Part No. P0993474 03

Business Communications Manager 3.0

IP Telephony Configuration Guide

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

Trademarks

Table of Contents

Chapter 6

Appendix A

Figures

Tables

Preface

This guide describes IP Telephony functionality for the Business Communications Manager 3.0 system. This includes information about Nortel IP terminals such as the i2002, i2004 telephone and the Nortel Networks i2050 Software Phone, the Symbol NetVision and NetVision data telephones (H.323-protocol devices), and VoIP trunks and H.323 trunking with such applications as NetMeeting.

Before you begin

This guide is intended for installers and managers of a Business Communications Manager 3.0 system. Prior knowledge of IP networks is required.

Before using this guide, the Business Communications Manager 3.0 system must be configured and tested.

This guide assumes:

- You have planned the telephony and data requirements for your Business Communications Manager 3.0 system.
- The Business Communications Manager 3.0 is installed and initialized, and the hardware is working. External lines and internal telephones and telephony equipment are connected to the appropriate media bay modules on the Business Communications Manager 3.0.
- Configuration of lines is complete.
- Operators have a working knowledge of the Windows operating system and of graphical user interfaces.
- Operators who manage the data portion of the system are familiar with network management and applications.

Refer to Chapter 2, “Prerequisites checklist,” on page 29 for more information.

Symbols used in this guide

This guide uses these symbols to draw your attention to important information:

Caution: Caution Symbol
Alerts you to conditions where you can damage the equipment.

Danger: Electrical Shock Hazard Symbol
Alerts you to conditions where you can get an electrical shock.

Warning: Warning Symbol
Alerts you to conditions where you can cause the system to fail or work improperly.

➡ **Note:** Note/Tip symbol
Alerts you to important information.

➡ **Tip:** Note/Tip symbol
Alerts you to additional information that can help you perform a task.

Text conventions

This guide uses these following text conventions:

angle brackets (< >)	Represent the text you enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <`*`ip_address`*`>`, you enter`:` `ping 192.32.10.12`
`bold Courier text`	Represent command names, options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
italic text	Represents terms, book titles and variables in command syntax descriptions. If a variable is two or more words, the words are connected by an underscore. Example: The command syntax `show at <`*`valid_route`*`>`, *`valid_route`* is one variable and you substitute one value for it.
bold text	Represents fields names, field entries, and screen names in the Unified Manager application.
`plain Courier text`	Represents command syntax and system output, such as prompts and system messages. Example: `Set Trap Monitor Filters`

Acronyms

This guide uses the following acronyms:

ATM	Asynchronous Transfer Mode
BCM	Business Communications Manager
CIR	Committed Information Rate
DID	Direct Inward Dialing
DOD	Direct Outward Dialing
DIBTS	Digital In-Band Trunk Signalling
DSB	DIBTS Signalling Buffer

DSL	Digital Subscriber Line
ICMP	Internet Control Message Protocol
IEEE802 ESS	Institute of Electrical and Electronics Engineers, Inc., standard 802 Electronic Switching System Identification code
ITG	Internet Telephony Gateway (for Meridian)
ITU	International Telecommunication Union
IXC	IntereXchange Carrier
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LATA	Local Access and Transport Area
LEC	Local Exchange Carrier
MOS	Mean Opinion Score
NVPA	NetVision Phone Administrator
PCM	Pulse Code Modulation
PING	Packet InterNet Groper
PiPP	Power inline patch panel
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Registration, Admissions and Status
RTP	Real-time Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTPS	UNISTIM Terminal Proxy Server
VoIP	Voice over Internet Protocol
VAD	Voice Activity Detection
VLAN	Virtual LAN
WAN	Wide Area Network

Related publications

Documents referenced in the *Business Communications Manager 3.0 IP Telephony Configuration Guide*, include:

- *Installation and Maintenance Guide*
- *Software Keycode Installation Guide*
- *Programming Operations Guide*
- *Telephony Feature Handbook*
- i2004, i2005, i2050 Software Phone user cards

How to get help

USA and Canada

Authorized Distributors - ITAS Technical Support

Telephone:
1-800-4NORTEL (1-800-466-7835)
If you already have a PIN Code, you can enter Express Routing Code (ERC) 196#.
If you do not yet have a PIN Code, or for general questions and first line support, you can enter ERC 338#.

Website:
http://www.nortelnetworks.com/support

Presales Support (CSAN)

Telephone:
1-800-4NORTEL (1-800-466-7835)
Use Express Routing Code (ERC) 1063#

EMEA (Europe, Middle East, Africa)

Technical Support - CTAS

Telephone:
00800 800 89009

Fax:
44-191-555-7980

email:
emeahelp@nortelnetworks.com

CALA (Caribbean & Latin America)

Technical Support - CTAS

Telephone:
1-954-858-7777

email:
csrmgmt@nortelnetworks.com

APAC (Asia Pacific)

Technical Support - CTAS

Telephone:
+61 388664627

Fax:
+61 388664644

email:
asia_support@nortelnetworks.com

Chapter 1 Introduction

IP Telephony provides the flexibility, affordability, and expandability of the Internet to the world of voice communications.

This section includes an overview of the components that make up the Business Communications Manager version 3.0 IP telephony and Voice over IP (VoIP) features:

- "IP telephones and VoIP trunks" on page 20
- "Creating the IP telephony network" on page 21
- "Key IP telephony concepts" on page 25

Business Communications Manager 3.0 with voice over IP (VoIP) provides several critical advantages:

- **Cost Savings.** IP networks can be significantly less expensive to operate and maintain than traditional networks. The simplified network infrastructure of an Internet Telephony solution cuts costs by connecting IP telephones over your LAN and eliminates the need for dual cabling. Internet Telephony can also eliminate toll charges on site-to-site calls by using your existing WAN. By using the extra bandwidth on your WAN for IP Telephony, you leverage the untapped capabilities of your data infrastructure to maximize the return on your current network investment.
- **Portability and flexibility**. Employees can be more productive because they are no longer confined by geographic location. IP telephones work anywhere on the network, even over a remote connection. With Nortel Networks wireless e-mobility solutions, your phone, laptop, or scanner can work anywhere on the network where a an 802.11b access point is installed. Network deployments and reconfigurations are simplified, and service can be extended to remote sites and home offices over cost-effective IP links.
- **Simplicity and consistency**. A common approach to service deployment allows further cost-savings from the use of common management tools, resource directories, flow-through provisioning, and a consistent approach to network security. As well, customers can centrally manage a host of multimedia services and business-building applications via a Web-based browser. The ability to network existing PBXs using IP can bring new benefits to your business. For example, the ability to consolidate voice mail onto a single system, or to fewer systems, makes it easier for voice mail users to network.
- **Compatibility**. Internet telephony is supported over a wide variety of transport technologies. A user can gain access to just about any business system through an analog line, Digital Subscriber Line (DSL), a LAN, frame relay, asynchronous transfer mode, SONET, or wireless connection.
- **Scalability**. A future-proof, flexible, and safe solution, combined with high reliability, allows your company to focus on customer needs, not network problems. Nortel Networks internet telephony solutions offer hybrid environments that leverage existing investments in Meridian and Norstar systems.

- **Increased customer satisfaction**. Breakthrough e-business applications help deliver the top-flight customer service that leads to success. By providing your customers with rapid access to sales and support personnel via telephone, the Web, and e-mail, your business can provide better customer service than ever before.

IP telephones and VoIP trunks

This section describes two similar applications for IP telephony on the Business Communications Manager 3.0 system: IP telephones and VoIP trunks. These applications can be used separately or together as a network voice/data solution.

- "IP telephones" on page 20
- "VoIP trunks" on page 20

IP telephones

IP telephones offer the functionality of regular telephones, but do not require a hardwire connection to the Business Communications Manager. Instead, they must be plugged into an IP network which is connected to the LAN or WAN card on the Business Communications Manager 3.0.

Calls made from IP telephones through the Business Communications Manager can pass over VoIP trunks or across a Public Switched Telephone Network (PSTN).

Nortel Networks provides two types of IP telephones. The IP telephones are wired to the IP network using Ethernet, in the case of the i2002 and the i2004, or are accessed through your desktop or lap top computer, as in the case of the Nortel Networks i2050 Software Phone. Emobility voice can be provided using Symbol© NetVision© or NetVision Data telephones, which connect through an access point wired to an IP network configured on the LAN. NetVision telephones use an extended version of the H.323 protocol to connect to the system.

VoIP trunks

VoIP trunks allow voice signals to travel across IP networks. A gateway within the Business Communications Manager 3.0 converts the voice signal into IP packets, which are then transmitted through the IP network to a gateway on the remote system. The device at the other end reassembles the packets into a voice signal. BCM, ITG (Meridian), and NetMeeting are devices that can use the H.323 protocol trunks which the 3.0 Business Communications Manager system supports.

Creating the IP telephony network

This section explains the components of the Business Communications Manager 3.0 system and the devices it interoperates to create a network.

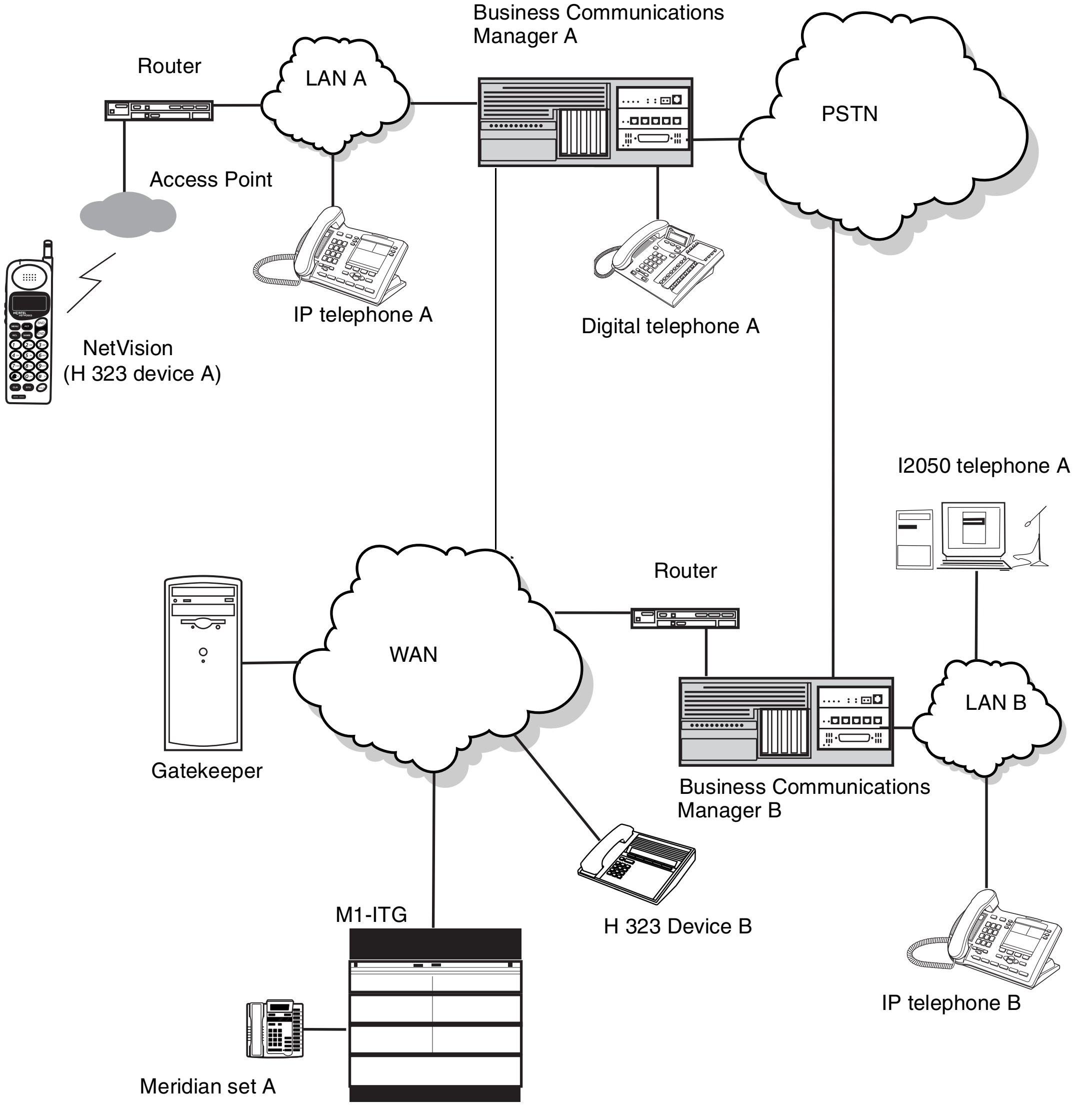
This section includes information about:

- “Business Communications Manager 3.0” on page 22
- “M1-ITG” on page 23
- “Telephones” on page 23
- “Gatekeepers on the network” on page 24
- “IP network” on page 24
- “Public Switched Telephone Network” on page 25

The following figure shows components of a Business Communications Manager 3.0 network configuration.

Note that the two Business Communications Manager systems are connected both through a PSTN connection and through a WAN connection. The WAN connection uses VoIP trunks. If the PSTN connections use dedicated ISDN lines, the two systems have backup private networks to each other. Both Business Communications Manager systems use VoIP trunks through a common WAN to connect to the Meridian (M1-ITG) system.

Figure 1 Network diagram



Business Communications Manager 3.0

The Business Communications Manager 3.0 is a key building block in creating your network. It interoperates with many devices, including the Meridian 1 system and H.323 devices. In the diagram shown in Figure 1 on page 22, the Business Communications Manager 3.0 system is connected to devices through multiple IP networks, as well as through the PSTN. Multiple Business Communications Manager 3.0 systems also can be linked together on a network of VoIP trunks and/or dedicated physical lines. Refer to Chapter 6, “Typical network applications using MCDN,” on page 115.

In the figure above, note that Business Communications Manager A is connected to a LAN through a LAN card, to a WAN through a WAN card, and to a PSTN through trunk media bay modules. Through these networks, the system accesses other systems and network equipment connected to the network.

M1-ITG

The Meridian 1 Internet Telephony Gateway (M1-ITG) allows Meridian 1 systems to communicate with the Business Communications Manager 3.0 via H.323 trunks. In Figure 1 on page 22, telephones on the M1, such as Meridian telephone A, can initiate and receive calls with the other telephones on the system across IP networks.

To provide fallback at times when IP traffic cannot pass, you can also connect the Meridian to the Business Communications Managers through ISDN PRI SL-1 lines, which provide the same MCDN capability that you can achieve through the VoIP trunks with MCDN active.

Refer to the *Business Communications Manager Programming Operations Guide* for a description of MCDN features and networking with PRI SL-1 lines. "Typical network applications using MCDN" on page 115 describes how to provide the same network over VoIP lines.

A Business Communications Manager connected to an M1-ITG using the MCDN protocol can provide access to a central voice mail and call attendant systems, which can streamline multi-office telephony administration.

