VocalTec Communications Ltd.

The VocalTec Architecture

System Guide

release 1.5

VocalTec System Guide 6th Edition — September 2001.

VocalTec Communications Worldwide Offices
www.vocaltec.com

Headquarters
Israel
Tel:972-9-970-7777
Fax:972-9-956-1867

Americas
USA
Tel:1-201-228-7000
Fax: 1-201-363-8986
South America
Tel: 1-786-425-2099
Fax: 1-786-425-9790

Europe, Middle East and Africa
Italy (HQ)
Rome
Tel:39-06-302-60311
Fax:39-06-302-60312
Milan
Tel: 39-02-380-93278
Fax: 39-02-380-93305

Europe, Middle East and Africa
France
Tel:33-1-4471-3666
Fax: 33-1-4471-3696
Germany
Tel:49-228-30887-20
Fax:49-228-30887-11
Romania
Tel:40-94-364-646
40-93-170-800
Fax:40-1-230-1690
Spain
Tel:34-91-350-6633
Fax:34-91-350-7014
UK
Tel:44-1372-723622
Fax:44-870-1315771

Asia and Pacific Rim
Hong Kong (HQ)
Tel:852-2530-0452
Fax:852-2801-4555
Australia
Tel: 61-2-9006-1310
Fax: 61-2-9006-1010
China
Tel:86-10-641-07140
Fax:86-10-641-07143
Japan
Tel:81-3-5791-1405
Fax:81-3-5791-1406
Singapore
Tel:65-238-2415
Fax:65-238-8230

Publication number: VTMN760115F2

Preface

This section describes the organization of the VocalTec System Guide and indicates where to find information contained in other, related documentation.

Using this Manual

The VocalTec system guide is intended for system administrators who are responsible for the general planning, installation. configuration and management of the VocalTec network.

Organization of this Manual

This manual is divided into the following chapters:

Chapter	Title	Description
Chapter 1	Introduction	Introduces the VocalTec architecture including features, the network configuration and VocalTec components.
Chapter 2	Network Planning	This section provides an in-depth discussion of various considerations that need to be taken into account when designing an IP Telephony network. This includes an example of how to calculate the bandwidth requirements of the network.
Chapter 3	VocalTec Services	Describes the multiple services supported by VocalTec, such as calling card, voice VPN, PC-to-Phone and Web-to-Phone
Chapter 4	Setup and Installation	Outlines the integrated setup process for the VocalTec architecture, and provides references to appropriate documentation on the setup and installation of each of the VocalTec components.
Chapter 5	Troubleshooting	Discusses general VocalTec architecture system problems and solutions to these problems.

Chapter	Title	Description
Appendix 1	Quality Measures	Presents different measures of voice over IP quality.
Appendix 2	Performance Measures	Provides measures of VGK, VNM and VGW performance.

Related Documentation

For information on other VocalTec system documents, refer to the following table.

Name	Description
VocalTec Network Manager Administrator's Guide	Provides a full description of VNM, used for remote monitoring and control of gateways, SIP servers and gatekeepers and for database management.
VocalTec Gatekeeper Administrator's Guide	Provides a full description of VGK, used for addressing and routing of gateways and system security, collection of statistics and CDR generation and as the interface to third party billing systems.
VocalTec Provisioning Utility Administrator's Guide	Provides a full description of VGK DB Admin, the VocalTec Gatekeeper utility used for batch mode operations that add multiple subscribers, gateway and dialing plan entries to the database.
VocalTec Gateway 4/8 Installation and Administration Guide	Provides a comprehensive introduction to VGW 4/8 hardware and software installation and configuration.
VocalTec Gateway 120 Installation Guide	Provides a comprehensive introduction to VGW 120 hardware and software installation.
VocalTec Gateway 480 Installation Guide	Provides a comprehensive introduction to VGW 480 hardware and software installation.
VocalTec Gateway 2000 Installation Guide	Describes how to install the Gateway 2000 hardware platform.

Contents

Appendixes

Chapter 1

Introduction

This chapter provides an overview of the VocalTec architecture, describing the main features, the network configuration and system components.

Overview

The VocalTec architecture is an open, standards-based software platform that forms the foundation for IP Communications solutions from VocalTec. The third generation architecture is capable of sustaining large-scale deployment of IP Communications in the corporate and service provider environments.

Features

The VocalTec architecture is designed to be:

- **Scalable** – Able to support millions of subscribers and an unlimited number of endpoints.
- **Manageable** – Centralized management of network elements.
- **Reliable** – No single point of failure.
- **Flexible** – Modular, supporting configurations for a variety of applications.
- **Secure** – Authentication, authorization and token-based access to services. Fail-over mechanism and information backup.
- **Open** – Runs on industry-standard hardware and software. A variety of APIs allow third parties to interface their systems.
- **Standards-based** – Compatible implementation of the latest industry standards – H.323 V2 and conformance to the IP Implementation Agreement 1.0 and the emerging ETSI TIPHON specification. The VocalTec architecture also supports the iNOW profile.

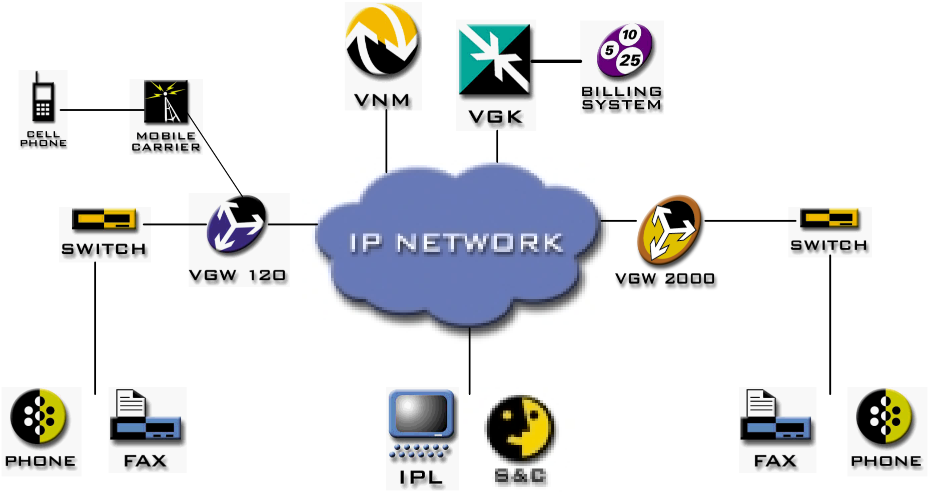


Figure 1-1. VocalTec Architecture Network

VocalTec Network Components

The VocalTec architecture consists of the following network elements:

Network Management Elements

VocalTec Network Manager

The network management utility, for use by service providers in centrally managing and monitoring all the VocalTec architecture devices.

Servers

VocalTec Gatekeeper

The intelligent H.323 V2 IP Telephony service and control server, providing addressing, routing, and system security.

VSS 4000

VocalTec SIP Server 4000 (VSS 4000) is a SIP-based front-end server used for originating calls from SIP clients and passing the calls on to H.323 gateways for termination. VSS 4000 can support up to 4000 simultaneous calls.

VocalTec Gateways

VGW 4 and 8

VocalTec Gateways 4 and 8 (VGW 4 and VGW 8, respectively) are cost-effective H.323 gateways that deliver IP telephony voice and fax services to branch offices, small businesses and home offices. VGW 4 provides up to 4, and VGW 8 provides up to 8, analog telephony interfaces for connection to either an enterprise PBX or to telephones and fax machines.

VGW 120 and 480

VocalTec Gateways 120 (VGW 120) and 480 (VGW 480) are Windows NT based H.323 gateways that bridge the PSTN network to IP networks such as the Internet or intranet. VGW 120 supports up to 120 lines and VGW 480 supports up to 480 lines per gateway.

VGW 2000

VocalTec Gateway 2000 (VGW 2000) provides a high-density, carrier grade, H.323 gateway. The gateway is encased in an ETSI standard shelf, which complies with the ETSI 300 119 requirements. A single shelf supports up to 480 universal ports (16 x E1 trunks). Each port supports a full range of telephony services (voice, fax or voiceband data). VGW 2000 is configured using VocalTec Network Manager 2000 (VNM 2000).

VSG 131/231

VocalTec's Signaling Gateway (VSG) is a signaling front-end that provides connection to Voice Over IP networks. VSG provides SS7 service switching point (SSP) functionality (including IN and CLASS services), and is compatible with national and international carriers worldwide. Comprehensive SS7 tunneling enables end-to-end connectivity in an integrated signaling solution.

End-user Clients

These optional additions to the VocalTec architecture include:

Internet Phone® Lite™ - A client for PC-to-Phone communications, aimed at service providers wishing to redistribute to their subscribers.

Surf&Call™ - A Web plug-in for PC-to-Phone calling from a Web page to any telephone number.

VocalTec Gatekeeper

VocalTec Gatekeeper™ (VGK), the 'intelligent hub' of the VocalTec network, is a Windows NT, standards-based, advanced IP Telephony services and control server. VGK adds intelligence to complex IP Telephony networks by providing centralized addressing, security and accounting for IP Telephony networks.

VGK enables easy interfacing for third party billing, customer care and provisioning systems. VGK is compatible with H.323 V2 compliant IP Telephony elements such as Gateways and Internet Telephony clients. VGK is managed by the VocalTec Network Manager and can also be monitored by a SNMP-based Manager.

Features

- **Addressing** - PC-to-phone, phone-to-phone and Web-to-phone calls and dynamic IP support.
- **Gateway routing** - Flexible gateway least cost routing, permissions, restrictions, hours of service, load balancing and prioritization.
- **Security** - ITU-H.235 based (X.509), authentication, authorization and cryptographic addressing for terminals and gateways supporting IP terminals. Service authorization and authentication.
- **Billing** - Centralized accounting, supporting credit and debit billing.
- **Centralized management** - Manageable through VocalTec Network Manager.
- **Log generation** - Centralized CDR (Call Detail Record) generation; Statistics and event log generation.
- **Reliability** - Through fail-over, replication and watchdog functions.
- **Open** - APIs for interfacing to third party systems including authentication, authorization, accounting, provisioning and routing APIs.
- **Standards based** – ITU-T H.323 v2 RASv2, ITU-T H.235 security, SNMP remote monitoring.
- **Interdomain** - inter-gatekeeper communication, including clearinghouse and settlement capacity.

For more information refer to the *VocalTec Gatekeeper Administrator's Guide.*

VocalTec Network Manager

The VocalTec Network Manager™ (VNM) for Windows NT is an Operations, Administration, Management, and Provisioning (OAM&P) workstation for server elements of the VocalTec Ensemble Architecture.

VNM allows network administrators to manage and monitor the VocalTec architecture gateways and gatekeepers. Servers can be monitored and configured remotely. New users can be provisioned. Alerts are received in real time. VNM provides network administrators with an OAM&P tool capable of managing large scale, distributed IP Telephony Networks.

Features

Remote Device Monitoring

- Graphical network status monitoring by location, status, and device type and Centralized alert collection.
- Statistics monitoring of individual devices.
- Gateway line monitoring.

Remote Device Configuration and Control

- Starting and stopping devices and changing operational modes.
- Controlling device parameters, such as gateway line configuration.
- Changing gateway routing policy and global control over the network dialing plan.
- Database replication control.
- Domain management and dialing plan policy for remote domains.

Service Provisioning

- Centralized provisioning of user services.
- User authorization policy based on global rules and user groups with varying profiles.
- Provisioning for Surf&Call links.

For more information refer to the *VocalTec Network Manager Administrator's Guide.*

VocalTec Gateways

VocalTec Gateway 120/480

The VocalTec Gateway 120/480 (VGW 120/480) provides a bridge between packet networks (Internet/intranets) and the Public Switched Telephone Network. A fully integrated operational design supports multiple types of calling:

- Phone-to-Phone
- PC-to-Phone and Phone-to-PC
- Fax-to-Fax
- Web-to-Phone

VGW processes real-time voice/fax traffic and delivers it (using the VocalTec architecture) to the many points of presence established in key service areas.

VTGW is designed to be:

- **Scalable** - Line density supports multiple T1/E1 spans.
- **Manageable** - Using VocalTec Network Manager, gateways are centrally and remotely managed.
- **Open** - Runs on industry standard hardware. Enables future enhancements and seamless integration of third-party software.
- **Standards Based** - Compatible with the latest industry standards - H.323 V2.

Features

- **Real Time Audio Communication** - Two way, full-duplex audio communication.
- **DSP Based Call Processing** - Incorporating DSP-based call processing affords several operational benefits; achieves higher port density by reducing host utilization for voice algorithm computations and lowers

demands on the CPU to accommodate third-party software add-ons in the same machine.

- **Standards Support** - Allows interoperability between different vendor solutions, including increased firewall support. Provides H.323 support for calls to other H.323 clients and gateways.
- **Codec Support** - High quality codecs, including VocalTec High Quality Codec (VHQC), G.723.1 and G729.
- **Prepaid Debit Card and Credit Billing Support** - Provides the ability to set up timed calls with an enhanced configurable IVR front-end.
- **Remote Management** - Manageable from within the VocalTec Network Manager and compliant with the industry standard, Simple Network Management Protocol (SNMP), for remote monitoring.
- **Telephony Network Interfaces** - Supports E1/T1, PRI, CAS, Analog and SS7.
- **Open Architecture** - Enables future enhancements and third-party software integration.
- **Security** – Password protection for administration functionality with authenticated connection between other VocalTec architecture elements; token-based call setup.

For more information, refer to the *VocalTec Gateway 120/480 Installation Guides.*

VocalTec Gateway 2000

VocalTec Gateway 2000 processes real-time voice/fax traffic and delivers it (using the VocalTec architecture) to the points of presence established in key service areas.

The gateway is encased in an ETSI standard shelf which complies with the NEBS and ETSI 300 119 requirements. A single shelf supports up to 480/384 universal ports (16 x E1/T1 trunks). Each port supports a full range of telephony services (voice, fax or voiceband data). By cascading up to 3 gateways in a rack, a single rack installed in a site can handle up to 1440/1152 simultaneous calls.

The Gateway 2000 fully complies with the ITU-T Recommendation H.323 for gateway applications, ensuring interoperability in a multi-vendor environment and providing the required capabilities for the services' provision.

Features

- High capacity, IP telephony gateway specifically designed for telcos and PTTs.
- Scalable from 2 to 16 E1/T1 trunks per Gateway 2000 shelf. Higher capacities may be achieved by stacking up to 3 shelves per rack and/or using multiple racks in large locations.
- Full support of up to 480/384 Universal ports per shelf (E1/T1), each providing voice, fax and Voiceband Data services interworking, by using field proven signal classification algorithms.
- Compliance with standard compression algorithms, G.711, G.723.1, G.729A as well as proprietary algorithms (e.g., VHQC) with enhanced performance features optimized for IP networks.
- Built in echo canceling according to ITU-T Recommendation G.168, with up to 32 msec tail delay.
- Fax support over high delay networks by invoking remod/demod and spoofing algorithms. Fax-relay support (up to 4.5 sec one-way);. Group 3 fax up to 14.4 kbps (T.38).
- Modular architecture with convenient upgrade paths.
- Provides all VOIP services, e.g., phone-to-phone, PC-to-phone. web-to-phone and fax-to-fax services.
- A standards-based solution that supports H.323 V2 (H.225 RAS) for inter-vendor compatibility and interoperability.
- Working in conjunction with VocalTec Gatekeeper, a full signaling terminating point is provided, thus supporting all the routing and switching needs to interwork between the PSTN and IP network.
- Full Failure, Configuration, Alarm handling, Performance and Security (FCAPS) management support, complying with carrier class system standards.
- Enhanced management facilities for the ITSP - in conjunction with the VNM 2000 centralized management console with SNMP support.

- A highly reliable system with fail-over mechanisms, information backup and full redundancy.
- Open for 3rd party utilities integration with other external systems that can enhance IVR services, billing facilities, network management facilities and customer care control.
- Remote provisioning, and remote software download of new version upgrades.
- Supports PSTN core signaling protocols: PRI ISDN and SS7.
- One-step and two-step dialing support with internal or IVR.
- Built in IP switch function between 10BaseT and 100BaseT interfaces.
- Full carrier class shelf complying with both ETSI and NEBS standards.

Internet Phone Lite

Internet Phone® Lite™ (IPL) is a compact, efficient client application that allows service provider customers to call from their PC to any telephone. The calling process is similar to using a regular telephone.

Internet Phone Lite is available on the VocalTec Architecture CD and can be distributed by service providers to their customers (check the VocalTec licensing agreement).

Service providers may create private label (customized) versions of Internet Phone Lite using the Internet Phone Lite Service Provider Kit.

Implementation of the Internet Phone Call Waiting (never busy) service enables users to receive incoming phone calls on their PC, while they are connected online to the network and their phone line is busy.

Features

- **Phone List and Quick Dial Options** - Configurable quick dial buttons and a phone list enable users to enter frequently used numbers and call with a single click. Other calling options make calling quick and easy.
- **Audio wizard** – A built-in audio wizard enables users to fine-tune their audio for optimum performance
- **High quality audio codecs –** Proprietary VHQC and high quality codecs such as G.723.1 provide near telephone like voice quality.
- **Service options** – Enable users to automatically update existing services and install new services.
- **Connection options** – Allow users to connect to the Web site of their service provider.

