DEPLOYING MIVOICE BUSINESS MULTI-INSTANCE

SOLUTIONS GUIDE

DECEMBER 2014

Mitel®

NOTICE

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

Trademarks

Mitel is a registered trademark of Mitel Networks Corporation.

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

MiVoice Business Multi-instance Deployment Guide for Release 2.0
Release 4.0
December 2014

CHAPTER 1: INTRODUCTION

CHAPTER 2: MIVOICE BUSINESS MULTI-INSTANCE DEPLOYMENT

CHAPTER 3: DESIGN COMPONENTS

Chapter 1

INTRODUCTION

Introduction and Purpose

Large and small enterprises use MiVoice Business (MiVB) Multi-instance to reduce their hardware requirements and administration costs, and service providers use MiVB Multi-instance to offer a hosted solution to multiple end customers.

MiVoice Business is Mitel's call control software. recently renamed. It was previously called Mitel Communications Director (MCD). MiVoice Business runs on the Mitel 3300 ICP hardware, on industry standard servers (ISS), and as a virtual appliance on the VMware or Microsoft Hyper-V platforms.

MiVoice Business Multi-Instance (previously called Multi-instance Communications Director (MICD)), is a platform that allows you to create and manage multiple instances of MiVoice Business on an ISS.

MiVoice Business Multi-Instance deployment configurations

The MiVoice Business Multi-Instance can be configured in two modes: non-VLAN and VLAN. In non-VLAN mode, the MICD operates with one IP network address space

In VLAN mode, the MiVoice Business Multi-Instance uses VLAN tagging with each MCD instance. It also allows the use of overlapped IP addresses that are unique to each VLAN. This allows for both a single deployment where MiVoice Business instances are identified by their VLANs, or a hosted solution where the deployments are common and the individual hosted customers are identified through their VLAN tags. Typical configurations for deployment are:

- Non-VLAN mode, enterprise operation, single network
- Non-VLAN mode, public hosted via common MiVoice Border Gateway (MBG) to public network
- VLAN mode, private hosted to many customers across private networks

These configurations are described in more detail in this document. Also see the *MiVoice Business Multi-Instance Engineering Guidelines*

This guide also presents discussions of the many items you have to consider when planning an MiVoice Business Multi-instance network. It starts by describing the general types of Enterprise and service provider network configurations, and includes everything from assigning IP address ranges and determining the Quality of Service settings to use, to planning the purchase and configuration of servers, and the room they will reside in. Staging suggestions and management considerations complete the discussion.

Note: MICD Release 1.1 was released with MCD Release 4.2.
MICD Release 1.2 was released with MCD Release 5.0.
MiVoice Business Multi-instance 2.0 is being released with MiVoice Business 7.0.

Terms and Acronyms

The following table defines some of the terms used in this guide.

Table 1: Terms and Acronyms

TERM	DEFINITION
ACL	Access Control List
BSS	Business Support System
DSCP	Differentiated Services Code Point
DPM	VMware Distributed Power Management
DRS	WMware Distributed Resource Scheduler
DTMF	Dual Tone Multi-Frequency
FCAPS	ISO Telecommunications Management Network model and framework. FCAPS is an acronym for Fault, Configuration, Accounting/Administration, Performance, Security.
HA	VMware High Availability feature
HSRP	Hot Standby Routing Protocol (Cisco)
ISS	Industry Standard Server
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
MBG	MiVoice Border Gateway (formerly Mitel Border Gateway)
MCD	Mitel Communications Director (now called MiVoice Business)
MET	MiVB Multi-instance Engineering Tool: Configuration calculations spreadsheet for MiVB Multi-instance
MiVB	MiVoice Business (formerly Mitel Communications Director - MCD)
MiVB Multi-instance	MiVoice Business Multi-instance (formerly Multi-instance Communications Director - MICD)
MPLS	Multi-Protocol Label Switching
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
OSS	Operations Support System
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
SBC	Session Border Controller
SET	System Engineering Tool: Configuration calculations spreadsheet for network planning
SIP	Session Initiation protocol
SLA	Service Level Agreement
STP	Spanning Tree Protocol
TDM	Time Division Multiplexing

Table 1: Terms and Acronyms (continued)

TERM	DEFINITION
UC	Unified Communications
VLAN	Virtual LAN (supported in MiVB Multi-instance for Release 1.2+)
VRF	Virtual Routing and Forwarding (router)
VRRP	Virtual Router Redundancy Protocol

References

Use the following tools and guides for more information

- System Engineering Tool (SET)
- MiVB Multi-instance Engineering Tool (MET)
- *3300 ICP Technician's Handbook*
- *3300 ICP Engineering Guidelines*
- *Engineering Guidelines for ISS and MiVoice Business Virtual*
- *MiVoice Business Multi-instance Installation and Administration Guide*
- *MiVoice Business Multi-instance General Information Guide*
- *MiVoice Business Multi-instance Engineering Guidelines*
- MiVoice Business Multi-instance Manager Online Help
- Media Server Manager Administrator Online Help
- *MSL Installation and Administration Guide*
- MSL Qualified Hardware List
- *MiVoice Border Gateway Engineering Guidelines*
- *Using System Data Synchronization Solutions Guide*
- *Provisioning Users Solutions Guide*
- *Multi-node Networking Solutions Guide*

Chapter 2

MIVOICE BUSINESS MULTI-INSTANCE DEPLOYMENT

MiVoice Business (MiVB) Multi-instance Network Planning

MiVoice Business Multi-instance is intended for use in enterprise applications and service provider networks. Although the same MiVoice Business Multi-instance base software is used for both, the licensing is different depending on the planned deployment and the desired commercial model (Capital Purchase or Subscription).

Note that small enterprise deployments generally need MiVoice Business Multi-instance only if there are multiple remote offices. For a small, single-site deployment, use the Mitel 3300 ICP with MiVoice Business, stand-alone MiVoice Business on Industry Standard Server (ISS), or MiVoice Business Virtual.

The following sections describe how to deploy MiVB Multi-instance in the various network configurations, and some of the basic configuration considerations for each of the network types.

- "Using MiVoice Business Multi-instance in Enterprise networks (non-VLAN mode)" on page 9
- "Using MiVoice Business Multi-instance in service provider networks" on page 11
- "Configuration Basics" on page 15

Using MiVoice Business Multi-instance in Enterprise networks (non-VLAN mode)

Enterprise networks are often deployed with centralized phone service using one common network. MiVB Multi-instance is generally used to consolidate and centralize multiple MiVoice Business instances on to a reduced number of platforms, and potentially, to a reduced number of data centers. The large enterprise deployment uses a single IP address space. The MiVoice Business Multi-instance, all controllers, and all applications across the network reside within this common IP address space.

MiVB Multi-instance can also be used by companies that are interested in providing hosted PBX services for their internal enterprise customers. The large enterprise hosting deployment assumes a single network customer and full-feature operation. Three common implementations are Hosted Hospitality, Leased offices, and Franchise Business. In these three implementations, service is provided to one organization with all voice being hosted centrally, and some specific functionality isolated to the "branch offices", where the branch offices may be individual hotels, local franchise locations, or individual businesses in a leased office complex. Embedded Voice Mail is available for each MiVoice Business instance.

The Enterprise deployment shown in Figure 1 is used to provide services to just one customer. Since all devices in the deployment reside in a common IP address space there is no need for Network Address Translation (NAT) between Headquarters and remote sites.