Telephones

The Business Communications Manager 3.0 system can communicate using digital telephones (M7000/T7000, T7100, M7100, M7100N, T7208, M7208, M7208N, T7316, M7310, M7310N, M7324, and M7324N), cordless telephones (Companion, DECT, T7406), IP telephones and applications (i2002, i2004, Nortel Networks i2050 Software Phone), and IP/wireless telephones (NetVision and NetVision Data telephones). With this much flexibility, the Business Communications Manager can provide the type of service you require to be most productive in your business.

VoIP trunks and analog/digital telephones

While analog and digital telephones cannot be connected to the Business Communications Manager 3.0 system with an IP connection, they can make and receive calls to and from other systems through VoIP trunks. Calls received through the VoIP trunks to system telephones are received through the LAN or WAN card and are translated within the Business Communications Manager to voice channels.

VoIP trunks and IP telephones

The IP telephones connect to the Business Communications Manager across an IP network through either a LAN or a WAN. From the Business Communications Manager connection, they can then use standard lines or VoIP trunks to communicate to other telephones on other public or private networks. The Business Communications Manager also supports H.323 and +H.323 third-party devices through this type of connection.

Gatekeepers on the network

A gatekeeper tracks IP addresses of specified devices, and provides authorization for making and accepting calls for these devices. A gatekeeper is not required as part of the network to which your Business Communications Manager 3.0 system is attached, but Gatekeepers can be useful on networks with a large number of devices. Referring to Figure 1 on page 22, for example: Digital telephone A wants to call IP telephone B, which is attached to Business Communications Manager B, over a network that is under the control of a gatekeeper. Digital telephone A sends a request to the gatekeeper. The gatekeeper, depending on how it is programmed, provides Digital telephone A with the information it needs to contact BCM B over the network. BCM B then passes the call to IP telephone B.

Note: The Business Communications Manager does not contain a gatekeeper application. If you want to put a gatekeeper on your network, it must be put on a separate gatekeeper server. The Business Communications Manager is compatible with RadVision and CSE 1000 gatekeepers. Refer to Appendix D, “Interoperability,” on page 143.

IP network

In the network shown in Figure 1 on page 22, several LANs and a WAN are shown. When planning your network, be sure to consider all requirements for a data network. Your network administrator should be able to advise you about the network setup and how the Business Communications Manager fits into the network.

WAN

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as state or country. For Business Communications Manager 3.0, a WAN is any IP network connected to a WAN card on the Business Communications Manager 3.0 system. This may also be a direct connection to another Business Communications Manager 3.0 system.

If you want to deploy IP telephones or NetVision telephones that will be connected to a LAN outside of the LAN that the Business Communications Manager is installed on, you must ensure the Business Communications Manager has a WAN connection. This includes ensuring that you obtain IP addresses and routing information that allows the remote telephones to find the Business Communications Manager, and vice versa.

The *Business Communications Manager 3.0 Programming Operations Guide* has a data section that describes the internet protocols and data settings that the Business Communications Manager requires or is compatible with. Ensure that this connection is correctly set up and working before you attempt to deploy any remote IP devices.

LAN

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. For Business Communications Manager 3.0, a LAN is any IP network connected to a LAN card on the Business Communications Manager 3.0 system. Often, the LAN can include a router that forms a connection to the Internet. A Business Communications Manager can have up to two LAN connections.

Public Switched Telephone Network

The Public Switched Telephone Network (PSTN) can play an important role in IP telephony communications. In many installations, the PSTN forms a fallback route. If a call across a VoIP trunk does not have adequate voice quality, the call can be routed across the PSTN instead, either on public lines or on a dedicated ISDN connection between the two systems. The Business Communications Manager also serves as a gateway to the PSTN for all voice traffic on the system.

Key IP telephony concepts

In traditional telephony, the voice path between two telephones is circuit switched. This means that the analog or digital connection between the two telephones is dedicated to the call. The voice quality is usually excellent, since there is no other signal to interfere.

In IP telephony, each IP telephone encodes the speech at the handset microphone into small data packets called frames. The system sends the frames across the IP network to the other telephone, where the frames are decoded and played at the handset receiver. If some of the frames get lost while in transit, or are delayed too long, the receiving telephone experiences poor voice quality. On a properly-configured network, voice quality should be consistent for all IP calls.

The following sections describe some of the components that determine voice quality for IP telephones and trunks:

- “Codecs” on page 26
- “Jitter Buffer” on page 26
- “QoS routing” on page 27

Codecs

The algorithm used to compress and decompress voice is embedded in a software entity called a codec (COde-DECode).

Two popular Codecs are G.711 and G.729. The G.711 Codec samples voice at 64 kilobits per second (kbps) while G.729 samples at a far lower rate of 8 kbps. For actual bandwidth requirements, refer to "Determining the bandwidth requirements" on page 121, where you will note that the actual kbps requirements are slightly higher than label suggests.

Voice quality is better when using a G.711 CODEC, but more network bandwidth is used to exchange the voice frames between the telephones.

If you experience poor voice quality, and suspect it is due to heavy network traffic, you can get better voice quality by configuring the IP telephone to use a G.729 CODEC.

The Business Communications Manager supports these codecs:

- G.729
- G.723
- G.729 with VAD
- G.723 with VAD
- G.711-uLaw
- G.711-aLaw

Jitter Buffer

Voice frames are transmitted at a fixed rate, because the time interval between frames is constant. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter, and degrades the perceived voice quality. To minimize this problem, configure the IP telephone with a jitter buffer for arriving frames.

This is how the jitter buffer works:

Assume a jitter buffer setting of five frames.

- The IP telephone firmware places the first five arriving frames in the jitter buffer.
- When frame six arrives, the IP telephone firmware places it in the buffer, and sends frame one to the handset speaker.
- When frame seven arrives, the IP telephone buffers it, and sends frame two to the handset speaker.

The net effect of using a jitter buffer is that the arriving packets are delayed slightly in order to ensure a constant rate of arriving frames at the handset speaker.

This delaying of packets can provide somewhat of a communications challenge, as speech is delayed by the number of frames in the buffer. For one-sided conversations, there are no issues. However, for two-sided conversations, where one party tries to interrupt the other speaking party, it can be annoying. In this second situation, by the time the voice of the interrupter reaches the interruptee, the interruptee has spoken (2*jitter size) frames past the intended point of interruption. In cases where very large jitter sizes are used, some users revert to saying *OVER* when they wish the other party to speak.

Possible jitter buffer settings, and corresponding voice packet latency (delay) for the Business Communications Manager 3.0 system IP telephones are:

- None
- Small (.06 seconds)
- Medium (.12 seconds)
- Large (.18 seconds)

QoS routing

To minimize voice jitter over low bandwidth connections, the Business Communications Manager programming assigns specific DiffServ Marking in the IPv4 header of the data packets sent from IP telephones.

The DiffServ Code point (DSCP) is contained in the second byte of the IPv4 header. DSCP is used by the router to determine how the packets will be separated for Per Hop Behavior (PHB). The DSCP is contained within the DiffServ field, which was known as the ToS field in older versions. The Business Communications Manager assigns Expedited Forwarding (EF) PHB for voice media packets and the Class Selector 5 (CS5) PHB for voice signaling (control) packets. On the Business Communications Manager, these assignments cannot be adjusted.

The Business Communications Manager 3.0 system performs QOS routing, but if one or more routers along the network route do not support QOS routing, this can impact voice quality. Business Communications Manager 3.0 system QoS can also be configured so that the system reverts to a circuit-switched line if a suitable QoS cannot be guaranteed.

Chapter 2
Prerequisites checklist

Before you set up VoIP trunks or IP telephones on a Business Communications Manager, complete the following checklists to ensure that the system is correctly set up. Some questions do not apply to all installations.

This guide contains a number of appendices that explain various aspects of the system directly related to IP telephony functions. However, refer to the *Business Communications Manager Programming Operations Guide* for specific information about configuring the data portion of the Business Communications Manager.

This section includes the following checklists:

- "Network diagram" on page 29
- "Network devices" on page 30
- "Network assessment" on page 30
- "Resource assessment" on page 31
- "Keycodes" on page 33
- "Business Communications Manager system configuration" on page 34
- "IP telephones" on page 37

Network diagram

To aid in installation, a Network Diagram is needed to provide a basic understanding of how the network is configured. Before you install IP functionality, you must have a network diagram that captures all of the information described in the following table. If you are configuring IP telephones but not voice over IP (VoIP) trunks, you do not need to answer the last two questions.

Table 1 Network diagram prerequisites

Prerequisites	**Yes**
1.a Has a network diagram been developed?	
1.b Does the network diagram contain any routers, switches or bridges with corresponding IP addresses and bandwidth values for WAN or LAN links? Also refer to Appendix D, "Interoperability," on page 143.	
1.c Does the network diagram contain IP Addresses, netmasks, and network locations of all Business Communications Managers?	
1.d Answer this if your system will use IP trunks, otherwise, leave it blank: Does the network diagram contain IP Addresses and netmasks of any other VoIP gateways that you need to connect to?	
1.e Answer this only if your system will use a gatekeeper, otherwise, leave it blank: Does the network diagram contain the IP address for any Gatekeeper that may be used?	

Network devices

The following table contains questions about devices on the network such as firewalls, NAT devices, and DHCP servers.

- If the network uses public IP addresses, complete 2.d.
- If the network uses private IP addresses, complete 2.e to 2.f.

Table 2 Network device checklist

Prerequisites	Yes	No
2.a Is the network using DHCP?		
2.b If so, are you using the DHCP server on the Business Communications Manager?		
2.c Is the network using private IP addresses?		
2.d Are there enough public IP addresses to accommodate all IP telephones and the Business Communications Manager?		
2.e Does the system have a firewall/NAT device, or will the Business Communications Manager be used as a firewall/NAT device? NOTE: NetVision handsets do not work on a network that has NAT between the handset and the system.		
2.f If the Business Communications Manager is to be used as a firewall/NAT device, do the firewall rules fit within the 32 input rules and 32 output rules that the Business Communications Manager provides?		
2.g A hub-based core will not have suitable performance for IP Telephony. Does the network use a non-hub solution at its core?		

Network assessment

The following table questions are meant to ensure that the network is capable of handling IP telephony, and that existing network services are not adversely affected.

Table 3 Network assessment

Prerequisites	Yes	No
3.a Has a network assessment been completed?		
3.b Has the number of switch/hub ports available and used in the LAN infrastructure been calculated?		
3.c Does the switch use VLANs? If so, get the VLAN port number and ID.		
3.d Have the used and available IP addresses for each LAN segment been calculated?		
3.e Has DHCP usage and location been recorded?		
3.f Has the speed and configuration of the LAN been calculated?		

Prerequisites	Yes	No
3.g Has the estimated latency values between network locations been calculated?		
3.h Have the Bandwidth/CIR utilization values for all WAN links been calculated?		
3.i Has the quality of service availability on the network been calculated?		

Resource assessment

Answer the questions in the following table to determine if you have allocated sufficient resources on the Business Communications Manager for IP telephony.

For information about changing the DS30 split for the Business Communications Manager and allocating media resources, refer to the *Business Communications Manager Programming Operations Guide* (data sections).

Table 4 Resource assessment

Prerequisites	Yes	No
4.a Has a Business Communications Manager Resource Assessment been performed using the resource questionnaire in the *Programming Operations Guide*?		
4.b Has an analysis been done to determine which DS-30 split is appropriate for the system? Has the DS30 split been changed to 3/5, if necessary?		
4.c Have all necessary media resources for IP trunks, clients, vmail or WAN dialup been assigned or dedicated?		
4.d Have the necessary media gateway, IP client, and IP trunks resources been set? (Refer to “Configuring media gateway parameters for IP service”.)		

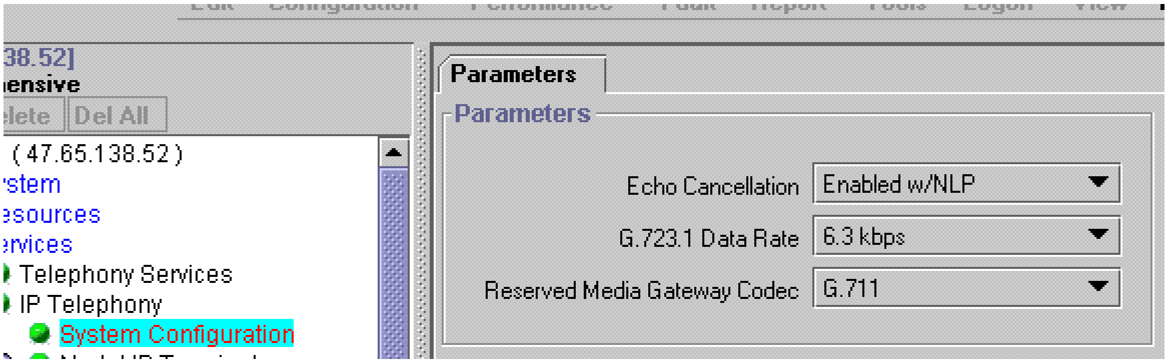
Configuring media gateway parameters for IP service

To set up the media gateway resources that you require for optimum IP telephony, set the fields on the **System Configuration** window.

1. Click the keys beside **Services, IP Telephony**.
2. Click on **System Configuration**.

   The Parameters screen appears in the right frame.

Figure 2 System Configuration, Parameters screen



Echo Cancellation: Enabled w/NLP
G.723.1 Data Rate: 6.3 kbps
Reserved Media Gateway Codec: G.711

3. Change the settings for the fields below, as required for your system.

Table 5 IP terminals general record fields

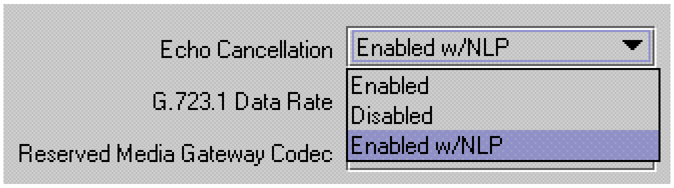
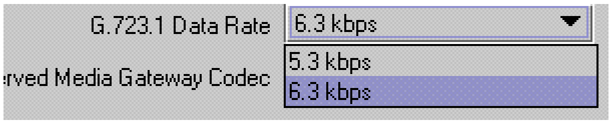
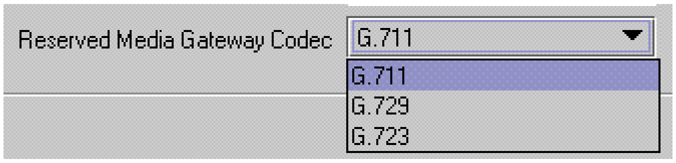
Field	Value	Description
Echo Cancellation	Enabled w/NLP Enabled Disabled	Enable or disable echo cancellation for your system.  G.723.1 Data Rate Reserved Media Gateway Codec Enabled Disabled Enabled w/NLP Echo Cancellation: Enabled w/NLP **Echo Cancellation** selects what type of echo cancellation is used on calls that go through a Media Gateway. NLP refers to Non-Linear Processing.