For more information on implementing the PC-to-Phone service, refer to the *PC-to-Phone Services Supplementary Document.*

Surf&Call

Surf&Call™ is a Web browser plug-in for real-time voice communications. Surf&Call buttons are embedded on the company's Web pages. When a user clicks upon a button with a predefined number or enters a number and then clicks the Surf&Call button on the Web page, the user is immediately connected to the number and can start speaking, just as with a regular telephone using the speakers and microphone connected to the PC.

Various options that can be accessed by right-clicking the Surf&Call button enable users to adjust the volume and sound quality and end the conversation. The first time that the user accesses the Surf&Call-enabled page, the required Surf&Call files are downloaded to the user's computer. For most Web browsers, the download is automatic and quick.

The VocalTec Surf&Call API enable developers to customize the Surf&Call functions and events accessed from Java and JavaScript.

Features

- **Pay by Phone** – Online shopping sites gain the critical human voice interaction element with links to live operators who can take down ordering and credit card information.
- **Call for Assistance** - Provides a quick means for online customer support and assistance.
- **Call Centers** – Call Centers can add an easy-to-navigate Web interface to their 1-800 numbers. Users simply click on the appropriate Surf&Call button and are immediately connected to the 1-800 number. Data sharing functionality can be added to the call session, in a VocalTec Surf&Call Center configuration.
- **Online Directory Service** - Enterprises can use a Web-based database of Surf&Call links to publish a corporate or public phone directory. Employees or customers click the desired link to call the number over the Internet.
- **Toll-free Calling** - Service providers can host Surf&Call links to their gateways, thereby adding services like 1-800 to their telephony offerings.

The VocalTec Architecture As a Services Platform

Applications of the VocalTec architecture include the following solutions for carriers and service providers:

- **Phone-to-Phone** - Calling from a telephone to a telephone.
- **Fax-to-Fax** - Calling from a fax machine to a fax machine.
- **Voice VPN** - Calling over a voice Virtual Private Network.
- **PC-to-Phone** - Calling from a PC client such as Internet Phone Lite to a telephone.
- **Web-to-Phone** - Calling from a Surf&Call enabled Web page to a predefined telephone number.
- **Internet Call Waiting (ICW)** - Forwarding of a user's phone calls to their PC client (e.g., Internet Phone Lite) while they are logged online to the Internet and their phone line is busy.
- **Exchange Carrier** - Interdomain clearinghouse interconnectivity between the domains of different service providers.
- **Tandem Switch** - Provides a packet-based class 4 switch solution as an alternative to PSTN class 4 switches.

The VocalTec architecture offers an open platform upon which advanced communication services can be built. Add-on modules offering these services are available from VocalTec.

For more information on the VocalTec architecture services, refer to *Chapter 3, VocalTec Services.*

Call Flow Scenarios

The following scenarios illustrate basic intra-domain call flows (under the H.323 standard recommendations). A domain is the area or network controlled by a single service provider. The call flows do not contain all message flows that are passed by all components during a call. The call flows described in this section include:

- Phone-to-Phone
- PC-to-Phone
- Phone-to-PC (Internet Call Waiting)
- Web-to-Phone (using Surf&Call)

For more information on interdomain call flows, refer to the *VocalTec Interdomain Technical Description Document.*

RAS Protocol Messages

An explanation of the RAS protocol messages discussed in the call flows is provided in the following table:

Protocol Message	Description
ACF	Admission Confirm. The gatekeeper returns permission to make the call plus a list of gateways to service the call.
ARJ	Admission Reject. Client request is not permitted.
ARQ	Admission Request. Client requests permission to make the call.
DCF	Disengage Confirm. End Call status is confirmed.
DRJ	Disengage Request Rejected. End Call status is not acknowledged.
DRQ	Disengage Request. The client requests End Call status.

Protocol Message	Description
IACK	Information Acknowledge. The gatekeeper acknowledges the Information Request response sent from the client
IRR	Information Request Response. Information response sent from the client to the gatekeeper.
LCF	Location Confirm. The gatekeeper confirms the client's location request.
LRJ	Location Reject. The gatekeeper rejects the client's location request.
LRQ	Location Request. The client requests a location service from the gatekeeper.
RBI	Resolve Billing Information. Billing information is resolved.
RCF	Registration Confirmed. The gatekeeper confirms that the client is logged on.
RRQ	Registration Request. The client logs on to the gatekeeper.

Table 1-1. RAS Protocol Messages

For a comprehensive list of relevant RAS protocol messages, refer to the *ITU-T H.323 Recommendation Specifications.*

Phone-to-Phone

This scenario represents a typical IP Telephony service where two gateways in the same domain communicate with each other to enable a phone-to-phone call, routed over the IP network. The local VGK authorizes the phone call, directs it through the appropriate gateway, which terminates the call on the PSTN, and generates billing information.

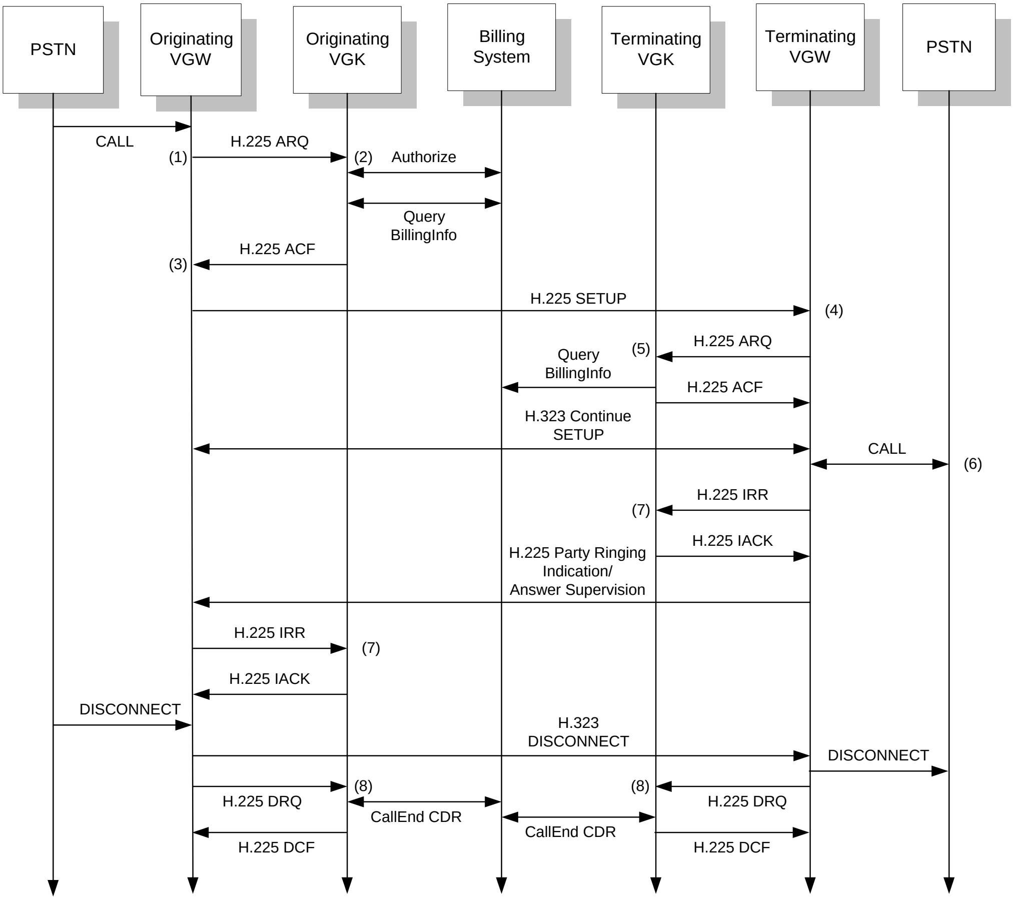


Figure 1-2. Phone-to-Phone (Intra-domain) Call Scenario

1. A call is placed from a telephone on the PSTN. The IVR system on the gateway (VGW) collects user credentials and the telephone number, or

ANI and DNIS and sends the call request to the originating gatekeeper (VGK).

2. The originating VGK authenticates the user information (either querying subscriber information in the database or in the billing system) and authorizes the call request (if external authorization is used). It generates a token and routes the E164 number to an available VGW.

3. The originating VGW checks the list of terminating gateways sent by VGK and sends a token to the first terminating gateway on the list.

4. The terminating VGW validates the token and requests permission to make the call from the terminating VGK.

5. The terminating VGK authorizes the call and sends information to the billing system. The call setup continues.

6. The remote PSTN party hears ringing and answers the call.

7. The originating and terminating VGWs send a *CallStar*t indication to the originating and the terminating VGKs.

8. When the call is disconnected (e.g., one of the parties hang up) the originating the terminating VGKs generate Call Detail Records (CDRs) and send these to the billing system.

PC-to-Phone

This scenario is a typical IP Telephony service where an Internet Phone Lite client wishes to call a standard telephone. The Internet Phone Lite client calls the local VGK, which refers the call to an appropriate gateway. The flow illustrates a user calling from a PC to a regular phone. VGK authorizes the call, directs it through the gateway and generates billing information.

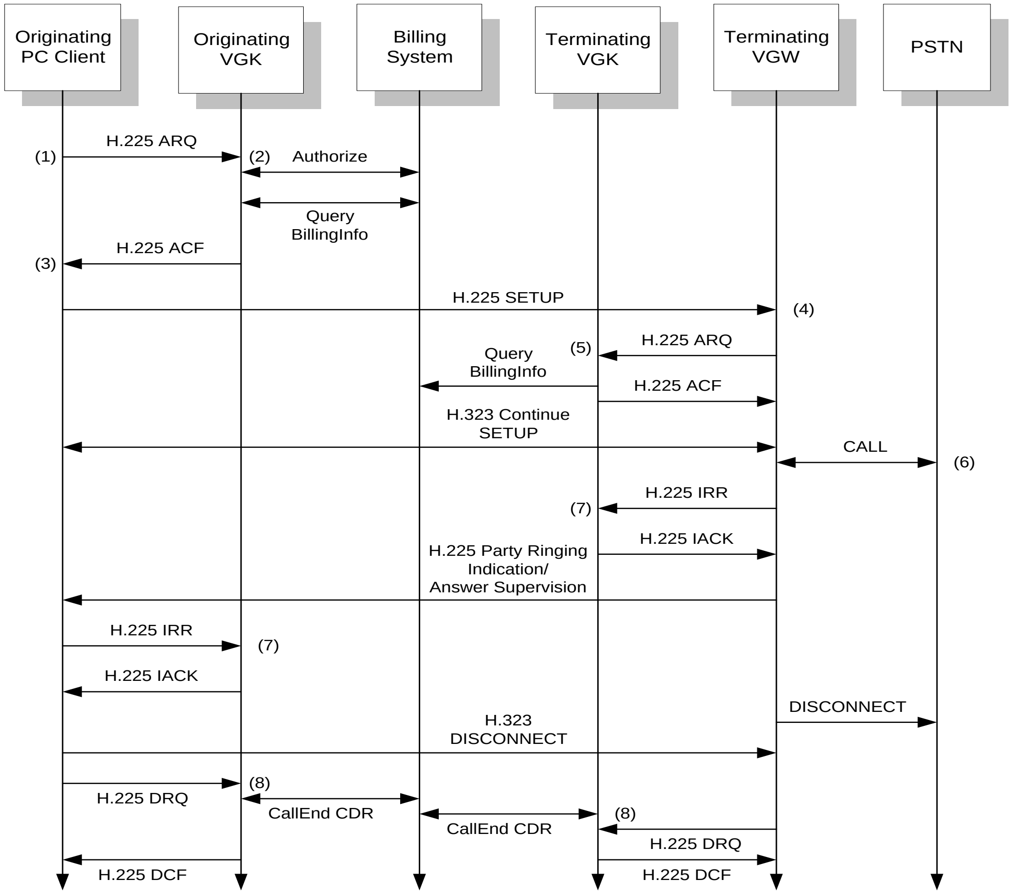


Figure 1-3. PC-to-Phone (Intra-domain) Call Scenario

1. A call is placed from the originating PC client (e.g., Internet Phone Lite) to a PSTN number. The call request is sent to the originating gatekeeper

(VGK).

2. The originating VGK authenticates the user information (either querying subscriber information in the database or in the billing system) and authorizes the call request (if external authorization is used). It generates a token and routes the E164 number to an available VGW.

3. The originating client checks the list of terminating gateways sent by VGK and sends a token to the first terminating gateway on the list.

4. The terminating VGW validates the token and requests permission to make the call from the terminating VGK.

5. The terminating VGK authorizes the call and sends information to the billing system. The call setup continues.

6. The remote PSTN party hears ringing and answers the call.

7. The originating PC client and terminating VGW send a *CallStar*t indication to the originating and the terminating VGKs.

8. When the call is disconnected (e.g., one of the parties hang up) the originating the terminating VGKs generate Call Detail Records (CDRs) and send these to the billing system.

Internet Call Waiting

This scenario describes an incoming phone call that is forwarded to the Internet Phone Lite client when the user is logged online to the Internet and the phone line is busy. Once the service is activated by the user, any incoming phone call that cannot be terminated on the PSTN is redirected by the switch to the user's PC,

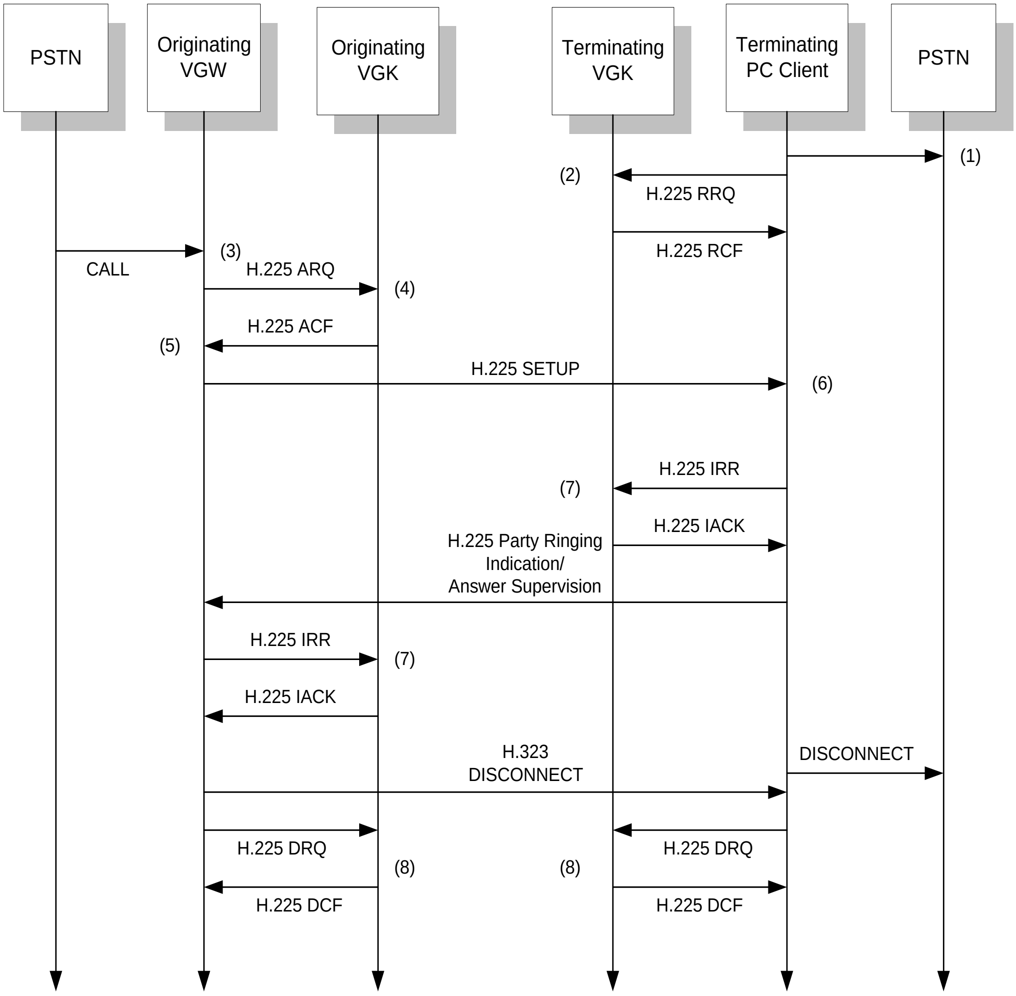


Figure 1-4. Internet Phone Call Waiting (Intra-domain) Call Scenario

1. A subscriber to the ICW service activates the call forwarding mechanism on the switch (either this is done automatically upon dialup by an application on the PC, or it is initiated by the subscriber sending a predefined number sequence to the switch over the telephone). All calls to the subscriber’s phone line will be redirected by the switch to the originating gateway’s (VGW) access number, while the subscriber is logged on to the network.

2. The subscriber connects online to the network (modem/dialup connection) and opens the PC client (Internet Phone Lite). The terminating gatekeeper (VGK) registers the subscriber’s IP address in its dynamic repository.

3. A call is placed from a telephone on the PSTN to the subscriber’s telephone. Since the subscriber is logged online, the line is busy and the switch redirects the number to the originating VGW. The VGW collects the ANI and DNIS or redirect number and sends the call request to the originating VGK.

4. The originating VGK maps the E164 number to the subscriber’s phone number in the database and retrieves the current IP address of the PC client in the dynamic repository. It generates a token and sends the client’s IP address to the originating VGW.

5. The originating VGW receives the PC client’s IP address and sets up a connection with it.

6. The PC client party hears ringing and answers (or rejects) the call.

7. The originating VGW and terminating PC client send a *CallStar*t indication to the originating and the terminating VGKs.

