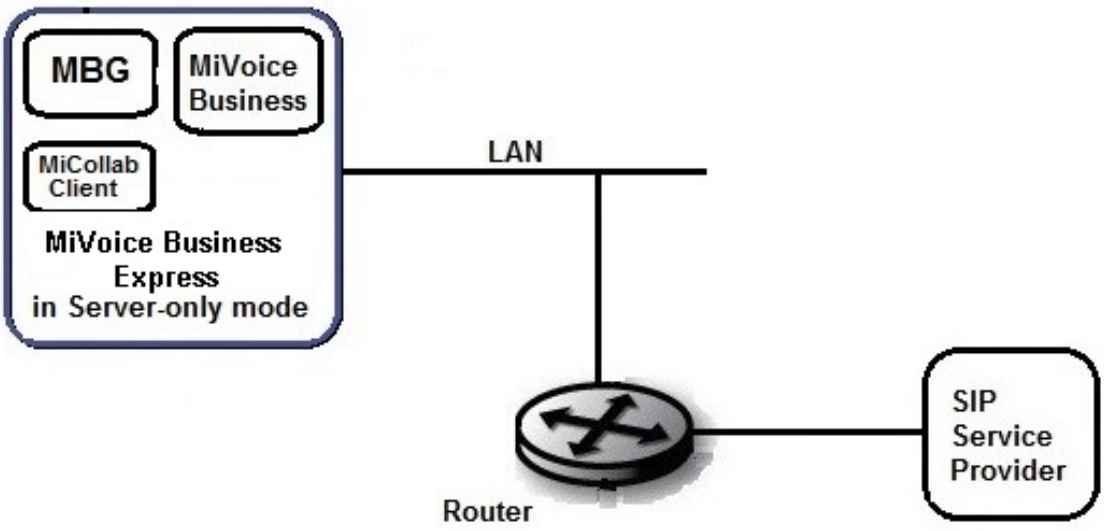

Figure 5: No SIP Proxy

CONFIGURATION OF SIP PROVIDER VIA A SESSION BORDER CONTROLLER

You can connect a MiVoice Business Express that is deployed in server-only mode to an external Session Border Controller. A Session Border Controller (SBC) is an external server provided by your SIP Provider that controls the signaling and media streams involved in setting up, conducting, and tearing down SIP calls. During initial configuration, you enter the IP address or hostname of the external Session Border Controller in the SIP Provider panel of the Initial Configuration Wizard (ICW).

Note: Do not confuse the external Session Border Controller with the MiVoice Border Gateway.

Figure 6 shows a deployment configuration with an external Session Border Controller. In this configuration, an external MBG is deployed in series with the External Session Border Controller to perform Keypad Markup Language (KPML) digit detection for mid-call features.

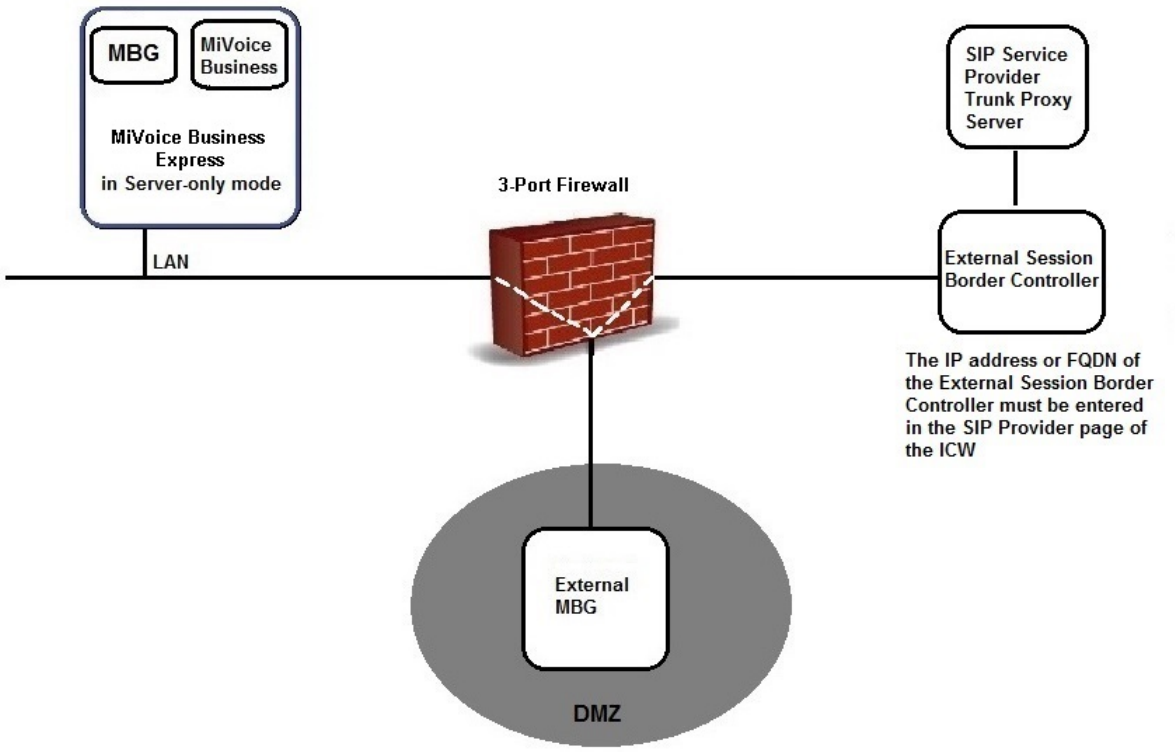

Figure 6: SIP Provider via a Session Border Controller

FIREWALL CONFIGURATION

EXTERNAL FIREWALL

The configuration of MiVoice Business Express through the use of a firewall is supported. The following configuration rules apply when deploying MiVoice Business Express behind a firewall:

Teleworker sets cannot be deployed on the LAN.

- Users who have Collaboration Client mobile clients that are deployed on the WAN behind MBG using an LTE network cannot bring their phones into the office and connect their mobile clients to a WIFI network.
- The firewall must provide static 1:1 Network Address Translation (NAT) between an externally-visible address and the WAN address of MiVoice Business Express.
- The firewall must preserve the TCP and UDP port numbers in packets exchanged between the MiVoice Business Express and the external network. In other words, only the address field may be changed
- The public Wide Area Network (WAN) address used for MiVoice Business Express must be a static IP address visible from the external network (Internet). This should be a separate address from the external IP address of the firewall, although some firewalls that support port forwarding may allow sharing the address. It is vital that this address be static because any change to this address will cause remote sets to lose connectivity.

FIREWALL CONFIGURATION FOR APPLICATIONS

A MiCollab deployment requires a suitable firewall that can provide the necessary port mapping for the packaged applications. Required Firewall features are as follows:

- Stateful Inspection or Dynamic Packet Filtering
- DMZ support
- SIP Aware
- VPN Support

The MiCollab server firewall is enabled by default in server-only mode. Therefore, the server firewall rules must be configured to allow all local networks (or "trusted networks") to have access to the MSL server. See the MSL Installation and Administration Guide for more details on how to configure local networks on MSL.

Note: It is very important that you restrict access to the MiCollab server as much as possible to ensure the highest level of security. See MiCollab Client Port Usage on page 47 for a table of the ports.

NETWORK EDGE INFRASTRUCTURE CONFIGURATION REQUIREMENTS

SYSTEM IP ADDRESSES

In Network Edge mode, MiVoice Business Express requires four IP addresses (see Figure 7):

Two IP addresses on the private network (LAN)

- MSL LAN network interface IP address (IP1)
- MiVoice Business IP address (IP2)

Two IP addresses on the public network (WAN):

- MSL WAN network interface IP address (IP3)
- AWV port 443 IP address (IP4)

DNS CONFIGURATION FOR THE WEB PROXY

About Split DNS

A split DNS setup is one where a single domain is split into two "zones" – an internal zone and an external zone. Internal hosts are sent to an internal DNS server for name resolution and external hosts are sent to an external DNS server. The same DNS query produces different results depending on the source of the request.

Split DNS set-up for the Web Proxy

An example of a split DNS entry for the web proxy is show in the table of Figure 7. The following rules apply:

- External DNS must be programmed to resolve requests for vucc.mitel.com to the public IP address of MiVoice Business Express on the WAN (IP3 in Figure 7).
- Internal DNS must be programmed to resolve requests for vucc.mitel.com to the private IP address of MiVoice Business Express on the LAN (IP1 in Figure 7).
- Firewall is configured to perform Network Address Translation (NAT) between the organization public network and the provider public network. See Table 5 on page 49 for details.

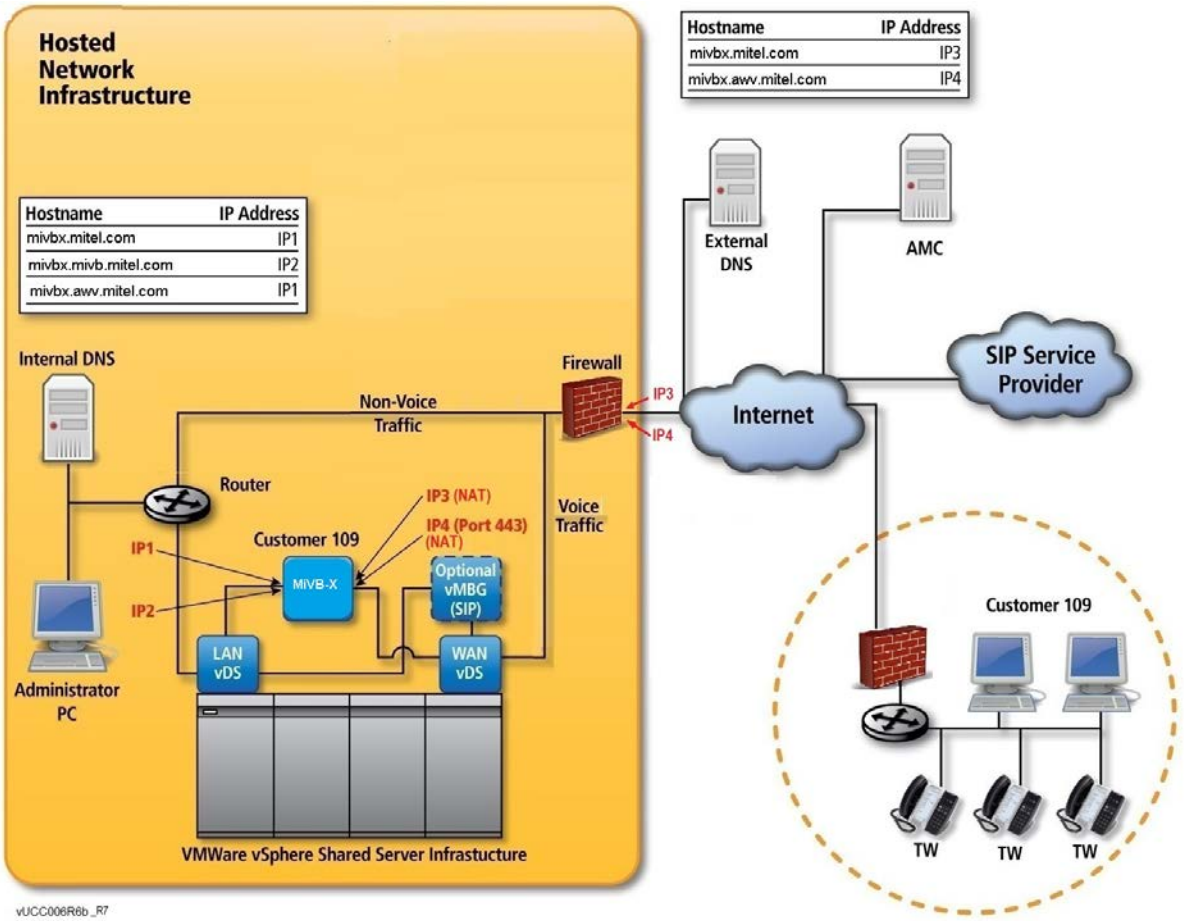

Figure 7: IP Address and DNS Settings (Network Edge)

Note: The DNS server must be set-up to support reverse DNS lookup for the MiCollab Client Service application.

AWV with Web Proxy DNS Settings

The AWV application has special IP network configuration requirements. A web browser can request a web page (for example, server manager) or a Connection Point (for file sharing). Both of these web browser requests are made on port 443. To separate the two types of requests using port 443, the MBG firewall within MiVoice Business Express must have two IP addresses (one IP address for accessing the MBG server manager remotely, a second IP address for web collaboration client communication to the Connection Point).

MSL firewall rules are programmed to forward traffic from the second IP to a programmed port on the Web Proxy (default 4443). The Web Proxy within MBG then forwards the traffic to port 4443 on the MiVoice Business Express server. Internal and external DNS must be programmed to resolve requests for AWV Connection Point traffic to the second IP address on the corporate firewall.

LAN MODE (SERVER ONLY) INFRASTRUCTURE REQUIREMENTS

SYSTEM IP ADDRESSES

In LAN mode, MiVoice Business Express requires two IP addresses on the private network (LAN):

- MSL LAN network interface IP address (IP1)
- MiVoice Business IP address (IP2)

DNS CONFIGURATION FOR LAN MODE

Figure 8 shows a typical DNS configuration for a MiVoice Business Express that is deployed in LAN mode (server-only). Note that the internal MiVoice Business Express MBG and the external MBG must be clustered for management purposes. When Teleworker devices are provisioned in the Users and Services application of the MiVoice Business Express, they are automatically provisioned on the external MBG.

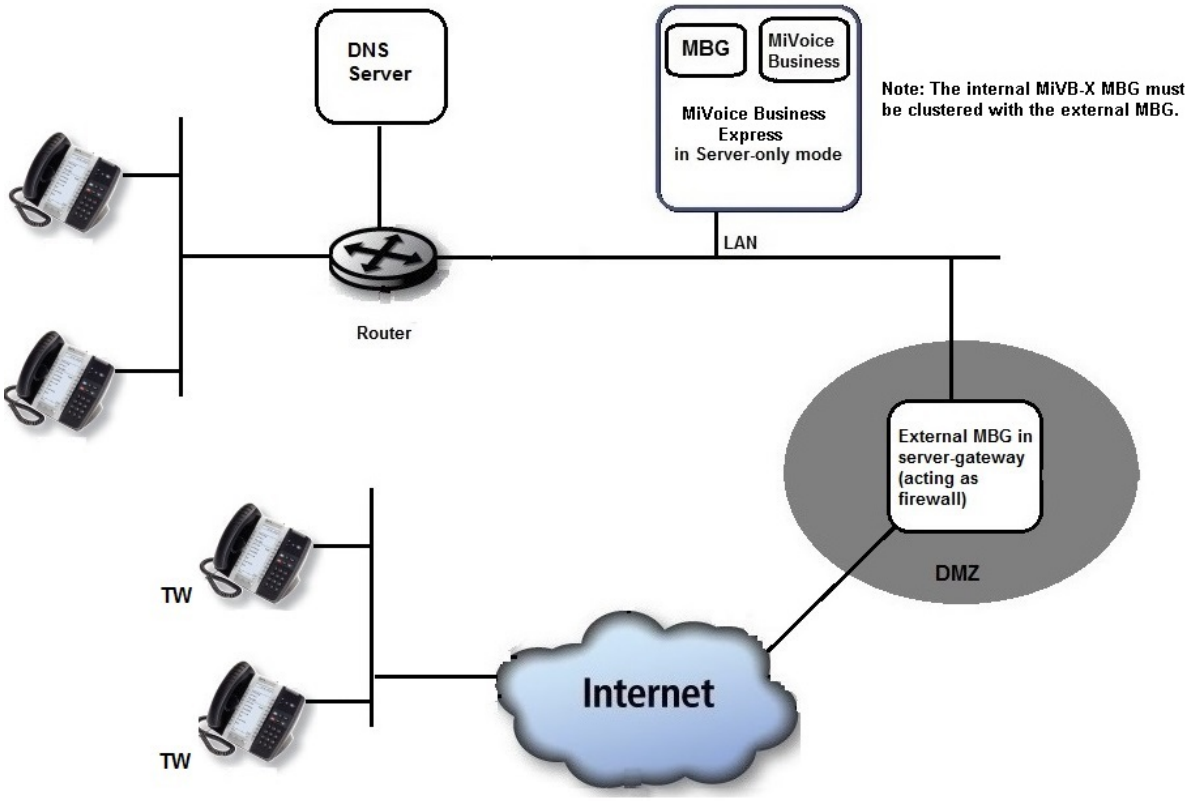

Figure 8: Typical DNS Configuration for LAN Mode

OPTIONAL LAN INTERFACE

MiVoice Business Express supports an optional third LAN interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.

The additional LAN network allows MiVoice Business Express to be deployed in network topologies where the SIP Service Provider can only be reached through a private network rather than through the Internet. In this deployment, the MiVoice Border Gateway (MBG) internal SIP Proxy redirects the SIP traffic flow to the optional LAN network while maintaining separate network connectivity to the internet to support Teleworker IP phones and remote applications.

Figure 9 and Figure 10 show examples of Network Edge and LAN Mode deployments with optional LANs.