Table 5 IP terminals general record fields (Continued)

Field	Value	Description
G.723.1 Data Rate	5.3 kbps 6.3 kbps	Choose the preferred data rate for the channel.  G.723.1 Data Rate 6.3 kbps G.723.1 Data Rate selects what data rate is used for transmissions from the Business Communications Manager to an IP device when the G.723.1-family codec is used (G.723.1 or G.723.1A). This has no effect on any other codec. The possible values are 5.3 kbps and 6.3 kbps.
Reserved Media Gateway Codec	G.711 G.729 G.723	Choose the preferred codec that you are using with your IP network.  Reserved Media Gateway Codec G.711 **Reserved Media Gateway Codec** should be set to whatever is the most-commonly used codec for Media Gateways. It determines the amount of codec resources reserved for each Media Gateway. Reserving resources speeds up establishment of connections. For example, if most calls through a Media Gateway use the G.711 codec, set this to G.711. If most calls use G.729, set this to G.729. Note that the higher the setting (G.723 > G.729 > G.711) the more resources are set aside for Media Gateways. This may result in calls failing to go through because of lack of available resources.
For a more detailed descriptions of the media gateway or other information about the media services card (MSC) settings for the Business Communications System, refer to the *Programming Operations Guide*, MSC section.		

Keycodes

All elements of VoIP trunks and IP telephony are locked by the Business Communications Manager keycode system. You can purchase keycodes for the amount of access you want for your system. Additional keycodes can be added later, providing there are adequate resources to handle them.

Table 6 Keycodes

Prerequisites	Yes	No
5.a Complete this question only if you are using VoIP trunks: Do you have enough VoIP keycodes?		
5.b Complete this question only if you are using IP telephones: Do you have enough IP client keycodes? (Note: IP clients and IP telephones are a 1:1 ratio. Include any NetVision telephones to your calculations. As soon as an IP telephone is registered, it occupies an IP client, whether it is active or not.).		

Table 6 Keycodes (Continued)

Prerequisites	Yes	No
5.c If you are using VoIP trunks, do you need to activate MCDN features? Note: If MCDN is already configured on your system for private networking over land lines, you do not need a separate MCDN keycode for VoIP trunks.		

Business Communications Manager system configuration

Several sections of the Business Communications Manager must be properly configured prior to activation of IP telephony.

Answer the questions in the following table to determine if your Business Communications Manager has been correctly configured.

Table 7 Business Communications Manager system configuration

Prerequisites	Yes	No
6.a Is the LAN functioning correctly with the Business Communications Manager?		
6.b Is the WAN functioning correctly with the Business Communications Manager?		
6.c Have you determined the published IP address for the system? Refer to "Defining published IP address" on page 35.		
6.d Has a dialing plan been created, taking into account special considerations for IP telephony and private and public networking?		
6.e Do you want the system to auto-assign DNs? If no, complete 6.f.		
6.f Have DN records been programmed for the corresponding IP clients?		

Defining published IP address

The published IP address is the IP address used by computers on the public network to find the Business Communications Manager. For example, if a Business Communications Manager has a LAN interface (LAN1) that is connected only to local office IP terminals and a WAN interface (WAN1) that is connected to the public network, then WAN1 should be set to the published IP address.

Setting the Global IP (published IP)

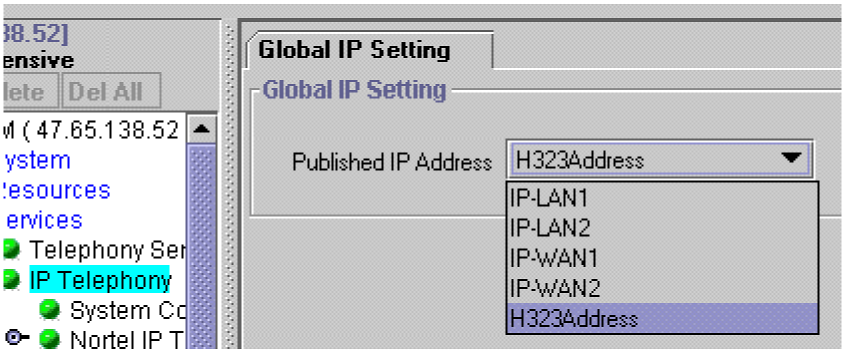
To set the published IP address:

1 In Unified Manager, open **Services** and click on **IP Telephony**.

The Global settings tab appears, as shown in the diagram below.

2 From the **Published IP Address** menu, select the appropriate network interface.

Figure 3 Global IP settings



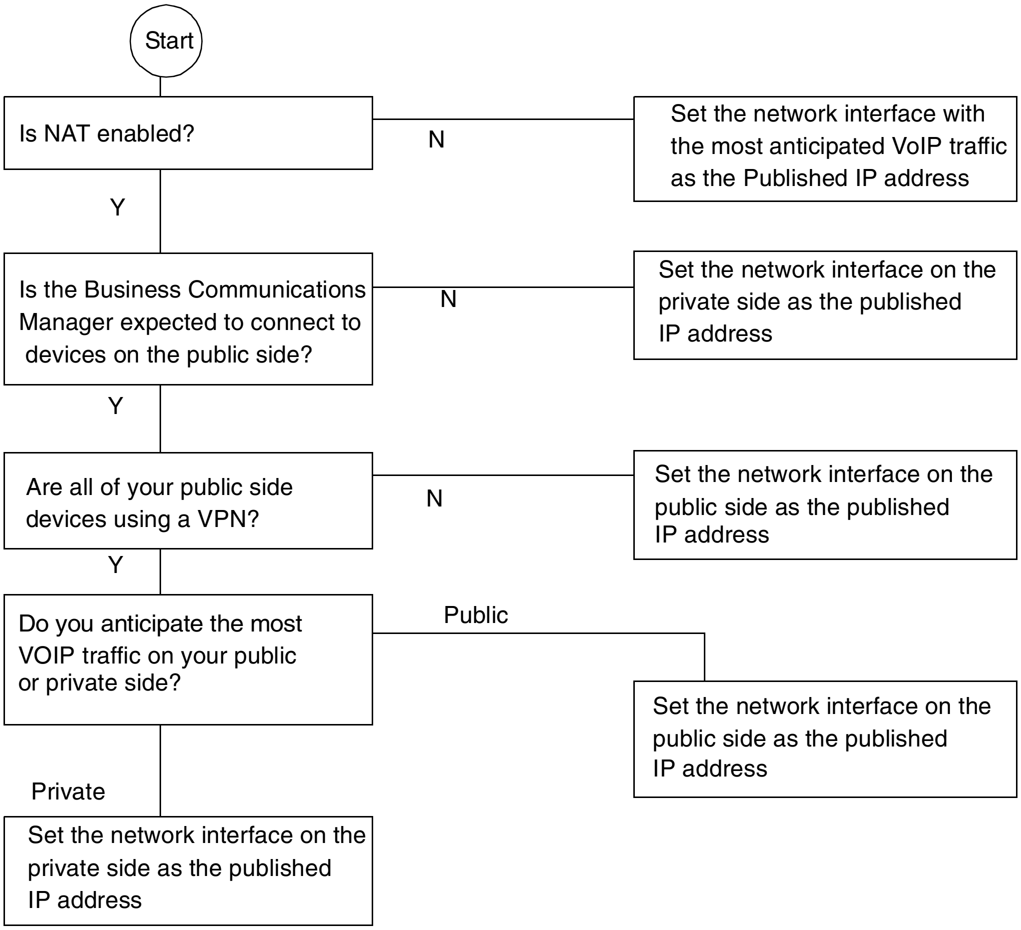
Global IP Setting

Published IP Address: H323Address

Determining the published IP address

Use the flowchart in the following figure to determine which card should be set as the published IP address.

Figure 4 Setting the Published IP address


Start
Is NAT enabled?
N
Set the network interface with the most anticipated VoIP traffic as the Published IP address
Y
Is the Business Communications Manager expected to connect to devices on the public side?
N
Set the network interface on the private side as the published IP address
Y
Are all of your public side devices using a VPN?
N
Set the network interface on the public side as the published IP address
Y
Do you anticipate the most VOIP traffic on your public or private side?
Public
Set the network interface on the public side as the published IP address
Private
Set the network interface on the private side as the published IP address

The flowchart shown above makes reference to public and private IP addresses. The public and private IP addresses are concepts relating to Network Address Translation (NAT). The decision also depends on whether a Virtual Private Network (VPN) is enabled. For information about NAT and VPN, refer to the *Business Communications Manager 3.0 Programming Operations Guide.*

If you use IP telephones on the network, they must be set to have the IP address of the network card they are connected to for their Default Gateway, and the Published IP address as the S1 IP address. For more information about this, see "Configuring the i2002 or i2004 telephone to the system" on page 44.

IP telephones

Complete this section if you are installing IP telephones.

Table 8 IP telephone provisioning

Prerequisites	**Yes**	**No**
7.a Are IP connections and IP addresses available for all IP telephones?		
7.b If DHCP is not being used, has all telephone configuration been documented and made available for telephone installers? Hint: Use the Programming Record form.		
7.c If DHCP is not being used, or if you want to enter the port manually, has the VLAN port number been supplied, if one is being used on the switch?		
7.d Have telephone power and connectors been provisioned?		
7.e Do computers that will be using the Nortel Networks i2050 Software Phone meet the minimum system requirements, including headset?		

NetVision wireless telephones

Refer to “Gathering system information before you start” on page 69.

Chapter 3
Installing IP telephones

An IP telephone converts the voice signal into data packets and sends these packets directly to another IP telephone or to the Business Communications Manager over the LAN or the internet. If the destination is an IP telephone, the arriving voice packets are converted to a voice stream and routed to the speaker or headset of the target telephone. If the destination is the Business Communications Manager, the voice stream is routed to a circuit switched connection, such as a telephone (internal) or line (external PSTN or private network), or some form of gateway (VoIP).

➡ **Note:** IP telephones require an IP network to reach the Business Communications Manager. However, they do not need to use VoIP trunks to communicate beyond the Business Communications Manager. They can use any type of trunk in the same way that digital telephones do.

Before setting up IP clients, you must enable keycodes for IP telephony. For information about entering **IP Client keycodes**, see the *Keycode Installation Guide*.Each IP Client keycode opens a specific number of IP telephone channels on the system. Channels are distributed on a one-to-one basis as each IP telephone or NetVision handset registers with the system.

This section includes information about:

- "Supporting IP telephony" on page 39
- "Configuring Nortel Networks i-series telephones" on page 40
- "Modifying IP telephone status settings" on page 53
- "Working with the features list" on page 55
- "Download firmware to a Nortel IP telephone" on page 60
- "Deregistering DNs for IP telephones" on page 62
- "Moving IP telephones" on page 63
- "Configuring the Nortel Networks i2050 Software Phone" on page 64

Supporting IP telephony

The Business Communications Manager supports two types of IP telephony protocols, UNISTIM and H.323.

- The Nortel Networks i-series telephones use the UNISTIM protocol.
- The Symbol NetVision and NetVision Data telephones use H.323+. Refer to Chapter 4, "Installing NetVision telephones," on page 67.

The applications that control these protocols on the Business Communications Manager provide an invisible interface between the IP telephones and the digital voice processing controls on the Business Communications Manager.

About Nortel Networks IP telephones

The i2002 and i2004 telephones are hardwired to an internet connection. They can be installed on any internet connection that has access to the network connected to the LAN or WAN of the Business Communications Manager.

The Nortel Networks i2050 Software Phone runs on any computer running Windows 98, Windows 2000, or Windows XP. The computer must be connected to the LAN or WAN that the Business Communications Manager is connected to.

Configuring Nortel Networks i-series telephones

The configuration menus for the Nortel Networks i-series IP telephones (i2002, i2004, i2050) are under **Services, IP Telephony, Nortel IP Terminals** and **Services, Telephony Services, System DNs, Inactive DNs** (or **Active set DNs**, once the telephone connects to the system).

This section contains the following information:

- "Preparing your system for IP telephone registration" on page 40
- "Installing i-series telephones" on page 43
- "Configuring the i2002 or i2004 telephone to the system" on page 44
- "Troubleshooting an IP telephone" on page 48
- "Configuring DHCP" on page 49
- "Checking IP server status" on page 52

Preparing your system for IP telephone registration

When you install an IP telephone on a Business Communications Manager, you must activate terminal registration on the Business Communications Manager. If this is your first installation, you need to set the general parameters for IP registration.

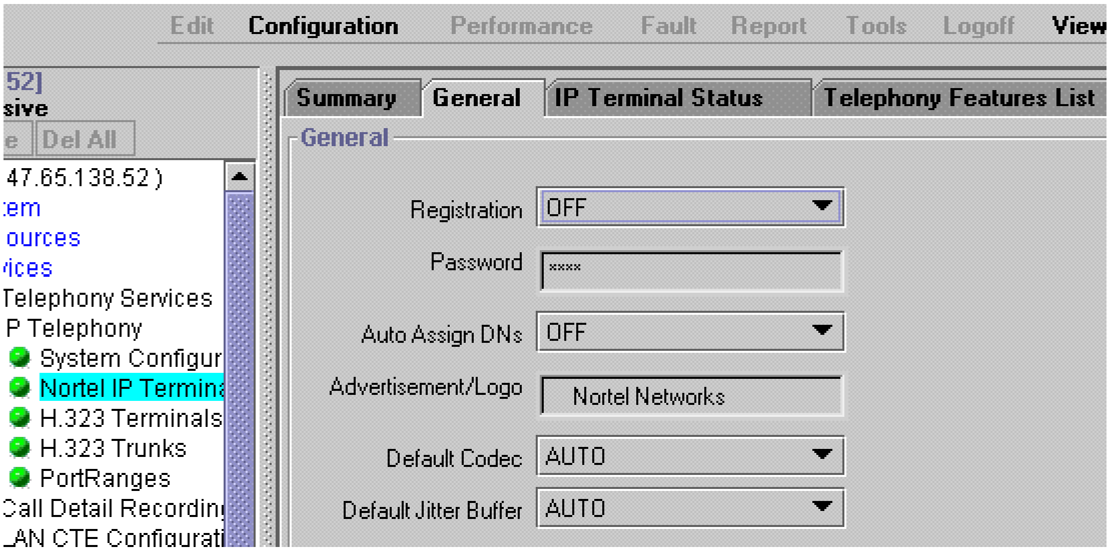
➡ **Note:** For the simplest installation possible, set telephone **Registration** and **Auto Assign DNs** to ON, and leave **Password** blank. IP telephones installed on the system LAN will connect and boot-up without manual registration.

Warning: Nortel cautions that leaving your system in this state may pose a security risk.