8. When the call is disconnected (e.g., one of the parties hang up) the originating the terminating VGKs generate Call Detail Records (CDRs) and send these to the billing system.

Web-to-Phone

The following scenario describes a call placed from a Web page, containing an embedded VocalTec Surf&Call button, to a predefined telephone number, over the IP network. VGK authorizes the IP-based call and the gateway terminates the call at the predefined phone number

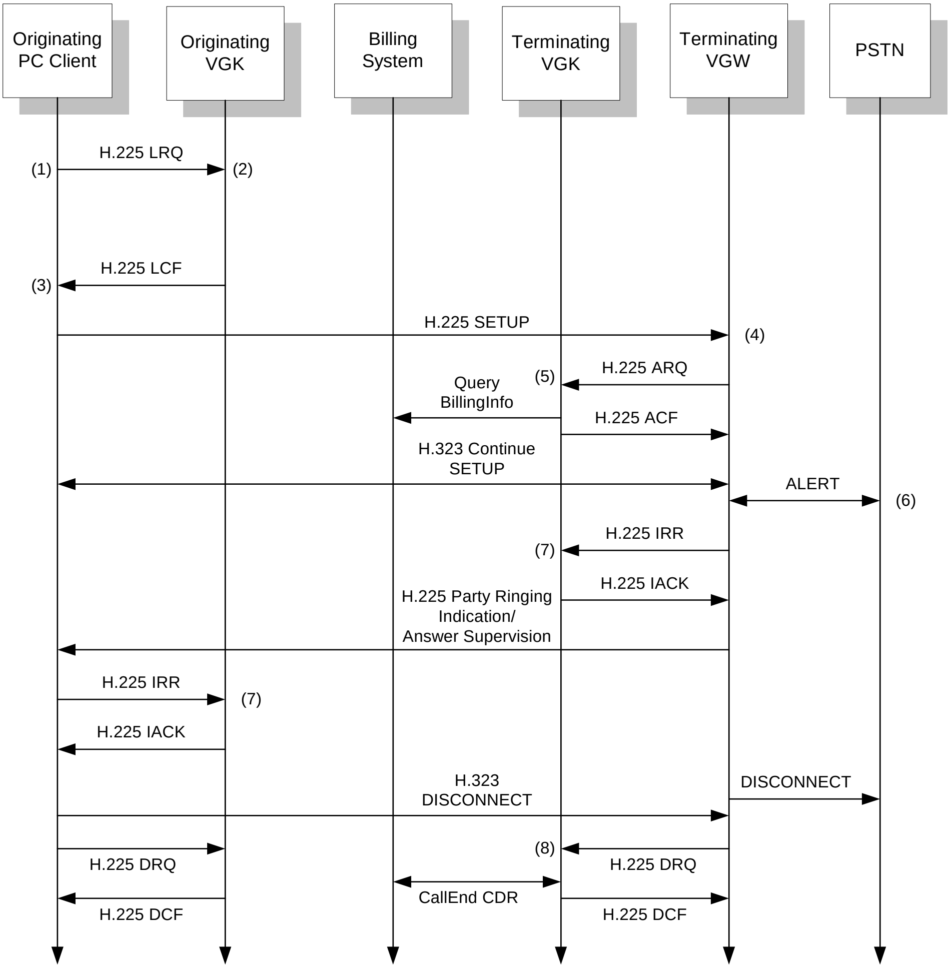


Figure 1-5. Web-to-Phone (Intra-domain) Call Scenario

1. A call is placed from the originating PC client (e.g., Surf&Call) to a PSTN

number, when the user clicks the Surf&Call button. The call request is sent to the originating gatekeeper (VGK).

2. The originating VGK maps the client ID to an E164 number in the database, verifies that the call is placed from a permitted URL and authorizes the call request. It generates a token and routes the E164 number to an available VGW.

3. The originating client checks the list of terminating gateways sent by VGK and sends a token to the first terminating gateway on the list.

4. The terminating VGW validates the token and requests permission to make the call from the terminating VGK.

5. The terminating VGK authorizes the call and sends information to the billing system. The call setup continues.

6. The remote PSTN party hears ringing and answers the call.

7. The terminating VGW sends a *CallStar*t indication to the originating and the terminating VGKs.

8. When the call is disconnected (e.g., one of the parties hang up) the terminating VGW/VGK generate Call Detail Records (CDRs) and send these to the billing system.

Chapter 2

Network Planning

This chapter provides guidelines and discusses important considerations in planning an IP Telephony network based on the VocalTec architecture.

IP Telephony Network Planning

Network planning of traditional telephony is an established field with its own methodology and tools. The development of IP telephony has opened a new field of network planning. IP telephony provides a service rich environment with its own set of network planning considerations.

Carriers and service providers that are starting to integrate IP telephony networks into their existing telephony framework need methodological tools to help them in their planning. Since IP telephony is a relatively new technology, the field of IP network planning is likely to undergo considerable change in the future.

This chapter provides guidelines, considerations and a methodology that can be used when planning an IP network. A basic example is included of one method of calculating network capacity. The contents of this chapter should be viewed as a supplement to traditional network planning methodology used by carriers, service providers, system integrators and network designers.

For more information, contact VocalTec Communications Ltd.

Components of IP Network Planning

When planning for an IP Telephony network, the following network considerations need to be taken into account:

- **Network requirements** - The services to be supported, the number of subscribers the network is intended to support, the type of billing system implementation, network assumptions and telephony interfaces.
- **Network performance** - Available bandwidth, performance, scalability and quality.
- **Network topology** - The type of network structure, design of Network Operating Centers (NOCs), Points of Presence (POPs) and domains.
- **Redundancy planning** - Setup of a fail-over mechanism for handling calls, accounts and the database.
- **Accounting and billing system** - The interface to the third party billing system and the type of billing supported, e.g., credit or debit mode.
- **Security and authentication** - Means for ensuring network security and limiting access to authenticated users, and the use of firewalls
- **Interdomain and settlement -** Bilateral agreements and arrangements with other service providers.
- **Network testing and simulation** - Means of testing the network. including various simulation, performance and quality tests.

The VocalTec architecture provides a full solution that addresses all of these issues. Each is described in further detail.

Network Requirements

Planning your network is based on information on the specific requirements of the service you are providing and basic network assumptions. These include:

- Types of services supported
- Number of subscribers and their distribution
- Characteristics of the billing system
- Network assumptions
- Interdomain and settlement characteristics

This information is used to define the specifications of your VocalTec network.

Types of Services Supported

The type of services supported include:

- Phone-to-phone
- PC-to-phone and Phone-to-PC (Internet Call Waiting)
- Web-to-phone
- Voice Virtual Private Network (Voice VPN)
- Interdomain (exchange carrier solution)
- Tandem switch replacement

Each service has different network requirements. The network interfaces, call set-up process, security, addressing and billing requirements are influenced by the type of service. The decision where to locate originating and terminating POPs may vary for different service types. Each service will require its own unique provisioning.

Number of subscribers and their distribution

The number of subscribers determines the number of available lines, which in turn influences the number of gateways and the distribution of POPs.

Characteristics of the Billing System

The characteristics of the 3rd party billing system (e.g., robustness, interfaces and architecture) influences network characteristics.

For more information refer to *Subscriber Management and Billing*, on page 47.

Network Assumptions

This includes basic information on telephony interfaces (e.g., PRI/E1/T1) the performance characteristics of the network such as the available bandwidth, the quality of the voice service, network security and network redundancy and peak load performance. Performance versus cost constraints determine the basic network constraints.

Interdomain and Settlement

Your network will need to take into account interdomain traffic, where calls are routed from your network to remote service providers or received on your network from other service providers, plus billing settlement of interdomain calls. Your domain may work in a bilateral agreement with service providers from other domains or in a exchange carrier (clearinghouse) arrangement.

Voice VPN

Voice Over IP (VOIP) Virtual Private Network (VPN) is a service that provides subscribers with a "virtual" private VOIP network that exists on the public infrastructure (the PSTN).

By adding VPN support to an interdomain configuration, we introduce two new features to the system: the ability to route calls to and from remote domains according to source VPN (source-base routing) and the ability to dial short extensions and terminate in remote domain.

Network Performance

Each network element has its own set of constraints. You need to look at the constraints of each component as well as for the entire network.

Network performance is influenced by:

- Bandwidth capacity
- Performance constraints
- Quality constraints

Determining Network Bandwidth Capacity

This section presents the considerations involved in determining the bandwidth, or bit rate, required for voice transmission over IP packet networks.

Unlike traditional telephony, there is no simple rule for calculating the bandwidth. Transmission equipment for voice over the open Internet, and sometimes intranets should be able to handle packet loss and inconsistent transfer rate, in order to deliver guaranteed quality of service.

Within IP networks, each packet includes a header, which contains the necessary information to support the flexible connection capabilities. These headers result in transmission overhead, not present on PSTN communication. The transmission overhead may be reduced in cases of simple connectivity structure, using channel aggregation schemes.

Capacity Analysis

Any capacity analysis should provide estimates of the network capacity requirements (bandwidth, number of lines and number of gateways) needed to support a given population of customers.

Determining the requirements for any segment of the network, requires considering the following elements:

- Number of customers
- Average and peak number of simultaneous calls
- Number of lines needed to support simultaneous calls
- Number of gateways needed in the gateway POP
- Bandwidth of the IP connection between gateway POPs

Figure 2-1 illustrates the elements in a segment of the network.

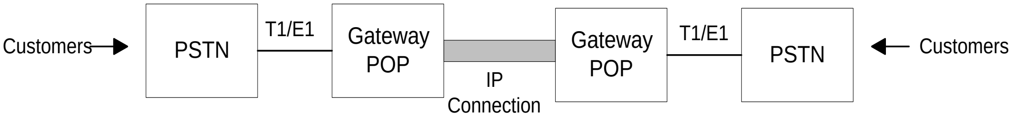


Figure 2-1. Network Segment

The following methodology is proposed as a way to determine the network requirements for a given number of customers:

- Estimate the peak hour characteristics
- Determine the permitted blocking rate during the peak hour and use Erlang's loss formula to calculate the number of users that should be supported simultaneously.
- Decide on the quality of voice and calculate the required bandwidth.

Estimating Peak Hour Characteristics

The peak hour load per customer is the expected percentage of the time that the customer utilizes the gateway during peak hours, assuming all calls are successful. For instance, if a customer is expected to make 2 calls of 6 minutes each during a peak hour, he/she generates a peak hour load of 0.2 (2*6/60=0.2), i.e., 20% of the line is devoted to active calls per peak hour.

There are many different methods of estimating the peak hour load. You can use your own methodology, or one of those outlined below.

One way to estimate the peak hour load is based on the total calling time of one customer per month and on the percentage of the calls that occur in one peak hour.

Another method of estimating peak load is to calculate the average load and multiply it by a factor (based on peak hour statistics of usage, e.g., 10 times the average call load is expected during peak hours). The average load values under various conditions of call usage is displayed in table 2-1.

% of Calls in Peak Hour	Average Customer Calling Per Month (hours)				
	1	2	4	8	16
.0014 (uniform distribution)	.0014	.0028	.0056	.0112	.0224
.0028 (calls 12 hours per day)	.0028	.0056	.0112	.0224	.0448
.0039 (calls during week only)	.0039	.0078	.0157	.0314	.0627

Table 2-1. Peak Hour Calls

Figures in the table represent the percentage of the call line used for active calls (i.e., 0.0224 = 2.24%). For example, assuming a uniform distribution of calls during peak hours (0.14%) and a customer calling an average of 16 hours per month, the percentage of the line used will be 2.24%.

The total peak hour load at one POP is simply the sum of the loads generated by the customers that are connected to the POP. If there are different types of users, you have to calculate them separately and then add them up.

Determining the Blocking Rate and Number of Simultaneous Users

The blocking rate at the peak hour is the percentage of calls that may be blocked under the peak hour conditions.

Erlang's model can be used to estimate the number of simultaneous users. This is the preferred method of most Telcos[1].

When calculating the number of simultaneous users it is important to consider both ends of the gateway. The PSTN end usually requires multiples of 30 (E1) or multiples of 24 (T1). Table 2-2, based on Erlang's loss formula, outlines the total load for multiples of 24 and 30 simultaneous users and for some typical values of blocking rate.

Simult-aneous Users	Blocking Rate							
	0.1%	0.2%	0.5%	1%	2%	5%	10%	20%
24	12.2	13.0	14.2	15.3	16.6	19.0	21.8	26.5
30	16.7	17.6	19	20.3	21.9	24.8	28.1	33.8
48	31.7	33	35.1	37.0	39.3	43.5	48.5	57.3
60	40.8	42.4	44.8	46.9	49.6	54.6	60.4	70.9
72	50.9	52.7	55.5	58.0	61.0	66.7	73.5	85.8
90	66.5	68.6	71.8	74.7	78.3	85.0	93.1	108.2
96	71.7	73.9	77.2	80.3	84.1	91.1	99.7	115.7
120	93.0	95.5	99.4	103.0	107.4	115.8	126.1	145.6

Table 2-2. Call Loads per Blocking Rates and Simultaneous Users

Table 2-2 represents the total call load that can be supported per number of simultaneous users and percentage blocking rate. For example, for 24 simultaneous users and a blocking rate of 0.5%, we can expect an average of 14.2 active lines or ongoing calls.

Calculating the Bandwidth

The type of codec used determines the best trade-off between quality and bit rate. The bit rate during active speech varies between 10Kbps to 40Kbps, depending on

[1] Erlang's model is a basic queuing theory model that assumes independent Poisson call arrivals and independent and identically exponentially distributed calls duration.

Erlang's loss formula computes the blocking rate (B) as a function of the total load (L) and the number of simultaneous users (N) as follows:

$B = (L^N / N!) / (1+L+L^2/2!+\ldots+L^N/N!)$

the following:

- The bit rate of the payload (voice). This depends on the coder you use (G.723, G.729, etc.), the number of frames per packet and whether or not redundancy is used.
- The network overhead bit rate that is generated by the header lengths (RTP, UDP, IP, Datalink layer, etc.).

Each coder has one basic frame size. For example, in the case of G.729 it is 10 ms (80 samples).

On multiple access networks, either LAN or WAN, the relevant figure to consider is close to the average bit rate, which is typically one half of the active-speech value (due to 50% silence compression). On modem connections the maximum bit rate has to be less than the allocated bandwidth.

The more bandwidth that is available, the smaller the packets that can be sent and the higher the sound quality.

Table 2-3 provides various figures for bit rates of coders on different types of networks.

Coder	Packet Size ms	Ethernet 50% Silence Kbps	FrameRelay 50% Silence Kbps	Modem Active bit rate Kbps
G.723	30	12 (15.9)	9.6 (13.5)	20.5 (29.0)
	60	7.6 (11.1)	6.4 (9.9)	13.8 (21.6)
G.729	20	17.2 (22.2)	13.6 (18.6)	29.0 (40.0)
	40	10.6 (15.1)	8.8 (13.3)	18.9 (28.8)
VHQC 9.6	20	18 (23.8)	14.4 (20.2)	30.8 (43.6)
	40	11.4 (16.7)	9.6 (14.9)	20.7 (32.3)

Table 2-3. Coder Bit rates with and without Redundancy

1) The numbers (without brackets) represent average bit rates, without redundancy. The numbers in brackets include redundancy.
2) The modem numbers are for peak rate without silence and include 10% V.42 overhead.

Add to the numbers in the table the overhead for signaling and control. A typical figure for overhead is 10%, depending on the service you provide.

Example

As an example suppose we want to build one POP to support 1500 customers. We should decide how many E1s to connect on the PSTN end and how much bandwidth to supply on the IP side in order to meet some quality of service requirements.

We use the three stages discussed previously:

1. **Estimate peak hour characteristics**.

As an example we assume that each customer will utilize the POP 2 hours per month. By taking a factor of 10 (ratio between peak hour load and average load) with respect to the uniform distribution we obtain a load of 0.028 per customer. The total load on the POP amounts to 42 simultaneous calls.

2. **Decide on the number of simultaneous users with Erlang's loss formula**.

Suppose we have a requirement for maximum 5% blocking rate. The PSTN connection (E1) allows us to use only multiples of 30. According to the Erlang table, for a load of 42 simultaneous calls, supporting 30 simultaneous users is not enough (exceeds 20% blocking) and 60 simultaneous users result in less than 0.2% blocking. A reasonable solution is to support 60 simultaneous users and to allow future growth of the load up to 54.6 simultaneous calls (more customers or more load per customer).

3. **Calculate the required bandwidth**.

We assume a WAN connection over Frame Relay. Although the total bandwidth is calculated to support 60 simultaneous users, it is important to remember that 60 simultaneous users are expected only under extreme conditions. As a result we may require a relatively low bit rate per user in this situation and use G.723 with a packet size of 30 ms. According to Table 2-3 this coder requires 9.6 Kbps, and the total bandwidth amounts to **576 Kbps**. Add to this figure 10% overhead for signaling and control. The final bandwidth required is **634 Kbps**.

4. **Calculate the Number of Gateways**

Now that we know the number of simultaneous calls we can determine the number of lines and gateways needed. To support 1500 customers, which works out to 60 simultaneous users we will need one VocalTec Gateway, with two E1 spans.

NOTE As more lines are available, the number of customers that can be supported per line increases, since the relative variance decreases.