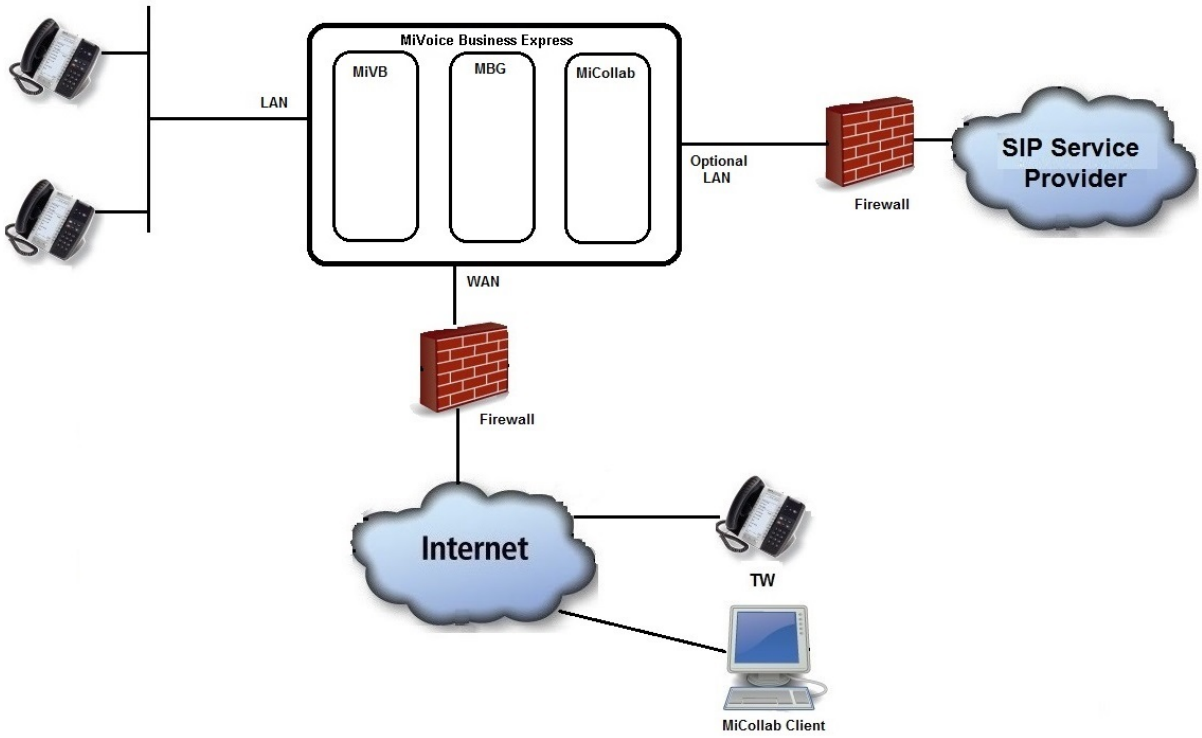

Figure 9: Deployment in Network Edge Mode with Optional LAN

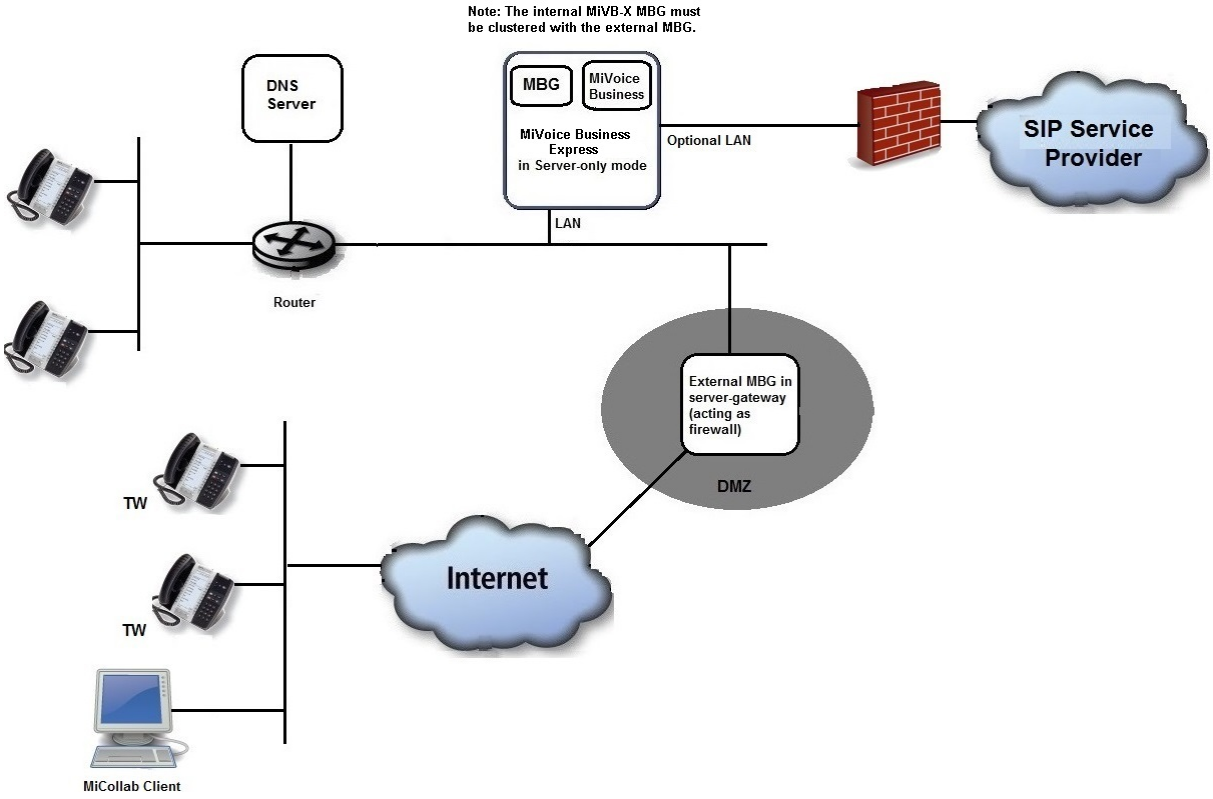

Figure 10: Deployment in LAN Mode with Optional LAN

SURVIVABLE GATEWAY DEPLOYMENT TOPOLOGIES

This section describes three survivable gateway deployment topologies:

- **Trunk Survivability**: If the trunk services from the SIP Service Provider fail, the MiVB trunking gateway in the customer environment provides the MiVoice Business Express users with trunk access to the PSTN.
- **Private Network** Survivability: If the MiCV appliance deployed in the cloud environment goes out of service, the MiVB controller located in the customer environment provides users with telecommunications services.
- **Public Network Survivability**: Normally, Teleworker IP Phones are supported by the MiCV MBG application in the cloud. If the MiCV appliance deployed in the cloud environment goes out of service, the Teleworker IP phones are redirected to the on-premise MBG and are serviced by a MiVB secondary controller.

LICENSE REQUIREMENTS

Survivable gateway topologies are only supported with Enterprise base kits. They are not supported with the MiCollab w/Voice Business base kits. An Enterprise base kit is required to set up IP trunking between the MiVoice Business (MiVB) component in the MiCV and the MiVB trunking gateway or MiVB controller located on the customer premise.

TRUNK SURVIVABILITY TOPOLOGY

Figure 11 shows a typical deployment topology for survivable trunking. In this topology, MiCV is deployed in the vCloud environment behind vCNS acting as a firewall. Access to the public telephone network is provided through a SIP Service Provider via the Internet.

A MPLS network infrastructure extends the customer's local area network (LAN) into the cloud network environment. IP phones and applications deployed on the customer's premise are serviced by the MiCV in the cloud environment.

A MiVoice Business (MiVB) trunking gateway is deployed at the customer premise to provide local PSTN access in the event of a SIP Service Provider outage. The gateway connects to the MiVB application in the MiCV appliance via IP trunking.

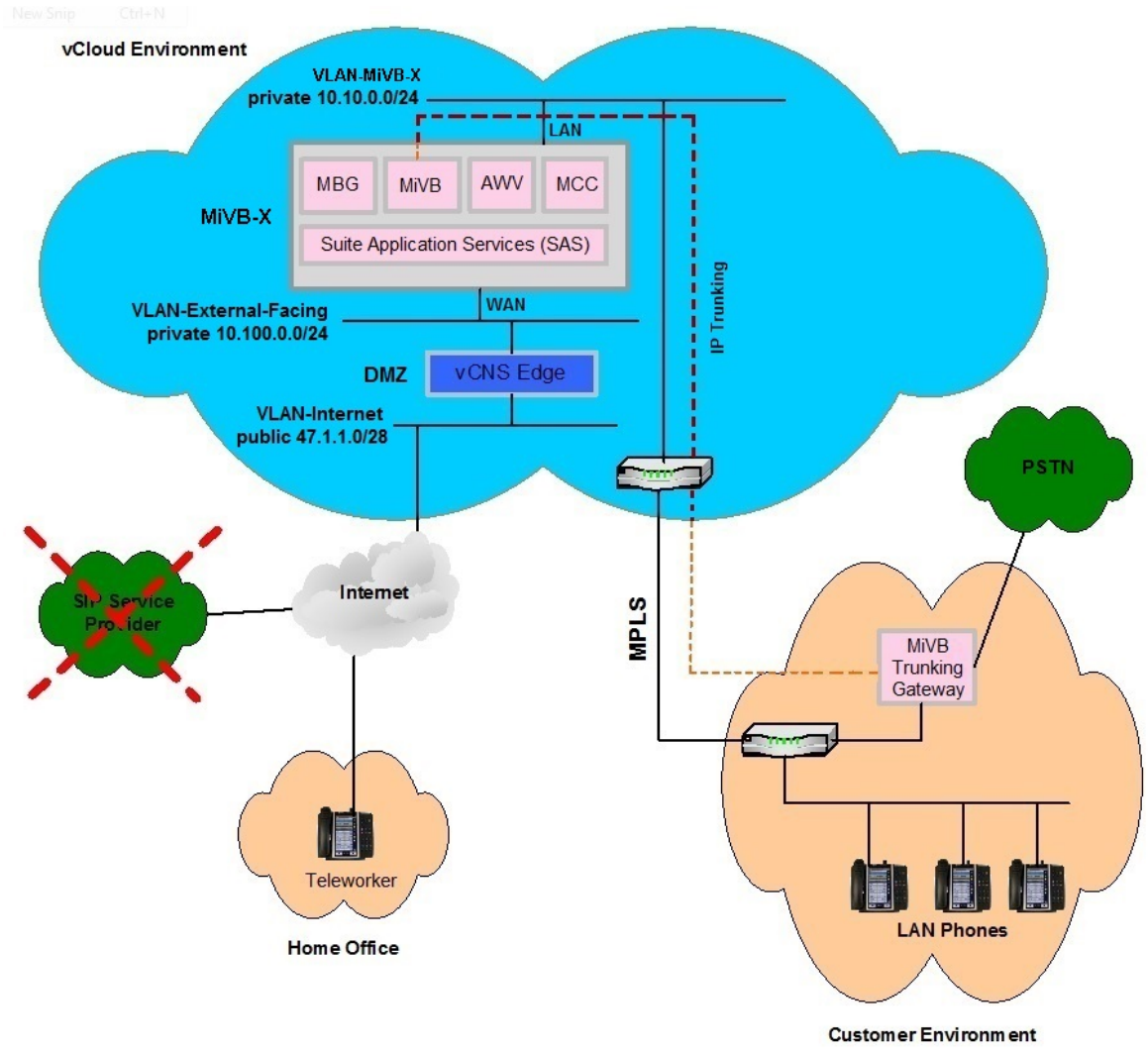

Figure 11: Trunk Survivability Deployment Topology

Trunk Survivability Deployment Conditions

- MPLS network connectivity is required between the customer and cloud environment.
- No MiVB resiliency between the two sites. VMWare High Availability only.

- Optional SIP trunking resiliency is available from the SIP Service Provider (not shown in Figure 11: Trunk Survivability Deployment Topology).
- If the SIP Service fails, outgoing calls are routed to the PSTN via the on-premise MiVB Trunking Gateway.
- The MiVB Trunking Gateway that is deployed on-premise is an existing MiVB system or partner purchased.
- On-Premise PSTN connectivity may vary from SIP, PRI, BRI or a POTS line.
- It is possible to co-locate the MiVB Trunking Gateway in the data center.
- All users must be configured through the MiCollab Users and Services application interface.
- The amount of trunking traffic flowing through the IP Trunking channel between MiVB in MiCV and the MiVB Trunking Gateway should not exceed the maximum of simultaneous connections supported by MBG.

Trunk Survivability Configuration Requirements

To configure a survivable trunking topology:

Note: Technicians must complete the MiCV Advanced Training prior to deploying this topology.

1. Set-up the network infrastructure as shown in Figure 11.
2. Deploy the MiCV OVA in the vCloud Environment using one of the MiCV Enterprise license base kits.
3. Provision the MiCV system using the Initial Configuration Wizard.
4. Provision the IP trunking between the MiVB application in the MICV and the MiVB Trunking Gateway. A route lists will need to be provision in the MiVB in MICV, to support a failover over IP trunking to the MiVB (MCD) Trunking Gateway PSTN. Refer to the MiVB Resiliency Guidelines and the MiVB System Administration Tool online help for details.

PRIVATE SURVIVABILITY TOPOLOGY

Figure 12 shows an example of the private MiCV survivable deployment topology. This deployment topology maintains telecommunication services in the event of a system outage or failure with the MiCV appliance that is deployed in the cloud environment.

The MiVB resiliency feature enables the network to maintain calls in progress, handle incoming calls, and handle outgoing calls in the event of system failure or network-level failure.

This deployment solution is ideal for mission-critical environments in which it is essential that a voice path be maintained even if the MiCV system is out of service. Resiliency is achieved through setting up a network of MiVB systems in a resilient cluster, which is a specially configured network of MiVB system that can direct IP phones and route and maintain calls.

In this deployment solution, an optional MBG can be deployed in the customer premise and work in tandem with MiVB to provide additional resiliency for Teleworker connected IP phones.

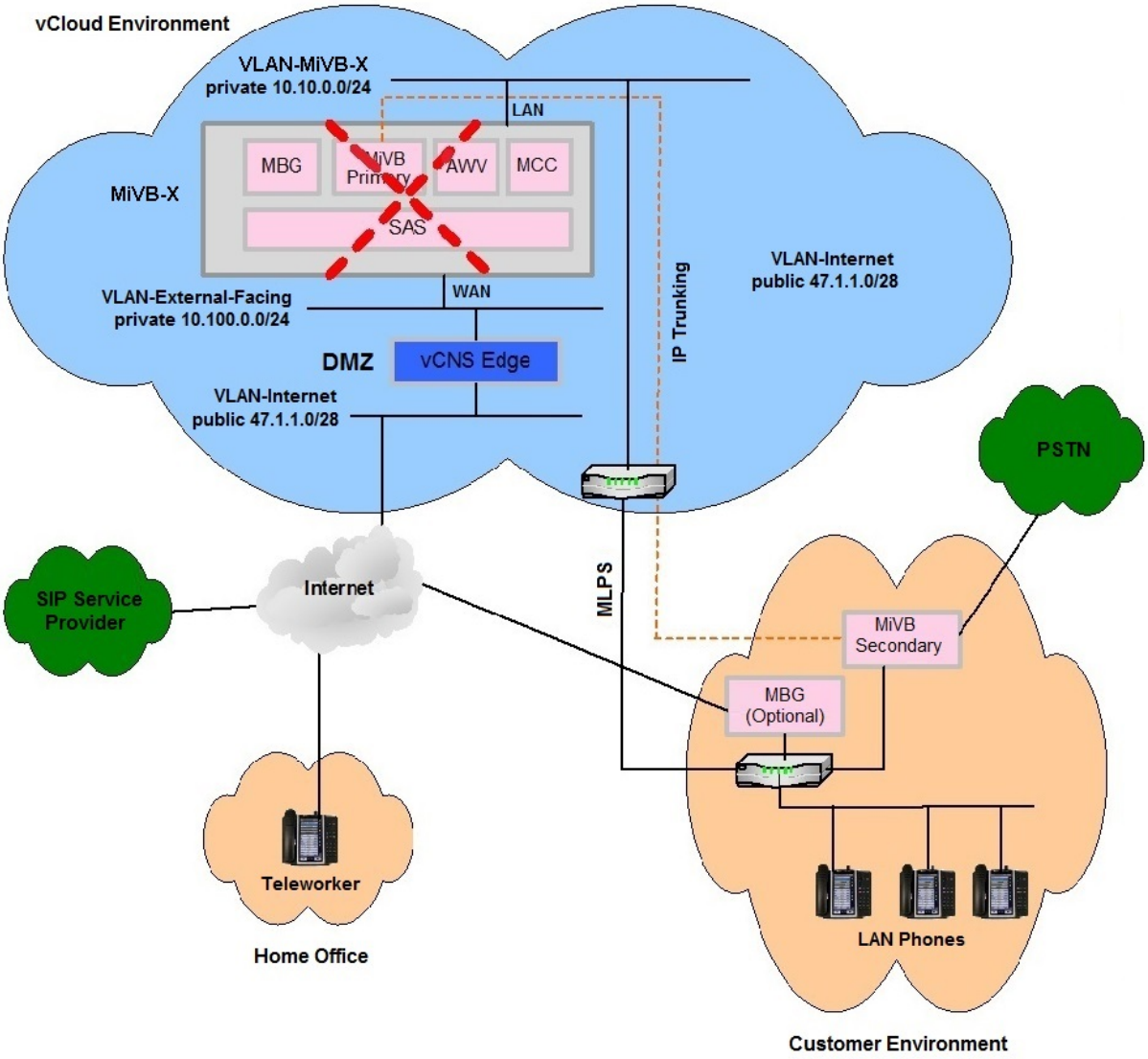

Figure 12: Private Survivability Deployment Topology

Private Survivability Deployment Topology Conditions

- MPLS network connectivity is required between the customer site and the cloud environment.
- IP phones are deployed on the on-premise LAN. Teleworker phones are deployed behind the MBG residing in MiCV
- VMware High Availability can be used in conjunction with MiVB resiliency to provide a higher Service Level Agreement (SLA) in the event of hardware failure.
- In the event of a failure, only voice services are maintained. There is no MiCollab application resiliency.
- Incoming/outgoing calls are routed to the PSTN via the on-premise MiVB secondary controller in the event of a MiVC system outage.
- The MiVB Trunking Gateway that is deployed on-premise is an existing MiVB system or partner purchased.
- On-Premise PSTN connectivity may vary from SIP, PRI, BRI or a POTS line.