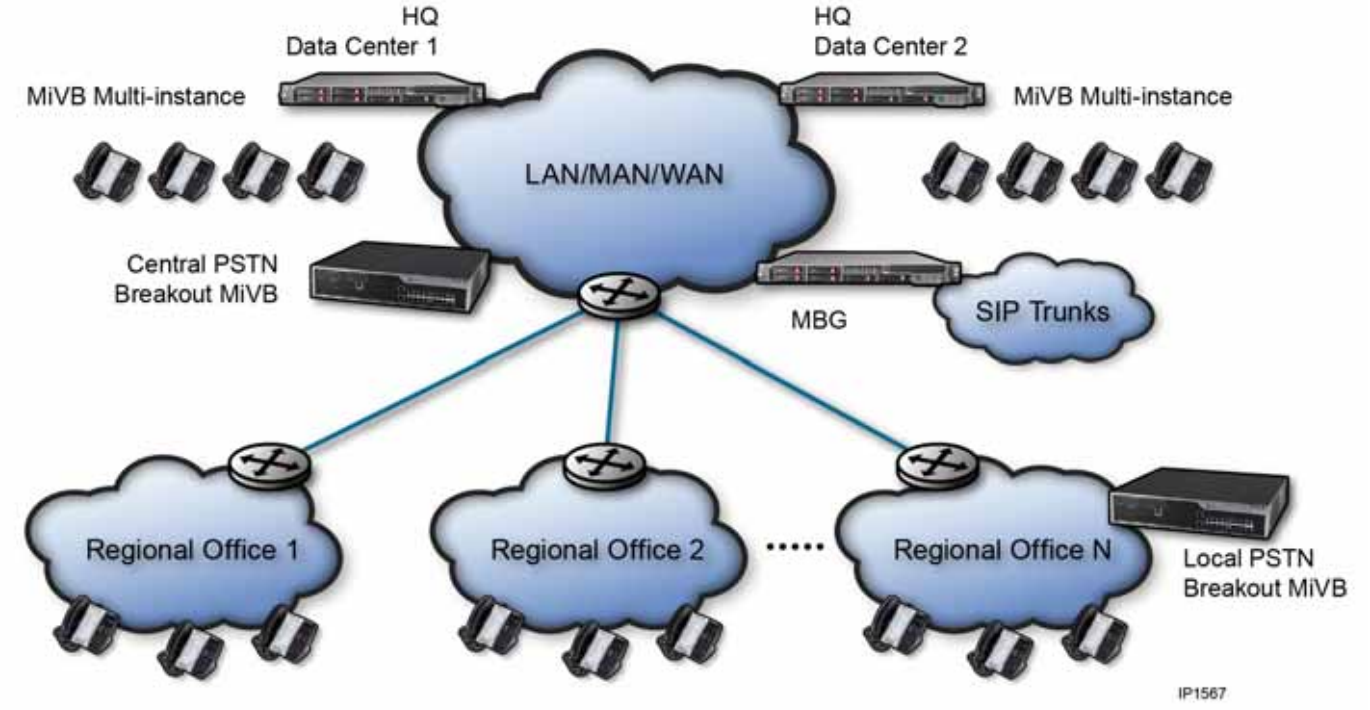
A MiVoice Border Gateway or Session Border Controller (SBC) is used to isolate the SIP trunks. The SIP service provider may employ an additional SBC.

a MiVoice Border Gateway (not shown in Figure 1) is provided at the connection to the public Internet space and provides the NAT function for any Teleworkers connecting via the Internet..

Common management access is provided to all customers, and a common external port can also be provided for configurations by individual offices or customers.

Use the following sections, and the information in Table 2, for guidance in planning and deploying the required network.

Figure 1: Large enterprise hosting



Operation in Virtual LAN (VLAN) mode is possible with Enterprise deployments, but there is little benefit, since all MiVoice Business instances belong to the same network address space, and the isolation afforded with the implementation of VLANs is not needed. Non-VLAN mode is the preferred operating mode for Enterprise deployments.

Note: With the release of MiVoice Business Multi-instance Release 1.2, migrating from physical 3300 ICP controllers to the multi-instance platform was simplified with the introduction of the VLAN (Virtual LAN) mode. In previous releases, the 3300 ICP databases being migrated to MiVoice Business Multi-instance had to be updated so that all of the IP addresses were in the same subnet, with no duplicates. This process is time-consuming and error-prone.
By configuring MiVoice Business Multi-instance for VLAN mode, you can set up each MiVoice Business on its own subnet.
This allows you to avoid changing all of the IP addresses to be on the same subnet within the MiVoice Business Multi-instance.

Some of the common Enterprise deployments:

- Hosted Hospitality Services

  There is a strong trend in the hospitality industry to centralize PBX services for multiple hotels in one location and MiVoice Business Multi-instance is well suited to this application.

- Leased offices

  Large office buildings, office parks, managed offices, and shopping malls can realize many administration and cost benefits by centralizing PBX functions with the MiVoice Business Multi-instance solution. Landlords supply and maintain the telephone services, and possibly data services as well, and charge each tenant a monthly fee for the service.

Note: This is similar to the service provider model in that multiple tenants are served, and there is no relationship between them. In this case, though, each customer probably needs a maximum of 10-20 phones, and often fewer than that.

- Franchise businesses

  Many franchised businesses have geographically distributed locations but they require voice resources to be centralized at their head office. MiVoice Business Multi-instance can provide the voice services.

- Hybrid deployment

  In a hybrid enterprise deployment, telephony is hosted at the head office, and each branch office takes care of its own local service using MiVoice Business deployed on a local 3300 ICP.

  A hybrid deployment can be easily configured for resiliency by configuring the local branch office ICP as the secondary MiVoice Business for the branch office phones.

- MiVoice Business consolidation

  Consolidating multiple business units into a common data center or location.

Using MiVoice Business Multi-instance in service provider networks

MiVoice Business Multi-instance deployments are ideal for service providers, and there are many different ways to configure a network, depending on customer requirements. Many customers can be served using the same MiVoice Business Multi-instance deployment.

Each MiVoice Business Multi-instance installation can host many MiVoice Business instances. Depending on the installation, it may be possible to trade off between the number of users and the number of instances per server. Use the System Engineering Tool (SET) and the MiVB Multi-instance Engineering Tool (MET) to calculate the configuration parameters for the required system. Refer to the *MiVoice Business Multi-instance Engineering Guidelines* for more information.

When providing telephone service hosting for multiple customers, the MiVB Multi-instance should be used in VLAN operating mode.

When the MiVB Multi-instance is configured for VLAN operating mode, each customer has a unique VLAN, which allows the same IP network addresses (if necessary) to be used for multiple customers while ensuring complete isolation from other customers hosted on the same MiVB Multi-instance.

Note: VLAN mode is available on MICD 1.2+ and MiVoice Business Multi-instance releases.

Use the following sections, and the information in Table 2 on page 15, for guidance in planning and deploying the required network.

Hosted Phone Service - Public Network

In this scenario, the service provider hosts customer telephone service using the public Internet, connecting to the customer telephones using their public IP addresses. See the example in Figure 2 on page 13.

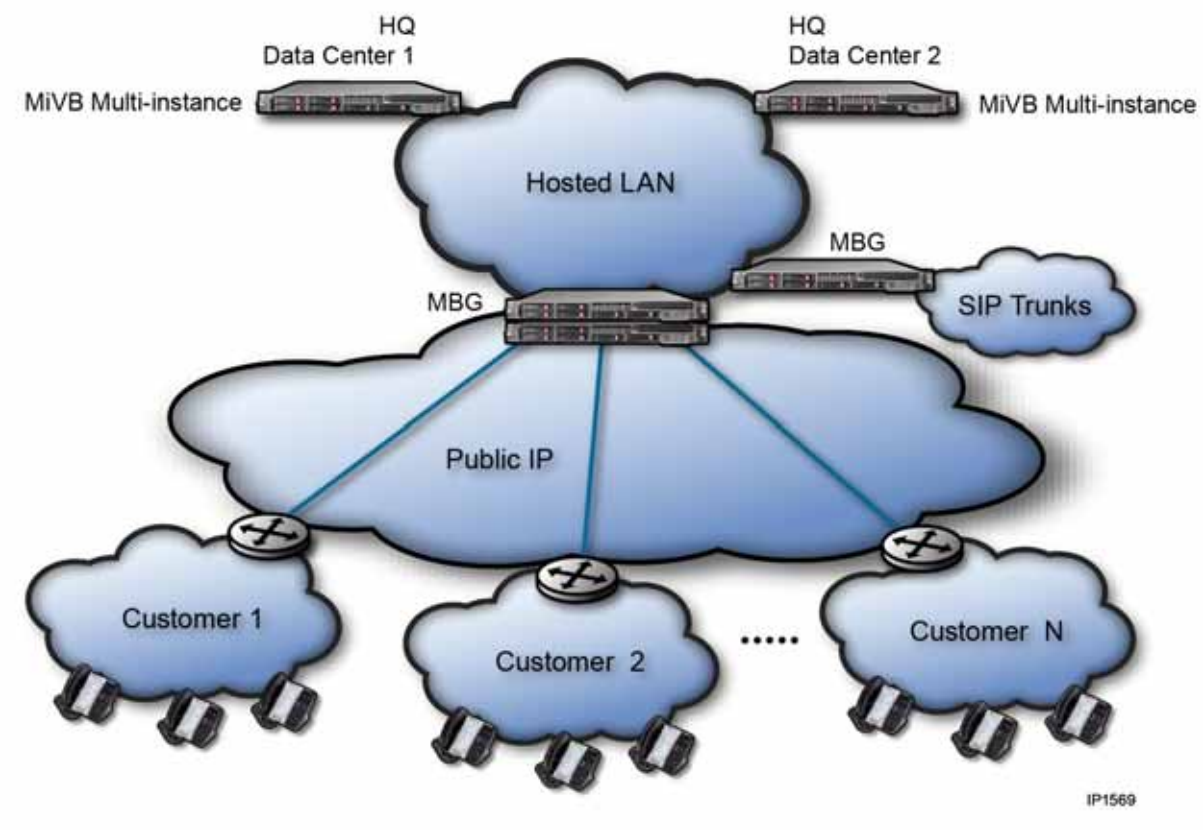
This is one of the easier networks to deploy and understand. Multiple customers can be served with basic telephony service and embedded voice mail per instance. The service provider uses a common hosting IP address space. The service provider has a common management interface, and customers can be provided with a management portal to manage their own MiVoice Business.