1 In Unified Manager, open **Services**, **IP Telephony**, and **Nortel IP Terminals**.

2 Select the **General** tab.
The General screen appears, as shown below.

Figure 5 Set registration properties



Registration: OFF
Password: ****
Auto Assign DNs: OFF
Advertisement/Logo: Nortel Networks
Default Codec: AUTO
Default Jitter Buffer: AUTO

3 Use the information in the table below to set up your IP terminals general information.

Table 9 IP terminals general record fields

Field	Value	Description
Registration	On Off	Set this value to ON to allow new IP clients to register with the system.
Password	<10 alphanumeric> Default: bcmi	This is the password the installer will enter on the IP telephone to connect to the Business Communications Manager. If this field is left blank, no password prompt occurs during registration.
Auto Assign DN	On Off	If set to ON, the system assigns a free DN as a set requests registration. It does not prompt the installer to enter a set DN. (Note: **Registration** must be ON and **Password** must be blank) If set to OFF, the installer receives a prompt to enter the assigned DN during the programming session.
Advertisement/Logo	<alphanumeric string>	Any information in this field appears on the display of all IP telephones. For example, your company name or slogan.
Default Codec	Auto G.711-aLaw G.711-uLaw G.729 G723 G.729 + VAD G.723 + VAD	If the IP telephone has not been configured with a preferred codec, choose a specific codec that the IP telephone will use when it connects to the system. If you choose Auto, the IP telephone selects the codec. For information about choosing a codec, refer to “Choosing a codec” on page 42. If you are unsure about applying a specific codec, ask your network administrator for guidance.

Table 9 IP terminals general record fields (Continued)

Field	Value	Description
Jitter Buffer	None Auto Small Medium Large	Choose one of these settings to change the default jitter buffer size: • NONE: Minimal latency, best for short-haul networks with good bandwidth. • AUTO: Business Communications Manager will dynamically adjust the size. • SMALL: Business Communications Manager will adjust the buffer size, depending on CODEC type and number of frames per packet to introduce a 60-millisecond delay. • MEDIUM: 120-millisecond delay • LARGE: 180-millisecond delay For information about choosing a Jitter Buffer, refer to "Choosing a Jitter Buffer" on page 43.

4 Go to "Installing i-series telephones" on page 43.

Choosing a codec

The default codec is used when an IP client has not been configured to use a preferred Codec. Refer to the next section for individual IP client Codec settings. If the default Codec is set to AUTO, the Business Communications Manager will choose the appropriate CODEC when an IP client makes a call. For example, if both endpoints of the call are IP telephones on the same subnet, the Business Communications Manager chooses G.711 for maximum voice quality. If the telephones are on different subnets, the Business Communications Manager will choose G.729 to minimize network bandwidth consumption by voice data packets.

Note: If the IP telephones are using VoIP trunks for the call, the codec set for the trunks overrides the telephone settings.

For IP telephones, the Business Communications Manager supports both a-law and mu-law variants of the G.711 CODEC, as well as the G.729 and G.723 CODECS.

- The G.711 CODEC samples the voice stream at a rate of 64Kbps (Kilo bits per second), and is the CODEC to use for maximum voice quality. Choose the G.711 CODEC with the companding law (alaw or ulaw) that matches your system requirements.
- The G.729 CODEC samples the voice stream at 8Kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.
- The G.723 CODEC should be used only with third party devices that do not support G.729 or G.711.
- Codecs with VAD (Voice Activity Detection) make VAD active on the system, which performs the same function as having silence suppression active.

Choosing a Jitter Buffer

A jitter buffer is used to prevent the jitter associated with arriving (Rx) voice packets at the IP telephones. The jitter is caused by packets arriving out of order due to having used different network paths, and varying arrival rates of consecutive voice packets.The greater the size of the jitter buffer, the better sounding the received voice appears to be. However, voice latency (delay) also increases. Latency is very problematic for telephone calls, as it increases the time between when one user speaks and when the user at the other end hears the voice.

Installing i-series telephones

The Nortel Networks i-series telephones can be configured to the network by the end user or by the administrator. If the end user is configuring the telephone, the administrator must provide the user with the required parameters.

A maximum of 90 IP telephones, including Nortel Networks i2050 Software Phones, and H.323 devices such as NetVision handsets, can be connected on the Business Communications Manager system.

Before installing

Before installing the i2002 or i2004 telephone, ensure that:

- ensure the telephone has the appropriate power supply for your region
- if powered locally, ensure the installation site has a nearby power outlet; otherwise, it can be powered through a Power Inline Patch Panel (PiPP)
- the installation site has a 10/100 BaseT Ethernet connection
- if you are using an IP telephone that does not have a 3-port switch, ensure you have 10/100 BaseT Ethernet connections for both the telephone and for your computer equipment.

Caution: Do not plug the telephone into an ISDN connection. This can cause severe damage to the telephone. Plug the telephone only into a 10/100 BaseT Ethernet connection.

Using a 3-port switch

In an office environment where a LAN network already exists, most computers will already be connected to a LAN line. To avoid the necessity of installing duplicate network connections, you can use a Nortel Networks 3-port switch for older model i2004 telephones. This switch allows the telephone and computer to connect to the same network connection. For more information, consult the i2004 and the 3-way switch documentation. The i2002 and newer models of the i2004 telephone have an adapter that replaces the requirement for this switch.

Connecting the i2002 or i2004 telephone

Follow these steps to connect an i2002 or i2004 telephone:

1 Connect one end of the handset cord to the handset jack on the telephone base.

2 Connect the other end of the handset cord to the handset.

3 Connect one end of a Cat-5 line cord with RJ45 connectors to the line cord jack on the telephone base.

4 Connect the other end of the line cord to the Ethernet connection or to the 3-way switch connector.

> **Note:** Newer i20XX terminals have a 3-way switch built into the telephone. Refer to the installation card that comes with the telephone for specific directions.

5 Plug the AC Power adapter into the base of the telephone, and then plug the adapter into the AC outlet.

6 Go to "Configuring the i2002 or i2004 telephone to the system" .

Configuring the i2002 or i2004 telephone to the system

Configuring IP telephones involves two processes:

- If DHCP (Distributed Host Control Protocol) service on the Business Communications Manager is active or the Customer DHCP server has been configured to hand out the specific Business Communications Manager details, the IP telephone will automatically attempt to find the server. Refer to "Configuring DHCP" on page 49, which describes the secific DHCP requirements for IP telephones, and to the *Programming Operations Guide*, which provides detailed DHCP configuration information.

  Once you register the telephone to the system, as described in "Registering the telephone to the system", the telephone assumes the parameters it receives from the system, which are described in "Configuring telephone settings".

- If DHCP is not configured to provide system information, or if you are not using DHCP on your network, you need to configure your telephone parameters before the telephone can register to the system. In this case, follow the directions in "Configuring telephone settings", and then follow any of the prompts that appear, as described in "Registering the telephone to the system".

Registering the telephone to the system

When you first connect the telephone to the IP connection, you may receive one of the following:

- If the telephone is not yet registered, and if a password was entered in the Terminal Registration screen, the telephone prompts you for that password.
- If you set **Auto Assign DN** on the Business Communications Manager to OFF, the telephone prompts you for a DN.
- If you are prompted for a password, enter the password and press OK.
- If you are prompted for a DN, enter the DN you want assigned to this telephone and press OK.

When the telephone registers, it downloads the information from the Business Communications Manager IP Telephony record to the telephone configuration record. This might include a new firmware download, which occurs automatically. If new firmware downloads, the telephone display indicates the event.

Note: If the telephone displays a prompt that indicates it cannot find the server, follow the instructions in “Configuring telephone settings” to enter the specific network path. “Troubleshooting an IP telephone” on page 48 describes other possible prompt messages.

Once registration has completed, you do not need to go through the registration steps described above unless you deregister the terminal. For information about setting the registration settings, see “Preparing your system for IP telephone registration” on page 40.

Configuring telephone settings

If you are not automatically registered to the Business Communications Manager, you can configure your telephone settings to allow you to access a system on the network. You will also need to perform these steps if your IP telephone is not connected to the same LAN to which the Business Communications Manager is connected.

Follow these steps to access the local configuration menu on an i2002 or an i2004 telephone:

1. Restart the telephone by disconnecting the power, then reconnecting the power.
   After about four seconds, the top light flashes and `NORTEL NETWORKS` appears on the screen.

2. When the greeting appears, immediately, and quickly, press the four display keys, one at a time, from left to right. These keys are located directly under the display.
   These keys must be pressed one after the other within 1.5 seconds or the telephone will not go into configuration mode.

   - If `Manual Cfg DHCP(0 no, 1 yes)` appears on the screen, you successfully accessed the configuration mode.
   - If any other message appears, disconnect, then reconnect the power, and try to access the configuration mode again.

3. Enter the network parameters, as prompted.
   As each parameter prompt appears, use the keypad to define values.

Use the ***** key to enter the period in the IP addresses.
Press OK to move forward.

The following table describes the values for each display parameter.

Table 10 IP telephone server configurations

Field	Value	Description
DHCP	0 or 1	Enter 0 if your network is not using a DHCP server to dispense IP addresses. (Partial DHCP) Enter 1 if your network does use a DHCP server. If you choose to use a DHCP server rather than allocating static IP addresses for the IP telephones, skip the remainder of this section. For information about setting up DHCP server information for the IP telephones, see "Configuring DHCP" on page 49.
SET IP	<ip address>	The set IP must be a valid and unused IP address on the network that the telephone is connected to.
NETMASK	<subnet mask address>	This is the subnet mask. This setting is critical for locating the system you want to connect to.
DEF GW	<ip address>	Default Gateway on the network (i.e., the nearest router to the telephone. The router for IP address W.X.Y.Z is usually at W.X.Y.1) If there are no routers between the telephone and the Business Communications Manager network adaptor to which it is connected, (for example a direct HUB connection), then enter the Published IP address of the Business Communications Manager as the DEF GW. If the IP telephone is not connected directly to the Published IP address network adaptor, set the DEF GW to the IP address of the network adaptor the telephone is connected to. For information on setting the published IP address of the Business Communications Manager, see "Defining published IP address" on page 35.
S1 IP	<ip address>	This is the Published IP address of the first Business Communications Manager that you want to register the telephone to.
S1 PORT	Default: 7000	This is the port the telephone will use to access this Business Communications Manager.
S1 ACTION	Default: 1	
S1 RETRY COUNT	<digits between 0 and 255>	Set this to the number of times you want the telephone to retry the connection to the Business Communications Manager.
S2 IP	<ip address>	This is the Published IP address of the second Business Communications Manager that you want to register the telephone to. It can also be the same as the S1 setting.
S2 PORT	Default: 7000	This is the port the telephone will use to access this Business Communications Manager.
S2 ACTION	Default: 1	
S2 RETRY COUNT	<digits between 0 and 255>	Set this to the number of times you want the telephone to retry the connection to the Business Communications Manager.

Table 10 IP telephone server configurations (Continued)

Field	Value	Description
VLAN	0: No VLAN 1: Manual VLAN 2: Automatically discover VLAN using DHCP	Choose 0:NO VLAN if there is no VLAN on the network. If you do not have DHCP on the network, or if DHCP is supplied by a remote server, select number 1 and enter the VLAN ID*. If you have the Business Communications Manager DHCP active on your system, select number 2 if you want DHCP to automatically find the VLAN assignment. Refer to "Configuring DHCP" on page 49. *VLAN is a network routing feature provided by specific types of switches. To find out if VLAN has been deployed on your system, check with your network administrator. If VLAN is deployed, the system administrator responsible for the switch can provide the VLAN ID(s) for your system. Refer to the *Programming Operations Guide* for information about VLAN configuration and DHCP. Also refer to "Using VLAN on the network" on page 148.

When you have entered all the configuration information, the telephone attempts to connect to the Business Communications Manager. The message `Locating Server` appears on the display. If the connection is successful, the message changes to `Connecting to Server` after about 15 seconds. Initialization may take several minutes. Do not disturb the telephone during this time.

When the telephone connects to the server and is ready to use, the display shows the time and date. As well, the six keys at the top of the display are labelled.The telephone is ready to use.

Note: If the DN record has not yet been configured, as will be the case with auto-assigned DNs, you will only be able to make local calls, until other lines have been assigned in the DN record.

Note: If the telephone has not been registered before, you will receive a `New Set` message. Enter the information, as prompted. Refer to "Registering the telephone to the system" on page 45.

Troubleshooting an IP telephone

If the system is not properly configured, several messages can appear.

Table 11 IP telephony display messages

Message	Description/Solution
`SERVER: NO PORTS LEFT`	The Business Communications Manager has run out of ports. This message will remain on the display until a port becomes available and the telephone is powered down then powered up.To obtain more ports, you may need to install additional VoIP keycodes. See the *Keycode Installation Guide.*
`Invalid Server Address`	The S1 is incorrectly configured with the IP address of a Business Communications Manager network adapter other than the published IP address.
`IP Address conflict`	The telephone detected that a device on the network is currently using the IP address allocated to the telephone.
`Registration Disabled`	The Registration on the Business Communications Manager is set to OFF.

`SERVER UNREACHABLE.`
`RESTARTING . . .`
	Check that you have entered the correct Netmask and gateway IP addresses.
	If the settings are correct, contact your system administrator.

`NEW SET`	The telephone has not been connected to the Business Communications Manager before, and must be registered.

Note: To see the configuration information for a telephone connected to the Business Communications Manager: When the telephone is not on a call, press the ⇨□ key (bottom-right corner of the telephone), followed by the 🌐 key (next to the ⇨□ key). The display will automatically scroll through the configuration settings.

To see the Codec data for a telephone while it is on a call: Press the ⇨□ key, followed by the 🌐 key.

Other troubleshooting tips

Here are a few possible issues you may encounter, plus a description of what may cause them, and how to troubleshoot the issue.

Table 12 IP telephone troubleshooting

Problem	Suggested solution or cause
Telephone does not connect to system	If an IP telephone does not display the text `Connecting to server` within two minutes after power up, the telephone was unable to establish communications with the Business Communications Manager. Double check the IP configuration of the telephone, and the IP connectivity to the Business Communications Manager (cables, hubs, etc.).
Slow connection between the handset and the Business Communications Manager	If the connection between the IP client and the Business Communications Manager is slow (ISDN, dialup modem), change the preferred CODEC for the telephone from G.711 to G.729. See “IP telephone server configurations” on page 46.

Table 12 IP telephone troubleshooting

Problem	**Suggested solution or cause**
One-way or no speech paths	Signaling between the IP telephones and the Business Communications Manager uses Business Communications Manager port 7000. However, voice packets are exchanged using the default RTP ports 28000 through 28255 at the Business Communications Manager, and ports 51000 through 51200 at the IP telephones. If these ports are blocked by the firewall or NAT, you will experience one-way or no-way speech paths. **Firewall note:** If you have the firewall filter set to **Pass Outgoing and Block Incoming Except IP Phones**, this only allows IP telephony registration traffic through, but blocks all other traffic, including H.323 calls on this interface. You must still specify an H.323 rule to allow IP call voice traffic. Also, Registration must be turned on in the **Services, IP Telephony, Nortel IP Telephone, General** page, before the telphone can access the system to register.
Change the contrast level	When an IP telephone is connected for the first time, the contrast level is set to the default setting of 1. Most users find this value is too low. Therefore, after the telephone is installed, use **FEATURE *9** and use the UP or DOWN key to adjust the contrast.
Block individual IP sets from dialing outside the system.	If you want to block one or more IP telephones from calling outside the system, use Restriction filters and assign them to the telephones you want to block. Restriction filters are set up under Services, Telephony Services, Restriction filters. Restriction filters are discussed in the *Programming Operations Guide*.