- It is possible to co-locate the MiVB Trunking Gateway in the data center.
- All users must be configured through the MiCollab Users and Services application interface.
- Existing MiVB IP phone users can be migrated to UCC Basic users and exported out of an existing MiVB database and imported into the MiCV database using the Bulk User Import Tool in the MiCollab User and Services interface.
- SDS synchronizes MiVB primary controller database in MiCV with the on-premise MiVB Secondary controller database.
- The system administrator must reach-through to the MiVB system administration interface in MiCV to configure resiliency for each user.
- It is possible to deploy several local MiVB gateways to manage local trunks and resilient users.
- The administrator must ensure the E911 calls are properly routed to the appropriate Public Safety Answer Point (PSAP) in the case of a failover scenario.

System Configuration Requirements

To configure a private survivable topology:

Note: Technicians must complete the MiCV Advanced training prior to deploying this topology.

1. Set-up the network infrastructure as shown in Figure 12.
2. Deploy the MiCV OVA in the vCloud environment using a MiCV Enterprise license base kit.
3. Optionally, export the IP phone users from the existing on-premise MiVB controller(s).
4. Optionally, convert the MiVB phone users to UCC Basic Users and apply UCC user license uplift.
5. Provision the MiCV system using the Initial Configuration Wizard.
6. Set up the resiliency cluster with IP trunking between the MiVB Primary in MiCV and the on-premise MiVB gateway(s).
7. Optionally, import IP phone users using the Bulk User Import Tool in the MiCV MiCollab User and Services interface.
8. Optionally, modify the resiliency controller for each user by using the MiCV's MiVB administrator interface.
9. Optionally, cluster the MiCV MBG application with the on-premise MBG. For load balancing use a weight of 100 for the MBG in MiCV and a weight of 0 for the on-premise MBG. This will ensure that the Teleworker IP phones failback to the MBG in the cloud when the MiCV returns to service.

PUBLIC SURVIVABILITY TOPOLOGY

The public survivability deployment topology is similar to the private survivability deployment topology with the following exceptions:

- The MiCV vCloud internal LAN network extends to the customer’s private network through a VPN/IP Sec tunnel. In the vCloud environment, the VPN tunnel is created by deploying an additional vCNS Edge firewall. The firewall that is deployed on the customer premise must allow VPN tunnelling.
- Teleworker IP Phones are deployed on the customer's premise.

Some of the key benefits of using this deployment topology are

- cost savings over MPLS.
- no deployment of additional network gear in the data center.
- data center VPN connectivity is available through vCloud vCSN Edge

Figure 13 shows a typical public survivability deployment topology. During normal operation, the Teleworker IP phones are connected to the MBG component in MiCV in the cloud. If the MiCV in the vCloud environment goes out of service, the Teleworker IP phones are redirected to the MBG on the customer premise and are supported by the MiVB secondary controller.

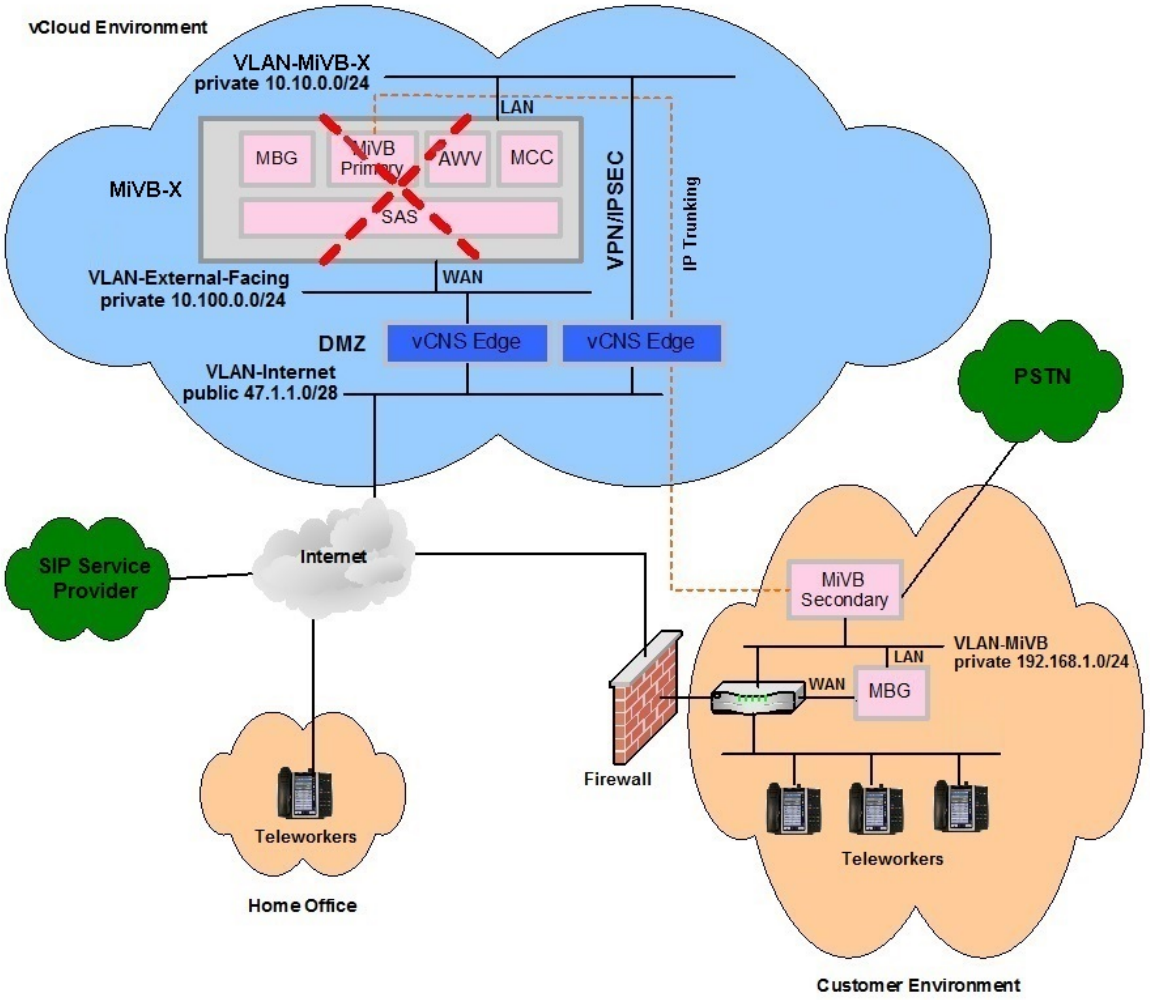

Figure 13: Public Survivability Deployment Topology

Public Survivability Deployment Topology Conditions

- VPN/IPSec network connectivity is required between customer and cloud environment.
- IP Trunking and System Data Synchronization (SDS) traffic between the MIVB component in MiCV and the MiVB (MCD) secondary controller is carried over the VPN/IPSec connection.
- MBG cluster heartbeat is configured through the WAN rather than the VPN/IPSec connection.
- Teleworker IP Phones are only deployed in the customer environment.
- VMware High Availability can be used in conjunction with MiVB resiliency to provide a higher Service Level Agreement in the event of hardware failure.
- In the event of a system outage, only voice services are maintained. There is no MiCollab application resiliency.

- In the event of a system outage, incoming and outgoing calls are routed to the PSTN via the on-premise MiVB secondary controller.
- The MiVB secondary controller that is deployed on-premise is an existing MiVB controller or partner purchased.
- On-Premise PSTN connectivity may vary from SIP, PRI, BRI or a POTS line.
- It is possible to co-locate the MiVB Trunking Gateway in the data center.
- All users must be configured through the MiCollab Users and Services application interface.
- Existing MiVB IP phone users can be migrated to UCC Basic users and exported out of an existing MiVB database and imported into the MiCV database from the Bulk User Import Tool in MiCollab User and Services interface.
- SDS synchronizes the MiVB primary controller database in the MiCV with the on-premise MiVB secondary controller database.
- The system administrator must reach-through from the MiVB secondary to the MiCV MiVB system administration interface to configure resiliency for each user.
- It is possible to deploy several local MiVB gateways for managing local trunks and resilient users.
- The administrator must ensure the E911 calls are properly routed to the appropriate Public Safety Answer Point (PSAP) in the case of a failover scenario.

System Configuration Requirements

To configure a private survivable topology:

Note: Technicians must complete the MiCV Advanced Training prior to deploying this topology.

1. Set up the network infrastructure as shown in Figure 13.
2. Deploy the MiCV OVA in the vCloud environment using an Enterprise license base kit.
3. Optionally, export the IP phone users from the existing on-premise MiVB controller(s).
4. Optionally, convert the MiVB IP phone users to UCC Basic Users and apply UCC user license uplift.
5. Provision the MiCV system using the Initial Configuration Wizard.
6. Set up the resiliency cluster with IP trunking between the MiCV MiVB primary and the on-premise MiVB gateway(s).
7. Optionally, import IP phone users using the Bulk User Import Tool in the MiCV MiCollab User and Services interface.
8. Optionally, modify the resiliency controller for each user by using the MiCV MiVB system administrator interface.
9. Cluster the MiCV MBG application with the on-premise MBG. For load balancing use a weight of 100 for the MBG in MiCV and a weight of 0 for the on-premise MBG. This will ensure that the Teleworker IP phones failback to the MBG in the cloud when the MiCV returns to service.

SURVIVABLE GATEWAY SOLUTION DEFICIENCIES

E911 Call Routing

In the event of a SIP Provider Service failure in the trunking survivable topology or a MiCV/public internet failure in the private or public survivability topologies, E911 calls are routed through the local trunking gateway or on-premise MiCV. Users typically have a CESID associated with the SIP trunks.

When they dial out the local analog trunks, that CESID will be presented. However, the analog carrier will most likely use a different PSAP/ALI database, so calls will not be identified.

To resolve this issue, use SIP trunks that do not use registration from the same SIP carrier on both the hosted and local trunk gateway. If the hosted MiCV or data connection to the hosted MiCV fails, 911 calls are routed out the local gateway SIP trunks, providing that the SIP trunks have a working public internet connection.

However, note that if more than four 911 survivable gateways are required, then ARS becomes complex because the MiCV has a maximum of six entries in the route list form.

Public Survivable Topology Internet Failure

In the event of an Internet connection failure, the Teleworker IP phones deployed in the customer environment may not be able to reach the on-premise MBG due to the fact that the Teleworker IP phones use a public Internet IP which may be routed by an external router to reach the on-premise MBG.

External firewall and routers must be configured to allow on-premise Teleworker phones to reach the on-premise MBG in the event of Internet connectivity failure.

Unexpected MiCV component failure

MiCV is comprised of several software components which may fail and restart. In the public survivable topology deployment, the MiVB and MBG components work together to provide services to the Teleworker IP phones that are deployed in the customer environment. If one of these components unexpectedly fails, a failover occurs. It would be ideal if both components failed together to provide a unique failover scenario where all Teleworker IP sets are re-directed to the on-premise MBG and to the MiBV for services. These additional failover scenarios may result in unexpected traffic when the MBG components within the MiCV communicate with the on-premise MiVB through the VPN/IPSec tunnel.

It is expected that a single component failure within MiCV will cause a failover. However once that component has restarted, a failback should take place such that all services are restored to the hosted environment.

Incoming call re-routing from SIP Service Provider to local PSTN

To have incoming calls re-routed to the local PSTN (PRI, BRI, Analog Trunks, SIP) via the on-premise MiVB during a hosted MiCV failure, special arrangements must be made with the SIP service provider. This would also be required to support an E911 emergency callback.

MIVB-X VOICE RESILIENCY SUPPORT

The MiVoice Business Express resiliency solution provides:

- **Device resiliency** - A secondary ICP/MiVoice Business system provides call control services in the event of a failure in the MiVB component of the MiVoice Business Express system or in the event of a networking failure between the phones and their primary system.
- **Call resiliency** - Calls in progress are maintained if the primary system (MiVoice Business Express) goes out of service.
- **Feature resiliency** - Many features are resilient and are available to devices while they are in service on the secondary ICP (MiVoice Business) system. Note that some of these features may behave differently when the devices on the secondary system.
- **ACD resiliency** - Resiliency is supported for hotdesk ACD agents. Resiliency is not supported for traditional ACD agents and ACD Express Groups.
- **Multi device group resiliency** - Multi device groups (MDUGs) are resilient. Support for the MDUG passes to the secondary ICP/MiVoice Business if the primary fails.

- **Flow Through Provisioning** - The Users and Services application within the MiVoice Business Express allows you to provision resilient devices on the primary system. SDS shares the user information between the primary and secondary.
- **SIP Trunking resiliency** - SIP trunking resiliency is supported through the MiVoice Business Gateway component within the MiVoice Business Express.

Note: MiVoice Business Express application resiliency is not supported.

RESILIENCY LICENSING REQUIREMENTS

Installers must create separate, distinct licences (Application Record IDs) for the MiVoice Business Express and the MiVoice Business secondary controller in the Application Management Center (AMC). Also, Enterprise base software part numbers must be assigned to both the MiVoice Business Express server and the MiVoice Business server.

In this licensing construct, the Designated License Manager (DLM) cannot be used to share licenses between the MiVoice Business components. Also the MiVoice Business secondary controller ARID cannot be placed in the ULM group of an ARID that is being used by the MiVoice Business Express.

BASIC RESLIENT MIVB-X CLUSTER

Figure 14 shows the topology of a basic resilient MiVB-X cluster:

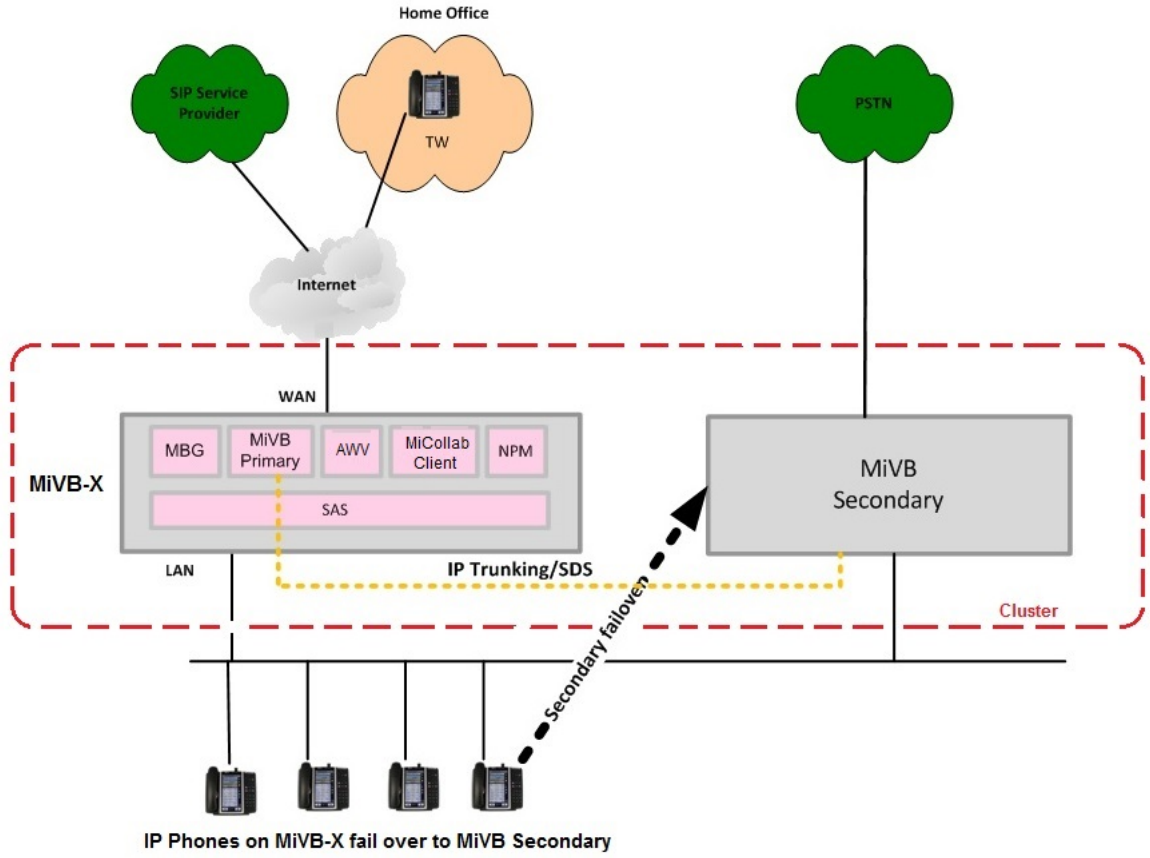

Figure 14: Basic MiVB-X Resiliency deployment

In the event of a primary system outage, phone services are transferred from the primary and secondary MiVoice Business Express systems as well as the maintenance of calls in progress ensures that most system failures are not noticed by desktop users.

MiVB-X resiliency is primarlily an IP-enabled capability that uses existing MiVB clustering and call routing. Existing MiVB clustering techniques are used to set-up a cluster, which is then made resilient through the programming of boundary nodes, transit nodes, and call routing ARS.

The following conditions apply to this resilient configuration:

- The secondary controller is an existing 3300 ICP or a virtual MiVoice Business system. It is connected to the PSTN through PRI, BRI, or LS trunks. It might also share a connection to the SIP Provider with the primary.
- The MiVoice Business primary component within MiVoice Business Express is cluster with the external MiVoice Business system.
- System Data Synchronization is enabled and sharing data between the MiVoice Busness Express system and the MiCollab.
- IP trunking is set-up between the primary and the secondary controller.This provides some trunking resiliency in the event of a SIP Provider failure.
- All IP Phones are registered to the MiVoice Business primary component within MiVoice Business Expres over the LAN or an MPLS connected network.
- If the MiVoice Business Express goes out of service, the IP Phones failover to the MiVoice Business secondary controller.
- During the outage, users can originate and receive calls through the PSTN via the MiVoice Business secondary. Special arrangements must be made with the SIP provider to have calls routed to the PSTN in the event of a failure with the MiVoice Business Express.
- Under normal operation calls are only answered from the primary MiVoice Business component in MiVoice Business Express.
- Teleworker IP Phones located on the Internet are not resilient.
- The MiVB-X applications are also non resilient.