This deployment is similar to the Large Enterprise Hosting solution shown in Figure 1, except that access to the remote sites and customers occurs over a common public network rather than using a private connection. The public network may not provide SLAs that could be expected and demanded with private networks.

Isolation of the hosted network from the public networks is achieved using a MiVoice Border Gateway or MiVoice Border Gateway cluster. The MiVoice Border Gateway provides isolation and Network Address Translation (NAT). Each remote site—these may be individual customers—is uniquely identified through its public address at the local firewall/NAT router.

SIP trunks are consolidated at the hosted network. Isolation of the hosted network to the SIP Trunk provider may require a MiVoice Border Gateway or a Session Border Controller (SBC). The IP Trunk service provider may use an additional SBC in this connection.

Figure 2: Hosted phone service - public network



Hosted Phone Service - Private Network

In this scenario, each customer has a private IP address space. This is a more complex configuration than the others discussed in this guide because there are more paths into the hosted space. See the example in Figure 3.

Primary benefits to the customer are guaranteed QoS across the network, rights to the SIP trunking gateway, and the ability to use Teleworker phones outside of the business network. Each MiVoice Business instance in the MiVB Multi-instance also offers embedded voice mail.

To ensure continued QoS across the SIP trunks, you must establish this requirement using an SLA with the SIP trunk provider.

In this configuration, there are multiple networks to consider. There is the local address space for the hosting service provider, plus the multiple address spaces from each customer that have been extended across a private carrier network into the physical hosting environment.

Note: The hosting network and the private carrier network do not have to belong to the same provider.

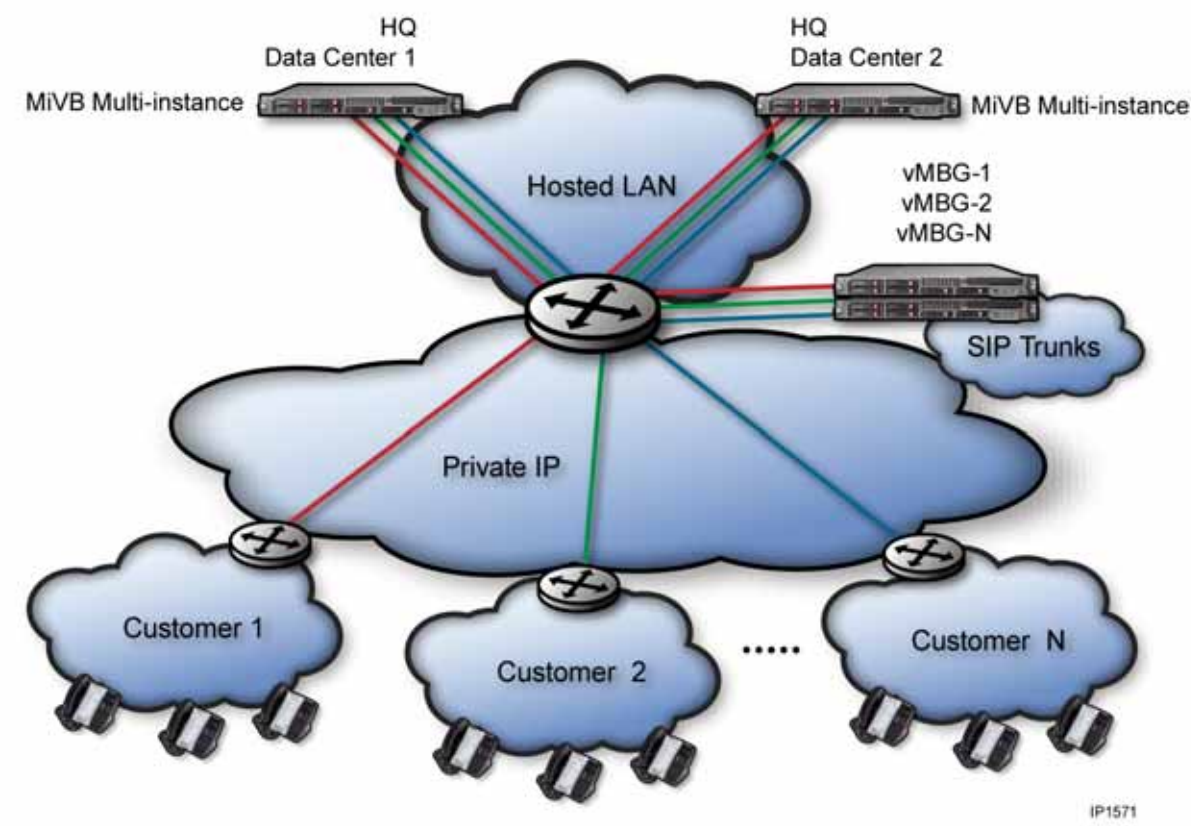
Each customer network must remain isolated from all of the other customer networks, and also from the hosted address space. The hosting address space must also remain isolated from the customer networks.

For ease of deployment and management, there is also a high probability that all of the hosted deployments will be similar. This makes the management easier for the hosting provider, but results in potential overlap of IP addresses of the different customer sites.

In non-VLAN mode, to maintain isolation and allow use of overlapped IP addresses, each customer requires a MiVoice Border Gateway or MiVoice Border Gateway Virtual at the external SIP trunk connection. MiVoice Border Gateway provides access control and privacy for each customer, so there is no risk of finding the duplicate IP address on another customer site.

In VLAN mode, every MiVoice Business instance is on its own VLAN, so trunks are provisioned per customer (as are Teleworker phones).

Figure 3: Hosted phone service - Private network



Everything can be virtualized, and each customer can be provisioned with management access to the Network Operations Center. The service provider can also host the customer applications, if customers prefer it. Each customer has private management.

In addition, inclusion of a per-customer 3300 ICP, for example, local trunk breakout at a remote customer site is also possible.

Disaster Recovery Services

Companies that provide disaster recovery services to other corporations can use the MiVoice Business Multi-instance solution to rapidly provide their customers with PBX capabilities in a situation where a disaster disables the customer's PBX infrastructure.

Disaster Recovery services can be provided by having MiVoice Business instances on cold standby in the data center. When services at the customer site are lost, the users can be re-deployed off the disaster recovery instance in the core. Depending on the type of service (and the Service Level Agreement) this may involve restoration of backup database, and possibly re-deployment of phones to a new location.

In the event that an Enterprise loses its data center and all MiVoice Business instances and 3300 ICPs at the site, all the user phones could be without service if there is no access to an alternative secondary controller. The disaster recovery MiVB Multi-instance would be programmed to replicate the MiVoice Business instances that were lost, and to take the existing database information and IP information. The MiVB Multi-instance disaster recovery would then be deployed as one of the following:

- Physical servers within the customer premise, at a different location on the same network
- Remotely hosted back to the customer using an additional connection to the customer inter-site VPN
- Remotely hosted through the public IP network (Internet) and have the phones re-home to a public IP address

External trunks would be provided via SIP trunks, or additional 3300ICPs to the PSTN connections.

Configuration Basics

Table 2 offers general starting guidelines for the types of network needed for each of the application types described above.

The following network configurations are provided as suggested deployment topologies only. Each customer will have different requirements and different new or existing topologies to work with. Each customer deployment must be individually analyzed to determine these requirements and the deployment must be tailored to meet these requirements. The following notes are provided as a guide to suggest aspects of the deployment to consider during such analyses.