What To Do During Non-peak Hours

Determine different levels of network load (i.e., high, medium and low load hours). During low or medium load hours you may:

- Upgrade the voice quality to consume more bandwidth per customer (e.g., reduce blocking rate and use a better coder).
- Utilize the bandwidth for other services (e.g., fax and data).
- Use a combination of the above two methods.

The VocalTec Architecture System Performance

Call Setup Time

Call setup time refers to the time interval from when the call number is placed until the phone starts ringing at the far end. This should not exceed 5 seconds from PSTN to PSTN signaling, in the worst-case scenario.

Factors that influence call setup time include:

- Response time from originating gateway to the gatekeeper
- Call load on the gateway and gatekeeper
- Performance of the billing system
- IP delays between nodes on the network
- Gatekeeper to gatekeeper communications (interdomain)

The gatekeeper and billing system POPs should be situated either as close as possible to the gateway originating the call request or in a configuration that maximizes throughput and minimizes response times.

For information on Call Setup times, refer to *Appendix 2, VocalTec Performance Measures.*

Call Throughput

Call throughput refers to how many call setups can be done within a certain time interval. This depends on the network load and the number of gateways.

The number of call setups per second also depends on:

- Number of requests the gatekeeper can receive per second.
- Number of responses the gatekeeper can send per second.

Gateway Performance

Gateway performance is influenced by the number of lines that can be supported simultaneously and by the delay required from the end of one call until the start of the next call on the same line.

For information on gateway performance, refer to *Appendix 2, VocalTec Performance Measures.*

Gatekeeper Performance

The performance of the gatekeeper is mainly determined by the number of **call setups per second** that it can support. All other performance issues such as concurrent calls or gateways per gatekeeper are derived from this limit.

Call Setup measures take into account all the communication between the Gatekeeper and **one** endpoint, including communication at the beginning of the call, during the call and at the end of the call. Since, two endpoints are involved in every call, **two call setups** should be counted.

Call setups arrive at the gatekeeper according to a Poisson distribution. If the Gatekeeper supports x call setups per second you must take into account that in certain seconds **there will be more than x call setups** and the gatekeeper will handle them.

Number of Gateway Ports Supported by a Gatekeeper

This number is limited only by the number of call setups per second that the Gatekeeper supports. To translate the number of call setups per second to the number of ports we need some statistical assumptions as to how many call setups per second are generated by one port. If one port generates y call setups per second, the gatekeeper can support x/y ports. The number of call setups per second generated by one port is the inverse of the average holding time per call (including uncompleted call attempts). For example if the average holding time is 180 seconds then each port generates 1/180 calls per second; a gatekeeper that supports x call setups per second can support x / (1/180) = 180 * x ports. If the gatekeeper manages both legs of every call, it will support 180 * x / 2 calls.

For information on VGK performance, refer to *Appendix 2, VocalTec Performance Measures.*

VNM Performance

Any VocalTec architecture set-up needs to consider the number of devices that VNM can support simultaneously.

For information on VNM performance, refer to *Appendix 2, VocalTec Performance Measures.*

Quality Constraints

Quality measures include MOS quality and Mouth to Ear Delay.

For more information on quality measures, refer to *Appendix 1, Quality Measures.*

Network Topology

The VocalTec architecture platform consists of network elements that can be configured under various POP designs. Figure 2-2 and 2-3 show two examples of possible network configurations.

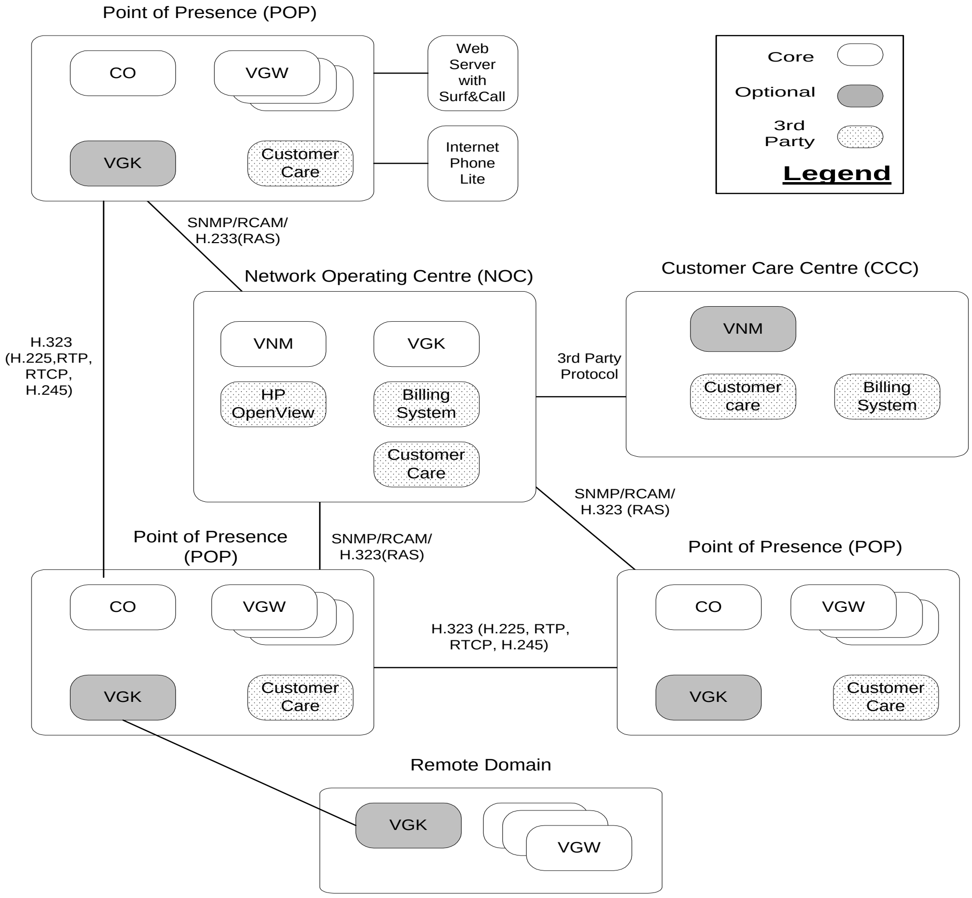


Figure 2-2. VocalTec Architecture Network Configuration Example

In this configuration, a Network Operating Center (NOC) connects to several Points of Presence (POPs) and to the third party billing or Customer Care Center (CCC).

The following diagram (Figure 2-3) shows an example of an alternative VocalTec architecture configuration, using two NOCs for redundancy. The contents of each center can be inferred from the previous example.

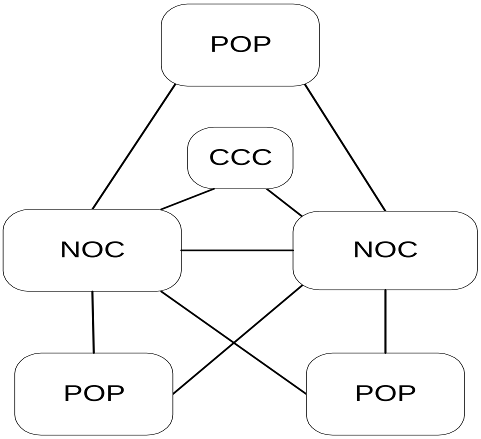


Figure 2-3. Example of an Alternative Network Configuration

The following diagram (Figure 2-4) illustrates the optional and mandatory component services that are installed on the VNM, VGK, VTGW and Billing platforms.

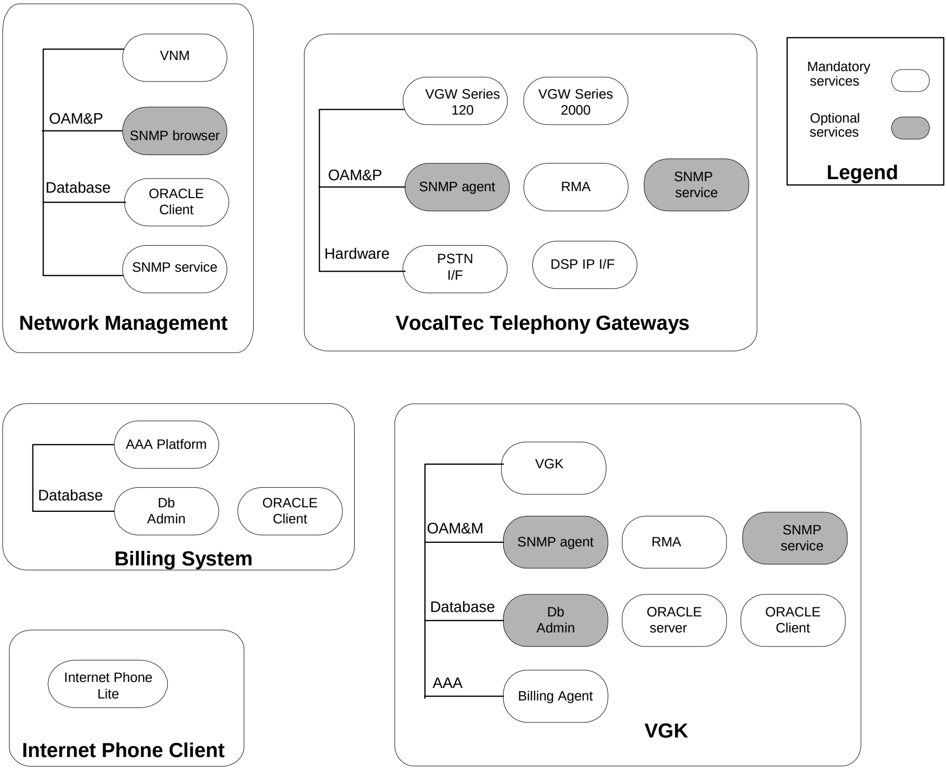


Figure 2-4. Components of The VocalTec Architecture

Network Management Workstation

Network management is provided by the following components:

- *VNM software* - VocalTec Network Management software.
- *SNMP browser* - Optional SNMP applications for remote monitoring of network elements (on the same or a separate workstation).
- *Oracle Client* - Application for connecting to and remote control of the database.

Billing System

The Billing system includes the following components:

- *AAA SDK* - VocalTec's Authentication, Authorization and Accounting software development kit for managing 3rd party billing systems.
- *Oracle Client* and *VocalTec Provisioning Utility* (VGK_DB Admin) - For remote control and configuration of the database.

VocalTec Gateways

The gateway includes the following components:

- *VGW 4/8/120/480/2000* - VocalTec Gateway software
- *SNMP agent* - For remote monitorning of the gateway
- *RMA service* - For remote watchdog monitoring and control of the gateway
- PSTN interfaces and DSP IP interface
- *SNTP servic*e

VocalTec Gatekeeper

The gatekeeper server includes the following components

- *VGK* - VocalTec Gatekeeper software
- *DNS* Installation
- *SNMP and RMA* services
- V*ocalTec Provisioning Utility, Oracle Server* and *Oracle Clien*t
- Third party billing agent
- *SNTP* service
- *Annex G* service (optional)
- *Routing API* - VocalTec's routing software development kit

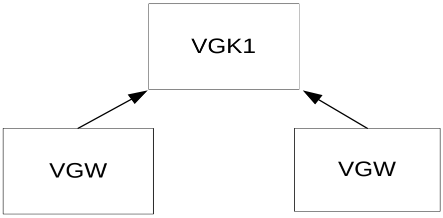
System Configuration Options

This section describes several different gateway and gatekeeper configuration options.

Scenario 1 - Gateways Registered to a Single Gatekeeper

In this scenario, VocalTec Gateway 2000 (VGW 2000) or VocalTec Gateway 120/480 (VGW 120/480) are registered (logged in) to a single gatekeeper (VGK1). There are three possible combinations:

- All gateways are VGW 120/480
- All gateways are VGW 2000
- There is a heterogeneous network of VGW 120 and VGW2000 gateways



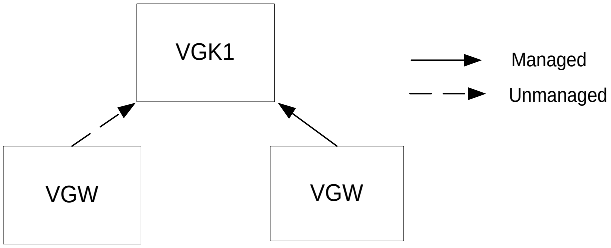
Scenario 2 - Gateways Registered to Multiple Gatekeepers

In this scenario, one gateway is registered (logged in) to one gatekeeper (VGK1). The other gateway is registered to another gatekeeper (VGK 2) and is defined in the VGK1as an unmanaged gateway.

The gateway can be either VGW 2000 or VGW 120. There are three possible combinations:

- All gateways are VGW 120
- All gateways are VGW 2000

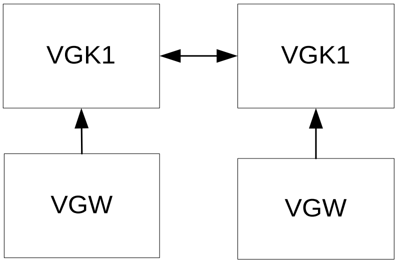
- There is a heterogeneous network of VGW 120 and VGW2000 gateways



Scenario 3 - Interdomain Bilateral Model

In this scenario, two gatekeepers from different domains communicate directly with each other. The gateways can be either VGW 2000 or VGW 120. There are three possible combinations:

- All gateways are VGW 120
- All gateways are VGW 2000
- There is a heterogeneous network of VGW 120 and VGW 2000 gateways

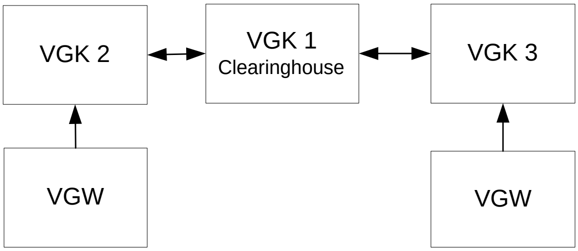


Scenario 4 - Interdomain Clearinghouse Model

In this scenario, the local and remote gatekeepers (VGK 2 and VGK 3) interact via an intermediary Clearinghouse gatekeeper (VGK 1). The gateways can be either VGW 2000 or VGW 120. There are three possible combinations:

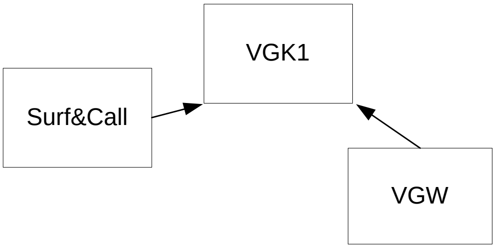
- All gateways are VGW 120
- All gateways are VGW 2000

- There is a heterogeneous network of VGW 120 and VGW2000 gateways



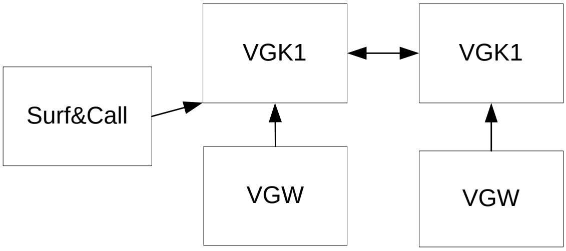
Scenario 5 - Surf&Call

This scenario defines a call from a web page enabled with Surf&Call to a phone number in the local domain, through VocalTec Gateway.



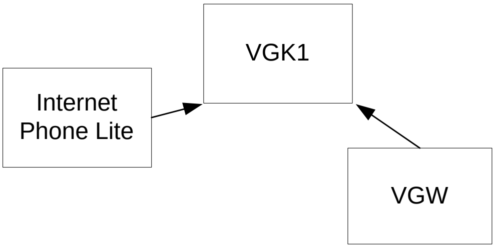
Scenario 6 - Surf&Call in Interdomain

In an interdomain scenario, the call from the web is to a phone number in a remote domain.



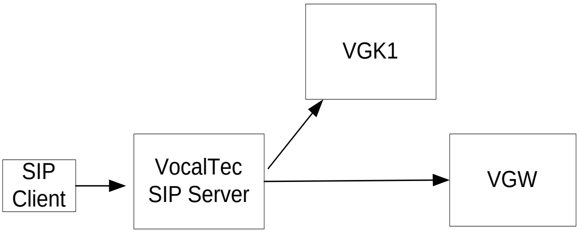
Scenario 7 - Internet Phone Lite

This scenario defines a call from the Internet Phone Lite PC client to a phone, or an Internet Call Waiting (ICW) from a phone to a PC client.



Scenario 9 - VocalTec SIP Server

This scenario defines a call from a SIP client to a VocalTec SIP Server.



Support for Third Party Gateways

VocalTec supports a heterogeneous network of specific third party gateways (e.g., Cisco) and VocalTec gateways. Interdomain capability for third party gateways is also provided. Third party gateways can be managed by VocalTec Gatekeeper or by third party gatekeepers. For more information refer to the *Support for Cisco Gateways Document*.

Subscriber Management and Billing

The availability of a reliable, real-time billing solution is a key component of any IP telephony network.

VocalTec provides an Authentication, Authorization and Accounting (AAA) SDK and corresponding programming interfaces (API) that are used by VocalTec's Gatekeeper for managing interactions with 3rd party billing system providers.

In addition, all billing events are stored in a log file on the Gatekeeper. This log file may be collected and processed later by third party billing systems operating in batch mode and may be utilized in cases where the third party developer does not wish to provide an implementation of the Billing System using the API.

Figure 2-5 provides a description of different options for implementation of the billing system with the gatekeeper.