MIVB-X HEADQUARTER WITH MIVB BRANCH SITES

In hosted Service Provider deployments, you might have the main office MiVoice Business Express connected through a MAN to one or more branch office sites. These branch sites can part of a resilient cluster at the main office and have corporate PSTN access while also retaining PSTN access to a local MiVB controller. In this way, branch site(s) can continue to operate independently and retain PSTN services for things like emergency in the event of the LAN/MAN link to the main office.

This is also advantageous for sites that want to concentrate their network at the main office or headquarters and retain the options of including branch offices (local or remote) in their main resilient cluster..

MIVB-X TELEWORKER PHONE AND SIP TRUNK RESILIENCY

The following deployment blueprint provides Teleworker phone in addition to LAN Phone resiliency. For hosted deployment, the deployment of LAN phone resiliency is optional.

This deployment is achieved by deploying a pair of MiVoice Business Express systems and clustering the MiVoice Business and MiVoice Business Getwa as shown in Figure 15

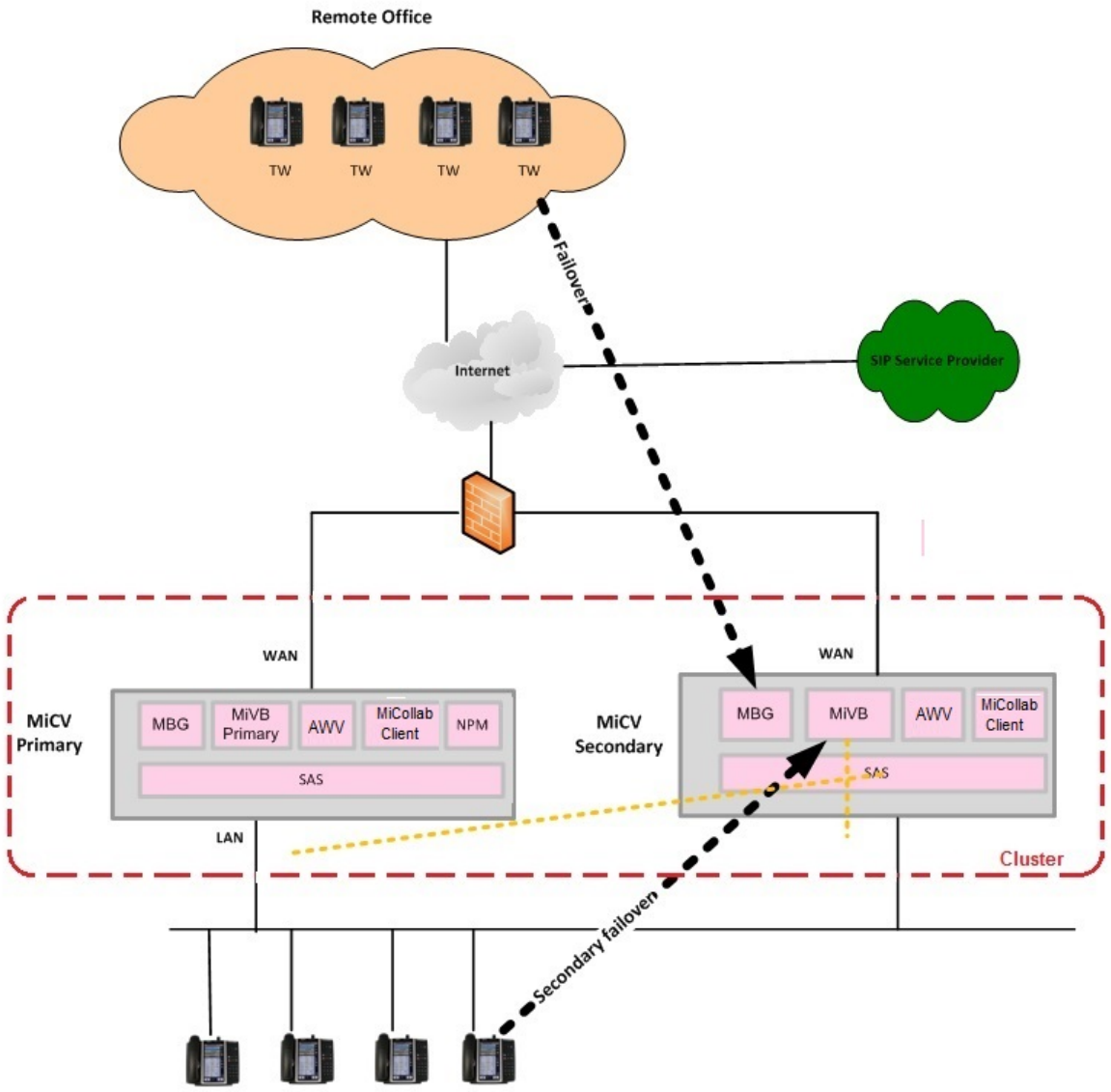

Figure 15: MiVoice Business Express Teleworker Phone Resiliency

The following conditions apply to this resilient configuration:

- The MiVoice Business components within the primary and secondary MiVoice Business Express are clustered.
- System Data Synchronization is enabled and sharing data between the two MiVoice Business systems and the primary MiCollab.
- The MiVoice Border Gateway component within the Primary MiVoice Business Express is clustered with the secondary MiVoice Border Gateway component.
- The Primary MiVoice Border Gateway is set-up with a cluster weight of 100%, while the secondary MiVoice Border Gateway has a cluster weight of 0%.
- The MiVoice Border Gateway cluster health communication is configured over the internet.
- All Teleworker IP phones are registered to the primary MiVoice Border Gateway.

- In the event that the MiVoice Business Express goes out of service, the Teleworker IP phones failover to the MiVoice Border Gatway component on the MiVoice Business secondary controller and register with the secondary Mivoice Business Express.
  - During the outage, users can originate and receive calls through the SIP Service Provider via the secondary.
  - Once service is restored on the primary MiVoice Business Express, the Teleworker IP Phones will fail back to the primary MBG and register with the primary MiVoice Business Express.
  - Under normal operation calls are only answered from the primary MiVoice Business component of the MiVoice Business Express.
  - The primary and secondary MiVoice Business Express must use a distinct credential/business number with the SIP Service provider to avoid a registration overlap. In a failover scenario, incoming calls destined to the primary MiVoice Business Express are redirected to the secondary MiVoice Business Express by the SIP Service Provider.
  - Enterprise base licenses are required for both the primary and secondary MiVoice Business Express systems. The secondary MiVoice Business Express requires 1 UCC user Entry/Standard/Premium license to allow the ICW to proceed with the initial configuration.
  - User provisioning is performed from the primary MiCollab only.

MIVB-X BEHIND AN MIVB ACD AGENT GATEWAY

This configuration deploys MiVoice Business Express as a back office solution behind a MiVoice Business ACD agent gateway when the ACD requirements of a customer exceed the capacity of that which is supported by the MiVoice Business Express (maximum of 50 ACD Agents).

The customer's deployment consists of a MiVoice Business Express that supports general business users and a standalone MiVoice Business ACD Controller that supports the business's ACD agents. In this deployment, the MiVoice Business is networked back to the MiVoice Business Express to connect the two groups.

A small ACD installation with a MiVoice Business Express as the back office controller is depicted in Figure 16.

This basic call centre ACD installation uses a separate MiVoice Business ACD controller with all the trunks, agents, groups and paths configured on it. IVRs and Call Centre Management services are provided by the MiContact Center which is connected to this controller through the local network. A separate MiVoice Border Gateway handles the additional SIP trunking capacity as well as the remote teleworker ACD agents. Calls coming into the call centre from the SIP Provider are routed via the MiVoice Border Gateway to the IVR on MiContact Center and queued to a path on the MiVoice Business ACD Controller.

Additional VoiceMail and MiCollab services are provided by the MiVoice Business Express. For example, an ACD agent can be equipped with a MiCollab Client Softphone which is being serviced by the MiCollab Client component in MiVoice Business Express. MiContact Center 7.1 provides the Contact Centre *Ignite* application which integrates with the MiCollab Client. It replaces previous Contact Center Client.

Conference resources are needed in an ACD environment for Silent Monitor, Whisper Coach, and Consultation Calls by the agents. In this installation, these resources are provided on the ACD agent controller.

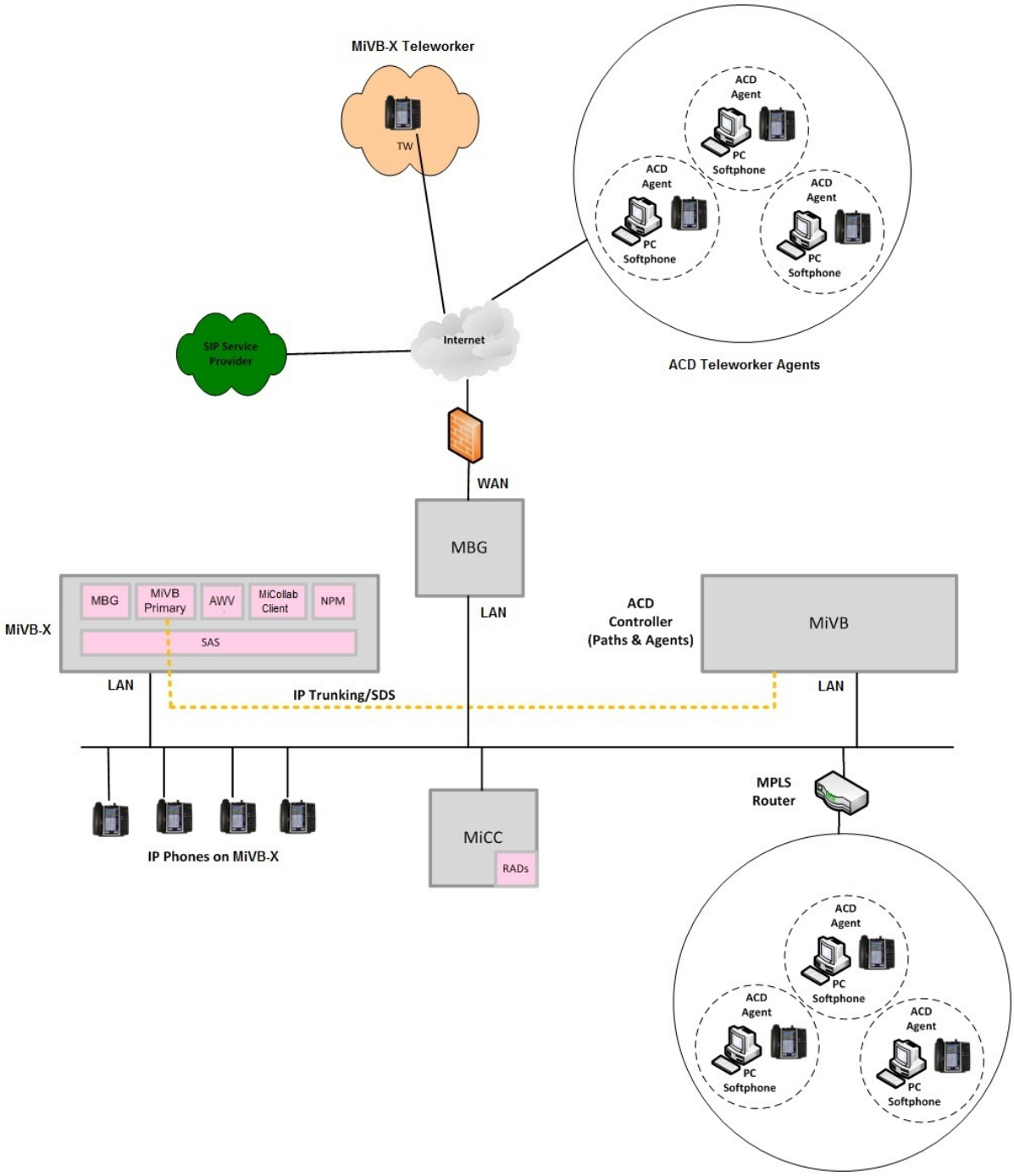

Figure 16: Example of a Small Standlone ACD Installation with MiVB-X

For larger call centre installations, use the network ACD topology that is described in the MiVoice Business Engineering Guidelines. The MiVoice Business Express is simply a node linked to this topology through IP trunking.

The following conditions apply to this ACD installation:

- All ACD agents are being serviced by the ACD Controller.
- In a hosted environment, ACD agents may be deployed as teleworker ACD agents or deployed behind an MPLS network.
- As specified in the MiVoice Business Engineering Guidelines, the trunk to agent ration is 1.5 (lower trunk ratios will increase system capacity at the expense of more rejected (busy tone) calls).
- There are additional performance impacts if you use MiContact Center to provide call handling and reporting on the ACD Controller.
- All active ACD agents must be members of a single group.
- EHDA will affect the agents and amount of traffic that can be supported by the ACD agent controller. Refer to the MiVoice Business Engineering Guidelines for more details.
- The number of Voice Mail and MiCollab Client resources being consumed by both the MiVoice Business Express and ACD Controller on the MiVB-X system should not exceed what is currently specified in the MiVoice Business Express Engineering Guideline.
- All trunk traffic between the MiVoice Business Express and the ACD Controller is carried over the IP trunk.
- The MBG component within MiVoice Business Express is clustered with the external MBG for ease of user configuration. The cluster weight needs to be set-up in such a way that most ACD agents are being serviced by the external MBG.
- MiCollab is used as the single point of user provisioning. ACD agents are provisioned on the external ACD controller through the MiCollab user provisioning interface. The MiVoice Business Express, the MiCollab application and the external ACD MiVoice Business Express Controllerare sharing data via SDS.

MIVB-X BEHIND AN MIVB TRUNK GATEWAY

In this deployment model, the MiVoice Business Express is connected using IP trunking to an existing MiVoice Business Trunking Gateway. A typical deployment configuration is shown in Figure 17.

The MiVoice Business Trunking Gateway provides access to the PSTN through PRI, BRI, SIP or LS trunks.

A similar deployment model uses a SIP trunk aggregator for multiple MiVoce Business Express nodes in the back end where each MiVoice Business Express node corresponds to a different customer entity. The main advantage of this deployment is that it localizes the management and provisioning of additional SIP trunking resource on a single node in the network.

The technician must de-program the SIP Trunking provisioning currently applied by the Integrated Configuration Wizard and then manually provision the IP trunking configuration (for example, ARS Routes, and Route Assignment) to the external MiVoice Business SIP Trunk Gateway.

As with our current reference deployment architectures, IP phones are hosted through the internal MiVoice Border Gateway within the MiVoice Business Express or they are deployed behind an MPLS network.

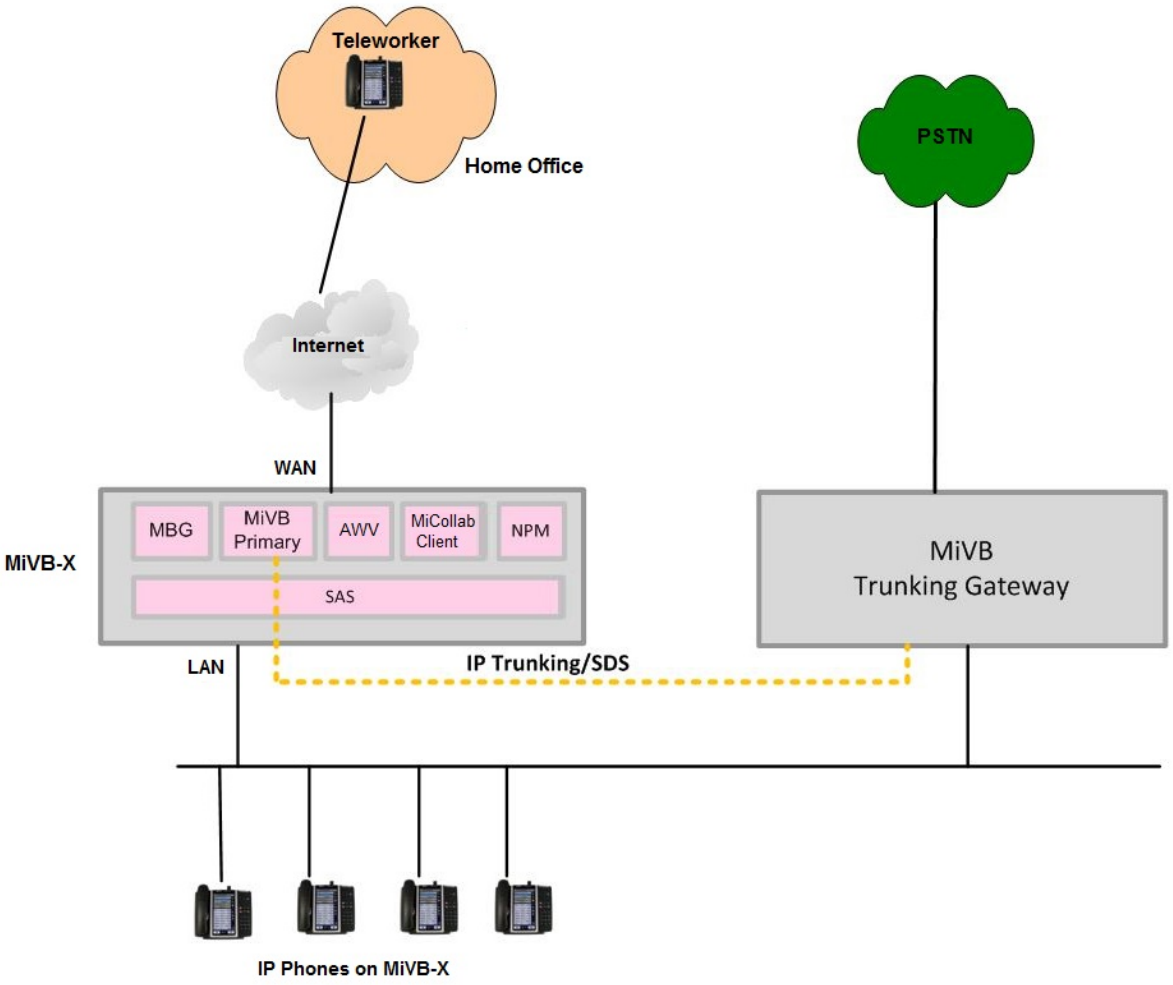

Figure 17: MiVB-X deployment behind a MiVB Trunking Gateway

The following conditions apply to this configuration:

- All IP Phones are deployed behind the MiVoice Business Express server. The MiVoice Business Trunking Gateway does not host any users or devices.
- The MiVoice Business secondary controller is an existing controller. It connects to the PSTN through PRI, BRI, or LS trunks.
- It is possible to deploy a MiVB/MBG which acts as a SIP Trunk aggregator for several MiVoice Business Express customer instances.
- The MiVoice Business components may be clustered share data to simplify management.
- As with the resilient configuration, license sharing through a DLM is not supported. Enterprise base part numbers are required. The MiVoice Business Express ARID cannot be grouped under the MiVoice Business ULM ARID for UCC user license distribution.
- There is no resiliency supported for this configuration.