Table 2: Network considerations by network type

BUSINESS TYPE	DEPLOYMENT CHARACTERISTICS	HARDWARE AND SOFTWARE REQUIREMENTS
What is the business?	Business Size Network Topology External Connection (QoS, VPN) Local Breakout and distributed/central IP Address space, overlapped? Applications (Telephony and business-oriented) Voice Mail End-customer Management IT staff necessary Trunks connections, PSTN, SIP	• MiVB Multi-instance • vMBG • 3300ICPs • MBG (User, SIP trunks) • vMBG (User, SIP trunks • Oria User Management Portal • Applications, virtual appliances • WAN connections, public Internet, VPN connections

Table 2: Network considerations by network type

BUSINESS TYPE	DEPLOYMENT CHARACTERISTICS	HARDWARE AND SOFTWARE REQUIREMENTS
Service Provider • Common hosting location • Hosting voice and applications to many end customers • End-customer IP addresses unmanaged	• Service provider business is large • Service provider network includes end-customer networks • End-customer business is large, typically medium Enterprise >500 users • HQ and multiple remote sites linked by common VPN • VPN and customer address space extend into hosted location • VPN provides QoS and bandwidth management • Customer IP address in service provider IP address space may overlap with other, similar customers, and must remain isolated • End customer voice and business applications may all be hosted • Central voice mail • Customer may have local IP staff with ability to manage voice system • Trunk connections: both SIP trunks centrally, and local breakout to PSTN	• MiVB Multi-instance (VLAN Mode) • MiVoice Business Virtual (if not covered by MiVB Multi-instance) • vMBG (SIP Trunks) • vMBG (Teleworkers) • MiCollab Virtual for telephony applications • Oria Management portal for end customers depending on SP • NuPoint Unified Messaging for central voice mail • Virtual appliances for customer business applications • WAN/VPN router with QoS
Service Provider • Common hosting location • Hosting voice to many end customers • End-customer IP addresses unmanaged	• Service provider business is large • Service provider network is common for all end-customers, but not accessible directly from end-customer • End-customer is small, typically < 150 users • Single business site or multiple independent sites • Access to public IP network • QoS may need to be provided by separate dedicated connection • End-customer deploys NAT and is isolated from service provider address space • Embedded voice mail • Limited application access • Teleworker inherent in deployment • Business applications on customer site • Unlikely to have full-time IP staff • Management portal provided by service provider to allow customer limited management access • Trunk connections via SIP trunks hosted centrally	• MiVB Multi-instance (Non-VLAN mode) • MBG (SIP Trunks) • MBG (Public IP User connection) • MiCollab Virtual (applications per customer access via MBG) • Oria management portal for end customers • Router/NAT combination • Dedicated public IP connection may be required for QoS

Table 2: Network considerations by network type

BUSINESS TYPE	DEPLOYMENT CHARACTERISTICS	HARDWARE AND SOFTWARE REQUIREMENTS
Hosted Enterprise • Services hosting from external resource (resource leasing) • Managed by enterprise • One end-customer	• Enterprise business requiring off-site hosting and leasing • Off-site may be dedicated virtual environment or allow dedicated server installation • Large enterprise 100-5000+ • HQ and multiple remote sites linked by common VPN • VPN and customer address space extend into hosted location • VPN provides QoS and bandwidth management • Customer IP address in service provider IP address space may overlap with other, similar customers and must remain isolated • End-customer voice and business applications may all be hosted • Central voice mail • Customer has local IP staff with ability to manage voice system • Trunk connections: both SIP trunks and local breakout to PSTM	• MiVB Multi-instance (depending on hosting provider) • MiVoice Business Virtual (if not covered by MiVB Multi-instance) • vMBG (SIP Trunks) • vMBG (Teleworkers) • MiCollab Virtual for telephony applications • vNuPoint UM • Virtual appliances for customer business applications • WAN/VPN router with QoS
Enterprise Consolidation • Services on premises, centrally located • Managed by Enterprise • One end customer	• Enterprise business consolidation into central data center • Large Enterprise, 2000+ • HQ, data centers nd multiple remote sites linked by common VPN • Once common address space across allocations • VPN provides QoS and bandwidth management • Business applications on premises • Central voice mail • Local IP staff with ability to manage voice system • Trunk connections, both SIP trunks and local breakout to PSTN	• MiVB Multi-instance (Non-VLAN mode) • MiVoice Business Virtual (if not covered by MiVB Multi-instance) • vMBG (SIP Trunks) • vMBG (Teleworkers) • MiCollab Virtual for telephony applications • vNP-UM for central voice mail • Virtual appliances for customer business applications • WAN/VPN router with QoS

Table 2: Network considerations by network type

BUSINESS TYPE	DEPLOYMENT CHARACTERISTICS	HARDWARE AND SOFTWARE REQUIREMENTS
Leased Offices • Leased phone service to end customers • On-site service provider” • Managed address space	• Service provider business is medium sized (up to 100 offices) • Service provider network is common to all end customers • Managed IP address • End-customer is small, typically < 50 users • Single business site • Access to internet via common firewall/NAT • On-site local hosting, VLANs and routing provide sufficient QoS and bandwidth • Embedded voice mail • Limited application access • Teleworker via common gateway • Business applications on customer site, or VLAN • Full-time IT staff for service • Trunk connections via SIP trunks hosted centrally	• MiVB Multi-instance (Non-VLAN mode) • MBG (SIP Trunks) • MBG (Teleworker, if needed) • MiCollab Virtual (applications per customer via VLAN) • Common Router • Internet access via common firewall/NAT
Leased Offices • Leased phone service to end customers • On-site or Off-site “service provider” • Unmanaged address space	• Service provider business is medium-sized (up to 100 offices) • Customer networks are unique and identified via VLAN • Unmanaged IP address • End-customer is small, typical < 50 users • Single business site • Access to internet via per-customer firewall/NAT • VRF Router common to all customers • On-site hosting via multiple dedicated VLAN in VPN or VLAN in VLAN mode • Embedded Voice Mail • Limited application access • Teleworker via per-customer vMBG • Business applications on customer site, or hosted on VLAN • Full-time IP staff for service provider • Trunk connections via per-customer SIP trunks hosted centrally	• MiVB Multi-instance (VLAN mode) • MiVoice Business Virtual per customer or MiVB Multi-instance • vMBG (SIP Trunks) • vMBG (Teleworker) • MiCollab Virtual (applications per customer via VLAN) • Common VRF Router • Internet access via per customer firewall/NAT • Dedicated hosted VPN/VLAN for off-site hosting

Table 2: Network considerations by network type

BUSINESS TYPE	DEPLOYMENT CHARACTERISTICS	HARDWARE AND SOFTWARE REQUIREMENTS
Franchise Business • Common hosted, central location • Hosting voice to many end-customers • Managed network	• Franchise HQ provides service to the remote businesses • Network is common to all end-customers, and accessible from customer sites • Limited management access from remote sites • Requires managed use of IP addresses to franchise sites, no overlap allowed • Franchise is small, typically < 150 users • Franchise is a single business site • Dedicated connection to site over VPN • Embedded voice mail per franchise site • Per-franchise application access • Teleworker via central MBG • Business application on franchise site and/or central site • HQ has full-time IT staff • Per-franchise isolation via VLAN and router ACLs, as required • Trunk connections via SIP trunks hosted centrally	• MiVB Multi-instance (non-VLAN mode) • MBG (SIP trunks) • MiCollab Virtual • Dedicated VPN connection to franchise sites
Disaster Recovery • Services hosted from external resource (resource leasing) • Managed network • One end-customer	• Enterprise business requiring off-site hosting and leasing • Off-site may be dedicated virtual environment or all dedicated server installation • Large enterprise 100-5000+ users • Link to HQ and multiple remove sites by VPN or extension to existing VPN • VPN and customer address space extend into hosted location • VPN provides QoS and bandwidth management • Customer IP addresses in service provider IP address space may overlap with other similar customers and must remain isolated • End-customer voice and business applications may all be hosted • Central voice mail • Customer has local IT staff with the ability to manage the voice system • Trunk connections: both SIP trunks and local breakout to PSTN	• MiVB Multi-instance (VLAN mode - use is dependent on hosting provider) • MiVoice Business Virtual (if not covered by MiVB Multi-instance) • vMBG (SIP Trunks) • vMBG (Teleworkers) • MiCollab Virtual or MiCollab for telephony applications • NuPoint Unified Messaging for central voice mail • Virtual appliances for customer business applications • WAN/VPN router with QoS

Note: With the introduction of MiVB Multi-instance Release VLANs, you may not need to use MBGs to isolate customers and franchises from each other. You must ensure that connection to individual customers is made through a VRF-capable router, or one capable of source routing.

Network planning

When planning the network deployment, start by finding the answers to the following questions.