Configuring DHCP

You can use DHCP to automatically assign IP addresses to the IP telephones as an alternative to manually configuring IP addresses for IP telephones. If you are using the Business Communications Manager as the DHCP server, you can also configure the server to automatically locate the VLAN ID for the system and assign it to the telephones that register.

Before setting up DHCP using the information below, refer to the *Business Communications Manager 3.0 Programming Operations* Guide for detailed information about DHCP.

➡ **Note:** Do not enable DHCP on the Business Communications Manager if you have another DHCP server on the network. Refer to the *Business Communications Manager 3.0 Programming Operations Guide* for detailed information about disabling DHCP or about using other types of DHCP.

To set up DHCP to work with IP terminals (refer also to "IP telephony DHCP notes" on page 50):

1 Ensure that **DHCP** (under **Services**) is set up with the following settings:

- **Global Options** tab: **NORTEL IP Terminal Information** box is set to:
  `Nortel-i2004-A, <ip address>:7000,1,250;<ip address>:7000,1,1.`

  Where `<ip address>` is the published IP address. Be sure to include the period at the end of the string (1,250.).

Nortel IP Terminal VLAN ID contains an identification if the system is using the VLAN option. If you do not know what the entry should be, contact the system administrator for the VLAN switch.

If you want DHCP to automatically assign VLAN IDs to the IP telephones, enter the VLAN IDs in the following format: `VLAN-A:id1,id2,...,idn` (Example, if your VLAN IDS are: 1100, 1200, 1300 and 1400, enter `VLAN-A:1100,1200,1300,1400`. (the entry must be terminated with a period).

If you do not want DHCP to automatically assign VLAN IDs to the IP telephones, enter VLAN-A:none. (the entry must be terminated with a period).

- **Summary** tab: **Status** box is set to **Enabled**.

2 Ensure that the **DHCP LAN** settings are correct (**DHCP, Local Scope, LANX**, where LANX is a LAN that contains IP sets that use DHCP):

- Scope Specific Options tab:
  Scope Status: **Enabled**
  Default Gateway Field: <*Published IP Address*>

- **Address Range** tab: contains the range of IP addresses you need.

3 Restart all existing connected IP telephones.

Note: Whenever changes are made to the DHCP settings, telephones will retain the old settings until they are restarted.

If the DHCP server is not properly configured with the Published IP address, the telephones will display `Invalid Server Address`. If this message appears, correct the DHCP settings, and restart the telephones.

IP telephony DHCP notes

The i2004 supports two forms of DHCP configuration: full and partial. If partial DHCP is selected, the user must manually enter the primary and secondary Business Communications Manager address/action/retry count. The i2004 then configures a IP address/netmask and default IP gateway via DHCP. If full DHCP is selected, the i2004 configures all parameters via DHCP.

Note: If partial DHCP is selected, the DHCP server does not need to send the vendor-specific or site-specific information outlined below. The information below pertains to Full DHCP only. In the case of partial DHCP, the i2004 requires only the Router option and Subnet Mask option to configure (along with IP address and lease time).

Full DHCP support in the i2004 terminal requires sending a Class Identifier option with each DHCP Discovery and Request message. Additionally, the i2004 checks for either a vendor-specific option message with a specific, unique to Nortel i2004, encapsulated sub-type OR a site-specific DHCP option. In either case, a Nortel i2004-specific option must be returned by the i2004-aware DHCP server in all Offer and Ack messages. The i2004 will use the information returned in this option to configure itself for proper operation. This includes binding a new IP address, netmask and gateway (for local IP stack) as well as configuring Server 1 (minimum) and, optionally, Server 2. By default, Server 1 is always assumed to be the primary server after a DHCP session.

The i2004 will not accept any Offers/Acks if they do not contain:

- a Router option (i2004 needs a default router to function) AND
- a Subnet Mask option AND
- an S1 Server Address and Port
- The i20XX sets require the scope value 128 to be configured on the DHCP server as follows: Format:

  `Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.`

  where,

  `Nortel-i2004-A` uniquely identifies this as the Nortel option

  Additionally, the -A signifies this version of this specification. Future enhancements could use -B, for example.
  ASCII **`,`** is used to separate fields
  ASCII **`;`** is used to separate Primary from Secondary Business Communications Manager information
  ASCII **`.`** is used to signal end of structure
  `iii.jjj.kkk.lll:ppppp` identifies IP:port for server (ASCII encoded decimal)
  `aaa` identifies Action for server (ASCII encoded decimal, range 0..255)
  `rrr` identifies retry count for Business Communications manager (ASCII encoded decimal, range 0..255). This string may be NULL terminated, although the NULL is not required for parsing.

Notes:

- **`aaa`** and **`rrr`** are ASCII encoded decimal numbers with a range of 0..255. They identify the **Action Code** and **Retry Count**, respectively, for the associated Business Communications Manager. Internal to i2004, they will be stored as 1 octet (0x00..0xFF). Note that these fields must be no more than three digits long.
- the Business Communications Manager is always considered the Primary server; the second server always considered Secondary.
- if only one Business Communications Manager is required, terminate primary TPS sequence immediately with **`.`** instead of **`;`**
  e.g. **`Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr.`**
- valid options are one Business Communications Manager or two Business Communications Managers (0, 3... not allowed).

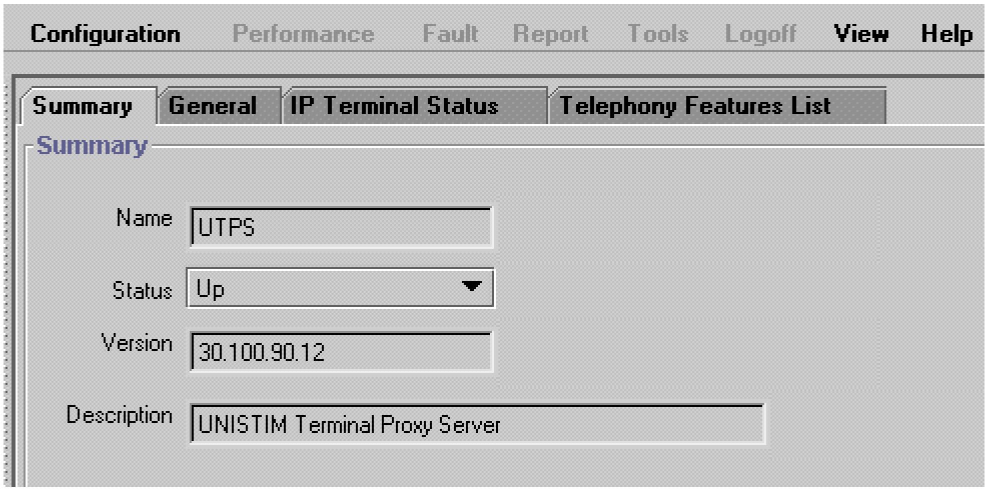
- Action code values:
  0 - reserved
  1 - UNIStim Hello (currently only this type is a valid choice)
  2..254 - reserved
  255 - reserved
- **iii,jjj,kkk,lll** are ASCII-encoded, decimal numbers representing the IP address of the Business Communications Manager. They do not need to be three digits long as the **.** and **:** delimiters will guarantee parsing. For example, **001**, **01** and **1** would all be parsed correctly and interpreted as value 0x01 internal to the i2004. Note that these fields must be no more than three digits long each.
- **ppppp** is the port number in ASCII-encoded decimal. It does not need to be five digits long as the **:** and **,** delimiters will guarantee parsing. For example, **05001**, **5001**, **1**, **00001**, etc. would all be parsed correctly and accepted as correct. The valid range is 0..65535 (stored internally in i2004 as hexadecimal in range 0..0xFFFF). Note that this field must be no more than five digits long.
- in all cases, the ASCII-encoded numbers are treated as decimal values, and leading zeros are ignored. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021 and 21 are all parsed and interpreted as decimal 21.

Checking IP server status

You can perform a status check on the Business Communications Manager server that gets used to register IP terminals:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary screen appears.

Figure 6 IP terminal registration server status



Name: UTPS
Status: Up
Version: 30.100.90.12
Description: UNISTIM Terminal Proxy Server

The following fields provide information about the IP server.

Field	Value	Description
Name	UTPS	Name of the server.
Status	Up Enabled Disabled	UP: server is operating Enabled: Server is using DHCP Disabled: server is not working.
Version	read-only	current version of server software
Description	read-only	description of server

Modifying IP telephone status settings

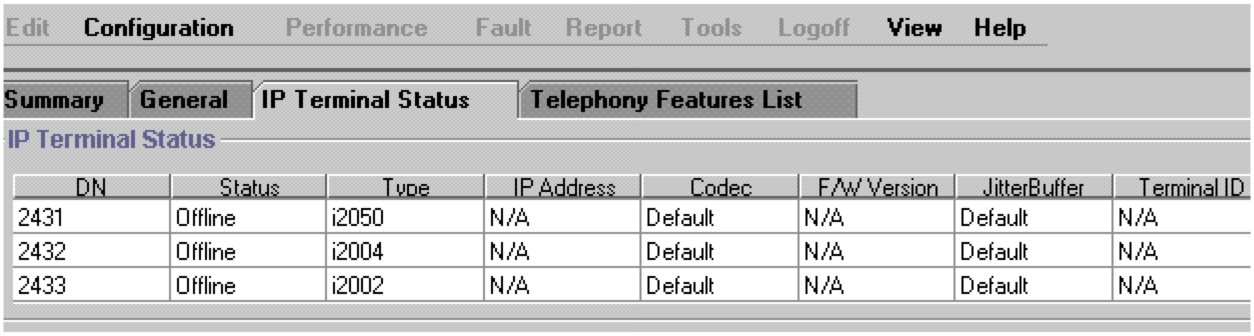
Settings such as jitter buffers and codecs for the Nortel IP telephones including the i2050, i2002 and i2004 can be modified through the Unified Manager:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click on the **IP Terminal Status** tab.

On the IP Terminal status screen, every IP telephone currently connected to the Business Communications Manager occupies a row in the IP Terminal Status table, as shown in the figure below.

Figure 7 IP Terminal status



IP Terminal Status

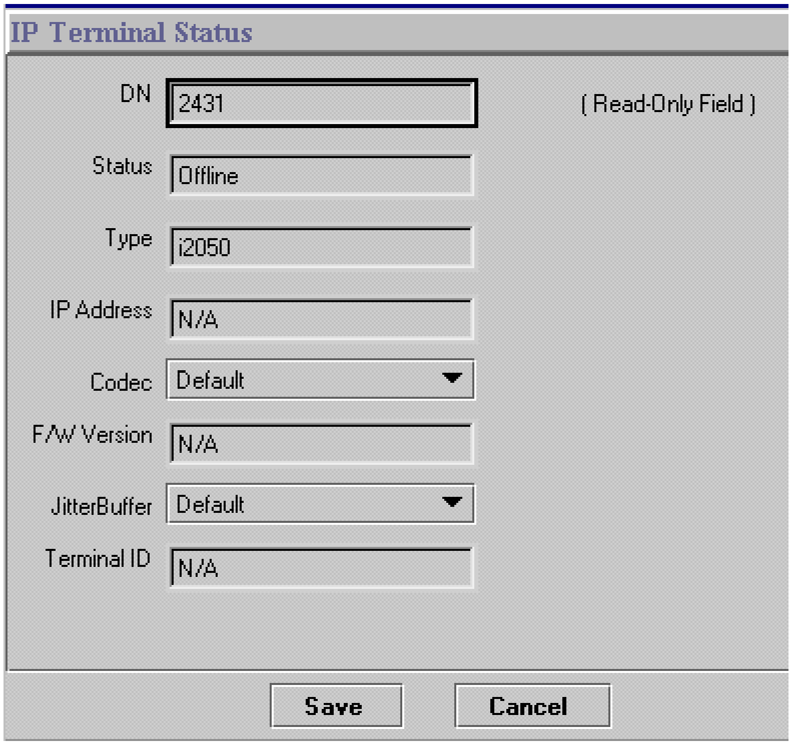
DN	Status	Type	IP Address	Codec	F/W Version	JitterBuffer	Terminal ID
2431	Offline	i2050	N/A	Default	N/A	Default	N/A
2432	Offline	i2004	N/A	Default	N/A	Default	N/A
2433	Offline	i2002	N/A	Default	N/A	Default	N/A

3 Select the IP Terminal that you want to change the properties for.

4 Open the **Configuration** menu, or right-click anywhere on the terminal listing to open the Configuration menu.

5 From the menu, select **Modify parameters**. The IP Terminal Status dialog box appears, as shown in the figure below.

Figure 8 IP Terminal status dialog



IP Terminal Status

DN: 2431 (Read-Only Field)

Status: Offline

Type: i2050

IP Address: N/A

Codec: Default

F/W Version: N/A

JitterBuffer: Default

Terminal ID: N/A

6 You can change the Codec or JitterBuffer settings for the terminal. The table below describes the fields on this screen.

Table 13 IP Terminal Status fields

Field	**Value**	**Description**
DN	Read-only	This is the DN record that is assigned to this terminal.
Status	Read-only	This is the current status of the terminal.
Type	Read-only	This is the type of IP telephone assigned to this record (i2050, i2004, i2002)
IP address	Read-only	This is the IP address assigned to this telephone
Codec	Default G.711-aLaw G.711-uLaw G.711 with VAD G.729 G.729 with VAD G.723	Specifying a non-default CODEC for a telephone allows you to override the general setting. You might, for example, want to specify a low bandwidth CODEC (g.729) for a telephone that is on a remote or busy sub-net. Refer to "Choosing a codec" on page 42.
F/W version	Read-only	

Table 13 IP Terminal Status fields (Continued)

Field	Value	Description
JitterBuffer	Auto Default None Small Medium Large	Increase the jitter buffer size for any telephone that has poor network connectivity to the Business Communications Manager. Refer to "Choosing a Jitter Buffer" on page 43.
Terminal ID	Read-only	

7 Click **Save**.

Working with the features list

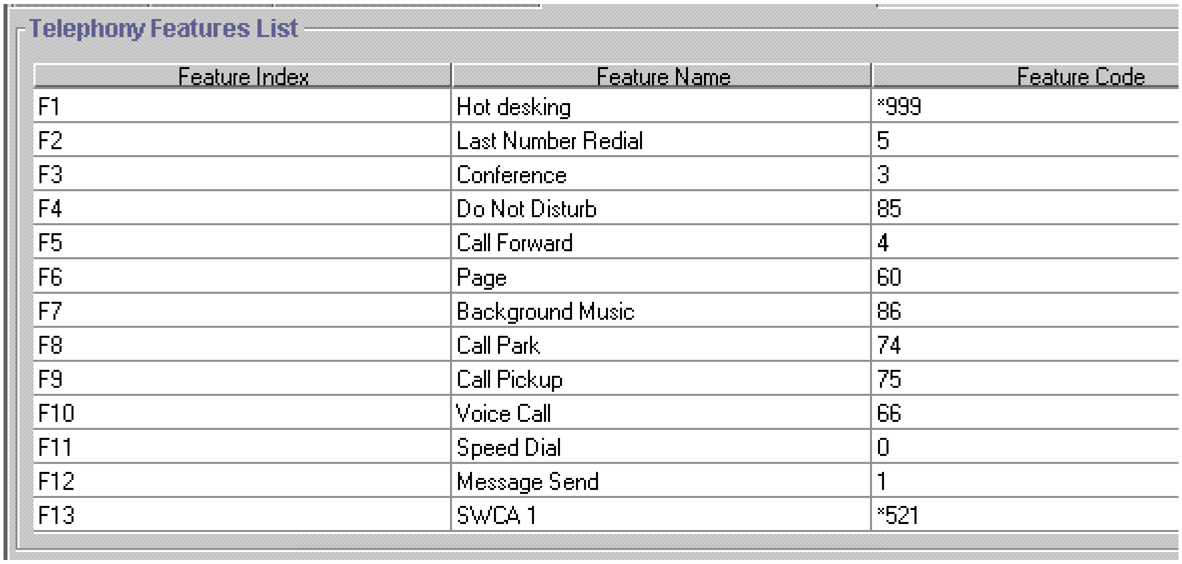
You can add and modify the features that display on the IP telephone feature list, which is accessed through the Services button or by using **FEATURE** *900. Refer to "Using the Services button to access features" on page 56. Note that the list assigns the hot desking feature to position 1 (refer to "Using the Hot Desking feature" on page 57).