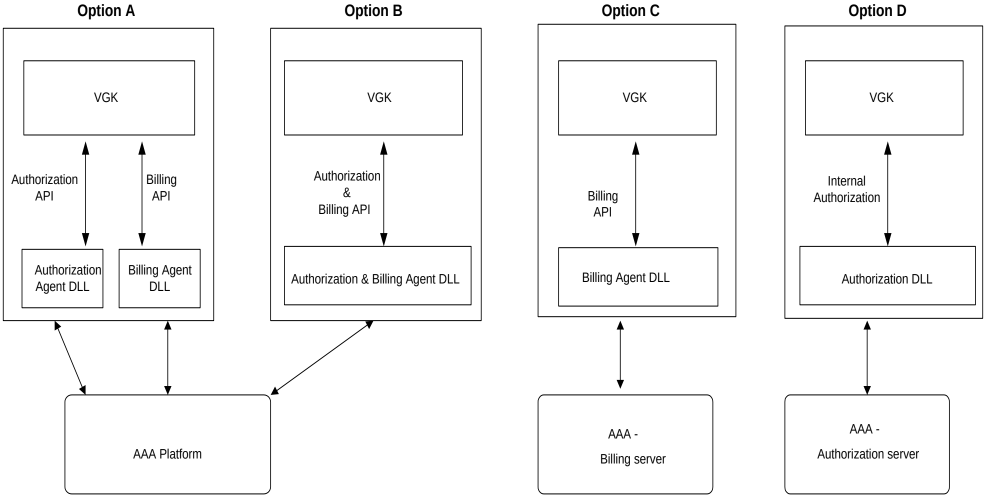


Figure 2-5. Implementation of the Billing System

Figure 2-5 describes four optional method for integrating billing with the VGK:

- **Option A** - each API has a different implemented agent DLL.

- **Option B** - both API's are implemented within the same DLL and connect the same unified billing system.
- **Option C** - same as B, except that the Agent DLL refers to the billing server.
- **Option D** - for authorization purposes only, is done internally on the gatekeeper.

For more information on billing system options, refer to the *VocalTec AAA SDK document*.

Authentication and Security

Network security is an important issue on IP telephony networks. Network security includes the following elements:

- **Authorization** - verifying the rights of a user
- **Authentication** - verifying the identity of a user
- **Authenticity** - verifying the authenticity of the message

The VocalTec architecture provisions for these security factors.

Authorization

VGK provides means for authorization through the use of defined user groups and access rights for gateways and subscribers and through various administrative rights and passwords to the database. Access to gateways and other services are restricted to authorized users. VNM enables provisioning of users and rule-based authorization.

Authentication

Two types of encrypted tokens are used to ensure authentication and provide access to the VocalTec system.

- Authentication tokens
- Access tokens

These tokens are based on H.235.

Authentication Tokens

Authentication tokens are used to authenticate the identity of the user to the gatekeeper. The authentication message is encrypted with user's private password. The authentication is for one time use only and is discarded after use.

Access Tokens

Access tokens verify the right of the user (i.e., via an origination gateway) to access a termination gateway. The access token is encrypted with the terminating gateway's private password and is passed via the H.225 signaling call setup.

Figure 2-6 describes the use of authentication and access tokens on the VocalTec network.

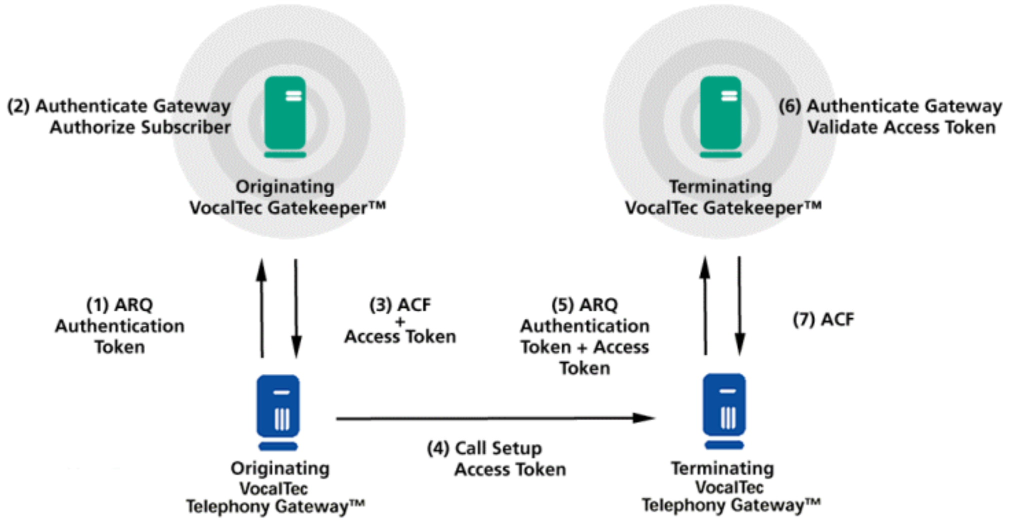


Figure 2-6. Authentication and Access Tokens

ANI Authentication

ANI Authentication is a means of identifying and authenticating a user, based on the incoming ANI. Interactive Voice Response (IVR) modes that support ANI authentication do not require the user to enter any user credentials (i.e., PIN or password). The user is identified based on the incoming ANI.

In a VocalTec architecture configuration, the gateway may offer several variations of ANI authentication. The subscriber may be a 'guest' user (not charged for the call) or not a guest user (charged for the call). The IVR modes also vary as to whether the user is required to enter a telephone number or whether the phone number that is used is the incoming DNIS.

The 'non-guest' IVR modes have two ANI authentication options:

- **ANI with Authentication -** the gatekeeper authenticates the ANI.
- **ANI without Authentication -** (the default mode) the gatekeeper does not authenticate the ANI. The ANI is used as the billing ID in the CDR and in the real-time Billing API.

For more information on ANI authentication, refer to the *VocalTec Gatekeeper Administrator's Guide.*

Other Security Mechanisms

The use of proprietary protocols on the VocalTec architecture provides a further level of security specific to the VocalTec system.

Various call statistics provided by VGK and VNM offer a means for tracking call patterns and identifying incidents of call theft and fraud.

Additional means of network security can be provided through the use of firewalls.

Redundancy and Recovery Planning

Redundancy in the network refers to the existence of backup elements in case of network failure.

By nature, an IP network provides built in rigor and recovery from network failure along any of the nodes, through automatic re-routing of call information to bypass down sections of the network. Various mechanisms keep the network functioning. These include regular polling by system servers and components for the status of devices on the network and for updating changes to the database, and automatic watchdog start-up agents that reboot components that fail (RMA services).

Gatekeeper fail-over can be supplied using DNS text entries. Gateways and desktop clients automatically search for the next gatekeeper in the list if the gatekeeper they are trying to connect to is not available. DNS redundancy is also available.

Gatekeeper redundancy requires a mechanism for replication and updating the database that is shared by multiple gatekeepers, so that the information will always be available, even if one or more gatekeepers go down.

Network Fault Management

Network fault management is concerned with the mechanisms that handle failure on any segment in the network. If temporary problems occur at one of the links in the network, there should be a means of working around this. All links in the network are critical for the correct operation of the network.

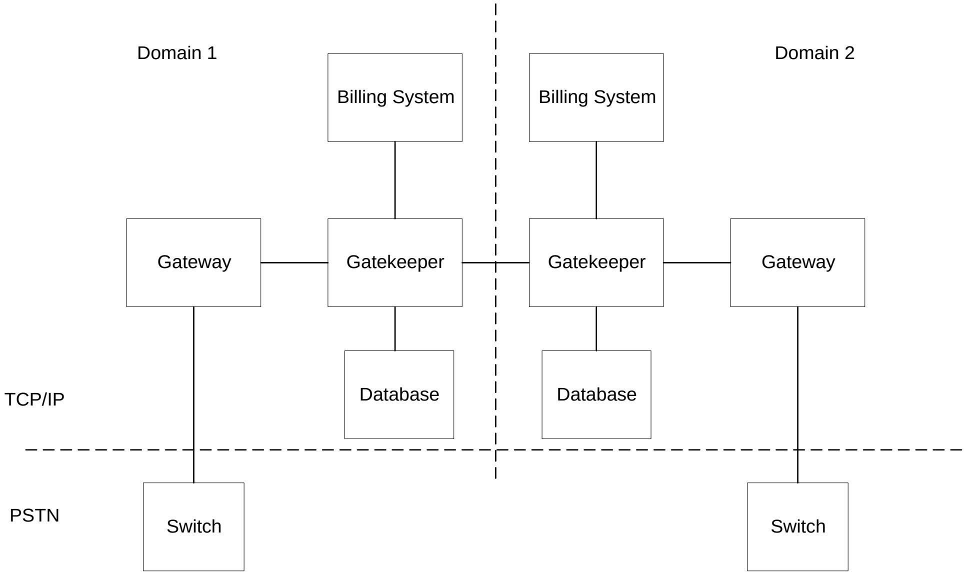


Figure 2-7. Interfaces Between Network Elements

Network Interfaces

The following interfaces should be considered in a VocalTec network:

- PSTN to Gateway
- Gateway to Gateway
- Gateway to Gatekeeper
- Gatekeeper to Billing System
- Gatekeeper to Database
- Gatekeeper to Gatekeeper (interdomain)

PSTN to Gateway Interface

Problems in the connection between the gateway and PSTN could be due to the switch failure or cable connection from the gateway to the switch.

When the gateway detects a lost connection to the PSTN, it goes out of service and logs out of the gatekeeper. As soon as the gateway detects a reconnect, it automatically logs on to the gatekeeper and goes into service.

Gateway to Gateway Interface

There are two types of connections between gateways:

- **RTP (media) connection** - the media (RTP) packets pass through the AudioCodes' TrunkPack 100 board NIC.
- **TCP/IP connection** - the TCP/IP messages of H.225 and H.224 pass through the PC's Host NIC.

When one of the NIC connections is lost, both gateway should detect this as soon as possible and end the call. There are two methods used by the gateway in detecting a lost connection:

TCP/IP Connection

Using an "I am Alive" mechanism, based on the H.225 protocol, the gateways ping each other to determine whether there is an IP connection. If there is no reply after the time-out period (default 30 seconds), the gateway disconnects the call. This is mostly useful for PC to Phone calls, where disconnection of the PC is more likely. This enables the gateway to release the line. However, it doesn't help if there is a disconnection only on the RTP link.

RTP Connection

The gateway detects a disconnection between the AudioCodes TrunkPack 100 card's NIC and its local router by sending frequent ARP messages to the router. If the AudioCodes card detects a disconnection on the RTP link, the gateway disconnects the call. This mechanism is efficient in checking for local disconnection from the router (e.g., the cable was disconnected or the local router is not operating). However it does not provide any indication whether the AudioCodes card's NIC is still connected to the remote side or disconnected from the remote side (for example - due to network problems somewhere on the route).

The gateway also checks returning RTCP packets from the remote gateway. If no RTCP packets are received during a period of 60 seconds, the gateway disconnects the call.

Gateway to Gatekeeper Interface

From the Gateway's perspective

If a gateway loses connection to the gatekeeper, it implements an automatic fail-over mechanism (using the DNS TXT records) to log onto an alternative gatekeeper. If it cannot connect to any gatekeeper, the gateway goes out of service (gracefully). No incoming calls from the Internet or PSTN are accepted during the period that there is no gatekeeper connection. When the master gatekeeper returns to service, the gateway reconnects to it.

The gateway reports all the current ongoing calls that were in session when the gatekeeper connection went down, to a temporary log file on the gateway. When the gatekeeper reconnects, the gateway sends this information to the gatekeeper as an *Update Call Log* (UCL) message. The gatekeeper sends the *Update Call Log* message to the billing system. If the gateway connects to a second gatekeeper, then the UCL message is sent to the new gatekeeper, even if the call session was completed only after reconnection to the new gatekeeper.

From the Gatekeeper's perspective

The gatekeeper keeps a dynamic repository of all calls going through it. If, during an ongoing call session, the gatekeeper detects a lost connection to either the originating or terminating gateway, it initiates *Call End* messages to real-time billing API and writes CDRs for all calls that originated or terminated from the disconnected gateway. The message contains a call duration of zero seconds and a specific disconnect reason.

Since identifying a "lost connection" is based on a specified timeout interval during which the gatekeeper has not heard from the gateway, the gateway does not know if this is a temporary network problem or if the gateway is actually down. If the gateway is in fact not down and the call ended normally, the gateway will eventually send an *Update Call Log* message to the gatekeeper. The billing system gives UCL messages priority over any previous gatekeeper initiated *Call End* messages.

Gatekeeper to Billing System Interface

In the event of a lost connection to a real-time billing system, the gatekeeper has two options:

- Allow call sessions to continue (but lose capability of real-time billing for these calls).
- Disconnect gracefully - complete current call sessions, but do not accept any new calls. The gatekeeper completes ongoing call sessions by writing relevant CDRs and sending *Call End* messages to the third party billing agent installed on the gatekeeper. The billing agent should buffer the *Call End* messages until it reconnects to the billing system.

Gatekeeper to Database Interface

If the gatekeeper experiences a problem connecting to the database it attempts to reconnect automatically after a specified interval. If it does not succeed in reconnecting to the database, the gatekeeper goes out of service and no new calls are accepted.

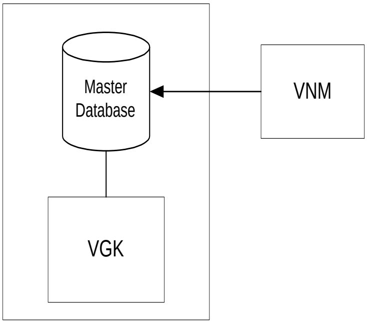
Gatekeeper to Gatekeeper (Interdomain) Interface

In the event of a failure on one of the links, (local or remote gateway to gatekeeper, or gatekeeper to gatekeeper) the gatekeeper transfers any *Update Call Log* messages to the remote gatekeeper.

Gatekeeper Database Options

There are several configuration options for ensuring gatekeeper connection to the database.

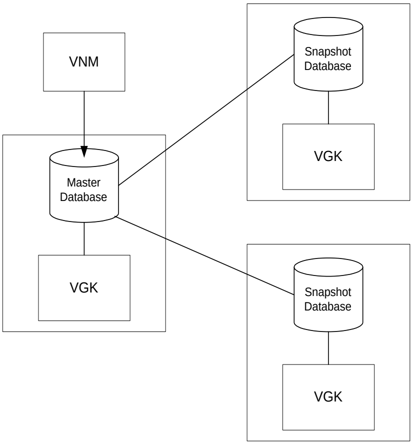
Scenario 1 - Single Gatekeeper - No Replication



In this scenario, the master database is installed on one gatekeeper (preferably at the Network Operating Center). Centralized database management is provided using VocalTec Network Manager.

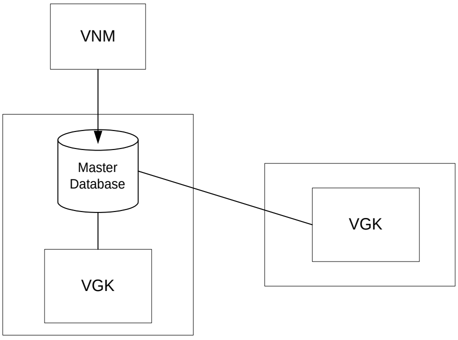
For more information, refer to the *VocalTec Network Manager Administrator's Guide* and the *VocalTec Gatekeeper Administrator's Guide*.

Scenario 2 - Multiple Gatekeepers with Snapshot Replication



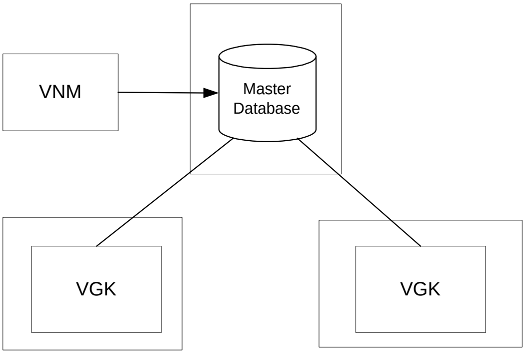
In this configuration, the master database connects to several distributed gatekeepers, each installed with the database "snapshot" versions. This ensures that call and device information is both available and timely (since there is no need to wait for information from the master). Changes to the database can only be made to one centralized source database, which updates all the "read-only" versions.

Scenario 3 - Multiple Gatekeepers - No Replication



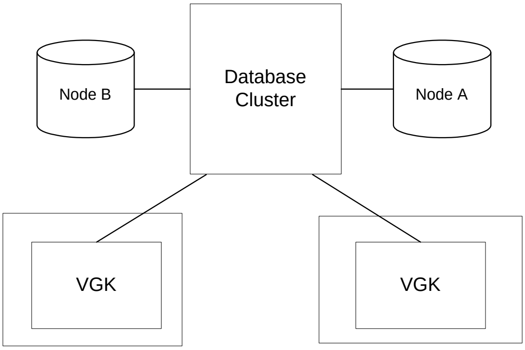
In this configuration, two gatekeepers are connected to the Master database.

Scenario 4 - Master Database on Separate Server



In this configuration, multiple gatekeepers connect to a master database installed on a separate server, apart from the VGK.

Scenario 5 - Gatekeeper Clustering



Clustering provides fail-over when one server in a cluster fails or is taken offline. The other server in the cluster takes over the failed server's operations. Clients using server resources experience little or no interruption of their work as the resource functions move from one server to the other.