Table 3: Network planning questions and answers

Network planning questions	Your answers
Is this a new network or will it be consolidated with an existing corporate network?	
Identify the IP address range	
• carve up address range to different functions over-provision addresses -- they will always get used • generate a pattern for easy replication and scaling • Think big -- highly scalable 10.0.0.0 and upwards • address space - hosted and customer • IP Addresses (Private and Public)	
Throughput and bandwidth calculation	
• System Engineering Tool • MiVoice Business Multi-instance Engineering Tool • *MiVoice Business Multi-instance Engineering Guidelines* • *MiVoice Business Engineering Guidelines* • *MiVoice Business Resiliency Guidelines* • Resiliency between data centers • Ensure that carrier can handle throughput and bandwidth.	
Location and layout of components	
• layout of Layer 2 and Layer 3 components • location of DNS. Is a local server needed? • location of firewall and MiVoice Border Gateway • DHCP - Location of server	
Voice and general data settings	
• DHCP forwarding or IP-Helper	
SMTP - e-mail forwarder for alarms	
TFTP - central or per MiVoice Business?	

Table 3: Network planning questions and answers

Network planning questions	Your answers
FTP	
• Central server? • Will individual customers also need an FTP site? • Location? • Storage size • Logs and backups • Allowed access	
Remote management	
• access to servers, • iLO (HP Integrated Lights Out) • VPN • RDP/VNC	
Logical path flow	
• Are MiVoice Border Gateways needed? • SIP path • Signalling path • Media path	
Practical Trunk and user paths	
• Public IP connection paths • Private IP connection paths • Inter-unit signalling	
Customer management	
• Common hosted provider or enterprise • Per customer access management portal	
Security	
• Access rights • Groups and user policies • Policing and authentication • Audit/modification trails	

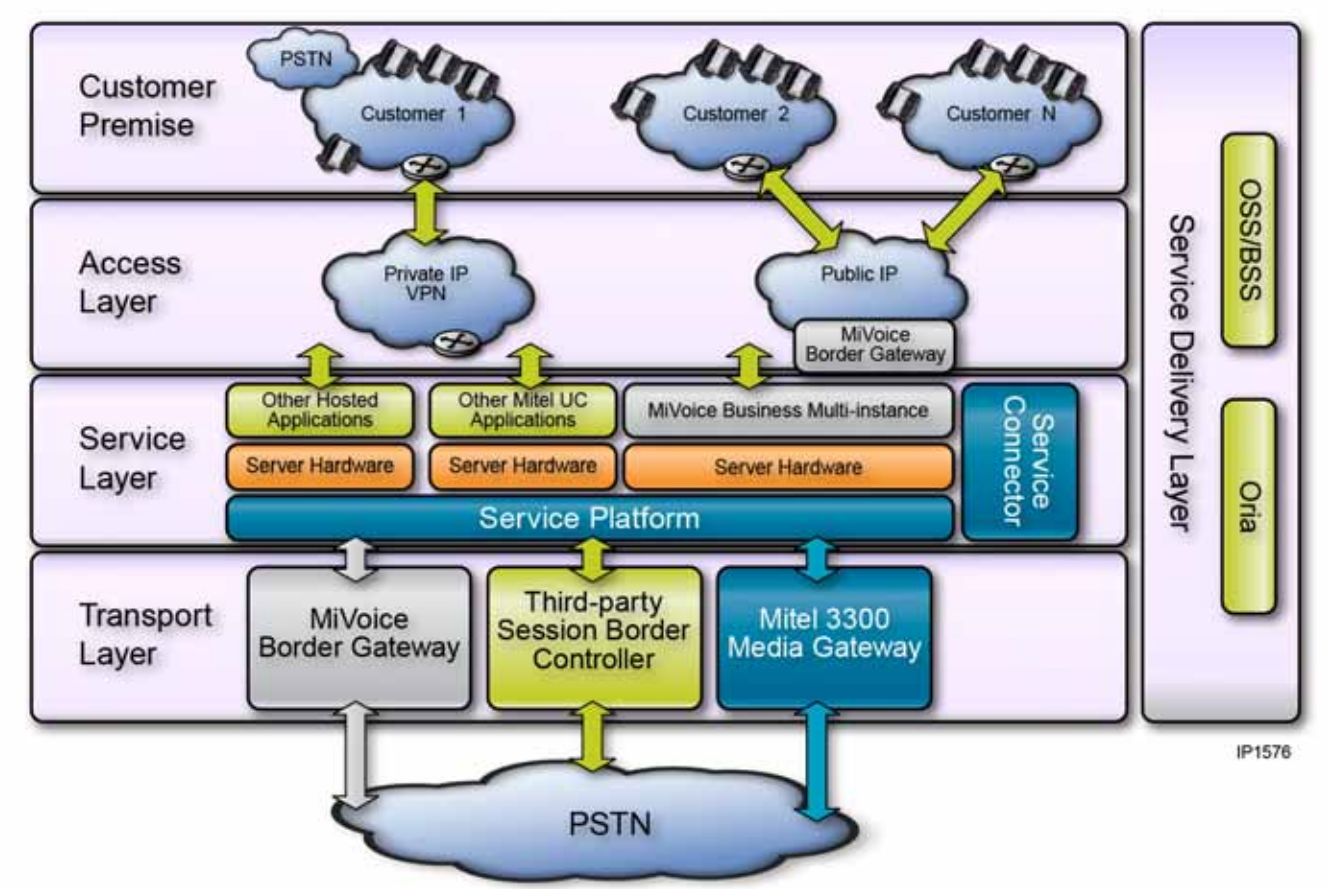
After determining the general network topology, use the following sections to work through the planning items that are specific to the network components.

Tip: Start with System Engineering Tool (SET). Then import the SET files into the MiVB Multi-instance Engineering Tool (MET) as described in the *MiVoice Business Multi-instance Engineering Guide*. Also see the MET Overview in DK119552.

Planning the MiVB Multi-instance System

A helpful way to plan the design of your system is to imagine it as a set of layers, each with specific and specialized functionality.

Figure 4: MiVB Multi-instance Deployment Layers



Service Layer

The Service Layer is made up of the systems that directly provide services to users, including phone calls, unified messaging, other unified communications services, and any other services the service provider is offering to their customers.

Hosted IP Telephony

The Hosted IP telephony functionality is delivered with the MiVB Multi-instance platform. This platform includes all call control, plus embedded functionality to provide:

- Unified Messaging
- Ad-hoc Conferencing
- Agent queuing for use with complementary MiContact Center applications
- Call twinning to allow up to eight devices to be associated with one user

Other Mitel Unified Communications Applications

Service providers can also choose to provide a more Unified Communications-enriched service by complementing the MiVoice Business Multi-instance with other Mitel UC applications. This is typically done using a virtual infrastructure, maintaining dedicated virtual applications for each customer. For information about the Mitel's Virtual Application portfolio, visit Mitel.com. For information about deploying virtual applications, refer to the *Virtual Appliance Deployment Solutions Guide* on Mitel OnLine.

Third-party Applications and Services

The service provider may be offering additional services to their customers as part of their service platform. These may be built and maintained by the service provider, or the service provider may be aggregating services from other cloud-based providers.

Access layer

There are several options for access to the Mitel Unified Communications Service Platform:

Secure WAN technologies

In cases where customers are serviced using secure WAN technologies such as MPLS or VPN, MiVoice Business Multi-instance and any UC applications being used can be configured to allow direct connection to the customer's network, and in complete isolation from other customers networks. This is facilitated by the multi-instance nature of Mitel UC Service Platforms. This is not achievable with more traditional multi-tenant platforms.

Public networks

For secure access across public networks, Mitel provides the MiVoice Border Gateway. The MiVoice Border Gateway allows secure connectivity between end-customers and their Mitel UC services within the service provider data center. The MiVoice Border Gateway also implements jitter buffers and packet loss concealment algorithms for use in maintaining voice quality. For scalability and improved availability, MiVoice Border Gateway can be deployed in an N+1 clustered architecture.

Customer Premise Equipment

In a typical service provider deployment, the only equipment required on the customer premise, other than the IP networking and Internet termination equipment, is the Phones. Mitel's full suite of IP desktop devices can be deployed, however, for ease of configuration and maintainability, the service provider should consider standardizing on Mitel's series of self-labeling sets (MiVoice 5320, 5330, 5340 and 5360 IP Phones).

For low density analog on-premise requirements, the service provider typically deploys a SIP-based Analog Termination Adapter (ATA) device. This provides a network facing IP connection, while providing various analog inputs for things like analog phones, door openers, overhead pagers, and so on. For a list of supported SIP ATA devices, please refer to the MiVoice Business Compatibility Reference Document available in the Mitel Knowledge Base on Mitel OnLine.

Higher density analog deployments can be facilitated with the use of a 3300 AX controller, which can terminate up to 256 analog devices and can be clustered for greater capacity.