The *Programming Operations Guide* provides a complete list of Business Communications Manager Features and index codes.

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click on the **Telephony Features list** tab.

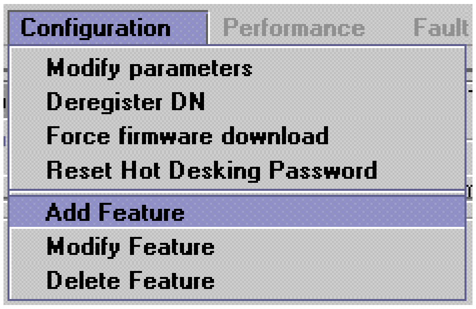
Figure 9 IP Telephony Features List



Telephony Features List

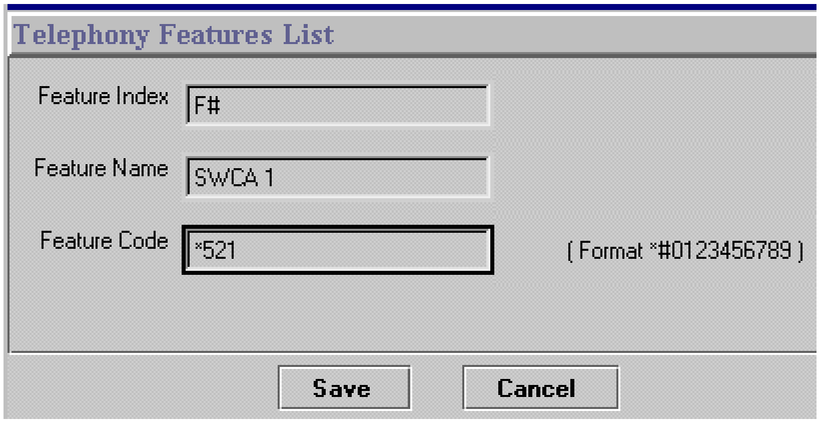
Feature Index	Feature Name	Feature Code
F1	Hot desking	*999
F2	Last Number Redial	5
F3	Conference	3
F4	Do Not Disturb	85
F5	Call Forward	4
F6	Page	60
F7	Background Music	86
F8	Call Park	74
F9	Call Pickup	75
F10	Voice Call	66
F11	Speed Dial	0
F12	Message Send	1
F13	SWCA 1	*521

3 Select the feature you want to modify and right click, or click on the **Configuration** menu item, then select the action you want to perform.



The Telephony Features list screen appears.

Figure 10 Add/Modify Telephony Features List



Feature Index: F#

Feature Name: SWCA 1

Feature Code: *521 (Format *#0123456789)

4 Enter or change the **Feature Name** and corresponding **Feature Code** in the appropriate fields.

5 Click **Save**.
The features list appears. Notice that the system assigns a **Feature Index** number, adding the feature to the bottom of the list.

Using the Services button to access features

The IP telephone has a limited number of memory buttons that can be configured with lines or features, however, a soft features menu also can be accessed by pressing the **Services** button .

- Use the arrow buttons or the Page + and Page - display keys to move quickly through the list.
- Use the up and down directional buttons to scroll to each feature.

- Press the Select display key to activate the feature, then use the feature as you normally would. For example: if you selected Call Forward, enter the number you to which you want to forward the call. Or, if you select speed dial (**FEATURE** 0), enter the speed dial code for the number you want the telephone to dial.

This feature allows you to assign your hardware feature keys to line and intercom applications, and still access the Business Communications Manager call features without needing to remember a feature code. Although the list is defaulted to the Services button, you can assign the display list to one of the other hard feature keys. The user can also assign it as a memory button, using **FEATURE** *3, at a specific telephone. Refer to the *Programming Operations Guide* for information about programming IP telephone memory buttons under **User Preferences**.

Note: If you move the feature to another memory button, the Services button no longer accesses the menu.

Using the Hot Desking feature

You can transfer your IP telephony features temporarily from one IP telephone to another using the Hot Desking feature. This feature is described in detail in the *Telephony Feature Handbook*. You use **FEATURE** *999 to enter the feature. To perform hot desking, you are prompted for a password, which is specified at the telephone, before you can complete the task.

The Hot Desking password can be reset from the Unified Manager. This allows users who forget their passwords to re-enter hot desking and to reset their password.

Note: This process also cancels hot desking for the telephone, if the application is currently active.

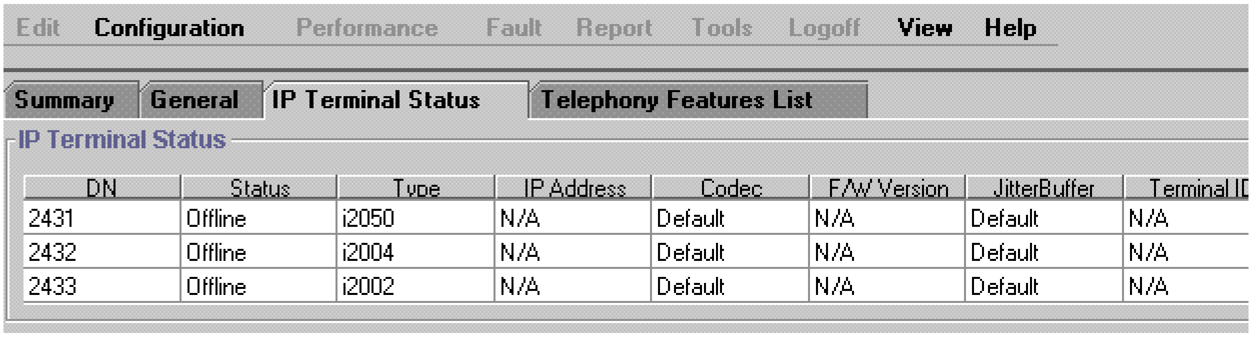
To reset the Hot Desking password field for a specific IP telephone:

1 Click on the key beside **Services** and **IP Telephony**.

2 Click on **Nortel IP Terminals.**

3 Click on the **IP Terminal Status** tab.

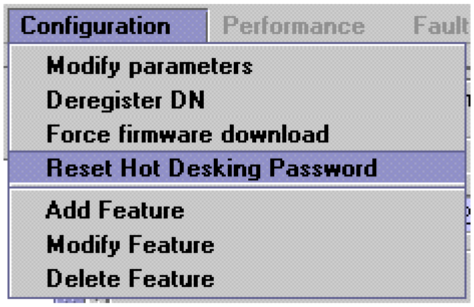
Figure 11 IP Terminal Status tab list



DN	Status	Type	IP Address	Codec	F/W Version	JitterBuffer	Terminal ID
2431	Offline	i2050	N/A	Default	N/A	Default	N/A
2432	Offline	i2004	N/A	Default	N/A	Default	N/A
2433	Offline	i2002	N/A	Default	N/A	Default	N/A

4 Select the IP telephone record you want to reset.

5 On the top menu, click **Configuration**, then select **Reset Hot Desking Password**.



6 A dialog box appears, prompting you to proceed. Click **Yes** to reset the password. The password resets to Null. The user can enter hot desking again to enter a new password.

Notes about Hot Desking

The Hot Desking feature allows a user to divert calls and signals from one IP telephone to another. For instance, if a user is temporarily working in another office, they can retain their telephone number by hot desking their usual telephone to the IP telephone in their temporary office.

Hot desking can be accessed using **FEATURE** *999 on the telephone to which the traffic will be diverted. The user can also evoke this feature from the Services key menu, where it is defaulted as the first item on the list.

Hot desking must be allowed on the originating telephone and you need to specify a password. These settings are found under the ADMIN key within the hot desking feature. Hot desking is invoked through the DIVERT key within the hot desking feature.

If the originating telephone does not have hot desking allowed, the user will receive a Not allowed prompt, indicating that the telephone is not available for hot desking. This prompt also occurs if the originating telephone is on a call when the diversion command was issued.

Once hot desking occurs between two IP telephones, no activity is allowed on the originating telephone, except to cancel hot desking. The display on the originating telephone indicates where it has been diverted. On the diversion telephone, the key displays will reflect the displays from the originating telephone.

Call forwarding to voice mail continues as normal. Voice mail can be accessed from the active IP telephone, as if it were the originating telephone.

When hot desking is cancelled, which can be performed from either telephone, the displays for each telephone return to normal.If you forget the password, hot desking can only be cancelled from the originating set.

➡ **Note:** When you cancel hot desking, ensure that the telephone is on-hook. If you have just hung up, wait 10 seconds before attempting to cancel hot desking.

Refer to the *Telephony Feature Handbook* for details about using this feature.

Customizing feature labels

When your IP telephone acquires a DN record, the default settings are applied to the telephone, including assigning features to the memory keys on the telephone. These features all have pre-defined labels, and the telephone automatically displays the appropriate labels beside the programmed buttons. If you want to customize these labels to be more appropriate, you can do so through the **Feature Labels** heading on the Unified Manager.

The screens under the Feature Labels heading allow you to define custom labels for 24 features. The system comes with 10 default labels, which are feature and language-specific, depending to which region your system was assigned. The default labels are mainly messaging and call attendant features.

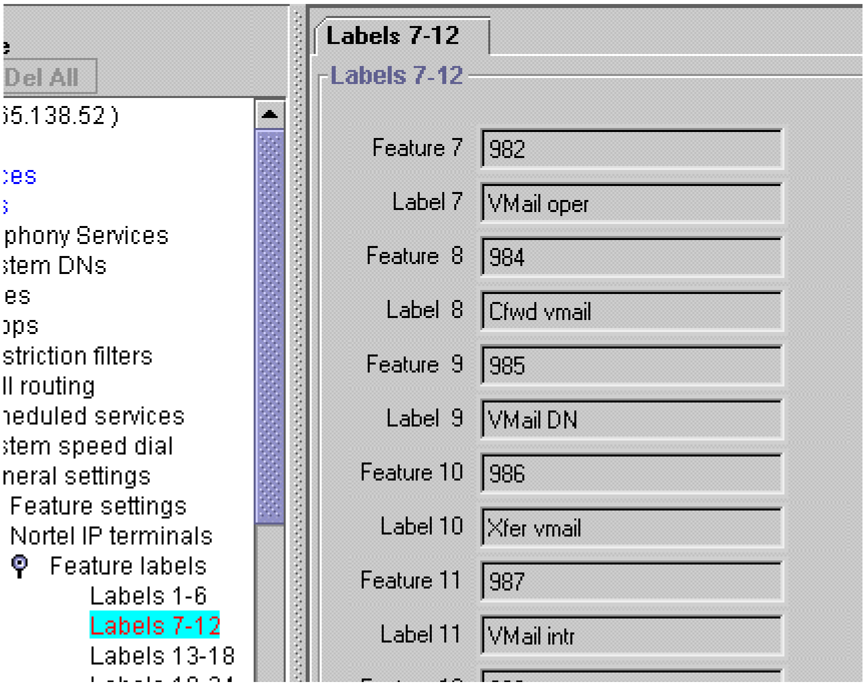
However, you can change any other feature label by adding to this list, or by deleting any of the default settings and inserting new codes and labels.

Follow these steps to change the features or labels on the memory buttons on your IP telephone:

1 Click on the keys beside **Telephony Services, General, Nortel IP terminals**, and **Feature labels**.

2 Click on the label set you want to view.
The Labels <label number> screen appears.

Figure 12 Label set defaults



Labels 7-12

Feature 7: 982
Label 7: VMail oper
Feature 8: 984
Label 8: Cfwd vmail
Feature 9: 985
Label 9: VMail DN
Feature 10: 986
Label 10: Xfer vmail
Feature 11: 987
Label 11: VMail intr

3 If you have an existing list, or you do not want to change any defaults, go to the first free label set.

4 In the **Feature <*label number*>** field, enter the dialing code for the feature you want to relabel. Example: enter 3 for conference call

5 In the **Label <*label number*>** field, enter the new label you want the telephones to display. Example: The current label for feature code 3 is Conference, you could change it to Conf Call

6 Click anywhere outside the field to save the changes.
The system automatically updates any i2002, i2004 or i2050 IP telephones that have a button appearance for the feature.

Some features, like Page and System Wide Call Appearances (SWCA), have several variations of feature invocation that you may want to customize for the users.

Paging can be F60, F61x, F62, and F63x. System-wide Call Appearance (SWCA) has 16 codes (*521 to *536). The following table shows examples of changing labels for page codes and SWCA codes:

Table 14 Relabelling examples

Feature code	New label
60	Gen Page
610	Pg Every
61	Zone <digit from 1-9>
62	Speak Pg
630	Speak, All

Feature code	New label
*521	SW Call 1
*522	SW Call 2
*523	SW Call 3
*524	SW Call 4
*525	SW Call 5

Note: Line names are defined when you configure the line, and can be changed through the **Lines** menus.

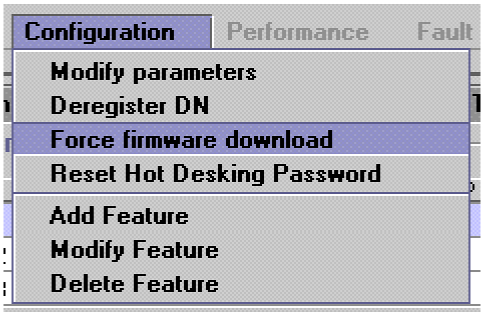
Download firmware to a Nortel IP telephone

Firmware is the software stored in the telephone. When the Business Communications Manager is upgraded with a new IP telephone firmware load, this firmware load will automatically be downloaded into the IP telephones when they next connect to the Business Communications Manager.