In a clustering configuration, one node, called a *primary node*, supports all clients, while its companion node is idle. The companion node is a dedicated spare, ready to be used whenever a failure occurs. If the primary node fails, the spare node immediately picks up all operations and continues to service clients at a rate of performance that is close or equal to that of the primary node.

Setting up a Firewall

When installing a VocalTec system, one issue is how to connect it to a firewall.

When the Internet connection to the local gateway is via a Firewall, you must enable access in the Firewall to allow communication with the gateway. The ports are the standard H.323 ports. Perform the following configuration settings at the Firewall.

RAS Ports

Open the following Firewall ports for both input and output.

TCP	UDP	Interdomain
1720	1718	1717
	1719	

RTP Ports

Open the following Firewall ports for both input and output:

	UDP
For 1 E1	4000 - 4400
For 2 E1	4000 - 4800
For 3 E1	4000 - 5200
For 4 E1	4000 - 5600

SNMP Ports

If the gateway is managed using an SNMP manager, open the following Firewall ports for both input and output.

UDP
161
162

Interdomain and Settlement

In a global network, different service providers must share IP telephony infrastructure via a "clearinghouse" or "exchange carrier" service provider. Interdomain capability is necessary for this exchange to take place. VocalTec provides an interdomain (IDM) solution, based on the VocalTec architecture, for phone-to-phone and PC-to-phone calling over IP networks.

By operating a single authority domain and using a clearinghouse entity, a service provider can establish a single point for external call routing. In the VocalTec IDM solution, the clearinghouse authority owns a domain of gatekeepers (VGKs). The gatekeepers act as mediators between foreign domains.

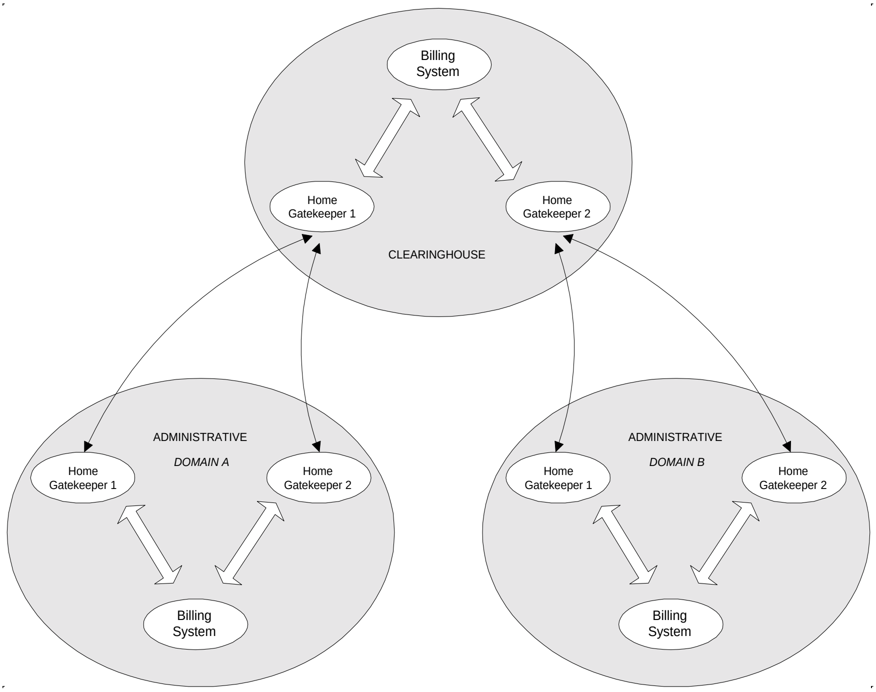


Figure 2-8. Interdomain Clearinghouse Configuration

A domain's gatekeeper is responsible for call management and acts as the central entity for billing. Similarly, in the clearinghouse, the gatekeepers act as a central entity for billing and call management by propagating all relevant call management and accounting messages to the clearinghouse VGK.

In addition to the clearinghouse model, two different VocalTec domains can choose to work in a bilateral model. In this model, the gatekeepers of both domains interact directly for call setup, termination and settlement.

A clearinghouse can terminate calls on gateways connected directly to the clearinghouse's gatekeeper. These gateways need not belong to the clearinghouse, and may be operated by small affiliates that have no gatekeepers and thus are associated with the clearinghouse gatekeeper instead.

VocalTec's commitment to interoperability testing with 3rd party gatekeepers, gateways and clients provides the clearinghouse service provider with flexibility in its interactions with other service provider gatekeepers and other VOIP standard equipment.

Security

Several VocalTec architecture mechanisms enhance network security. Basic VocalTec security mechanisms can be enforced both on subscribers, for regular ITSP domains and also on ITSP domains for a clearinghouse domain. The basic security mechanisms includes the following elements:

- Authorization - verifying the rights of a user/domain.
- Authentication - verifying the identity of a user/domain.
- Access validation - validate usage and access to network endpoints

The VocalTec architecture supports the required mechanisms for non-repudiation.

Domain Identification

In a VocalTec clearinghouse architecture, each domain (ITSP) requires a separate and unique domain ID. These IDs enable identification of different ITSPs for the purposes of settlement.

Each domain requires a pair of authentication private passwords in its relations with the clearinghouse; one for ITSP requests to the clearinghouse and one for the clearinghouse requests to the ITSP.

Authentication

Authentication tokens authenticate the identity of the user (or foreign domain gatekeeper) to the local gatekeeper. The authentication message is encrypted with the user's private password. The authentication is for one-time use only and is discarded after use.

Access Tokens

Access tokens verify the right of the user (i.e., via an origination gateway) to access a termination gateway. The access token is encrypted with the terminating gateway's private password and is passed via the H.225 signaling call setup.

These tokens are based H.235 and include information on the call, caller, domain of caller, valid time interval (start and end time) and other required pieces of information.

The termination domain's gatekeeper generates the access token.

Authorization

A VocalTec domain allows authorization through defined user groups and access rights for gateways and subscribers and through various administrative rights and passwords to the database. Gateway access and other services are restricted to authorized users. Thus, a clearinghouse may maintain specific privilege policies for each different domain. Authorization policies are managed by the VocalTec Gatekeeper RDBMS. VocalTec Network Manager performs provision and control.

Billing and Settlement

In each domain, VocalTec Gatekeeper is the central entity that maintains all call management (i.e. all VGK in a domain are aware of all active calls ongoing through their domain). VGK is also the central location for billing. All billing events are recorded as CDRs to a billing log file on the VGK. Billing events are also exposed to third party billing systems via the Authentication, Authorization, and Accounting software development kit for the VocalTec architecture.

The above billing mechanisms are useful for both the regular ITSP domain and also for the clearinghouse domain. Just as the clearinghouse VGK receives call information (call setup – *AuthorizeCall*, *CallStart* and *CallEnd*), the clearinghouse VGK will also be able to interact with a clearinghouse billing system for real-time settlement.

VGK uses a unique global call ID (based on 128-bit GUID) to associate call messages received at the clearinghouse from both sides of the call.

NOTE Currently, settlement/billing of domains must be post-paid, credit-based (not debit). However, subscriber billing can be both credit or debit.

Dialing Plan Provisioning

The following methods allow separate domains to pass dialing plan information to one another:

- **VocalTec Network Manager** – The clearinghouse network administrator may insert new domains and dialing plans manually.
- **VocalTec Provisioning Utility (DB Admin)** – This utility provides the 3rd party implementers with direct access to the gatekeeper database for addition/removal and update of domain information and dialing plan. This utility is available as a Microsoft® Windows NT™ command-line utility.

Network Management

In a clearinghouse environment, VNM will enable the network administrator to maintain and manage all ITSPs connected to the network. The following tasks can be managed:

- **Global Dialing Plan** - VNM can manage the global dialing plan and manage which domains support which PSTN terminations. Using VNM, an administrator can prioritize specific domains and load balance.
- **Domain Access Rights** - Using VNM, the administrator can manage the access privileges of domains to the clearinghouse domain.

Putting it all Together

Network Design Guidelines

1. Determine the type of IP telephony service you are providing.

2. Make a list of available network resources and budget constraints.

3. Estimate the number of users and their geographical distribution.

4. Use the above information to determine the number of gateways and their location. The number of users determines the number of available lines. The number of simultaneous lines supported determines the number of gateways.

5. Determine the number of gatekeepers. A single gatekeeper can support 92 CAPS (call setups per second), a few thousand user registrations and hundreds of thousands of subscribers in the database.

6. Use load balancing (via the dialing plan and gateway permissions) and redundancy planning to minimize overload to gateways during peak hours. For more information, refer to the *VocalTec Network Manager Administrator's Guide.*

7. Provide redundancy and load balancing for gatekeepers and redundancy through the DNS and secondary DNS setup. For more information, refer to the *VocalTec Gatekeeper Administrator's Guide.*

Guidelines for POP design

POP of Gateways

- Place gateways close to the CO (Central Office).
- Place gateways according to cost-effectiveness. For example, originating gateways should be placed close enough to areas where there is a large concentration of users, so that the cost of the connection to the originating gateway is minimized to a local call.
- Place gateways for cost-effectiveness at the terminating gateways.
- Place gateways for redundancy planning.

Location of Gatekeepers

- Place the gatekeeper on the same POP where there is a concentration of gateways. This will optimize the speed of the connection and reduce the cost of the connection.
- Connect gateways to the gatekeeper in a configuration that provides the maximum bandwidth and minimizes the amount of rerouting.
- Place the NOC gatekeeper (which contains the source or master database) close to VNM.
- Put the gatekeeper next to other gatekeepers for load balancing.

Redundancy Planning Guidelines

- Add an extra gatekeeper for redundancy in case a gatekeeper goes down. The VocalTec system should be configured so that requests can be re-routed. This is done through the use of text records in the DNS. Configure the DNS gatekeeper discovery plan accordingly.
- Provide for VGK load balancing through the DNS configuration.
- Configure DNS redundancy.
- Provision for Billing System redundancy (depending on the architecture).

- Provide alternative endpoints to PSTN terminations (i.e., there must be more than one gateway at critical points and more than one gateway in the same dialing plan group/POP.
- Ensure that different gateway groups are able to support the same calling permissions. The dialing plan is used to order or assign calling priorities to gateways, so that call requests will be transferred to an alternative gateway or gateway group in case a gateway with a higher priority is unable to accept the request (see Figure 2-9).

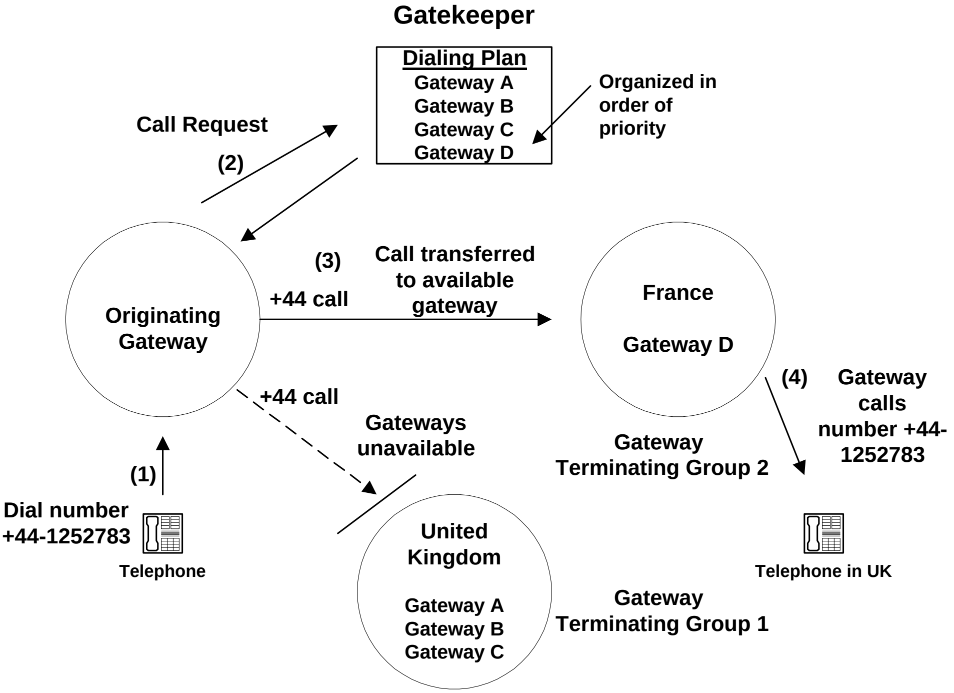


Figure 2-9. Call Redundancy Planning

In the above example, gateways in both France and the United Kingdom are given permissions to support +44 calls (calls to the United Kingdom). The gateways are configured in the dialing plan so that call priority is given first to the UK gateways, i.e., to Gateway A, the primary gateway and then to gateway B and C (secondary or redundancy gateways). If these three gateways are unavailable, the call is passed to Gateway D in France.

Chapter 3

VocalTec Services

This chapter describes the services supported by the VocalTec architecture.

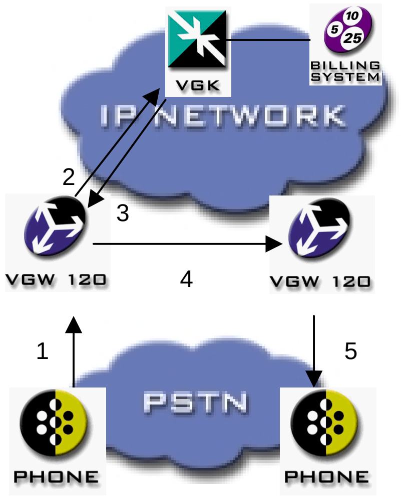
VocalTec Services

The VocalTec architecture supports the following services:

- **Calling Card** - Centralized, cost-effective prepaid/postpaid phone to phone and real-time fax to fax service.
- **Voice VPN** - Offer enterprises a “virtual” private network that runs on top of a shared IP network, typically managed by the service provider.
- **Exchange carrier** - Enables exchange carriers (clearinghouses) to offer service providers global call coverage, regardless of where the service provider owns and operates IP telephony facilities.
- **Trunk replacement** - Offers direct connection between points in the network, bypassing the PSTN and avoiding settlement and leased line costs. This solution is ideal for mobile carriers and long distance carriers.
- **Packet-based Tandem Switch** - combines all the features of a traditional Class 4 switch with the enhanced services of VOIP.
- **Web-to-Phone** - Calling from a Surf&Call enabled Web page to any telephone number.
- **PC-to-Phone** - This simple and innovative service allows business and residential customers to make PC-to-phone calls over the Internet, with VocalTec’s customizable client. The client can be distributed for free.
- **Internet Call Waiting (ICW)** - Forwarding of a user’s phone calls to their PC client (e.g., Internet Phone Lite) while they are logged online to the Internet and their phone line is busy.

Each of these services is described in more detail below.

Calling Card



1. Caller enters calling card PIN and personal ID.
2. VGK Authorizes user credentials (with billing system).
3. VGK returns authorization to gateway and a list of terminating gateways.
4. Gateway transfers call to remote, terminating gateway.
5. Call established with remote telephone.

Figure 3-1. Calling Card Call Flow

Today's Calling Card service providers are seeking ways to reduce costs, increase their service offerings, expand their network of supported call destinations and increase the number of minutes passing through their networks.

VocalTec's pre-paid/postpaid calling card solution is designed to give telephony service providers a competitive edge in the calling card market. Taking advantage of the intelligence embedded in IP network components, it allows service providers to centralize the service application in a single location at a low cost. Service providers can bypass circuit-switched networks, gain customers from countries where they currently have no presence, enjoy low cost termination rates and expand their service destinations using VocalTec's global partner base.

Calling Card Features

The Calling Card solution provides a complete set of traditional calling card features, plus exciting new features to complement the capabilities of current calling card vendors, including:

- **Real-time Billing** - Real-time billing for prepaid (debit) users. The system checks the user's account balance before authorizing the call.
- **Balance and Duration Announcements** - The system plays the remaining balance on the debit card, or the accumulated amount in the credit account. It announces the maximum duration allowed per call.
- **Credit Balance Inquiry** - Card holders may call in to check the remaining balance in their account, via a menu-driven Interactive Voice Response (IVR) system.
- **Balance Warning and Disconnect** - The system alerts the user before the debit card balance is empty and disconnects the call when the balance reaches zero.
- **Password Change** - Enables subscribers to replace their numeric passwords using the IVR menu.
- **Flexible IVR Call Flow** - A flexible interface allows the administrator to modify the IVR call flow.
- **Multiple Language Support** - Allows users to hear professionally recorded prompts and real-time balance announcements in their own language. Implementation options include:
    - **Menu-driven language selection** - the user can select the language desired for IVR prompts.
    - **Automatic language selection** - the system enables automatic language selection based on the ANI or DNIS and eliminates the need to select a language option prior to calling. (1) Future feature

For more information on setting up a calling card service, refer to the *VocalTec Calling Card Solution White Paper*.