If local breakout to the PSTN is required on the customer site, there are two options:

- Line Interface Module (LIM)

  This provides the ability to terminate a Line Station trunk directly on a Mitel IP Phone.

- 3300 Media Gateway

  Any of Mitel's 3300 ICP controllers can be deployed on-site to serve as a local breakout point for PSTN trunks, in addition to providing on-site survivability for all IP phones in the event of a WAN or data center failure.

In any case where a 3300 ICP controller is being installed on customer site for local media gateway, analog support, or on-site resiliency, private network configurations are required and must be considered in the design.

Service Delivery Layer

The Service Delivery Layer provides the provisioning, billing, and monitoring capability required to maintain the service provider's service platforms and networks. This includes traditional Operations Support System (OSS) and Business Support System (BSS) components. service providers typically own and maintain their own Service Delivery Platform (SDP), or use a standard platform from a third party. It is a high priority for service providers to have a consistent strategy across all the various aspects or modules of the services they are delivering.

Customer provisioning and billing

Deployment of the Mitel Unified Communications (UC) Service Platform includes the Right to Use (RTU) of the Oria platform. Oria is hosted centrally in the data center and provides configuration access to the MiVoice Business instances through a web interface accessible using standard browsers. The Oria web interface enables customer control, while maintaining the global control over the aggregated MiVoice Business instances with the service provider. Flexible feature allocation enables service providers to create bundles that allow the customer to easily manage their service usage, and presents the potential for the service provider to sell customers on additional advanced features.

Other OSS and BSS or SDP systems can be integrated with the Mitel Service Platform through standard API's provided by the Service Connector. This is accomplished through a web services-based API on the Oria platform, and allows integration of the Mitel platform into a common Service Delivery Platform.

Typically, billing for this type of service is managed through metering and billing at the user (or per seat) level along with metrics received from the SIP trunking network. Mitel does not supply billing systems, but can help you integrate a third-party billing system into your deployment.

Network Management System

Network Management allows the customer to provide proper fault, configuration, accounting, performance, and security management for the product as defined by the FCAPS ISO model.

- What system management and monitoring are needed?

- System management and monitoring
  - MiVoice Enterprise Manager
  - Voice quality monitoring
  - SNMP: alarms and traps
  - Unexpected access alarms and port shut down and blocking
- Is remote access required into the network?
- Is there a requirement for the ability to monitor and program network components remotely?
- Is remote reset capability needed?
- Is serial port access needed?

Management for MiVoice Business Multi-instance (non-VLAN mode)

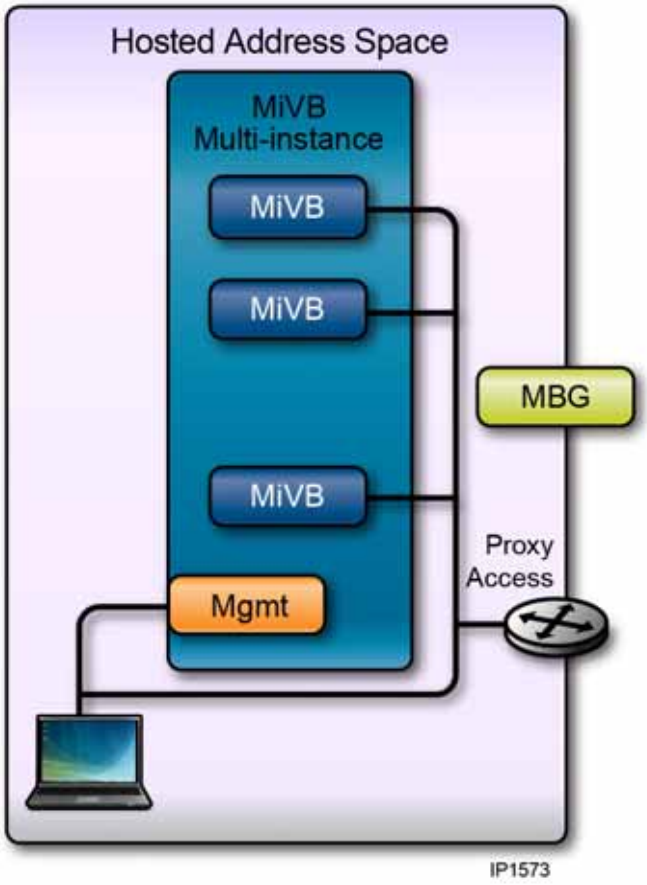
The MiVB Multi-instance can be configured to provide these management options for hosted solutions, both public and private.

With the hosted public network solution, there is one common address space for the hosted provider to manage. The customers can access their MiVoice Business instances only by using an external proxy that controls access.

Figure 5 illustrates the different management access options. Access is possible from within the hosted provider's address space to both the management interface of the MiVB Multi-instance and to each of the MiVoice Business instances. A proxy access is also provided to give customers access to their individual MiVoice Business instances.

Refer to the *MiVoice Business Multi-Instance Engineering Guidelines* for details.

Figure 5: Management access for non-VLAN installation



Management for MiVoice Business Multi-instance VLAN Mode

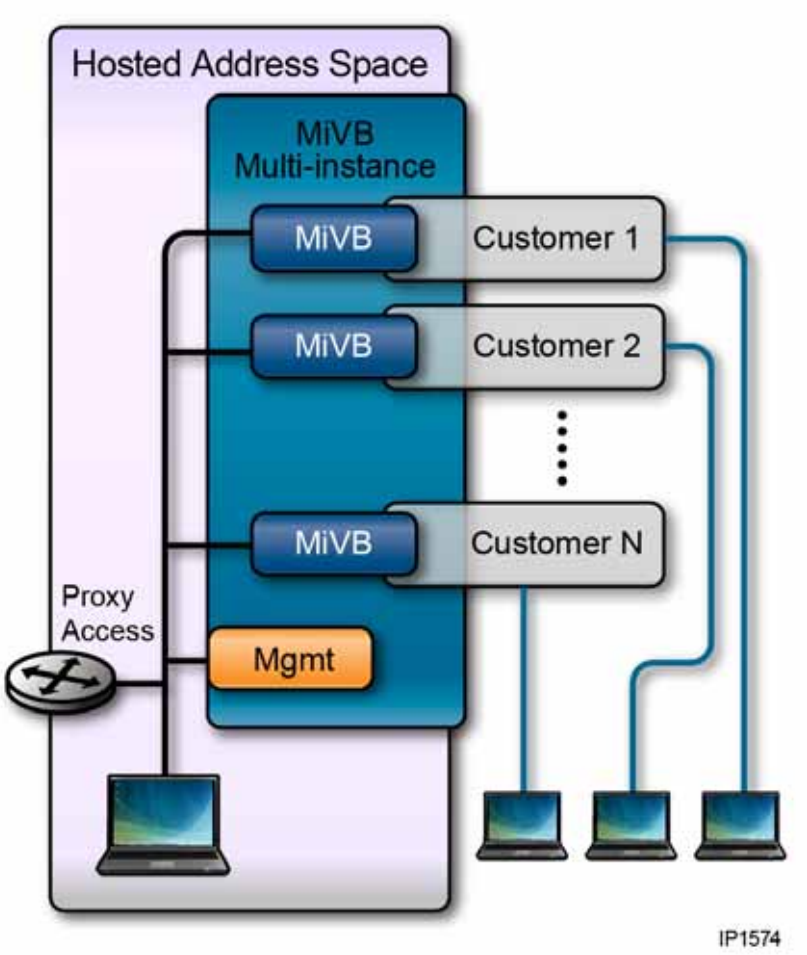
MiVB Multi-instance VLAN mode simplifies deployment and management when setting up a hosted private network solution.

- In a hosted private network solution, there are many address spaces within the hosted infrastructure. The hosted provider needs access to the MiVoice Business for configuration. Customers may be restricted, or they may need access to their local MiVoice Business instances.
- Access to MiVB Multi-instance management is possible from within the hosting provider's address space. Access to the MiVoice Business instances within the MiVB Multi-instance server is also possible from within the hosting provider's address space to assigned MiVoice Business addresses within the hosted space. The same MiVoice Business instances can also be accessed through proxy access. You can access only specific MiVoice Business instances or devices within the customer network using this method.
- Each customer has access to devices within their own network, including any customer-specific MiVoice Business instances. The customer also has access to MiVoice Business instances in the customer address space on an MiVB Multi-instance, depending on MiVB Multi-instance management settings. Customers do not have access to other MiVoice Busi-

ness instances on other customer networks, and they cannot access the management interface of the MiVB Multi-instance.

- You can restrict access to the management plane, in the hosted network or to the customer network. Access to the MiVoice Business instances from the customer network can also be restricted to specific devices and specific subnets within the customer network.