COMPRESSION AND BANDWIDTH MANAGEMENT ZONE CONFIGURATION

MiVoice Business zones are used to control compression, control bandwidth management, and place sets in specific time zones. The following zone configuration is recommended for MiVoice Business Express:

- Place the MiVoice Business, MBG, and NPM applications within the MiVoice Business Express virtual machine in the same zone. Ports used by NPM are created with a default zone of 1.
- For compressed calls to SIP trunks, the Initial Configuration Wizard applies a default zone of 2 in the SIP trunk dialog to all country variants with the exception of Netherlands. The wizard applies a default zone of 1 to the Netherlands.
- In the configuration described in "Hosting Remote Office via MLPS Router" on page 7, place sets in the same configuration zone as the MiVoice Business Express virtual appliance (for example, zone 1) assuming the sets are being placed in the same time zone as the MiVoice Business.
- In the configuration described in "Hosting Remote Office using Teleworker Service" on page 8, place Teleworker sets at the customer office in a different compression zone than the UCC VA. In this case, the following types of Teleworker calls would be compressed:
  - Calls to an MiVoice Business conference bridge
  - Calls placed on Music on hold
  - Paging calls
  - Calls to the voice mail system
  - External outgoing calls made on SIP trunks
- Calls between extensions in the customer office are not compressed. Teleworker sets from two or more remote offices should be placed in distinct compression zones.
- Use zones to place sets in the appropriate time zones.Music On Hold Requirements

MUSIC ON HOLD

The Music on Hold feature requirements:

- Supported audio file format: WAV, A-law or m-law (G.711), 8 kHz, 8-bit, mono.
- Maximum available recorded audio time: 32 minutes
- Maximum number of embedded MOH files: 64

When extracting a file from a CD (for a example, from your corporate Music on Hold CD) using a CD ripper application, choose a sampling rate as close as possible to 8 kHz. This should help prevent audio distortion introduced when converting a WAV file from a high sampling rate to a low sampling rate.

PERFORMANCE AND MAXIMUM CAPACITIES

USER CAPACITY

User capacity is determined by the type and number of user licenses. Each license utilizes a specific amount of system resource. A mix of user licenses is supported up to the Small Business or Mid-Market user license resource capacity and system maximum. Use Table 1 to calculate the resources utilized for a given mix of licenses.

Table 1: User License Capacity

Number of Licenses		Resource Utilized per License		Resource Utilized per Level
____ UCC Basic IPT	x	1	=	_____
____ UCC Standard IPT	x	1.7	=	_____
____ UCC Entry	x	2.5	=	_____
____ UCC Standard	x	5	=	_____
____ UCC Premium	x	10	=	_____
____ ACD Agent	x	40	=	_____
Total Resources Utilized on System:			=	_____

System resources must not exceed the maximums below:

System	License Resource Capacity	Maximum User Capacity (see Note 1 below)	Maximum ACD Agents
Small Business	1500	500	25
Mid Market	2500	1000	50

Notes

1. The actual number of users supported may be less than the stated Maximum User Capacity because system capacity is also limited by the License Resource Capacity. For example, if only UCC Premium licenses are used, then the small business resource capacity of 1500 can only support a maximum of 150 users. See other examples below.
2. UCC Standard IPT is only offered for Service Provider market. It does not exist as a specifically defined license for premise/CPE market. This license provides basic IPT plus voicemail.
3. The maximum user capacities are based on the assumption that Teleworkers are behind the same NAT. See Table 4 for more information.

Small Business License Capacity Examples

Example 1:

50 UCC Basic IPT x 1 = 50

200 UCC Standard IPT x 1.7 = 340

150 UCC Entry x 2.5 = 375

50 UCC Standard x 5 = 250

15 UCC Premium x 10 = 150

5 ACD Agents x 40 = 200

Total resources used = 1365 (less than maximum capacity of 1500)
Total users = 470 users (less than 500 maxium)
Total ACD agents = 5 (less than maximum of 25 agents)
Configuration is supported.

Example 2:

50 UCC Basic IPT x 1 = 50

250 UCC Standard IPT x 1.7 = 425

100 UCC Entry x 2.5 = 250

100 UCC Standard x 5 = 500

10 UCC Premium x 10 = 100

7 ACD Agents x 40 = 280

Total resources used = 1605 (**greater than** maximum capacity of 1500)
Total users = 517 users **(greater than** 500 maxium)
Total ACD agents = 7 (less than maximum of 25 agents)
Configuration is NOT supported.
In this example, you must reduce the number of licenses and users to bring them below the maximum allowable capacities.

Mid-Market Business License Capacity Examples

Example 1:

100 UCC Basic IPT x 1 = 100

100 UCC Standard IPT x 1.7 = 170

300 UCC Entry x 2.5 = 750

200 UCC Standard x 5 = 1000

20 UCC Premium x 10 = 200

5 ACD Agents x 40 = 200

Total resources used = 2420 (less than maximum capacity of 2500)
Total users = 725 users (less than 1000 maxium)
Total ACD agents = 5 (less than maximum of 50 agents)
Configuration is supported.

Example 2:

150 UCC Basic IPT x 1 = 150

600 UCC Standard IPT x 1.7 = 1020

200 UCC Entry x 2.5 = 500

100 UCC Standard x 5 = 500

35 UCC Premium x 10 = 350

10 ACD Agents x 40 = 400

Total resources used = 2920 (**greater than** maximum capacity of 2500)
Total users = 1085 users (**greater than** 1000 maxium)
Total ACD agents = 10 (less than maximum of 50 agents)
Configuration is NOT supported.

APPLICATION CAPACITIES

Table 2: Application Capacities for Small Business

APPLICATION	CAPACITIES	SIMULTANEOUS CONNECTIONS	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRESSION
Total Devices: 675					
NuPoint Unified Messaging	330 NP-UM voice mail users 250 Standard UM users 250 Advanced UM users 20 WebView Sessions 2 SoftFAX ports	12 (See Note 4) 2 SoftFax	10 CCS	100 sec	G.711 or G.729
MiVoice Border Gateway	150 simultaneous MBG/TW + SIP calls (See Note 4 to Note 6)	150	6 CCS (SIP) 6 CCS (TW/TW)	100 sec 100 sec	G.711, G.722, G729 with no transcoding.
Audio, Web and Video	25 AWV Audio Ports	25			G.711, G.722.1, and G.729
	25 AWV Web & Collaboration Sessions	25 (See Note 7)			
	12 point-to-point HD video integrations with AWV	12			
MiCollab Client	500 clients (deskphones or softphones) 500 contacts	500 500			G.711 and G.722 (See Note 10)
MiVoice Business	75 simultaneous SIP trunk calls 16 conferee	75 calls 16	6 CCS (See Note 9)	100 sec	G.729 G.729

Table 3: Application Capacities for Mid Market Business

APPLICATION	CAPACITIES	SIMULTANEOUS CONNECTIONS	CENTUM CALL SECOND (CSS)	AVG HOLD TIME (SEC)	COMPRESSION
Total Devices: 1375					
NuPoint Unified Messaging	660 NP-UM voice mail users 500 Standard UM users 500 Advanced UM users 40 WebView Sessions 6 SoftFAX ports	24 (See Note 4) 6 SoftFax	10 CCS	100 sec	G.711 or G.729
MiVoice Border Gateway	300 simultaneous MBG/TW + SIP calls (See Note 4 to Note 6)	300	6 CCS (SIP) 6 CCS (TW/TW)	100 sec 100 sec	G.711, G.722, G729 with no transcoding.
Audio, Web and Video	50 AWV Audio Ports	50			G.711, G.722.1, and
	50 AWV Web & Collaboration Sessions	50			

APPLICATION	CAPACITIES	SIMULTANEOUS CONNECTIONS	CENTUM CALL SECOND (CSS)	AVG HOLD TIME (SEC)	COMPRESSION
		(See Note 7)			G.729
	25 point-to-point HD video integrations with AWV	25			
MiCollab Client	1000 clients (deskphones or softphones) 1000 contacts	1000 1000			G.711 and G.722 (See Note 10)
Mitel Communications Director	150 simultaneous SIP trunk calls 25 conferee	150 calls 25	6 CCS (See Note 9)	100 sec	G.729 G.729

Notes:

4. NuPoint ports are licensed on the MiVoice Business Express system based on the number of UCC user licenses purchased. However the Integrated Configuration Wizard (IWC) configures fewer than the actual number of licensed NuPoint ports to allow RAD configuration. Refer to "NuPoint Voicemail Port Allocation" in the MiVoice Business Express Deployment Guide for details.
5. Some types of MiVoice Business Express calls require more than one call path on the MBG. The table below identifies the number of MBG call paths required for each type of call. For example, establishing a call from a Teleworker IP phone located in remote Office A to another Teleworker IP phone located in Office B counts as two simultaneous calls from an MBG perspective.

Table 4: Number of Simultaneous MBG Calls Required

Calls From/To	Teleworker IP Phone in Office A	Teleworker IP Phone in Office B	SIP Trunk	IP Phone on LAN	+ Secure Recording Connector
Teleworker IP Phone in Office A	0	2	2	1	1
Teleworker IP Phone in Office B	2	0	2	1	1
SIP Trunk	2	2	2	1	1
IP Phone on LAN	1	1	1	0	N/A (See Note 11)
Teleworker IP Phone in the Cloud	N/A	N/A	2	N/A	1

6. If the system is supporting Teleworkers in remote offices, you should implement the following configuration to better utilize compression resources:
   - Assign compression licenses on the MiVoice Business to support TW phones using G.729 in a quick conference.
   - Enable G.729 compression on NP-UM
   - Do not use MBG transcoding licenses
   - Deploy the TW phones in remote Office A and remote Office B in different MiVoice Business zones.
   - Use local streaming at the remote office; do not use local streaming in MBG.

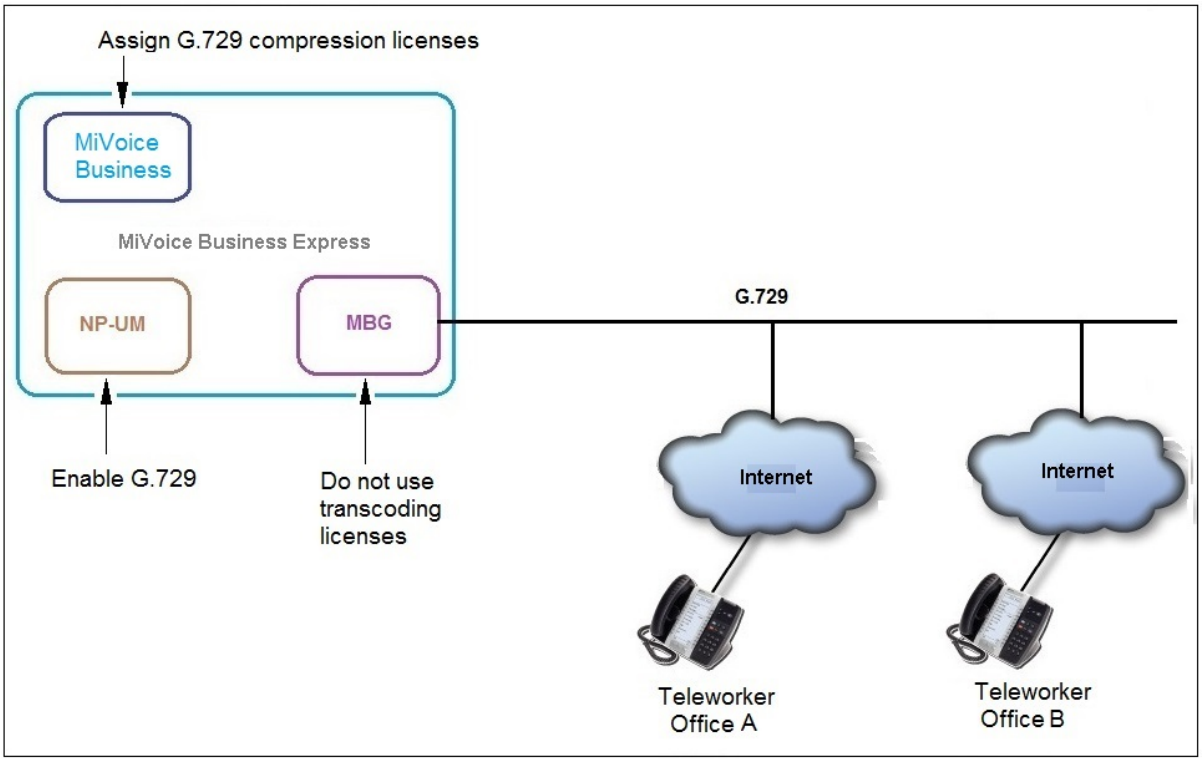

Figure 18: Recommended MiVoice Business Express Teleworker Configuration

7. If your system has both Web session licenses and HD Video integration (H.264 codec) licenses, the number of supported web sessions is equivalent to the number of HD Video integration licenses purchased.
8. Perform bulk user imports off business hours because they may cause voice degradation on calls.
9. Additional 6 CPH required for multi-device user groups.
10. MiCollab mobile clients support G.711 and G.722, but not G.722.1. However, AWV, MBG, and the Mitel deskphones support G.711 and G.722.1, but not G.722. Therefore, ensure that you enable MiCollab clients with G.711 to support interoperability across a range of devices.
11. An internal MBG cannot be used as a SRC to tap an IP Phone in a lab environment.

UPGRADE CONSIDERATIONS

- For major upgrades (for example from Release 6.0 to 6.1 or from Release 6.0 to 7.0) you must deploy a new OVA file.
- For service pack upgrades (for example from Release 6.0 to 6.0 SP1) you can install applications from the web-based server manager interface.
- For MiVoice Business Express there is no support for converting existing MiVoice Business or MiCollab installations to a MiVoice Business Express installation. MiVoice Business Express is intended for new “Greenfield” sites only.

APPLICATION SPECIFIC GUIDELINES

Refer to the MiCollab Engineering Guidelines for application guidelines.

APPENDIX A: PORT USAGE

MICOLLAB PORT USAGE

TCP/IP ports 10255, 10256, 10257, 10258, 10259, and 10260 are open on the MSL IP address. They are external ports on the MiCollab server that provide external Application Programming Interfaces (APIs) with access to the MiCollab system. APIs can be used to support management applications.

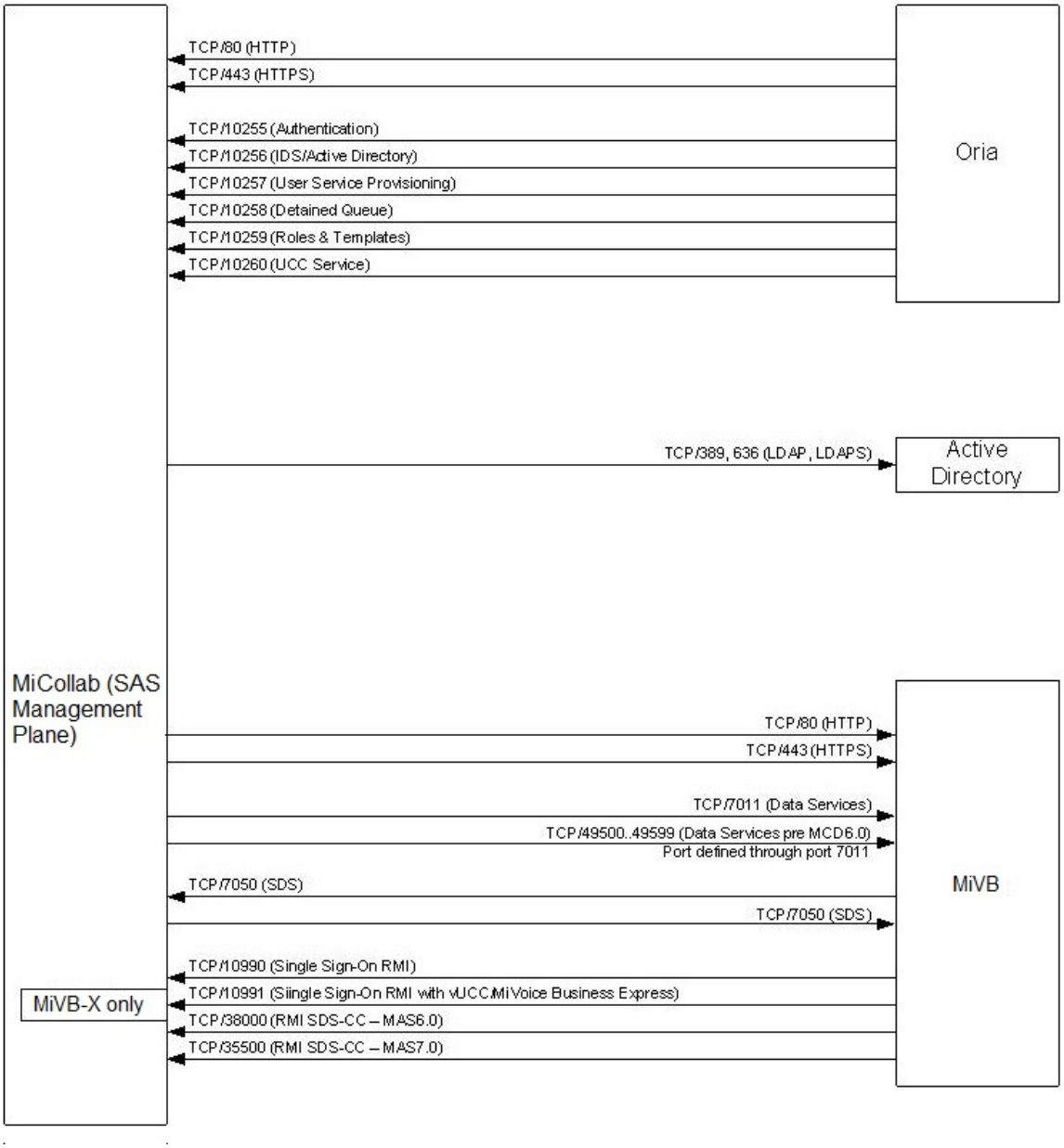

Figure 19 MiCollab Port Usage

NUPOINT UNIFIED MESSAGING PORTS

If MiCollab Server or MiCollab Virtual Appliance is connected to a MiVoice Office, you must configure port 5058 on the MiVoice Office to support SIP communication from the NuPoint application.