Voice Virtual Private Networks

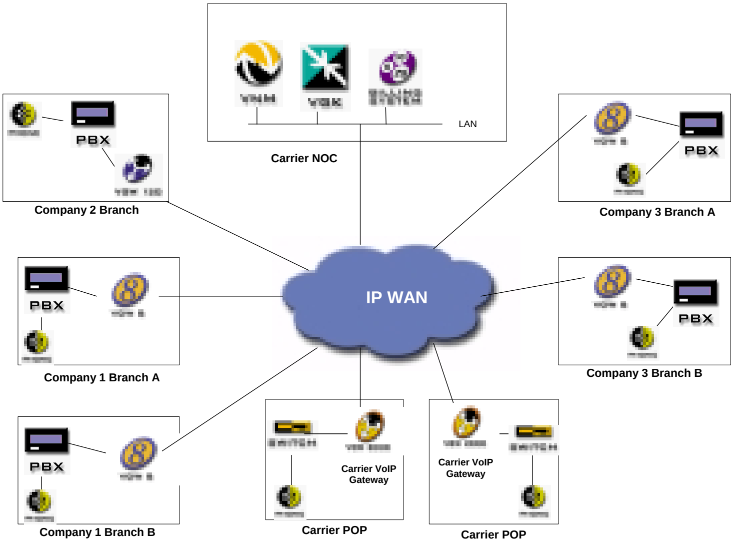


Figure 3-2. Voice VPN Architecture

Voice Over IP (VOIP) Virtual Private Network (VPN) is a service that provides subscribers with a "virtual" private VOIP network that runs on top of a shared IP network, typically managed by the service provider. All subscribers who share the same VPN can call each other seamlessly (either while on the private network or from off the network) as though they were talking on a totally private network.

By adding VPN support to an interdomain configuration, we introduce two new features to the system: the ability to route calls to and from remote domains according to source VPN (source-base routing) and the ability to dial short extensions and terminate in remote domain.

The VPN solution supports a network of Carrier gateways, such as VocalTec Gateway 2000 and Customer Premise Equipment (CPE) gateways, including VocalTec Gateway 4/8 and VocalTec Gateway 120. The VPN solution is also interoperable with third party gateways (e.g., Cisco Gateways).

VPN Call routing is managed by VocalTec Gatekeeper.

Features

- **Private Numbering Plan** - Distant corporate branches within an organization can call each other using PBX extensions or by dialing abbreviated numbers.
- **Multiple VPN Support** - Service providers can support multiple VPNs and offer VPN calling between different organizations, using the same management system. Detailed accounting information on each VPN is supplied.
- **Routing Services** - The same underlying VOIP infrastructure is used for switching calls that may be originated or terminated at a PSTN phone number.
- **Detailed Dialing Plan Configuration** - Network administrators can configure dialing number prefix permissions and restrictions in the same manner as ordinary telephony prefixes.
- **PC-to-Phone** - Allows subscribers to call from their computer to a PBX extension belonging to your organization.
- **Security** - Access to network resources is controlled. Calls that are originated off-site are authenticated. Only users associated with a VPN have access to the VPN and only to the services that they are authorized to use.

Call Modes

The VPN configuration supports the following call modes:

- **On net to On Net** – Intra-organizational calls between two callers on the same VPN.
- **On net to Off Net** – Calls from an organization that terminate outside the company's VPN (in the PSTN).
- **Off net to On Net** – Calls from outside the company's VPN (from the PSTN) that terminate within the VPN.
- **Off net to Off Net** – Calls from outside the company's VPN (from the PSTN) that terminate off net (in the PSTN).

Exchange Carrier

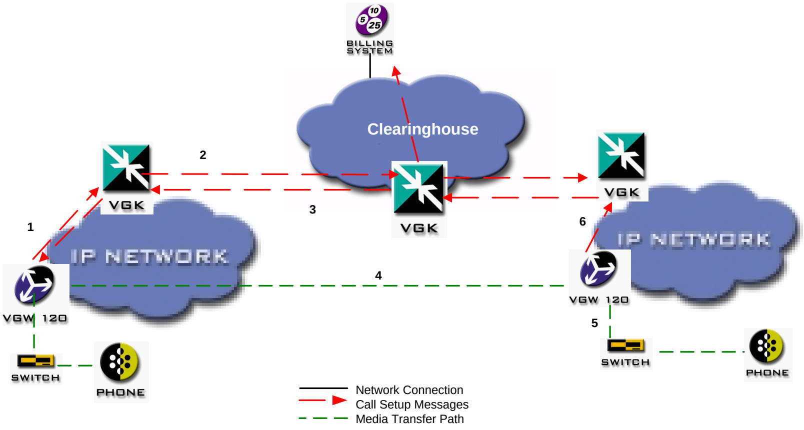


Figure 3-3. Exchange Carrier Architecture

VocalTec 's exchange carrier (clearinghouse) solution provides a cost-effective, flexible, scalable solution.

Multi-tier Exchange Carrier Solution

Exchange carriers are able to operate not only with service providers but also with other exchange carriers. This enables exchange carriers to expand their global coverage options to areas currently not supported.

Domain Identification

Each affiliate domain is identified by a unique ID, which is used for authorization and settlement.

Authentication passwords enable domains to identify each other.

End-to-end Security

The solution provides end-to-end security. Exchange carrier can keep domain information private from other affiliate domains. All service requests from affiliates are authenticated and authorized by the exchange carrier, who can refuse service.

Interdomain security mechanisms include:

- **Authorization** - verifying the rights of users and domains.
- **Authentication** - verifying the identity of users and domains.
- **Access validation** – validating usage and access to network endpoints

Flexible, dynamic routing

Centralized provisioning enables the clearinghouse to control the dialing plan configuration of its affiliates and exchange dialing plan information.

Configuration can be highly specific and detailed.

Network Management

A single workstation provides a centralized point for remote control, configuration and monitoring of all elements in the domain and provisioning capabilities (subscribers, dialing plan and authorization privileges).

Accounting and Settlement

All call management, including accounting, is centralized. The domain is aware of all active calls passing through it.

Real-time Call Detail Records (CDRs) are received from both originating and terminating points.

The exchange carrier can also send their CDRs to terminating affiliates, providing the affiliate with an additional means of verifying call details for accounting and settlement.

Trunk Replacement

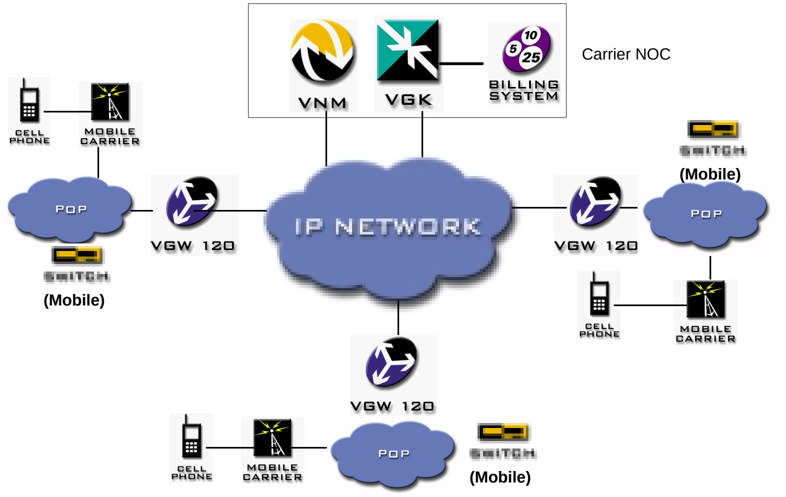


Figure 3-4. Trunk Replacement Architecture

VocalTec's trunk replacement application allows service providers and mobile carriers to transfer and terminate calls over their own VOIP-based network, rather than relying on a PSTN carrier. This provides an alternative channel for transferring calls, which can be used to supplement existing infrastructure and provide an additional layer of redundancy.

VocalTec's VOIP-based solution provides a low-cost alternative for long distance and international calling, enabling mobile carriers to bypass PSTN regulation and terminate traffic with other VOIP partners.

Features

- Provides transparent full-duplex communication for multiple E1 (2.048 Mbps) or T1 (1.544 Mbps) circuit switching connections.
- Excellent performance over distance, with high capacity and reliability.
- Easy setup, installation and operation.
- Support for multiple services
- Centralized management

- Transfers Calling Line Identification (CLI) information for long distance calls from origination to termination points
- Full support for SS7
- One step and two step dialing

For more information on trunk replacement and VOIP for mobiles services, refer to the *VocalTec Gateway 120, VocalTec Gateway 480* and *VocalTec Gateway 2000 Installation Guides*, or contact your nearest VocalTec representative.

Packet-based Tandem Switch

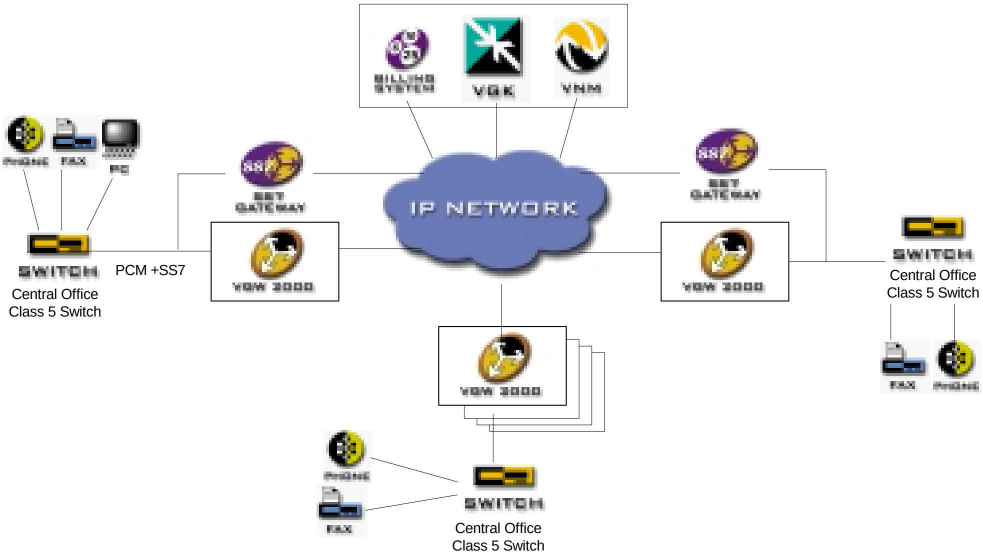


Figure 3-5. Tandem Switch Architecture

VocalTec's standards-based Packet Tandem Switch solution combines all the features of a traditional Class 4 switch with the enhanced services of VOIP, seamlessly integrating circuit and packet-switched networks.

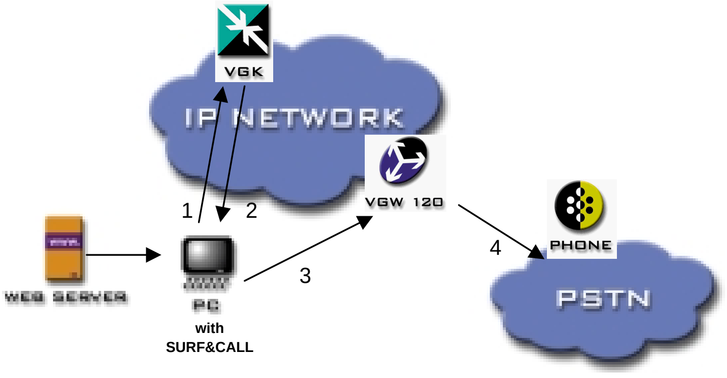
Carriers will benefit from reduced capital and operational costs, while maintaining the high service quality and features of the PSTN.

Features

- Seamlessly integrates with existing PSTN infrastructure
- Provides circuit-switched quality of service and 99.999% reliability
- Supports multiple domains (exchange carrier) and interdomain billing
- Interoperates with leading industry voice and fax equipment vendors
- Provides full SS7 interconnectivity
- Flexible and sophisticated routing options

For more information on the packet-based tandem switch solution, refer to the *Packet Tandem Switch Solution White Paper*.

Web-to-Phone



1. Request S&C authorization.
2. VGK authorizes call.
3. S&C sends call to gateway handling request.
4. VGW transfers call to phone.

Figure 3-6. Web-to-Phone Call Flow

Web-to-Phone is implemented through VocalTec Surf&Call. Surf&Call is a unique Web plug-in that enables a live voice connection from any Web site to any regular telephone over the Internet.

To the end-user, Surf&Call appears as a 'button' on a Web page. With most browsers, Surf&Call downloads and installs automatically when a user arrives at a Surf&Call-enabled Web page. After the plug-in is installed, surfers use their multimedia PC to speak with a representative at a preset phone number anywhere on the PSTN (Public Switched Telephony Network).

A simple mouse click on the Surf&Call button initiates a call from the user's PC over the Internet. The button references a PSTN number listed in the VocalTec Gatekeeper ™ database. VocalTec Gatekeeper verifies the call and provides token-based security. VocalTec Gateway bridges between IP networks and the PSTN. No callbacks or additional phone lines are necessary since a single connection is used for browsing and talking.

Features

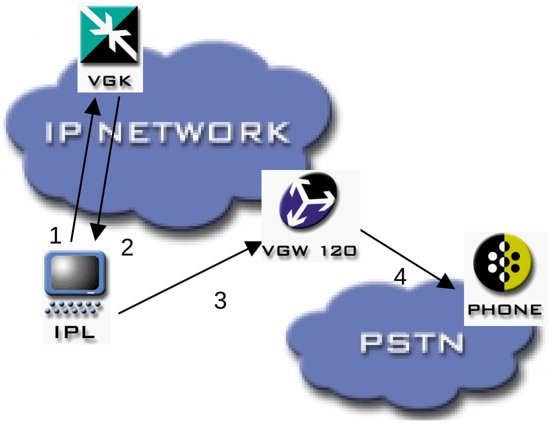
- Call from any Web page to any telephone over the Internet.
- Best Quality VOIP - State-of-the-Art VocalTec technology yields the highest level of voice quality demonstrated over IP networks.
- State-of-the-Art Web Support - Surf&Call downloads automatically within minutes using most popular browsers, including Netscape ® Navigator 4.0 and Microsoft ® Internet Explorer 3.02 and higher.
- Surf&Call is embedded in the Web page and is highly usable in the Web environment.

Development Options

Using the Surf&Call API (Application Programming Interface) developers and Web administrators can fully customize Surf&Call Graphic User Interface (GUI). For example, Surf&Call can display a telephone ringing or any other animation during the call session to indicate the call status (e.g., calling, connecting, during a call, disconnecting etc.) Interactive Voice Response (IVR) Compatibility Existing IVRs work with Surf&Call with full DTMF support. Users simply enter numbers from their keyboard to respond to the system inquiries.

For more information on setting up a Web-to-phone service, refer to the *Surf&Call Service Setup Document* and the *Surf&Call Web Administrator's Guide*.

PC-to-Phone



1. IPL Requests Authorization.
2. Gatekeeper verifies user credentials.
3. IPl turns to gateway to handle call.
4. Gateway transfers call to remote phone.

Figure 3-7. PC-to-Phone Call Flow

This simple and reliable service gives service providers the opportunity to sell low-cost PC-to-phone calling over the Internet to business and residential customers. VocalTec's Internet Phone ® Lite ™ software provides excellent VOIP voice quality. A customization kit enables the service provider to brand Internet Phone Lite to their corporate image and to sell advertising space on the application's user interface. The software can be distributed for free to customers.

User Benefits

Customers who want to use PC-to-phone calling simply download Internet Phone Lite, sign up for PC-to-phone calling service, and make live voice calls from their computer to any phone worldwide – over the Internet. Your subscribers will enjoy the following benefits:

- The integrated option of calling from their computer, without installing a second phone line.
- Subscribers who avoided making international calls will find discount PC-to-phone service more affordable.
- Traveling business executives will appreciate the convenience of using a single phone line for a dial-up connection and phone calls, as well as

reducing expenses on international calling.

- Quick dial buttons and a personalized phone list permit one-step calling.

Calling Card Program

A PC-based calling card can supplement a traditional calling card service. The service can be marketed through existing channels, such as a Web site or retail channel. Card recharging and maintenance can be done through the Web. A phone-to-phone service can be offered on the same platform.

Since the VocalTec architecture can be used in a prepaid or postpaid calling scenario, it is the perfect solution for carriers or calling card companies. The open billing interfaces in the VocalTec architecture permit integration with third-party or legacy billing systems.

Customizable Client

Service providers can custom-brand Internet Phone Lite to meet marketing and customer service needs or to generate revenue from selling advertisement space on it. A detailed design and customization kit for fully customizing the graphic look and feel, user activated Web and Phone links and other features is available from VocalTec.

Offer Internet Phone Lite as an incentive to try the PC-to-Phone Communication service. Users can easily download the client and sign up for the service from your Web site.

For more information on setting up a PC-to-Phone service, refer to the *PC-to-Phone Supplementary Document.*

Internet Call Waiting

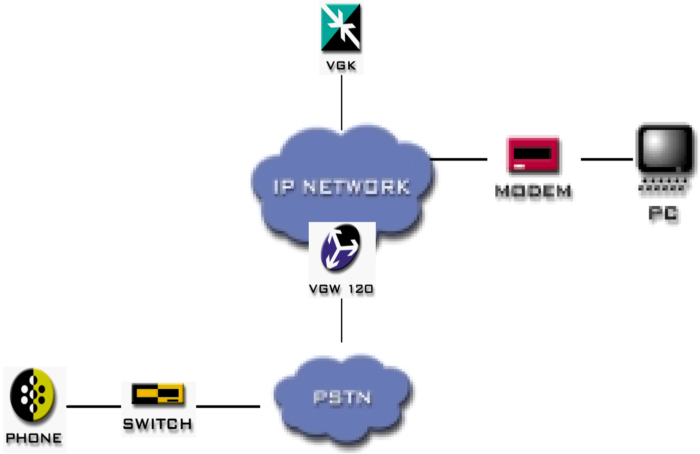


Figure 3-8. Internet Call Waiting Architecture

Internet Phone Lite can provide not only PC-to-phone calling, but Internet Phone ® Call Waiting ™ as well. Internet Phone Call Waiting is an attractive option, available with the same VocalTec infrastructure, which allows users to answer incoming phone calls, redirected to their PC or to an alternative phone, while they are on-line. The service allows users to have a “virtual second phone line.”