Figure 6: Management access for VLAN installation



Transport Layer

The service provider has several options for connecting the Mitel Unified Communications Service Platform to the Public Network. The PSTN is typically connected to SIP, a soft switch, or a Class 4/5 TDM Switch. These switches are owned and maintained by the service provider or by an independent third party.

MiVoice Border Gateway

MiVoice Border Gateway provides SIP Trunk Channel Proxy capability. In designing SIP trunk networks, pay special attention to tariffing and resiliency considerations from the SIP trunk provider, as these will influence how the SIP trunks are connected to the Mitel Service Platform and to the customers' specific instances. The MiVoice Border Gateway also provides other

functionality, such as IPV4/V6 bridging, and support for protocols such as Key Press Mark-up Language (KPML) for in-band DTMF tone detection.

Third-party Session Border Controller (SBC)

The service provider may also use third-party SBC equipment. Refer to the MiVoice Business Compatibility Reference Document available in the Mitel Knowledge Base on Mitel OnLine.

Mitel 3300 Media Gateway

For connections to PSTN using TDM, Mitel 3300 Media Gateways can be used. Media Gateways are typically networked with the MiVoice Business instances on the Mitel Service Platform using IP Trunking. Alternatively, third-party Media gateways can also be used with SIP trunks.

As discussed in “Customer Premise Equipment” on page 23, there are also options to access the PSTN from customer premise with LIMs and 3300 Media Gateways installed on site.

Chapter 3

DESIGN COMPONENTS

Networking

Networking describes the intra-company communication. This includes the SIP trunks, WAN access, and the Layer 2 and Layer 3 switches.

Network deployment must also consider any provisions for resiliency and redundancy, and quality of service requirements.

SIP Trunking

The Mitel SIP Center of Excellence publishes a SIP interoperability document in the Mitel Knowledge Base (08-5059-0014) that describes the Mitel integration/interoperability certifications for third-party products, services, and solutions.

This document also provides a list of SIP trunking service providers that have been tested for interoperability with MiVoice Business.

WAN access methods

The WAN link is the main link from the customer back to the hosting service provider. The WAN link may need to carry both voice traffic and general internet traffic, and possibly VPN connections between different offices. The primary concern with a hosted voice system is to ensure that the voice arrives in a timely manner, either on the uplink, or on the downlink back to the customer. Voice traffic requires equal bandwidth in both directions for callers to be able to have a conversation.

A number of WAN technologies are possible, but most rely on a limited number of access technologies. Some are described here:

- ADSL: This is primarily a data access connection and primarily used for Internet traffic. The bandwidth is limited and asymmetrical. As a result, it may work for one or two phones, but should not be relied on for voice traffic. aDSL is typically used by home subscribers.
- HDSL or SDSL: This is a higher bandwidth technology with symmetrical connections, typically at T1 or E1 rates. These technologies are more business-oriented, providing more symmetrical bandwidth and some bandwidth management and control.
- T1 or E1: These are dedicated symmetrical connections with known bandwidths. They are typically used for business connections, and will generally provide some bandwidth management and control.
- Wireless: This may provide the necessary bandwidth, but can also be a shared medium so peak and average bandwidths may change depending on the number of users. This may provide some bandwidth management and priority, but these may not always directly relate to LAN priority schemes. Service Level Agreements (SLA) may be more difficult to arrange and guarantee.

The primary requirements for a WAN link are:

- Ensure that there is sufficient bandwidth, both uplink and downlink. Symmetrical links will help guarantee this for both directions.

- You may need to provide a dedicated voice connection away from the existing Internet connection.
- Provide Quality of Service settings, and honour these at the WAN router or firewall.
- Ensure that the service provider can provide a voice and video SLA and honour the Quality of Service settings for downlink data.
- Ensure that the router or the firewall can be programmed to allow passage of particular voice and video traffic.

Layer 2 switches

- Calculate the throughput and number of ports needed.
- Do you need to add inter-switch trunking to provision additional bandwidth?
- Power over Ethernet (PoE): Are there any local maintenance test IP phones in the service provider installation?
- Chassis servers greatly reduce connections and wires.
- Do you need one or more VLANs?
- Can MAC addresses be handled across VLANs?
- Is Spanning Tree Protocol (STP) and roots per VLAN or region needed?
- Consider using Link Aggregation Control Protocol (LACP) between switches for redundant backup server connections.
- Provision throughput per rack. Make each rack self-contained and repeatable, by creating one power and cabling plan that you follow in building all the racks.

Layer 3 and routing

- Calculate requirements for bandwidth throughput and packets per second. Ensure that the plan meets these requirements.
- Minimize routing, while ensuring that you are not creating subnets that are too large, to ensure that broadcast traffic does not overwhelm the available bandwidth.
- Let Layer 2 switches and chassis deal with cross-connects where possible.
- Use a hardware accelerator for basic functions.
- Keep routing simple to maximize hardware acceleration.
- Use internal subnet routing.
- Provide Internet access for the AMC license server.
- Provide VPN for off-site maintenance.
- VPN between hosted sites may be on different routers than the maintenance VPN. This is useful if there is high traffic between sites, for example for resiliency between data centers.
- Program the router Access Control Lists (ACL) for different subnets for source and destination addresses if you need to control access to various areas.

Resiliency and Redundancy

- Plan for network resiliency and redundancy.
  - HSRP, VRRP, RSTP, MSTP, LACP
- Application resiliency and redundancy. Are there any critical applications or services that must be protected; voice applications or network applications, for example? Consider the following solutions:
  - Multiple instances of critical applications.
  - Clustered MiVoice Border Gateways and/or users with Mitel phones. When you use Mitel phones, one MiVoice Border Gateway can be configured as the resilient secondary for all of the MiVoice Border Gateways in the cluster. For full MiVoice Border Gateway resiliency, you need N+1 MiVoice Border Gateways.
  - 1:1 MiVoice Border Gateways on SIP for non-Mitel phones. When deploying third-party phones, MiVoice Border Gateway resiliency must be configured on a 1-to-1 basis; every MiVoice Border Gateway primary must have its own MiVoice Border Gateway secondary.
  - Plan the number of IP trunks and MiVoice Business instances (resilient paths) to call routing.
- Plan incoming and outgoing trunk flow and backup routes.

Note: MCD Release 4.2 has an IP trunk connection limit of 200; MCD Release 5.0 increased that to 2000 connections.

Quality of Service (QoS): Protocols and rules

- What quality of service is required?
  - Do different sites in the network require higher or lower Service Level Agreements (SLA)? Keep in mind that the SLA may or may not honour the QoS settings.
  - Consider whether you need to use Differentiated Services Code Point (DSCP) or 802.1p/Q.
- Is Cisco AutoQoS included? Understand the settings that Cisco AutoQoS deploys on routers and switches.
- What SLA is available with the network carrier? What is the guaranteed bandwidth and throughput? Does it support QoS settings?

Server hardware planning

This section provides guiding questions for the selection and deployment of server hardware. For a list of approved hardware platforms, refer to the MSL Qualified Hardware List.

Choosing servers, number and type

Use the points in this section as reminders for the items you need to plan. See the *MiVB Multi-instance Engineering Guidelines* for detailed server requirements and server configurations for typical MiVB Multi-instance deployments.

- How many servers are required?
- How many customers (or Enterprise branch offices) are there, and what are their typical sizes?
- Run the System Engineering Tool (SET) and the MiVoice Business Multi-instance Engineering Tool (MET) to determine servers and sizes.

Note: A customer-qualified server platform may be allowed. Contact Mitel for more information.

- Decide whether to use rack or blade servers. Consider the attributes of each as described in Table 4.

Table 4: Rack vs. Blade servers

RACK SERVERS	BLADE SERVERS
Unique deployment, differing formants, fixed location	Common chassis, standard format, hot swappable
Many power outlets	Common PSU and supply
Needs Layer 2 switch for interconnect and many connections	Integrated backplane
Resiliency and bonded NICs on each server	Use of VCs reduces resiliency and bonding to software configuration.
Cost effective with smaller number of servers	Cost effective with larger server deployments
Reduced power management	Reduced power consumption, increased efficiency
Rack space is good for small number of servers	Reduced rack space when compared to higher number of dedicated servers

Configuring the servers

- Map servers and functions to logical areas and IP addresses
- Plan primary and secondary devices for failover.
- Plan input and output devices.
- Plan call handling and applications.
- Use IP addresses and number conventions to ease “first sight” location of specific servers.
  - Given a name, could you find that server in the dark?