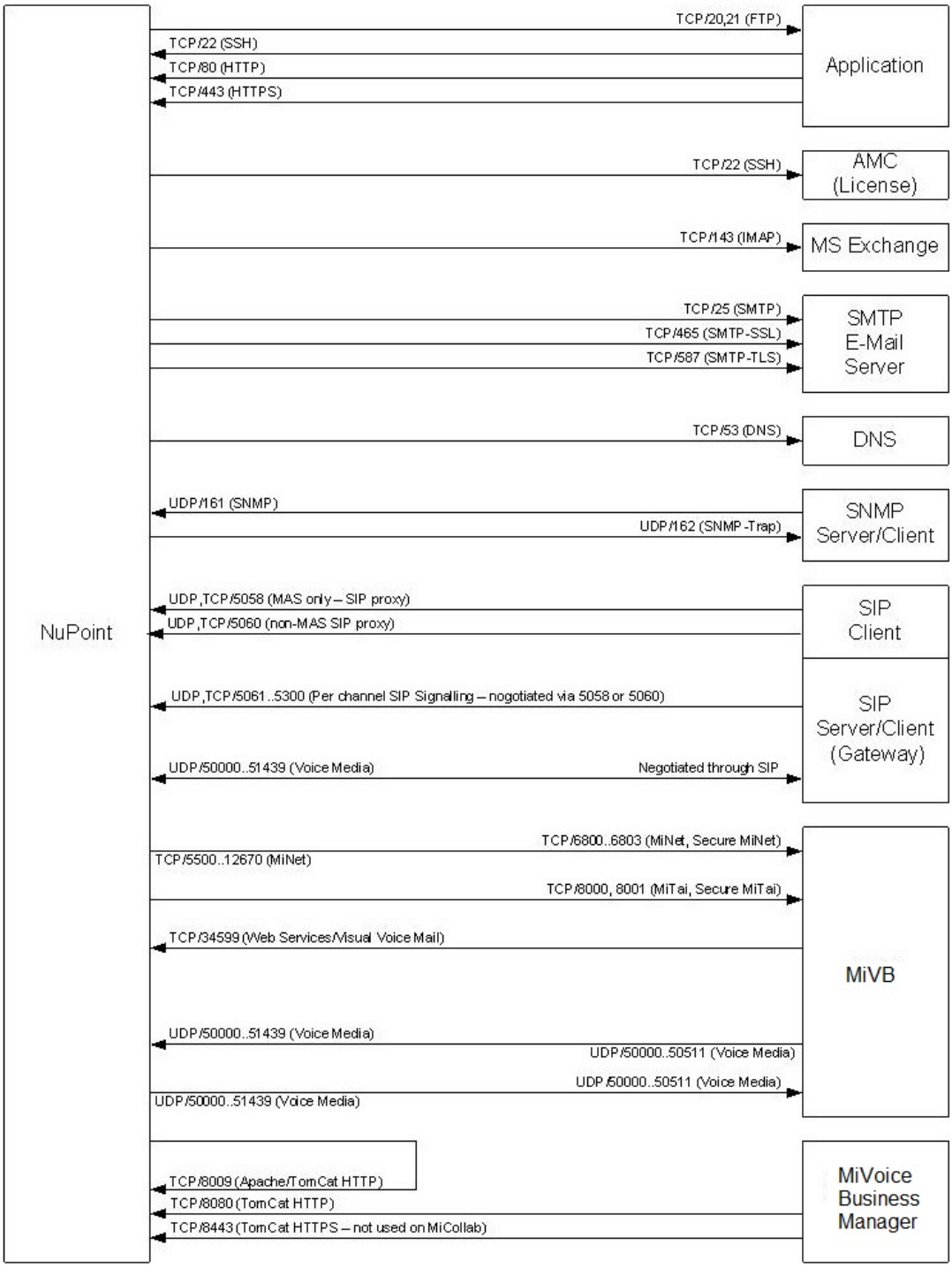

Figure 20: NuPoint Unified Messaging Ports (Diagram 1)

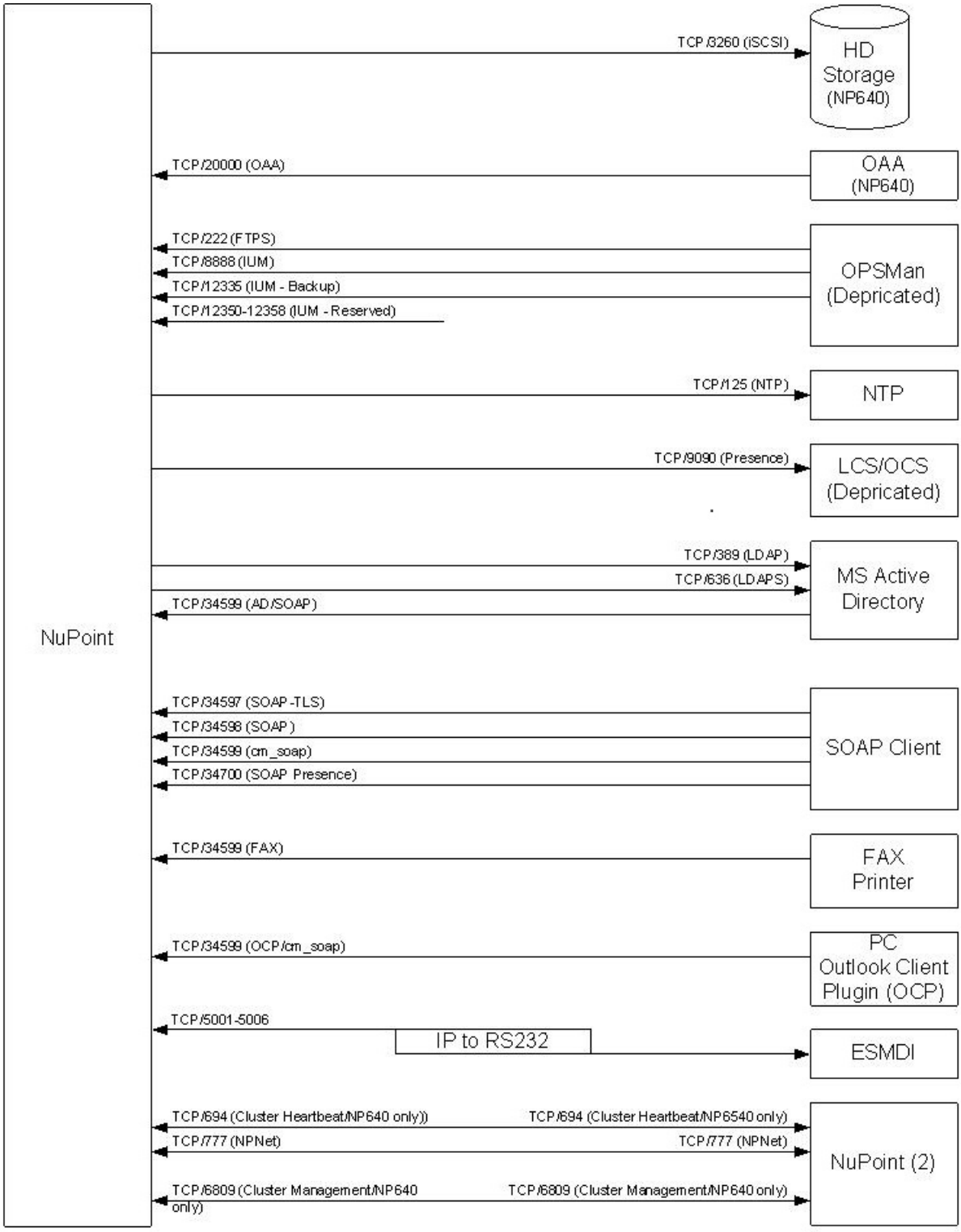

Figure 21: NuPoint Unified Messaging Ports (Diagram 2)

MIVOICE BUSINESS GATEWAY PORT USAGE

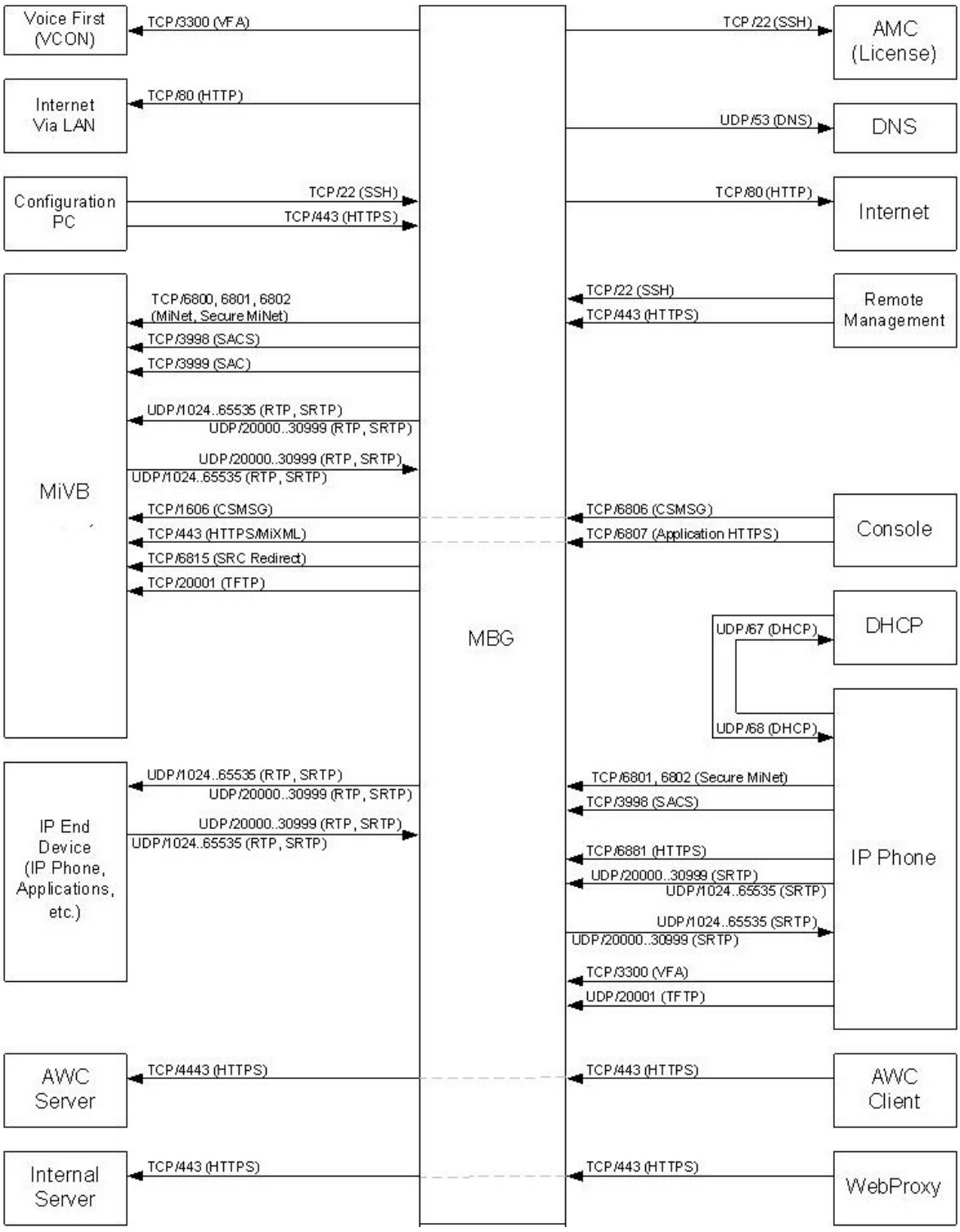

Figure 22: MiVoice Business Gateway Port Useage (Diagram 1)

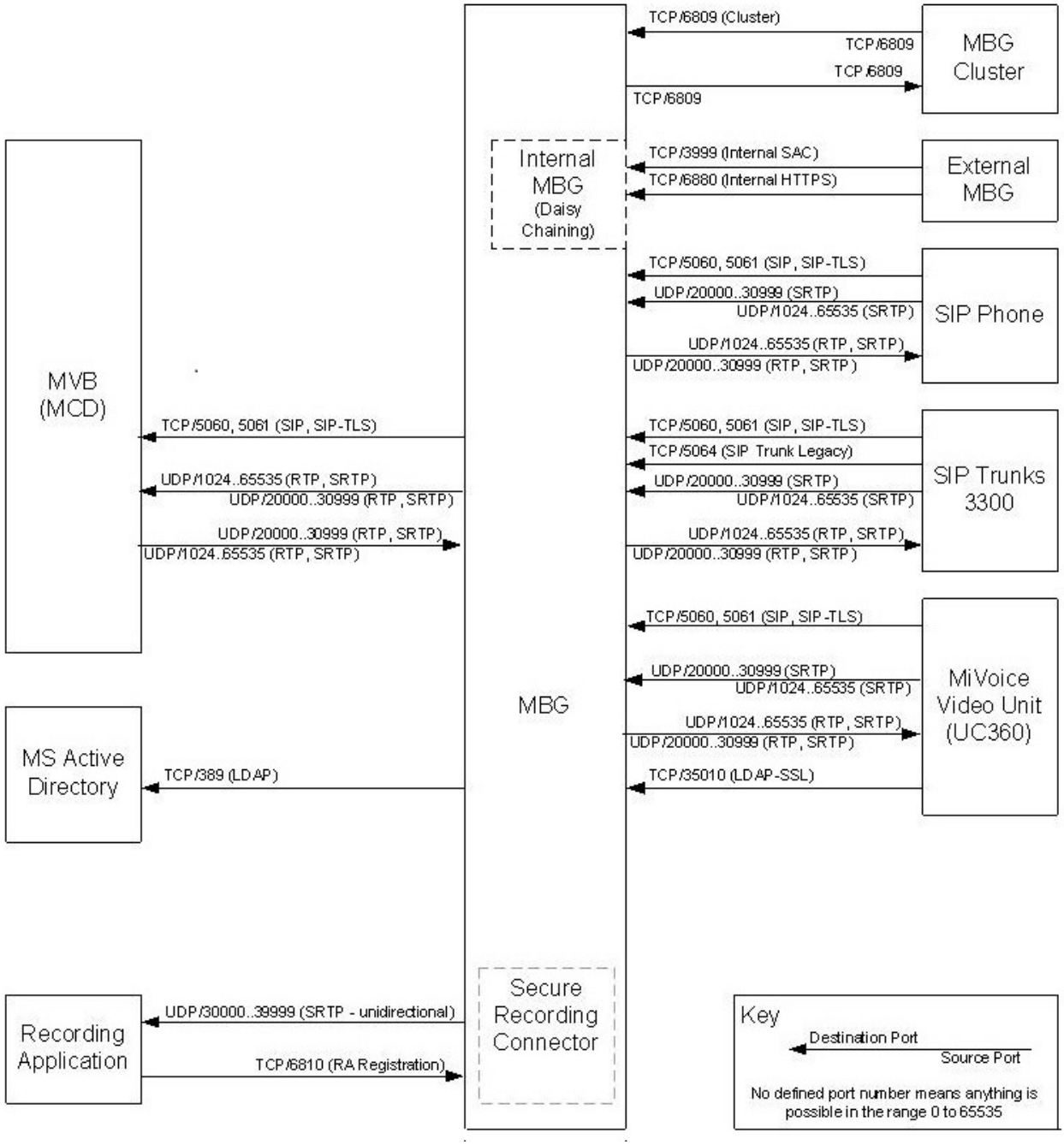

Figure 23: MiVoice Business Gateway (Diagram 2)