For more information on setting up an Internet Call Waiting service, refer to the *Internet Call Waiting Supplementary Document.*

Chapter 4

System Setup and Installation

This chapter describes the integrated setup and configuration of the VocalTec architecture components.

For more information about the installation of each component, refer to the specific Administrator’s Manual or Installation Guide.

System Building Blocks

The VocalTec architecture consists of the following components:

- VocalTec Gateways
- VocalTec Gatekeeper and database
- VocalTec Provisioning Utility
- VocalTec Network Manager
- Desktop Clients (Internet Phone Lite and Surf&Call)
- SNMP network management station (optional)
- AAA Software Development Kit for billing support

Table 3-1 describes the operating system, host hardware and additional specifications for the VocalTec components. For more information about each component, refer to the respective Installation or Administrator's Guide.

Component	Operating System	Host Hardware	Additional
VocalTec Gateway 120	Windows NT 4.0 and Service Pack 6	Fault Tolerant 19" Rack Mounted PC CPU: 850 MHz Pentium III Memory: 256 MB Disk: 4.3 GB Parallel Port 2 ISA slots and 4 PCI slots	Telephony Boards 1-4 Dialogic D300SC-E1 / D240SC-T1 or D600SC-2E1 / D480SC-2T1 DSP Boards 1-4 AudioCodes TrunkPack 100 boards

Component	Operating System	Host Hardware	Additional
VocalTec Gateway 480	Windows NT 4.0 and Service Pack 6	Fault Tolerant 19" Rack Mounted PC CPU: 800 MHz Pentium III Memory: 256 MB Disk: 4.3 GB Parallel Port 2 ISA slots and 4 PCI slots	Boards 1-4 AudioCodes TrunkPack 240 boards
VocalTec Gatekeeper 1000	Windows NT 4.0 and Service Pack 6	Fault Tolerant 19" Rack Mounted PC CPU: 850 MHz Pentium III Memory: 256Mb Disk: 4.3 GB	Database: Oracle version 8.0
VocalTec Network Manager 100	Windows NT 4.0 and Service Pack 6	CPU: 850 MHz Pentium III Memory: 256Mb Disk: 2GB	
Internet Phone Lite 6.1	Windows 95 or Windows NT 4.0	CPU: Pentium 133 Mhz or higher Memory: 16MB (Win 95/98) /32 MB (Win NT) TCP/IP connection	Multimedia equipment (sound card, microphone and speakers)

Table 3-1. Specifications for VocalTec Components

For specifications on the VocalTec Gateway 4/8 and VocalTec Gateway 2000, refer to the respective Installation Guide.

General Specifications

Some Pentium II boards have network and display controllers on board. In this case there is no need for the corresponding controllers specified above. Please make sure that the display controller meets hi-resolution requirements where specified.

For all computers, a SCSI interface is required so as to connect an external CD ROM, unless a built-in CD ROM is provided.

Protocol: **SCSI UltraWide**

Connector: **HD68** (68 pin high density)

For the rack mountable computers, KVM (Keyboard/Video/Mouse) is not specified since the computers will be connected to a KVM switch on the rack.

Where a Microsoft Windows NT workstation is specified, the server edition may be used but not vice versa. Computers should have Microsoft hardware compatibility testing certification (http://www.microsoft.com/isapi/hwtest/hcl.idc). We recommend that the computer vendor be a registered "Dialogic Partner".

System Installation Procedures

Follow the following steps in setting up the VocalTec system:

1. Set up the network, DNS
2. Install the Gatekeeper and database
3. Install VocalTec Network Manager
4. Add the Gatekeeper to the database using VNM
5. Install Gateways and SIP Servers
6. Add Gateways and SIP Servers to the database using VNM
7. Configure the dialing plan using VNM
8. Configure any VPNs using VNM
9. Install SNMP Manager
10. Set up PC to Phone and other services and install desktop clients
11. Configure interdomain parameters and connect to remote domain gatekeepers
12. Test the network functioning

1. Setting up the Network and DNS

For a detailed description of DNS setup and configuration, refer to *VocalTec Gatekeeper Administrator's Guide, Appendix 4, DNS Setup and Configuration.*

Figure 3-1 and Figure3-2 below provide examples of possible laboratory and full deployment configurations of the VocalTec architecture.

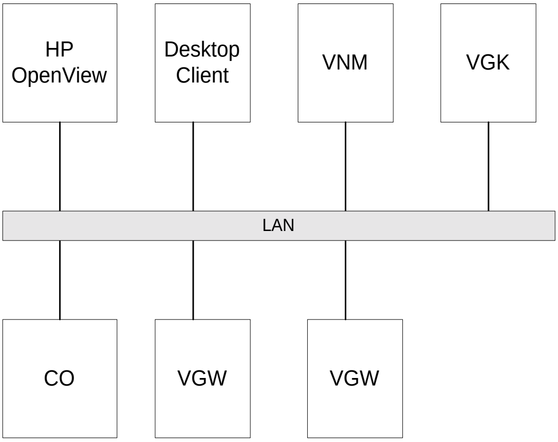


Figure 3-1. Demo/Lab Configuration

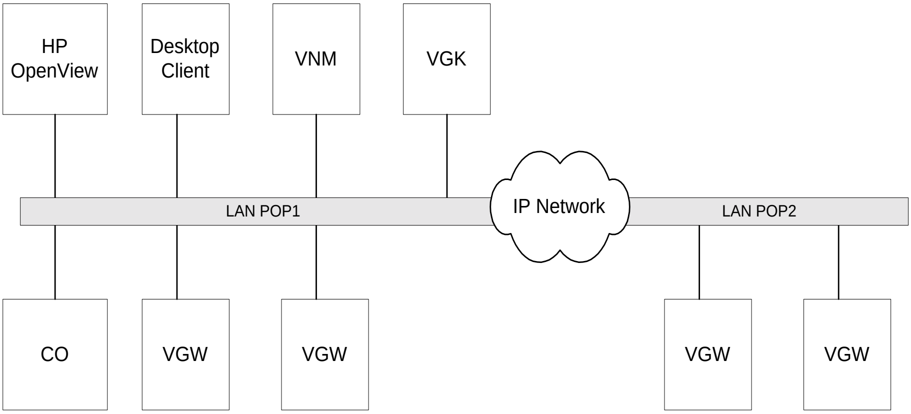


Figure 3-2. Full Deployment Configuration

2. **Installing the Gatekeeper and Database**

Refer to *VocalTec Gatekeeper Administrator's Guide, Chapter 2, Installing VGK.*

3. Installing VocalTec Network Manager

Refer to *VocalTec Network Manager Administrator's Guide, Chapter 2, Installing VNM.*

4. Adding the Gatekeeper to the Database using VNM

Refer to *VocalTec Network Manager Administrator's Guide, Chapter 4, Adding and Removing Gateways and Gatekeepers.*

5. Installing SIP Servers, Gateways and a CO

Refer to *VocalTec Gateway 8, VocalTec Gateway120 and VocalTec Gateway 240 Installation Guides.*

Refer to the *VocalTec SIP Server Installation Guide.*

6. Adding Gateways to the Database using VNM

Refer to *VocalTec Network Manager Administrator's Guide, Chapter 4, Adding and Removing Gateways and Gatekeepers.*

7. Configuring the Dialing Plan using VNM

Refer to *VocalTec Network Manager Administrator's Guide, Chapter 8, Configuring the Dialing Plan*.

8. Configuring VPNs using VNM

Refer to *VocalTec Network Manager Administrator's Guide, Chapter 14, Configuring VPNs.*

9. Installing the SNMP Browser

For more information on installing HP OpenView, refer to the *HPOV Documentation*.

10. Setting up Services and Installing Desktop Clients

For more information on setting up PC-to-Phone services, refer to the *PC-to-Phone Supplementary Document*.

For more information on installing and customizing Internet Phone Lite, refer to the *Internet Phone Lite User's manual* and the *VocalTec Internet Phone Lite Service Provider Kit Manual*.

For more information on setting up the Internet Phone Call Waiting service, refer to the *Internet Phone Call Waiting Supplementary Document*.

For more information on setting up the Web to Phone services provided by Surf&Call and customizing Surf&Call, refer to the *Surf&Call Web Administrator's Guide* and the *Surf&Call API Developer's Guide*.

11. Configuring Interdomain Parameters

Configure the local domain and the dialing plan parameters for routing calls to remote domains. For more information, refer to the *VocalTec Network Manager Administrator's Guide, Chapter 14, Working with Domains.*

12. Testing the Network Functioning

After the network is installed and configured, run laboratory and pilot tests to evaluate and fine-tune the system before full-scale deployment.

For information on VocalTec products that can be used for network simulation, quality and performance testing, contact VocalTec Communications or your nearest VocalTec representative.

Chapter 5

Troubleshooting

This chapter provides a description of common problems and their solution.

Troubleshooting Tips for Installation

- Use meaningful and logical names for system components
- The computer host name should be same as the device name
- Test each component individually in order to isolate problem sources

Event Logs

Event logs produced by the gateways and gatekeepers should be used for troubleshooting purposes. Logs include:

- VGK - event logs, alarms, RMA logs, CDRs and statistics
- VGW - event logs, alarms, RMA logs, and ICAPI logs

VGK and VGW logs are displayed on VNM and also saved locally on the gateway and gatekeeper. For more information on the location of these logs, refer to the relevant Administrator's Guide and Release Notes.

General Troubleshooting

Problem	Solution
Call does not go through the system	• Verify the dialing plan of the gateways. • Make sure that each gateway is in a different group. • Make sure the user has the correct access rights and user credentials. • Restart the gateways. • Restart the gatekeeper.
Desktop Clients do not log in to Gatekeeper	• Verify user groups access rights and security. • Restart the gatekeeper services. • Verify in the VNM global rules window that the subscriber *Registration* option is allowed. • Remove the user record from the database and add it again.

Problem	Solution
Gateways do not log in to Gatekeeper	• Check the DNS settings in the gateways (refer to the *VGK Administrator's Guide*). • Verify gateway access rights groups and services in VNM. • Compare local gateway information with information in the database, using VNM. • Restart the gatekeeper services. • Verify in the VNM global rules window that the gateway *Registration* option is allowed. • Remove the gateway from the database and add it again, using VNM.
SNMP Manager will not run	• Make sure the DNS server can resolve IP's to hostnames.
SNMP Manager will not show all devices	• Make sure all machines have a DNS entry. • Make sure that all machines have the SNMP services installed and running.
VNM will not connect to the database	• Check that the *TNSListener* service and the gatekeeper are running. • Check the TNS alias on VNM.
VNM will not connect to a device	• Make sure the device is running (i.e., service is started). • Verify that the following device information in the database is correct: IP address; Admin port. • Check that the administrative passwords on the VNM and on the local device correspond.

For more information on problems and solutions relating to gateways and gatekeepers, refer to the *VocalTec Telephony Gateway Installation Guide* and to the *VocalTec Gatekeeper Administrator's Guide.*

Appendix 1

Quality Measures

This appendix discusses various measures of audio quality. These include MOS, Call Setup time, Mouth-to-Ear delay, connection speeds.

Quality Measures

Audio Quality

Table 1 below provides some example measures of audio quality.

	4 (Best)	3 (High)	2 (Medium)	1 (Best Effort)
MOS Quality	4.0-5.0	3.8-4.2	2.9-3.8	2.0-2.9
Mouth-to-Ear Delay	0-150 ms	150-250ms	250-450ms	450ms and above
Call Setup	0 sec - 1 sec	1-3 sec	3-5 sec	5 sec and above

Table A1-1. Quality Measures

The system should maintain the same quality level on all parameters.

Speed of Connection

Quality, in terms of speed of connection, also depends on the type of connection The following table describes connection speeds for various media.

	4 (Best)	3 (High)	2 (Medium)	1 (Best Effort)
Direct IP	0 - 500ms	500ms - 1 sec	1 sec - 2 sec	2 sec and above
E.164 Number	0 - 1 sec	1 sec - 2sec	2 sec - 5 sec	5 sec and above
E.164 number via clearing house or roaming	0 - 2 sec	2 sec - 5 sec	5 sec - 10 sec	10 sec and above
E-mail address lookup	0 - 3 sec	3 sec - 10 sec	10 sec - 20 sec	20 sec and above

Table A1-2. Connection Speeds

Network Profiles

The following table provides network profiles for packet loss, delay and jitter, bitrate and buffer.

Loss	Network Delay	Delay Jitter	Bitrate (bps)	Buffer (bytes)
5%	150ms	75ms	28,800	4,094
15%	275ms	150ms	33,600	8,192
30%	450ms	250ms	33,600	8,192

Table A1-3. Network Profiles

Network Delay is the time interval from when the packet leaves the end point until it is received by the remote end point. While bitrate limited devices add delay, this is considered as different from the network delay.

A buffer is used when an end point is sending at a higher bitrate than the link can maintain. Up to a certain number of bytes can be queued for transmission (i.e., in the buffer). When more than the specified buffer accumulates, the data is discarded (i.e., packet loss occurs).

Appendix 2

Performance Measures

This appendix discusses various measures of performance for components of the VocalTec architecture. While these figures reflect currently known data, they may not necessarily correspond to the performance of your particular system configuration and they do not bind VocalTec in any way.

Gateway 120/480 Performance

Each gateway can currently support dual and quad span E1 (96 lines) and T1 (120 lines for VGW 120 and 480 lines for VGW 480).

Call Attempts per Second (CAPS)

92 CAPS with a single VGK 1000 (per Mier lab's report 083100). This measure is application dependent.

Gatekeeper Performance

One VGK (with a single 800 MHz CPU) can support approximately 92 completed call setups per second.

This figure is relevant for completed calls of Phone-to-Phone services. PC-based services will result in a lower number of supported call setups per second due to the additional registration load.

Number of Gateway Ports Supported per VGK

The number of ports supported by a VGK depends on the rate of busy hour call attempts (completed and uncompleted) that are generated by the ports. The rate of the completed call attempts and the rate of the uncompleted call attempts that are allocated to a given set of ports may dramatically change from one service to another, since it depends on calls duration, setup times and design parameters (blocking rate).

VNM Performance

VNM can support about 300 devices simultaneously (under conditions of passive monitoring of the network).

Glossary

The glossary contains an explanation of commonly used terms and abbreviations used in the VEA System Guide.

Dialing Permissions and Restrictions

Permissions/restrictions are dialing codes (number prefixes) that are allowed/ restricted for a specific gateways. Calls to areas that fall outside the allowed prefixes of the gateway will not be handled.

Dialing Plan

Every Internet telephony network has its own dialing plan, which maps the dialing prefixes (area and country codes) to the telephony gateways that can service these codes.

Domain

A group of gateways and gatekeepers.

DNS

Domain Name System. A general-purpose distributed, replicated, data query service used on the Internet for translating hostnames into Internet addresses.

H.323

A standard that defines how multimedia data is transmitted across non-guaranteed packet-based networks.

H.235

A standard for network-based security.

Internet Phone Lite users

Users that are calling from their PC using the Internet Phone Lite software and sound board hardware.

IVR

Interactive Voice Response. The IVR system interacts with callers through digitized voice, providing human speech prompts.

PBX or PABX

Private Branch Exchange (switchboard).

PSTN

Public Switched Telephone Network. An acronym for the traditional telephone system.

RAS

The protocol within H.323 for end-point to gatekeeper communications.

RCAM

Remote Control and Management service. A component of the RMA service.

RMA

Remote Master Agent service. RMA is a watch-dog agent that restarts the gatekeeper or gateway if it falls.

Service

A communication function provided using a set of devices, e.g., phone to phone, desktop to phone, fax to fax, collect calls and debit card calls.

SNMP

Simple Network Management Protocol. The Internet standard protocol, developed to manage nodes on an IP network. It can be used to manage and monitor network equipment such as gateways and gatekeepers.

SNTP

Synchronous Network Timing Protocol. A timing service installed either on the gatekeeper or an a separate workstation which controls the VocalTec system timing mechanism.

Snapshots

Read-only copies of a master database located on a remote node. A snapshot can be queried, but not updated; only the master database can be updated.

A snapshot is periodically refreshed to reflect changes made to the master table.

System security

The mechanisms that control the access to various resources and services on the system, such as valid username/password combinations, user authorization, and which system operations a user can perform.

TCP/IP

Transport Control Protocol/Internet Protocol. The most common transport layer protocol used on Ethernet and the Internet. TCP, built on top of Internet Protocol (IP), adds reliable communication, flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections.

VGK

VocalTec Gatekeeper. VGK is the intelligent hub of the communication network, providing centralized addressing, security and accounting.

VNM

VocalTec Network Manager. VNM provides network administrators with a tool capable of managing a large-scale, distributed IP communications network.

VGW

VocalTec Gateway. VGW 120 and VGW 2000 bridge the regular PSTN network to IP networks such as the Internet or intranet, enabling phone to phone, PC to phone and fax to fax calls over IP networks.

VSS

VocalTec SIP Server 4000 (VSS 4000) is a SIP-based front-end server used for originating calls from SIP clients and passing the calls on to H.323 gateways for termination. VSS 4000 can support up to 4000 simultaneous calls.

Index