    - Could you determine the IP address for that device?
- Can the servers use a common footprint for resources?
- Server performance will increase in future releases. Has this been planned for, or can it be used to advantage?
    - Or will you plan to consolidate on a set pattern irrespective of expected server changes?
- Plan required spares based on availability required: See *Telephone System Availability* White Paper (DK117892).
- How many users will be affected if a single server is out of service?
- Will remote access be required?
    - Plan for off-line access.
    - Plan for remotely controlled resets and power bars.
- Provide serial port access.
- Where will servers be physically located?
- Will you be using VMware and virtual Mitel (and/or third-party) applications?
- Plan internal and external connections.
- Plan firewall settings.

Physical site planning

Just as important as the server and provisioning planning is the physical site planning. Consider the elements in the following sections.

Data center

- Where is the data center located?
  - What country
  - City or nearest center
  - Type of building
  - Access to services
  - Is the room or rooms configured for computer equipment?
- How is it secured? Who has access?
- How is it connected to the network or public network?
  - Must have public IP access for AMC
  - What public addresses will be used and who supplies them?
- How much cooling is available?
  - air flow
- Type of server rack possible and how many?
- Simple isolation and identification of equipment (?)
- What is the weight supportable per square foot or square meter?
- Plan for future expansion on site and across sites

Power

- How much power is available and what type?
  - 120 VAC, 240 VAC, single phase or multi-phase?
- Power distribution and connector types
  - C13, C19, NEMA, non-NEMA, and so on.

Security

- Who has access to the data center?
- How is access controlled?

System Management

- How do maintenance staff get access to the management network?
- Use ACL (Access Control Lists) to control how messages are routed.
  - ACL can be used to isolate defined functions at Layer 3.
- User names and passwords

    - Record all names and passwords, especially factory settings. Store them in a secure location and allow access to a limited group of trusted employees.
    - Consider a management strategy to allow different levels of access.
    - Consider situation of someone leaving the management group and still having access.
    - Consider using a central security server, e.g Radius or Tacacs.
    - Provision users and groups of access levels.
- Upgrade process
    - Create a plan for switching users to backup servers. Plan resiliency.
    - Plan time to upgrade, switch databases, and so on. Will these actions be performed locally or remotely?
- Will you need to bring new instances online remotely?
- Will you need to bring new applications online remotely?

Staging area

It is recommended that you also plan for a staging environment. A staging area is more comfortable, and it will usually be less noisy. Repeatedly moving in and out of a secured data center may also be inconvenient for you and for the customer, and it is useful to set up the system first in a controlled environment. Consider the following requirements:

- Pre-stage and test
- Need access to AMC
- Your starting point may be basic, with limited network and management tools.
- Need a local Layer 2 switch with VLAN, and a router
- Need a PC with CD/DVD drive
- Install iLO on every server
- Chassis console and manual programming
- Determine what network equipment can be pre-staged, and what must be installed on-site. Some equipment may need to be integrated with an existing configuration; for example, if using common shared storage or common network configurations.

Licensing

The product licenses are bound to the server hardware. Reformatting the hard drive, or changing the disk (including reformatting) requires new product licenses.

MiVB Multi-instance Manager License (base part number 54004602):

- An MiVB Multi-instance Manager license will provide licenses keys for all instances of MiVoice Business on the MiVB Multi-instance.
- Enter your license ARID on the MSL server-manager Web page under the ServiceLink Blades section.
- The Media Server Manager does not require a license. Need to assign Media server to Application ID if you want to download/install Media Server Manager from AMC.

Offline Licensing is not supported by MICD 1.1 for bulk creation/licensing of MiVoice Business instances. MiVoice Business license updates are required during MiVoice Business Software Upgrades. Network connectivity with Mitel AMC is required.

The Managed Service Provider Program features three licensing models:

- Perpetual Enterprise
- Capital Purchase-based service provider
- Subscription-based service provider.

In all of the licensing models, you must first purchase a MiVoice Business Multi-instance Base SW License for the virtual machines required to turn up the individual MiVoice Business instances. One MiVB Multi-instance Base SW License is required for each MiVB Multi-instance Server; it allows an unlimited number of instances.

Each MiVoice Business instance created on the MiVB Multi-instance platform requires an MiVoice Business base kit with the required system and user licenses applied to that instance. Additional license packs are available that include MiVoice Border Gateway, the right to use Oria, agent licenses, and so on. Ask your Mitel representative for details.

Table 5: Capital Purchase-based Licensing for Enterprise deployments

CAPITAL PURCHASE BASED MIVOICE BUSINESS BASE PACK LICENSING FOR SERVICE PROVIDERS	PART NUMBER	PART REQUIREMENT	FEATURES
MiVoice Business Enterprise SW for MiVB Multi-instance	54005293	• Required per primary/active MiVoice Business instance	Includes: • 16 Enterprise users • 10 SIP Trunks • Does not permit Standard Users • Not for use in service provider deployments

Table 6: Capital Purchase-based Licensing for Service Providers

CAPITAL PURCHASE BASED MIVOICE BUSINESS BASE PACK LICENSING FOR SERVICE PROVIDERS	PART NUMBER	PART REQUIREMENT	FEATURES
MiVoice Business Multi-instance Enterprise Pre-Lic MiVoice Business SW for Service Providers	54005428	• Required per primary/active MiVoice Business instance	• No User Licenses included • Enabled for SIP Trunking and G.729 Compression • Can add only Enterprise-based User License bundles
MiVoice Business Multi-instance Standalone Pre-Lic MiVoice Business SW for Service Providers	54005429	• Required per primary/active Standalone MiVoice Business instance • No Resiliency allowed	• No User Licenses included • Enabled for SIP Trunking and G.729 Compression • Can add only Standard-based User License bundles

Subscription-based Service Providers have the following applicable MiVoice Business Base Packs for the MiVoice Business Multi-instance Platform. The MiVoice Business Packs come at no charge and are available only through entry into the Service Provider Program. Fees are charged on a monthly basis, based on total usage of User per Month Software.

Table 7: Subscription-based Licensing for Service Providers

SUBSCRIPTION MIVOICE BUSINESS LICENSING FOR SERVICE PROVIDERS	PART NUMBER	PART REQUIREMENT	FEATURES
MiVoice Business Enterprise SP Subscription	54005299	• Required per primary/active MiVoice Business instance	• 1000 MiVoice Business • 500 External Hot Desk licenses • 500 Mail box licenses • 2000 SIP Trunk licenses
MiVoice Business Enterprise Gateway SP Subscription	54005306	• Required per secondary/passive MiVoice Business instance, or as a trunking gateway • No Resiliency allowed	• 2000 SIP Trunk licenses

Applications

The applications that are allowed depend on the deployment. For example, some applications work through MiVoice Border Gateway, while others are limited or do not work with MiVoice Border Gateway at all.

Refer to the documentation for the specific application to determine compatibility with MiVoice Border Gateway. The application-specific information should also tell you which versions are compatible with the MiVoice Business Multi-instance you are deploying. Also refer to the *MiVoice Border Gateway Engineering Guidelines* for information about required port configuration.

Note: Both MiVoice Border Gateway and Virtual MiVoice Border Gateway are supported.

MiVoice Border Gateway is compatible with the following applications:

- MiCollab (both on the LAN and on the network edge)
- Mitel Phones
- IP Console
- SIP Phones
- SIP trunks
- MiCollab Mobile Client
- MiCollab Web Client
- MiCollab Client Softphone
- MiContact Center Softphone
- ACD Soft Client

In addition, MiVoice Border Gateway can be clustered with other MiVoice Border Gateways for resiliency, or can be connected in tandem to provide regional handling of trombone voice connections, effectively distributing the voice stream handling across multiple MiVoice Border Gateways. MiVoice Border Gateway can also be used with the integrated Secure Recording Connector (SRC) application to provide recording connections to a remote recording application.

MiCollab (formerly MAS) includes:

- MiCollab Client (formerly Unified Communicator Advanced)
- NuPoint Unified Messaging
- MiCollab speech auto attendant feature (formerly Speech Auto-Attendant)
- MiCollab Mobile Client (formerly UC Mobile)
- MiCollab audio, web, and video conferencing feature (formerly Mitel Collaboration Advanced (MCA))
- MiContact Center Office (formerly Customer Service Manager (CSM))

- MiVoice Business Dashboard
- Teleworker Solution (through an integration with MiVoice Border Gateway)

Additional applications:

- Oria, for integrating management and billing
- MiContact Center and MiVoice Call Accounting

User services/applications:

- Voice mail
- Dynamic extension
- Softphone
- Conferencing
- ACD agents
- Hospitality
- Conferencing and collaboration tools

Mitel
Powering connections

mitel.com