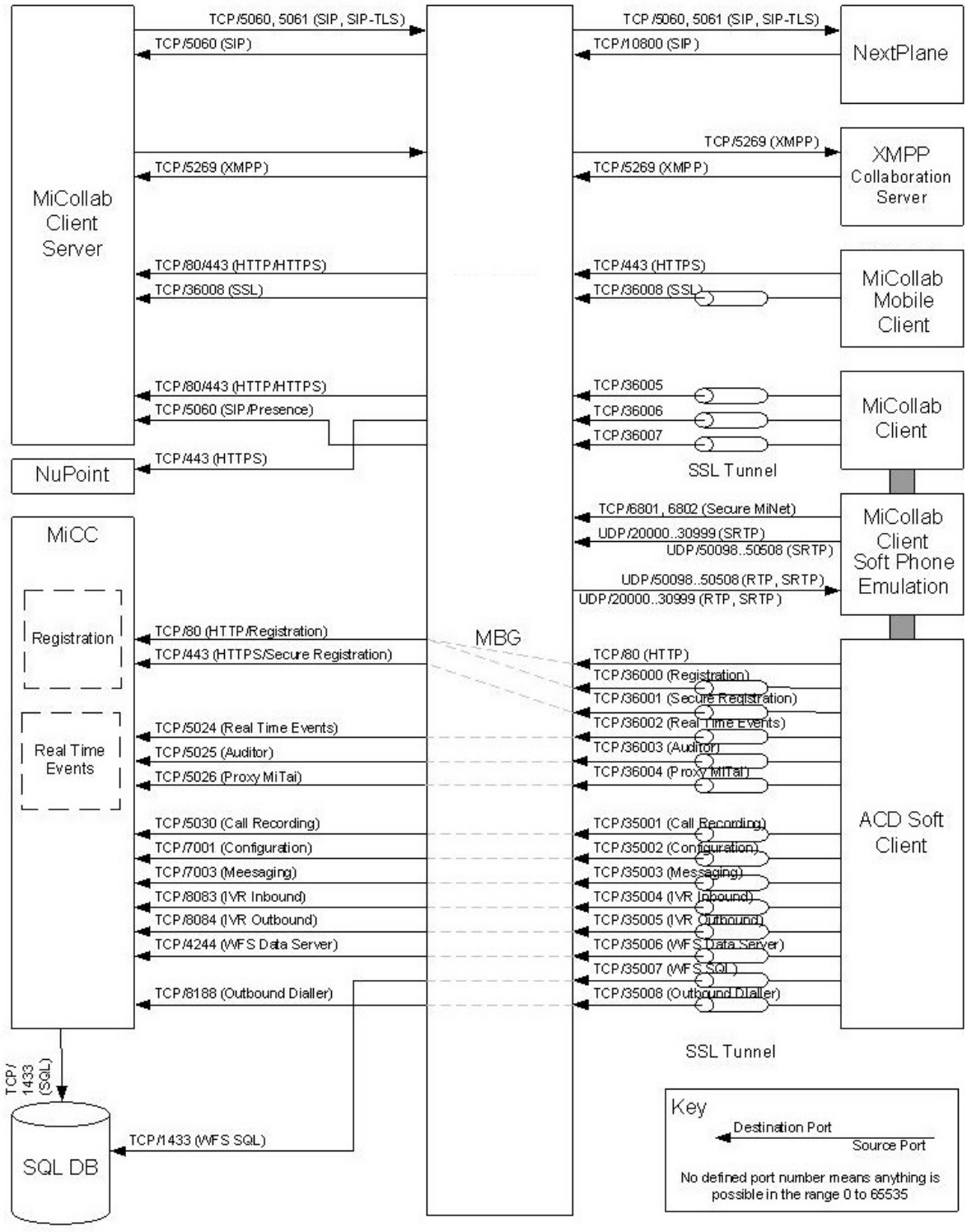

Figure 24: MiVoice Border Gateway Ports (Diagram 3)

MICOLLAB AWV PORT USAGE

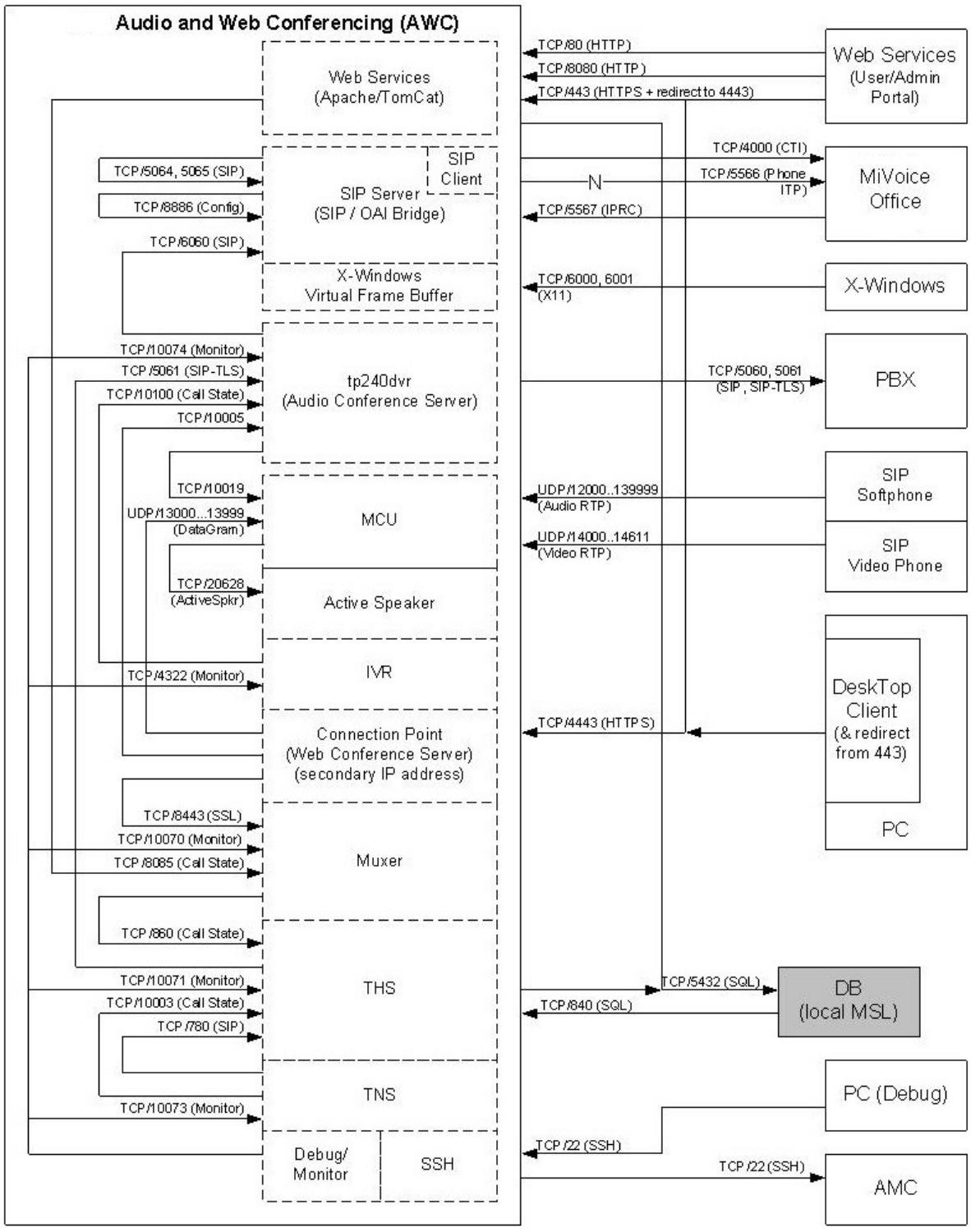

Figure 25: Audio, Web and Video Ports

MICOLLAB CLIENT PORT USAGE

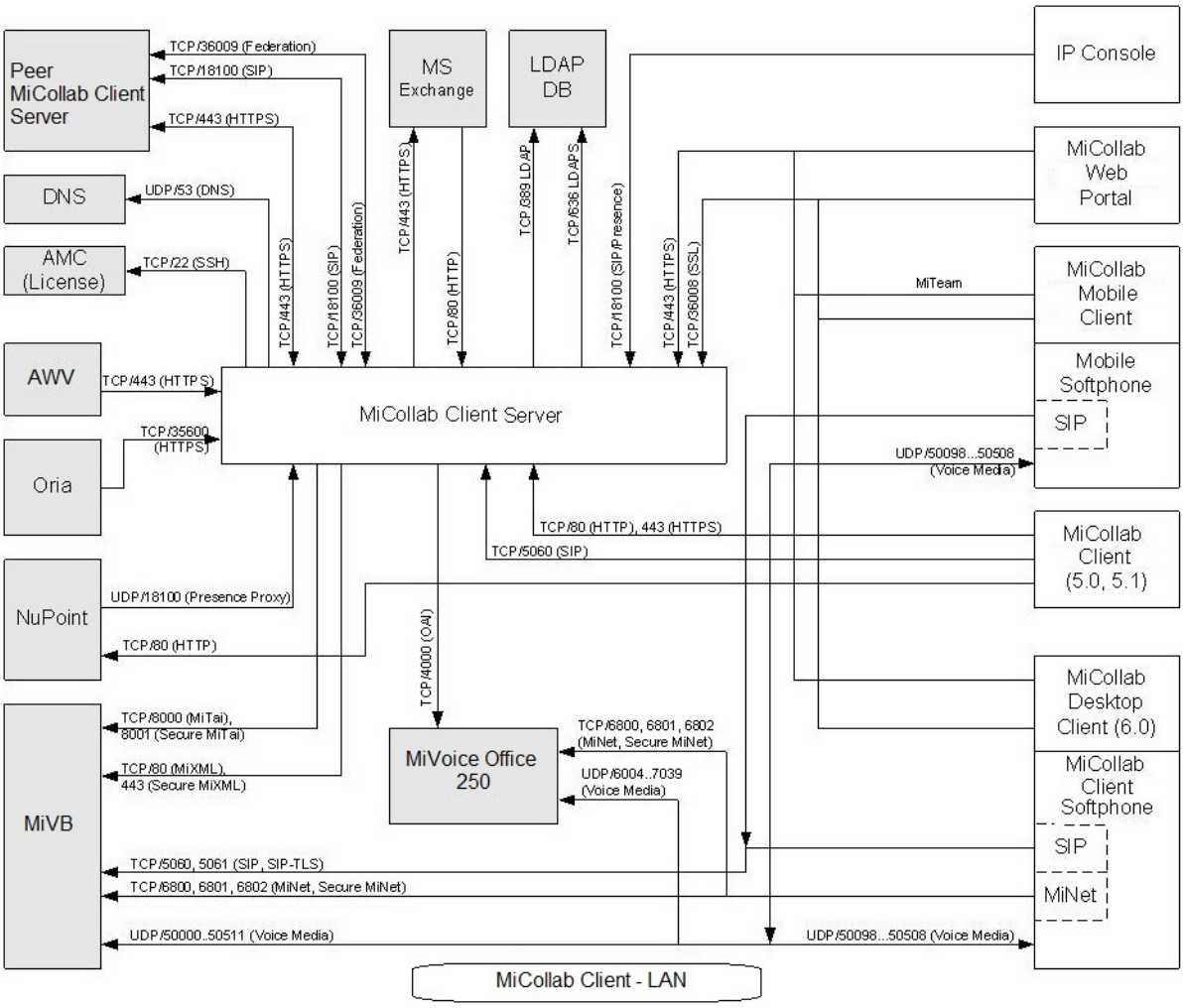

Figure 26: MiCollab Client Ports (Diagram 1)

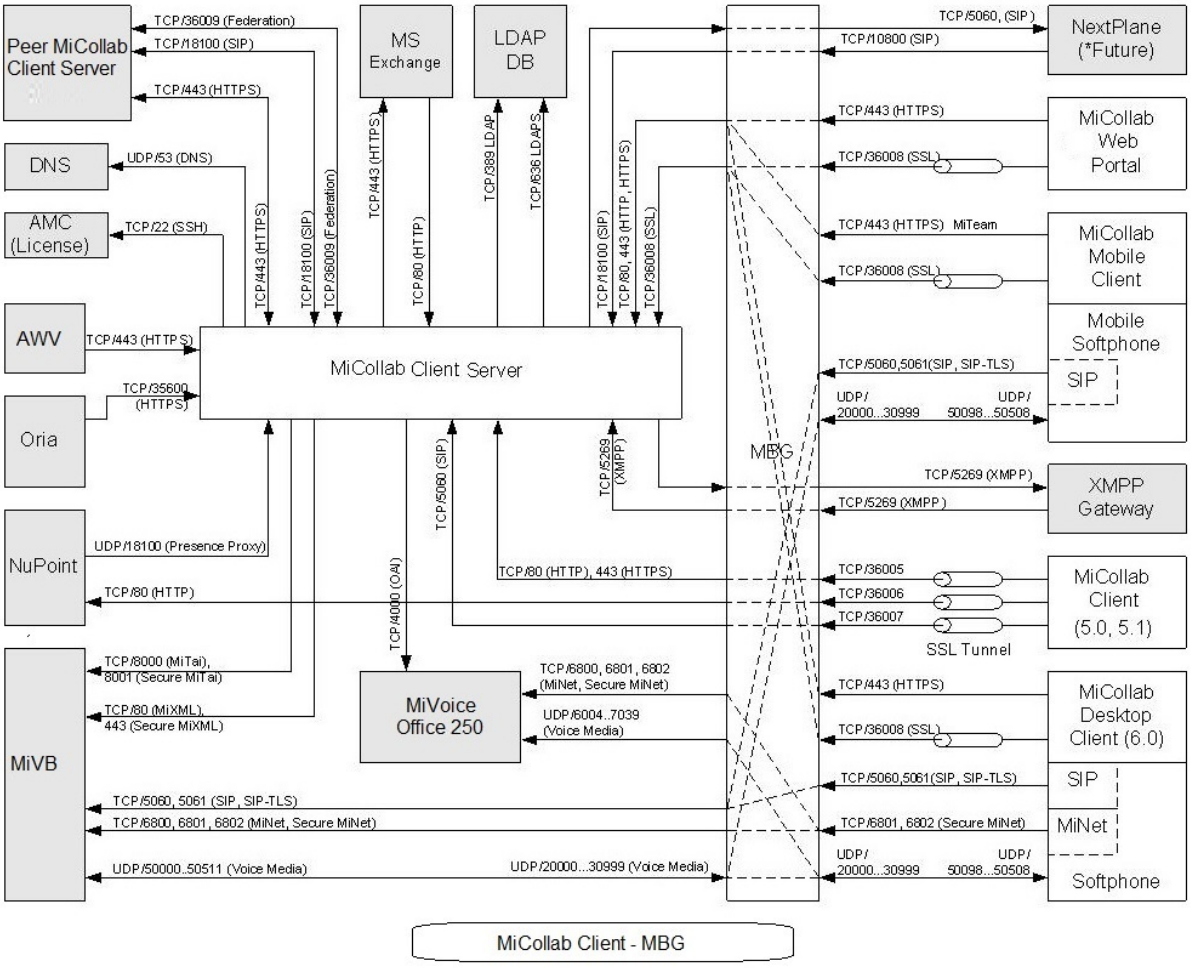

Figure 27: MiCollab Client Ports (Diagram 2)

MIVOICE BUSINESS EXPRESS PORT USAGE (FOR FIREWALL)

The information in this section is provided to allow you to configure a customer's firewall that is deployed in series with the MiVoice Business Express virtual appliance as illustrated in Figure 7 on page 14. It is assumed that the firewall is configured to perform Network Address Translation (NAT) between the organization public network and the provider public network.

In the Direction column of the following table:

- "WAN IP" refers to the organization public IP address (that is, “IP3 (NAT)” shown in Figure 7 on page 14.
- "2nd WAN IP" refers to the “IP4 (NAT)” address shown in Figure 7 on page 14.
- The arrow direction indicates permission to initiate new connections in that direction. These rules assume a firewall that will permit return traffic on an existing established connection.

Table 5: Firewall Configuration

PORT RANGE	DIRECTION	PURPOSE AND DESCRIPTION
TCP 22 (SSH)	WAN IP -> Internet	AMC Communications. Allow outbound packets (and replies) on TCP port 22 between the MiVoice Business Express and the Internet to enable server registration, software and license key downloads, alerts, and reporting.
TCP 22 (SSH)	Internet -> WAN IP	Remote SSH access (Optional). If the admin wishes to administer the MiVoice Business Express server remotely via the command line over the Internet, this rule is required.
UDP 53 (DNS)	WAN IP -> Internet	DNS. The server requires DNS to look up the IP address of the Mitel AMC and for correct operation of SIP. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the MSL Installation and Administration Guide for details.
TCP 443 (HTTPS)	Internet -> WAN IP	Remote Server Management (Optional). Allow inbound and outbound packets on TCP port 443 between the MiVoice Business Express server and the Internet to allow remote management of the server, if required. HTTPS access to the management on the external interface must also be explicitly enabled from the server manager interface. The MSL embedded firewall should be configured to limit HTTPS access to desired management hosts.
UDP 20000 to configured upper bound in Advanced tab (SRTP)	Internet -> WAN IP	Voice Communications. Allow incoming SRTP on UDP ports 20000 to the configured upper bound for Teleworker phone deployed on the WAN. Misconfiguration here is a common cause of one-way audio problems. Note that as of release 7.1, MBG defaults to using even- numbered ports for RTP, leaving the odd-numbered ports for RTCP. The Internet portion of this rule can be safely omitted in the absence of Internet traffic.
UDP 1024 - 65535 (RTP)	WAN IP -> Internet	Voice Communications. Allow outgoing SRTP on UDP ports greater than, or equal to 1024 for Teleworker phone deployed on the WAN. Misconfiguration here is a common cause of one-way audio problems. Note that as of release 7.1, MBG defaults to using even-numbered ports for RTP, leaving the odd-numbered ports for RTCP. The Internet portion of this rule can be safely omitted in the absence of Internet traffic.