You can use the **Force firmware download** option under the **Configuration** menu (**Nortel IP Terminals**) to force immediate download to a telephone. You would do this in situations where you suspect that a particular telephone has corrupted firmware.

Follow these steps to force a firmware download to a telephone:

1. In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.
2. Click on the **IP Terminal Status** tab.
3. Select the IP telephone that you want to download firmware to.
4. Open the **Configuration** menu, or right-click anywhere on the listing for the terminal to bring up the menu.



5. Select **Force Firmware Download**.
   A dialog appears asking if you want to confirm that you want to proceed.
6. Click the **Yes** button.
   The firmware download begins.

The system drops any active call on that telephone, and downloads a new firmware load into the selected telephones. The telephones will be unusable until the download is complete and the telephones have reset.

Note: In order not to saturate the IP network with download packets, the system will only download up to five IP telephones at any given time. Telephones requiring download will show a Unified Manager status of `Download Pending`, and the UNISTIM Terminal Proxy Server (UTPS) will initiate download as resources become available.

Deregistering DNs for IP telephones

You can deregister selected telephones from the Business Communications Manager, and force the telephone to go through the registration process again.

Warning: Once this feature is activated, all active calls are dropped.

To deregister a DN for a telephone:

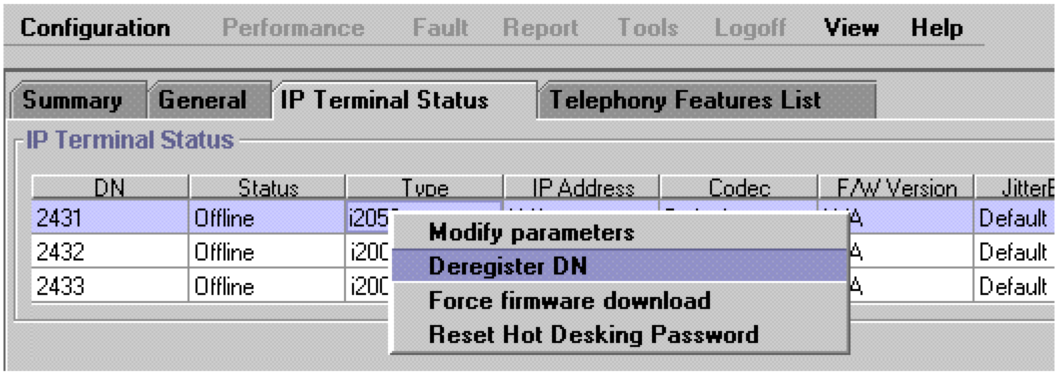
1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click on the **IP Terminal Status** tab.

3 Select the IP Terminal with the DN you want to deregister.

4 Open the **Configuration** menu, or right-click anywhere on the listing for the terminal to bring up the menu, as shown in the next figure.

Figure 13 Deregister DN from Configuration menu



DN	Status	Type	IP Address	Codec	F/W Version	JitterB
2431	Offline	i205			A	Default
2432	Offline	i200			A	Default
2433	Offline	i200			A	Default

5 Click **Deregister DN**.

6 Reregister the telephone, as described in “Configuring the i2002 or i2004 telephone to the system” on page 44.

Warning: Once this feature is activated, all active calls are dropped.

Moving IP telephones

IP telephones retain their DN when they are moved to a new location on the same subnet. The following instructions apply to Nortel IP telephones.

To move an IP telephone without changing the DN:

1. Disconnect the power from the IP telephone or 3-port switch.
2. Disconnect the network connection.
3. At the new location, reconnect the network cable and the power connection.
4. If the new location is on a different subnet, you will need to make the appropriate changes to the telephone IP addressing. However, do not change the S1 IP address or the S2 IP address.

Note: If your network is using partial DHCP, reconfiguration is not required at this step.

To move a Nortel IP telephone and change the DN:

1. Deregister the DN using the instructions in "Deregistering DNs for IP telephones" on page 62.
2. Disconnect the network connection and the power connection from the telephone.
3. Reinstall the phone at the new location and redconfigure the telephone. For information about this, see "Connecting the i2002 or i2004 telephone" on page 44.

Keep DN alive

This feature is only relevant to the i-series IP telephones (Model i2004/i2002/i2050).

If you want to retain DN-specific features such as Call Forward No answer and Call Forward on Busy if an IP telephone becomes disconnected, you must ensure the following setting is set to Y in the Unified Manager.

1. In the Unified Manager, under the Services, Telephony Services list, click on the DN record for the IP telephone.
2. Click the **Capabilities** heading.
3. Beside the **Keep DN alive** field, choose **Y**.

   Choosing **N** for this field allows the DN record to become inactive if the IP telephone is disconnected. This produces a `Not in Service` prompt if any of the special features, such as Call Forward, are invoked.

Warning: If the system is reset while an IP telephone is disconnected, the Keep DN alive feature becomes inactive until the telephone is reconnected.

Note: When an IP telephone is disconnected, there is about a 40-second delay before the system activates Keep DN alive during which incoming calls will either get a busy signal or be rerouted to the Prime set, depending on how your system is programmed. The same type of delay occurs when the IP telephone is reconnected to the system.

Configuring the Nortel Networks i2050 Software Phone

The Nortel Networks i2050 Software Phone allows you to use a computer equipped with a sound card, microphone, and USB headset to function as an IP terminal on the Business Communications Manager system. The Nortel Networks i2050 Software Phone uses the computer IP network connection to connect to the Business Communications Manager. The registration process is the same as for the i2002 and i2004 telephones ("Registering the telephone to the system" on page 45).

When you install the Nortel Networks i2050 Software Phone, on-screen documentation walks you through the steps for installing the software. You can also refer to the *i2050 Software Phone Installation Guide.*

To configure the Nortel Networks i2050 Software Phone to connect to the Business Communications Manager:

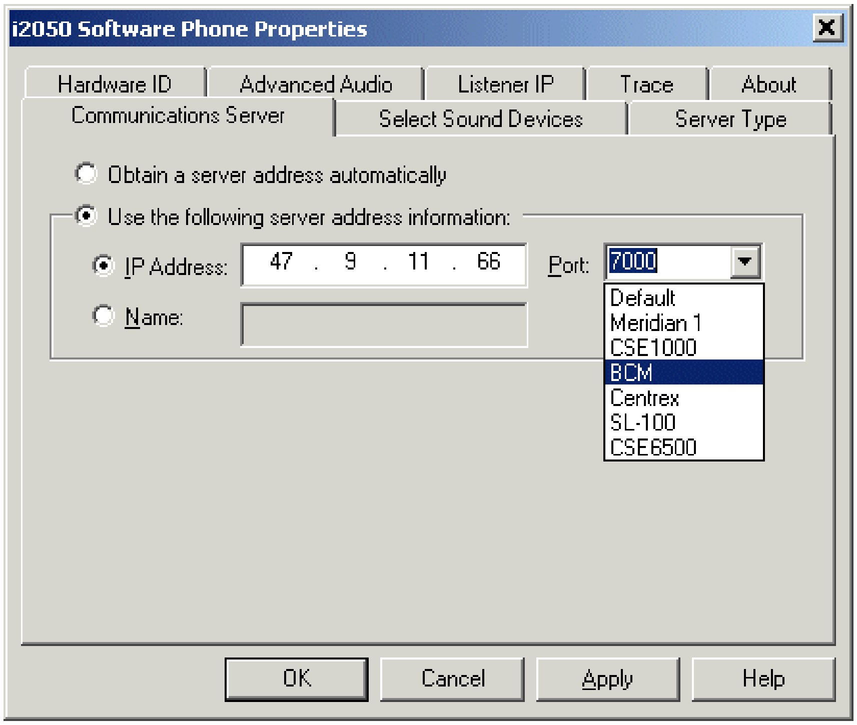
1 Click the **Start** button and then click **Settings**.

2 Click **Control Panel**.

3 Double click the **i2050 Software Phone** icon.

The utility opens to the Communications Server tab.

Figure 14 i2050 Communications server



i2050 Software Phone Properties

Communications Server

○ Obtain a server address automatically

● Use the following server address information:

● IP Address: 47 . 9 . 11 . 66

○ Name:

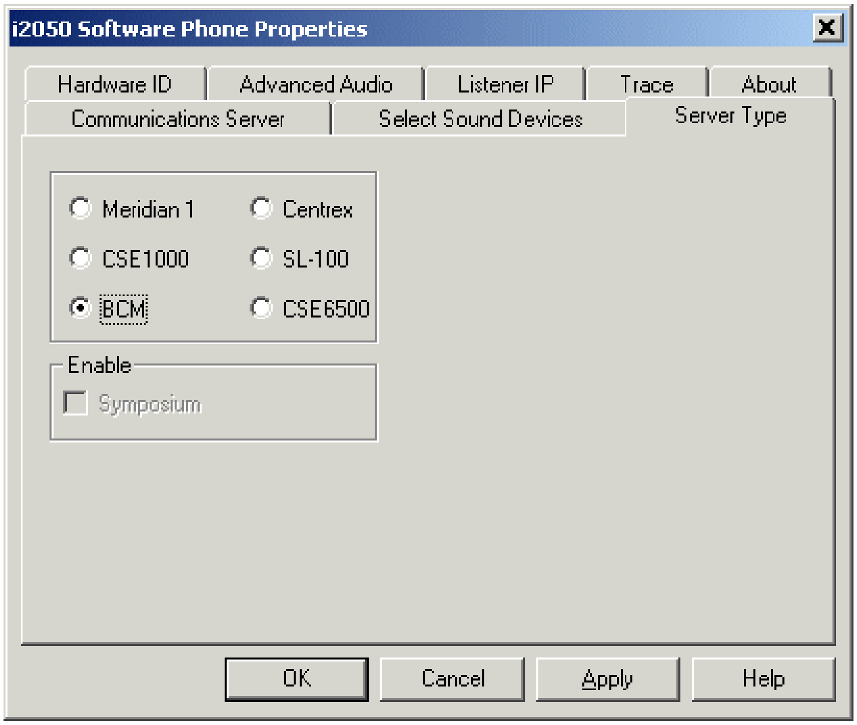
Port: 7000

4 Enter the Published IP address of the Business Communications Manager in the **IP address** field.

5 In the Port drop down menu, select **BCM**.

6 Select the **Server Type** tab.

Figure 15 i2050 Switch type



○ Meridian 1 ○ Centrex
○ CSE1000 ○ SL-100
● BCM ○ CSE6500

Enable
□ Symposium

7 Click on the **BCM** option.

8 Enable the **Select Sound Devices** tab for the USB headset.

To further configure this device through Unified Manager, see “Modifying IP telephone status settings” on page 53.

Chapter 4
Installing NetVision telephones

This section describes how to configure the Symbol NetVision handsets to the Business Communications Manager system.

The information in this section includes:

NetVision connectivity

The Business Communications Manager supports access points, NetVision handsets and other wireless IP devices that use either IEEE 802.11 (1 or 2 M-bits/sec, Frequency Hopping Spread Spectrum) or IEEE 802.11B (11 M-bits/sec, Direct Sequence Spread Spectrum) technology. NetVision telephones use an enhanced version of H.323, referred to as H.323+.

NetVision and NetVision Data wireless IP telephones connect to the Business Communications Manager over a LAN through the Business Communications Manager LAN or WAN card. The Business Communication Manager sees these telephones as IP telephones, which means that the DN records are assigned from the digital range rather than from the Companion or ISDN range of DNs.

The default codec for NetVision handsets is G.729. However, if the NetVision handsets connect over IP trunks, the codec of the IP trunk takes precedence.

➡ **Note:** NetVision handsets experience communications problems if your system has a NAT between the handset internet connection and the published address of the Business Communications Manager LAN. For this reason, this configuration is NOT supported.

From within the system, the handsets can make and receive calls from any trunk type supported by the system, which can include voice over IP (VoIP), digital and analog trunks. The handset DN record determines which lines the handset can access.

The handset can communicate with any other type of telephone supported by the Business Communications Manager system.

Access points

Instructions about installing an 802.11b access point are provided with the access point equipment, which is sold and installed separately. The access point is set up with a unique identifier (ESS ID) which is entered into the handset either through a configuration download or manually through the dialpad to allow the handset to access the system through that access point.

Keycodes

Before setting up NetVision telephones, ensure that you have enough IP client keycodes enabled to register all the NetVision telephones you require. For information about entering keycodes, see the *Keycode Installation Guide*. IP clients are distributed on a one-to-one basis with NetVision and IP telephones, so ensure that you take your entire system into consideration.

Handset and call functions

Symbol supplies a handset user guide that describes the features on the NetVision handset and how to use them to perform basic functions.

The *Business Communications Manager NetVision Feature card* explains how to use the handset to access features on the Business Communications Manager system and provides some quick tips for basic call functions.

The *Business Communications Manager Telephony Features Handbook* provides information about how to use Business Communications Manager call features.

The *Business Communications Manager NetVision Phone Administrator Guide* provides instructions for assigning features to the display list, and includes an appendix containing a list of the features that work with NetVision handsets.

Configuring NetVision records

This section provides the steps for configuring the various records that the NetVision telephone requires to work on a Business Communications Manager system.

This section describes:

- What information you require before you configure your handsets ("Gathering system information before you start")
- How to set up an H.323 Terminals record on the Business Communications Manager to allow the NetVision handset to connect to the system ("Assigning H.323 Terminals records" on page 69)

Note: DN records for NetVision handsets are created in the same way as for all other telephones on the system. The various settings for DN records are described in the *Business Communications Manager Programming Operations Guide*.

Choose model IPWls, when configuring NetVision DN records.

Gathering system information before you start

Ensure the following is complete, or the information is on hand before you start configuring your NetVision telephones:

1. The Business Communications Manager has been set up to allow IP telephones.	Refer to "IP telephones" on page 37.
2. If you are configuring the Business Communications Manager records before you configure the handset: You know which DNs you want to assign to the handsets and you have all the line, restrictions, and telephony information you require to create or update a DN record for each telephone.	DN records
3. Download the latest version of the NetVision Phone Administrator http://www.symbol.com/services/downloads/nvfirmware2.html Download the latest firmware version from the same website.	
4. You have obtained the Symbol NetVision serial cable, which is used to transfer configuration information between the computer where the tool is installed and the handset.	Purchased from Symbol at <http://symbol.com> (part number: 25-20528-01)
5. You have a list of names that you will use for the handsets. Each name must be unique to a handset. Both the H.323 Terminals record and the NVPA record must have exactly the same name.	Name field
6. You have identified a PIN for each handset.	Password field

Assigning H.323 Terminals records

The **H.323 Terminals** record (**Services, IP Telephony**) identifies the NetVision handsets within the Business Communications Manager. The Business Communications Manager uses the information from this file to determine if the handset will be allowed to connect to the system.