TCP 443 (HTTPS)	Internet -> 2nd WAN IP	ConnectionPoint traffic (Optional). To support MiCollab AWV Conferencing through the Web Proxy, a second, dedicated WAN IP address is required for the ConnectionPoint traffic.
TCP 80	Internet -> WAN IP	Certificate Management (Optional). On any server hosting clients that make use of MiSSLTunnel with a client certificate (MiCollab Client, CIS, etc), this port must be open to the Internet to permit the web service to submit a certificate signing request (CSR), check on the status of that request, and download the certificate. Also needed for CREs to register with SRC control interface.
TCP 36008	Internet -> WAN IP	MiCollab Client Release 6.0 or later support. To permit the MiCollab Client to connect to the MiCollab Client server for presence information, this port must be permitted.
TCP 6809	Between servers in a cluster	Cluster Comms. If clustering MBG embedded in MiVoice Business Express with an on-premise MBG. Refer to Public Survivability deployment topology.
TCP 6801 and 6802	Internet -> WAN IP	MiNet Call Control. Same as above. Port 6800 should not be used on the Internet as it is unencrypted. Port 6802 is not required with an Enhanced Security deployment.
TCP 3998, 6881	Internet -> WAN IP	SAC Connection Support. Allow incoming TCP from the Internet to the MiVoice Business Express server, on ports 3998 and 6880, to support applications and web browsing, respectively, on the 5235, 5330, 5340 and Navigator sets.
TCP 80	WAN IP -> Internet	SAC Connection Support (Optional). Allow TCP port 80 from the server to the Internet, and to the LAN, to support web browsing on the 5235, 5330, 5340 and Navigator sets. Also required to the Internet to allow browsing of the Internet from the set. This is only required if the phones are deployed on the LAN.
TCP 6806	Internet -> WAN IP	IP Console Support (Optional).
TCP 6807	Internet -> WAN IP	IP Console Support (Optional).
UDP 5060	WAN IP <-> Internet	SIP Support. This port is required for non-encrypted SIP signaling between MBG and the set, and for SIP trunking support.
TCP 5060	WAN IP <-> Internet	MiCollab Client SIP TCP Support (Optional). If SIP UDP is enabled and MiCollab Client is enabled then a tcp-udp bridge connector will be enabled. Open this port for SIP signaling over TCP between MBG and MiCollab Clients that have been updated to use TCP to port 5060.
TCP 5061	WAN IP <-> Internet	MiCollab Client SIP TLS Support. If SIP UDP is enabled and MiCollab Client is enabled then a tls-udp bridge connector will be enabled. This port is required for SIP signaling over TLS between MBG and MiCollab Clients that have been configured to use TLS to port 5061 (the default client configuration).

APPENDIX B: GLOSSARY

Term	Name	Description
3300 ICP	3300 IP Communications Platform	Mitel IP communications platform supporting 30 to 60,000 users. The 3300 ICP is the hardware platform that runs the MiVoice Business (MiVoice Business) software.
AMC	Application Management Center	A web-based service that handles licensing of Mitel products
ARID	Application Record ID	An identification number obtained from the Mitel Application Management Center (AMC). Used to license software on a specific Mitel product.
BUP	Bulk User Provisioning	A software tool within the USP application that allows you to bulk import user data from a .csv or LDIF file; use Quick Add to provision a single user; program a range of fields using Auto-Fill; apply roles to multiple users; and resolve detained and failed IDS updates.
CLID	Calling Line Identification	CLID enables the telephone number of the calling party to be displayed on the display screen of the receiver's telephone. There are now a number of contact-management applications that have made it possible to use CLID to automatically bring up client information from a database and display it on the screen of a personal computer (PC) before the call is answered.
Cluster		Refers to a grouping of elements (for example, a network of MiVoice Business systems) that share common dialing plans, or common directory information, such as Remote Directory Numbers with Telephone Directory.
CO	Central Office	A switch, installed in a telephone system serving the general public, that has the necessary equipment and operating arrangements for terminating and interconnecting lines and trunks.
CODEC	En**CO**der/**DEC**oder	Software or hardware that compresses and decompresses audio and video data streams.
CPN	Calling Party Number	CPN (Calling Party Number) substitution is typically used to show the customer's corporate name and number for all outgoing calls to the public network.
Directory Server		A directory server is not simply a form of database, but a specialized server for directories. A directory can be distinguished from a general-purpose database by the usage pattern. A directory contains information that is often searched but rarely modified. Host names or user names, for example, are assigned once and then looked up thousands of times. Directory servers are tuned for this type of usage, whereas relational databases are much more geared toward maintaining data that's constantly

		changing. Another difference is that relational databases store information in rows of tables, whereas in directory server they use object-oriented hierarchies of entries.
DMZ	Demilitarized Zone	In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ.
DHCP	Dynamic Host Configuration Protocol	This is a TCP/IP protocol that automates the assignment of IP addresses of devices on a network from a central server. The DHCP server is run on the host computer and the DHCP Client is the workstation. Information given to a client includes the subnet mask, gateway address, and DNS (Domain Name Server) address.
DSL	Digital Subscriber Line	A Digital Subscriber Line provides high-bandwidth information over conventional copper wiring. The four most commonly used types of DSL are: ADSL, HDSL, SDSL, and VDSL
DTMF	Dual Tone Multi-Frequency	Tones generated typically by touch tone phones.
E2T	Ethernet to TDM	Ethernet to TDM – a system component that provides a gateway function for voice samples, between the packet domain (Ethernet) and Time Division Multiplexing (TDM) domain.
G.711	ITU-T codec audio standard	This standard specifies an audio signal that uses a 3.4 KHz bandwidth (ordinary analog voice signal) over an A-law and µ-law digitized, linear PCM at 64Kbps. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.
G.729	ITU-T standard	This standard describes CELP compression where voice is coded into 8-kbps streams. The two variations of this standard (G.729A and G.729A Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.
ICP	IP Communications Platform	MiVoice Business IP Communications Platform
IDS	Integrated Directory Services	Synchronizes user and service data between a corporate directory server and the MiCollab-IDS using the Lightweight Directory Access Protocol (LDAP).
IPSect	Internet Protocol Security	A set of protocols for encryption of IP traffic over the Internet through virtual private networks (VPNs).
ISP	Internet Service Provider	An organization that provides users with an Internet connection.
IVR	Integrated Voice Response	Interactive Voice Response is an automated call handling system in which the caller interacts with a computer device which can interpret and react to voice or touch tone commands. The interaction can be through the use of a touch tone telephone or

		through speech recognition. This telephone-based application prompts the inbound caller for information using a recorded or synthesized human voice. Most IVR systems do not allow the caller to respond by voice, but require user input through touch-tone response
LAN Mode	Local Area Network Mode	A deployment model for the MiCollab (or Mitel Standard Linux) server. When MiCollab is deployed in server-only mode, it provides the network with services, but not the routing and security functions associated with the role of "gateway". The LAN mode configuration is typically used for networks that are already behind a separate firewall. In other words, a separate firewall fulfills the role of gateway, providing routing and network security. (Also known as Server-only mode).
LDAP	Lightweight Directory Protocol	Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.
MBG	MiVoice Border Gateway	Previously known as the Multi-Protocol Gateway. The MiVoice Border Gateway (MBG) is a multi-service software application with a Web proxy that provides a secure method for Teleworker Web clients to connect to the LAN.
MiCollab	Formerly Mitel Applications Suite	Mitel product that unifies communication applications for small and medium sized businesses into an easy -to-use, cost effective solution. MiCollab supports multiple Mitel applications on a single industry standard server.
MiCollab Client	Formerly Unified Communicator Advanced	Application that provides users with a single access point for all their business communication and collaboration needs. It converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications.
MiCollab Client Integration Wizard		A software application (wizard) that integrates MiCollab Client user and phone data with the MiCollab USP data (see MiCollab Client Integrated Mode). If you are installing a new MiCollab system into an existing site that consists of one or more MiVoice Business platforms, you can use this wizard to update the MiCollab database with the user and phone data from the MiVoice Business.
MiCollab AWV		Mitel software solution that provides conferencing and collaboration services using a Web-based

		browser. In previous MiCollab releases, the product name for this application was Mitel Conferencing Advanced.
MiCollab Server		MiCollab software installed in conjunction with the MSL operating system on a server platform.
MiVoice Business Express	Formerly Unified Communications and Collaboration Virtual Appliance (vUCC)	Mitel communications solution for small to medium business that runs as virtual appliance on a VMware vSphere or Microsoft Hyper-V infrastructure.
MiCollab Virtual Appliance	Formerly Mitel Applications Suite Virtual Appliance	MiCollab running as a virtual application (vApp) within the VMware vSphere or Hyper-V environment.
MiCW	Mitel Integrated Configuration Wizard	A standalone software application that performs initial system setup of the MiCollab server and the MiVoice Business software.
MiTeam	Mitel Team	MiTeam is a cloud-based mobile first collaboration tool that allows teams to work together in real time no matter where they are. It is integrated into the iOS and Android native mobile clients and launched from the MiCollab Client for Mobile left tab.
MiVoice Business	Formerly Mitel Communications Director (MCD)	MiVoice Business is the brand name of the call-processing software that runs on hardware platforms, such as 3300 ICP controllers.
MiVoice Business-ISS	Formerly Mitel Communications Director (MCD) for Industry Standard Servers	This communications platform consists of MiVoice Business call processing software running on an industry standard platform. MiCollab is supported for the MiVoice Business-ISS platform.
MiVoice for Lync		An application that integrates with Microsoft Lync Client and allows Microsoft Lync users to use Mitel telephony functionality through its feature rich MiCollab Client infrastructure.
MiVoice Office 250	Formerly Mitel 5000 Communications Platform	Mitel IP communications platform supporting up to 250 users.
MOL	Mitel Online	Mitel's web portal for authorized dealers and technicians.
MiNet	Mitel Network Layer Protocol	A layer 2 protocol used to transport messages between the PBX and all Mitel DNIC phones
MSL	Mitel Standard Linux	The operating system that supports MiCollab software; along with Mitel SDK components, it comprises a base for all MiCollab software.
My Unified Communications Portal		MiCollab application that provides a common interface for users to update/enter user-configurable information for all applications.
NAT	Network Address Translation	For a computer to communicate with other computers and Web servers on the Internet, it must have an IP address. An IP address is a unique 32-bit number that identifies the location of your computer on a network. An IP address is similar to a street address in that it is means to find out exactly where you are and deliver information to you. Network Address Translation allows a single device,

		such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers
Network Edge Mode		A type of deployment for the MiCollab (or Mitel Standard Linux) server. In this deployment configuration, MiCollab manages the connection to the Internet by routing Internet data packets to and from the network (which allows all the computers on the network to share a single Internet connection) and by providing security for the network, minimizing the risk of intrusions. When one of the computers on the local network contacts the Internet, MiCollab not only routes that connection, but seamlessly interposes itself into the communication. This prevents a direct connection from being established between an external computer on the Internet and a computer on the local network, which significantly reduces the risk of intrusion. (Also known as Server-gateway mode).
NP-UM	NP-UM Messaging	Server-based voice processing system that provides call processing along with voice messaging and paging support.
Oria	A system management and customer self-service application. It allows a service provider to manage and deploy hosted voice services to their customers. Oria also allows a service provider to offer each of their customers an administration and self-service portal to make site specific moves, adds, changes, and deletes.	
Outgoing Line	Mobile Extension software phone emulator which calls user mobile phone when a call is received at the User's desktop.	
OVA	Open virtual appliance or application	A packaging format for virtual machines that allows virtual machine templates to be distributed, customized, and instantiated on any OVA supporting VMM/hypervisor.
PPPoA	Point-to-Point Protocol over Asynchronous Transfer Mode (ATM)	A protocol that encapsulates PPP frames in ATM Adaptation Layer 5 (AAL5). PPPoA is used primarily in cable modems, wireless devices, and ADSL broadband local loops for Internet access.
PPPoE	Point-to-Point Protocol over Ethernet	An access control method that allows remote hosts to log on and off using a simulated dial-up connection. PPPoE is typically offered by cable and DSL Internet service providers.
PPTP	Point to Point Tunneling Protocol	A protocol that encapsulates data sent over the Internet within a virtual private network (VPN).
QoS	Quality of Service	Quality of Service. The performance of a communications channel or system is usually expressed in terms of QoS. The QoS will relate to the type of system. SNR (Signal to Noise Ratio), BER (Bit Error Ratio), maximum and mean throughput rate, reliably, priority and other factors specific to each service.
Role		A role defines the task, position, or responsibilities for a type of user within the organization. Roles are

		associated with user templates that define the common phone and application service settings for the roles.
RTP	Real Time Protocol (FRD 1889)	A transport protocol to deliver live media to viewers simultaneously.
SAA	Speech Auto Attendant	Speech-enabled software application that allows users to place calls quickly and efficiently by speaking a person's name, a department name, or telephone number.
SAS	Suite Application Services	This application provides single-point user services provisioning and centralized management of shared system resources for all the MiCollab applications. This application also provides the My Unified Communications web portal.
Server Console		A text-based control panel built into the Mitel Standard Linux operating system that technicians use to perform maintenance tasks such as • install the MAS software • configure network parameters • perform upgrades and software updates • upgrade application suite licensing • perform backups.
Server-gateway mode		See Network Edge mode.
Server manager		A web-based control panel, also called the "server manager", that administrators use to configure and administer the MAS applications • perform server administration tasks, such as view logs, display system information, assign system users, and perform backups • configure network and server security settings • set system-wide parameters, such as system language and password strength.
Server-only mode		See LAN mode.
SIP	Session Internet Protocol	SIP is an ASCII-character-based signaling protocol designed for real-time transmission using Voice over IP (VoIP). The appeal of SIP is the promise of interoperability of telephones from propriety PBXs. SIP extends the foundation of open-standards from the Internet to messaging, enabling disparate computers, phones, televisions and software to communicate. SIP is a streamlined protocol, developed specifically for IP telephony. It is smaller and more efficient than H.323. SIP takes advantage of existing protocols to handle certain parts of the process. For example, Media Gateway Control Protocol (MGCP) is used by SIP to establish a gateway to connect to the PSTN system. SIP operates independently of the underlying network transport protocol and is indifferent to media. Instead, it defines how one or more participant's end devices can create, modify and terminate a connection whether the content is voice, video, data

		or Web-based. Using SIP, programmers can add new fragments of information to messages without compromising connections.
SPP	Single Point Provisioning	A MiCollab feature that allows an administrator to perform user and service provisioning for a MiVoice Business platform from a single interface, the MiCollab Users and Services application. SPP uses MiMXL to apply updates to the MiVoice Business platform. Updates made on the MiVoice Business are not distributed back to the MiCollab.
SRC	Secure Recording Connector	Formerly a standalone call recording product, SRC is now incorporated in the MBG software.
STT	Speech to Text	An optional, licensed feature of NuPoint UM that converts voice mail messages to text, allowing users to discreetly access voice messages in a text format.
SRTP	Secure Real Time Protocol (IETF Standard: http://www.ietf.org/rfc/rfc3711.txt – Apr 04)	Defines a profile that can be used to provide encryption, message authentication and integrity, and protection from replay attacks to the RTP data for audio and video streams.
SSL	Secure Socket Layer	A technology that works at the transport layer that does authentication and encryption between a Web server and a Web browser.
Stateful Inspection		Stateful inspection is an advanced firewall architecture that was invented by Check Point Software Technologies in the early 1990s. Also known as dynamic packet filtering, it has replaced static packet filtering as the industry standard firewall solution for networks.
TCP	Transmission Control Protocol (RFC 1122 Section 4.1)	A transport layer protocol with sequencing error detection and flow control. Transmission Control Protocol is a method used along with the IP to send data in the form of message units between computers over a network. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data that a message is divided into for efficient routing through the Internet.
TFTP	Trivial File Transfer Protocol (RFC 783)	A simple file transfer protocol (no password protection or user directory services) that uses UDP to transfer files across a network.
Transcode	Changing audio digital format from one format to another (G.711 to G.729)	
TUI	Telephone User Interface	Prompts played by a system application over the telephone that instruct users on how to use application features, such as voice mail features, from the telephone.
TW	Teleworker	Software that connects a remote office to the corporate voice network to provide full access to voice mail, conferencing and all the other features of the office phone system.
UCC	Unified Communications and	Mitel's licensing model. The platform and application

Licensing	Collaboration Licensing	user licenses are bundled together to meet the needs of different user levels (for example, Entry, Standard, and Premium). Instead of ordering an MiVoice Business user license and multiple individual applications licenses for each MiCollab user, you order a single UCC license per user.
UC Portal	My Unified Communications portal	A MiCollab application that provides a common portal for users to update/enter user-configurable information for all applications.
UDP	User Datagram Protocol (RFC 1122 Section 4.1)	UDP is an alternative to the TCP and, together with IP, is sometimes referred to as UDP/IP. Like TCP, UDP uses IP to actually get a datagram from one computer to another. UDP does not provide the service of dividing a message into packets and reassembling it at the other end. UDP doesn't provide sequencing of the packets that the data arrives in. Network applications that want to save processing time because they have very small data units or don't require the above services may prefer UDP to TCP e.g. TFTP uses UDP instead of TCP.
USP	User and Service Provisioning	MiCollab tool used to provision users
VoIP	Voice over Internet Protocol	VoIP technology, also known as IP Telephony, is the technology used to deliver telephony over a data network instead of using the standard public switched telephone network Rather it uses the Internet Protocol. VoIP means that voice is converted from an analogue signal, encoded digitally, then is converted into packets. It then uses a data network to move those packets along the most efficient path to their destination, where they are reassembled and delivered and converted back into a voice transmission.
VPN	Virtual Private Network	VPN support by the firewall is one of the core features that enable flexibility in a variety of environments. The VPN supports both site-to-site and remote-access VPNs encryption. This dual support provides the ability to connect two branch offices together using only firewalls on each side (site-to-site), or to connect remote users to the office via a VPN across the Internet (remote-access). IPSec, PPTP, and L2TP are the main VPN technologies supported.

Mitel
Powering connections
mitel.com

© Copyright 2017, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.