Notes

The following are some notes about the process of configuring handsets to the Business Communications Manager.

- You must have an H.323 record configured before you configure the handsets with the Nortel NVPA.
- Each telephone that you configure will use one IP client assignment, so ensure that you added enough keycodes to accommodate both your IP telephones and your NetVision telephones.
- If you do not specify a DN in the H.323 record, one will automatically be assigned to the handset. If you specified a DN record, it will appear under the Active DNs heading once the handset connects to the system. If you want to specify a range of DNs, you can use the Add Users Wizard. This wizard is explained in the *Business Communications Manager 3.0 Programming Operations Guide*.

- You need to set up the DN record to determine what lines the handset can access and how it will behave on the system.
- The Name you specify in the H.323 record must match the User Name you specify in the Nortel NVPA tool, otherwise, the handset will not be allowed to connect to the Business Communications Manager.

If you need to change the H.323 Terminals record, refer to "Updating the H.323 terminals record" on page 71 and "Deleting a NetVision telephone from the system" on page 72. If you require information about changing the DN records, refer to the *Business Communications Manager 3.0 Programming Operations Guide* for details.

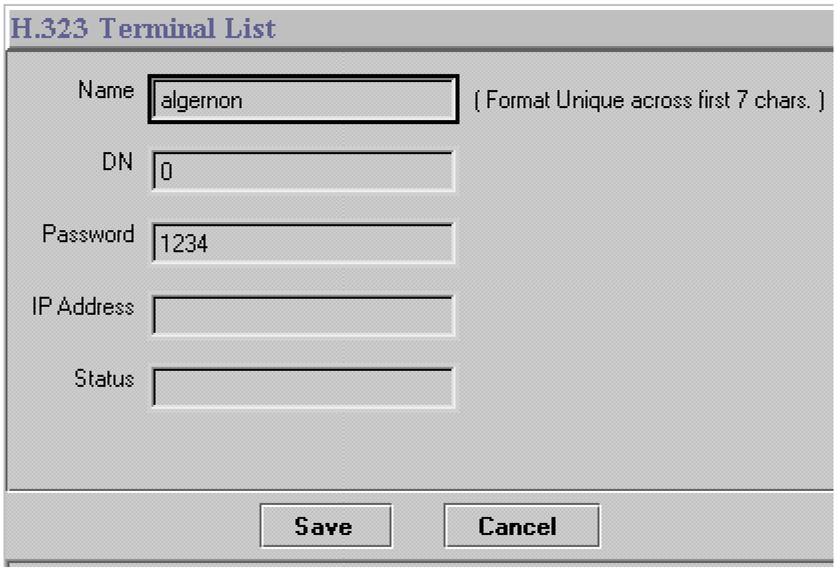
Adding a NetVision record in the Unified Manager

Follow these steps to preconfigure an **H.323 Terminals** record for each handset you install:

1 In the Unified Manager, open **Services, IP Telephony**, and click on **H.323 Terminals**.
The H.323 terminal list appears.

2 On the top menu, click **Configuration**, and then click **Add Entry**.
The H.323 Terminal List dialog appears.

Figure 16 H.323 Terminal list dialog



H.323 Terminal List

Name: algernon (Format Unique across first 7 chars.)

DN: 0

Password: 1234

IP Address:

Status:

3 Use the information in the table below to set up your NetVision handset IP system record.

Table 15 H.323 Terminal list

Field	Value	Description
Name	<alphanumeric>	This is the name for the handset. This name must have unique characters for at least the first seven digits.
	Note: This is the same name that you will enter in the Nortel NVPA configuration record for the User Name of the handset. This name must be unique within the first seven characters for each handset, and can be a maximum of 10 characters.	

Table 15 H.323 Terminal list (Continued)

Field	Value	Description
DN	<DN number> or 0	This is the assigned DN for this handset. If you want the system to dynamically define a DN, enter 0 (zero). Note: This field cannot be left blank.
Password	<numeric>	Enter a unique password. This is what the user must enter on the handset to connect to the system from the handset. You must enter at least four digits. This is a mandatory field.
IP Address	(read-only)	This field populates when the system assigns an IP address to the handset.
Status	(read-only)	This field populates when the system registers the handset.

4 Click **Save**.

Note: Shortly after the H.323 Terminals record is saved, the system moves the DN you specified to the Active DNs list. If you have not already done so, configure the DN record for user requirements. If you are not sure about how to configure DNs, refer to the *Business Communications Manager 3.0 Programming Operations Guide* for details about the various settings within this record.

Programming note: Ensure that you choose Model *IPWls* on the **General** screen.

Testing the handset functions

When the handset is registered, check the handset feature menu, and test the handset to ensure it is working as you expected. Refer to the *NetVision Telephone Feature User Card* for directions about using Business Communications Manager call features on the NetVision handset.

Updating the H.323 terminals record

If you need to change the password for a NetVision telephone, update the H.323 terminals record.

Follow these steps to update the H.323 Terminals record:

1 In the Unified Manager, click on the keys beside **Services** and **IP Telephony**.

2 Click on **H.323 Terminals**.

3 On the H.323 Terminal List screen, highlight the terminal you want to change.

4 At the top of the page, click on **Configuration** menu and select **Update Entry**.
The H.323 Terminal List dialog appears.

5 Enter a new password.

6 Click **Save**.

Changing a handset Name

The Name is the primary point of recognition for the Business Communications Manager to identify a handset. If you need to change the name of an assigned handset:

1 Delete the existing record. Refer to "Deleting a NetVision telephone from the system" on page 72.

2 Enter a new record with the new name.
You can assign the existing DN to the new record.

3 For security purposes, you should assign a new **Password**.

Changing the DN record of a handset

If you need to change the DN for a handset, use the Unified Manager (**Services, Telephony Services, General, Change DN**). The change will automatically be reflected in the H.323 Terminals record for the handset.

When you use the **Change DN** feature, the DN settings are transferred to the new DN and the system features remain active on the new DN.

⚠ **Warning:** Deleting an H.323 Terminals record will remove the DN from the Active DNs list. This means that system features such as Call Forward No Answer will also become inactive.

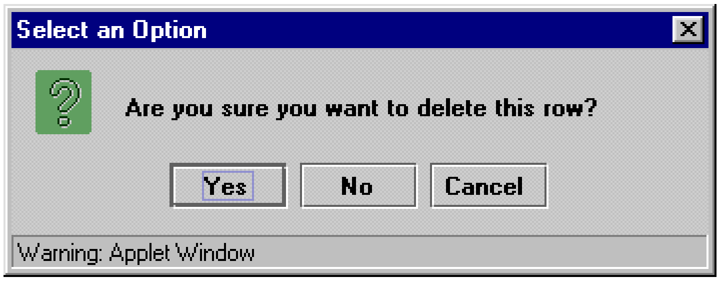
Deleting a NetVision telephone from the system

If you want to stop a terminal from having access to the Business Communications Manager, you can delete the DN record for the terminal:

1 In the Unified Manager, open **Services, IP Telephony**, and click on **H.323 Terminals**.

2 On the IP Terminal Status screen, select the terminal you want to change.

3 In the **Configuration** menu, click **Delete Entry**.
A query box appears.



Select an Option

Are you sure you want to delete this row?

4 Click **Yes** to delete the record.
Under the **Systems DNs** heading, the DN record returns to the Inactive DNs list.

Chapter 5
Configuring VoIP trunks

This section explains how to configure voice over IP (VoIP) trunks on a Business Communications Manager 3.0 system. A VoIP trunk allows you to establish communications between a Business Communications Manager and a remote system across an IP network.

➡ **Note:** VoIP trunks can be used for calls originating from any type of telephone within the Business Communications Manager system. Calls coming into the system over VoIP trunks from other systems can be directed to any type of telephone within the system.

You cannot program DISA for voice over IP (VoIP) trunks, therefore, you cannot use COS passwords to remotely access features over your system. The exception to this would be a tandem system, where the call comes into system A over the PSTN, then tandems to system B over an VoIP trunk. In this case, the remote access package set up for the COS password will determine which system features are available to the caller.

Configuring a VoIP trunk requires the following actions:

- “Pre-installation system requirements” on page 74
- “Configuring media parameters” on page 74
- “Outgoing call configuration” on page 76
- “Incoming call configuration” on page 89

➡ **Note:** If you are using the Business Communications Manager with a Meridian 1 (M1-ITG) system, you must set up the system to be compatible with the M1. Refer to “Interoperability” on page 143.

- This section also includes information about:
- “Example configuration, set to set” on page 91
- “Remote access over VoIP trunks” on page 97
- “Configuring Net Meeting clients” on page 98
- “Quality of Service Monitor” on page 100
- “Port settings” on page 101
- “Using a gatekeeper” on page 103

➡ **Note:** Also refer to Appendix D, “Interoperability,” on page 143 for information about interoperability issues.

Pre-installation system requirements

Ensure that you have obtained the following before continuing:

Keycodes

Before you can use VoIP, you must obtain and install the necessary keycodes. See the *Keycode Installation Guide* for more information about installing the keycodes. Talk to your Business Communications Manager sales agent if you need to purchase VoIP keycodes.

Each keycode adds a specific number of VoIP trunks. You must reboot your Business Communications Manager after you enter VoIP keycodes to activate trunking.

If you want to use the MCDN features on the VoIP trunks, you will need an MCDN keycode. However, if you have already deployed MCDN for your SL-1 PRI lines, you do not require an additional keycode.

Published IP address

You will require the public IP address to set up the gateways for VoIP trunks. Refer to "Defining published IP address" on page 35 for details.

Configuring media parameters

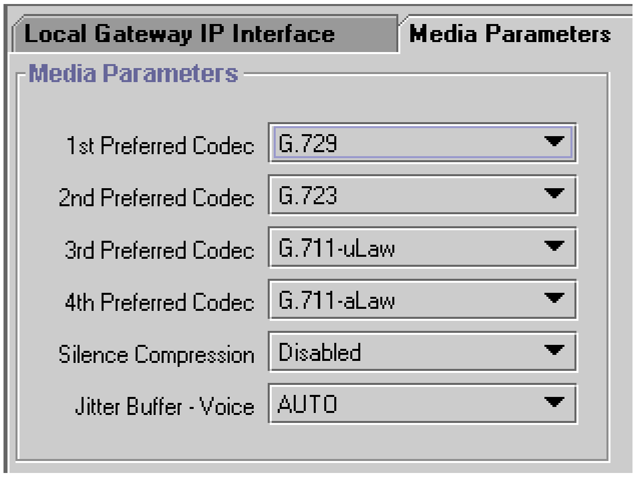
You can use the screen described in this section to determine the order the system will select codecs for your IP terminals, the silence suppression settings, and the jitter buffers.

1 In Unified Manager, click on the keys beside **Services**, **IP Telephony**.

2 Click on **H.323 trunks**.

3 Click on the **Media Parameters** tab.
The Media Parameters dialog appears.

Figure 17 Media parameters



Media Parameters

1st Preferred Codec: G.729
2nd Preferred Codec: G.723
3rd Preferred Codec: G.711-uLaw
4th Preferred Codec: G.711-aLaw
Silence Compression: Disabled
Jitter Buffer - Voice: AUTO

4 Use the information in the table below to set up the media parameters for your system.

Table 16 Media parameters record

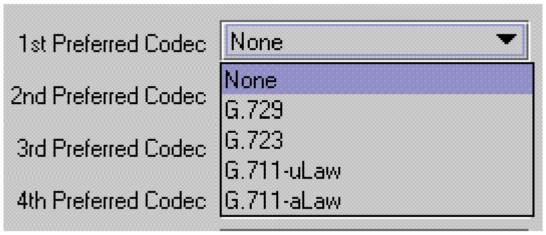
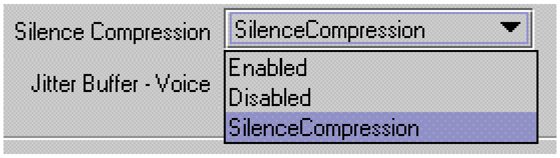
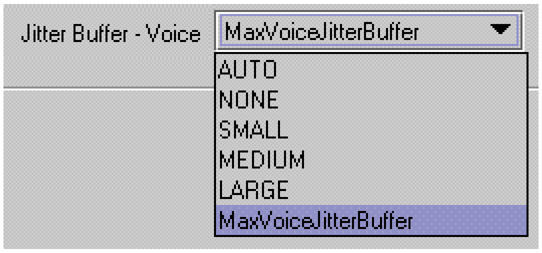
Field	**Value**	**Description**
1st Preferred Codec 2nd Preferred Codec 3rd Preferred Codec 4th Preferred Codec	None G.711-uLaw G.711-aLaw G.729 G.723 G.729 + VAD G.723 + VAD	Select the Codecs in the order in which you want the system to attempt to use them.  1st Preferred Codec None 2nd Preferred Codec 3rd Preferred Codec 4th Preferred Codec None G.729 G.723 G.711-uLaw G.711-aLaw **Performance note:** Codecs on all networked Business Communications Managers must be consistent to ensure that interacting features such as Transfer and Conference work correctly. Refer to “Codecs” on page 26.
Silence Compression	Enabled Disabled SilenceCompression	The silence compression identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If silence compression is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support silence compression. G.711 does not support silence compression.  Silence Compression SilenceCompression Jitter Buffer - Voice Enabled Disabled SilenceCompression **Performance note:** Silence Compression on all networked Business Communications Managers and ITG systems (VAD setting on ITG systems) must be consistent to ensure that interacting features such as Transfer and Conference work correctly. As well, the Payload size on the ITG must be set to 30ms.

Table 16 Media parameters record (Continued)

Field	**Value**	**Description**
Jitter Buffer - Voice	Auto None Small Medium Large MaxVoiceJitterBuffer	Select the size of jitter buffer you want to allow for your system.  Jitter Buffer - Voice: MaxVoiceJitterBuffer AUTO NONE SMALL MEDIUM LARGE MaxVoiceJitterBuffer Refer to "Jitter Buffer" on page 26.

Outgoing call configuration

This section explains how to set up your system to place calls through VoIP trunks. The system at the other end of the call must be set up to receive VoIP calls. For information about this, refer to "Incoming call configuration" on page 89.

Outgoing call configuration consists of the following steps:

- "Putting VoIP lines into a line pool" on page 76
- "Configuring telephones to access the VoIP lines" on page 78
- "Configuring a remote gateway" on page 78
- Optional: "Configuring PSTN fallback" on page 80

Putting VoIP lines into a line pool

Lines 001 to 060 are reserved for VoIP trunks. However, they can be used only if you have entered the appropriate keycodes to activate them.

When putting VoIP trunks into a line pool, choose a line pool that is not used for any other type of line. Once you have created a line pool, you create an access code that the user dials on their telephone to access the line pool.

Note: Set up an access code for the line pool only if you are NOT planning to use PSTN fallback. If you intend to use PSTN fallback, you must assign the line pool you create in this procedure to a route, and then you need to specify a destination code. Refer to "Configuring PSTN fallback" on page 80.

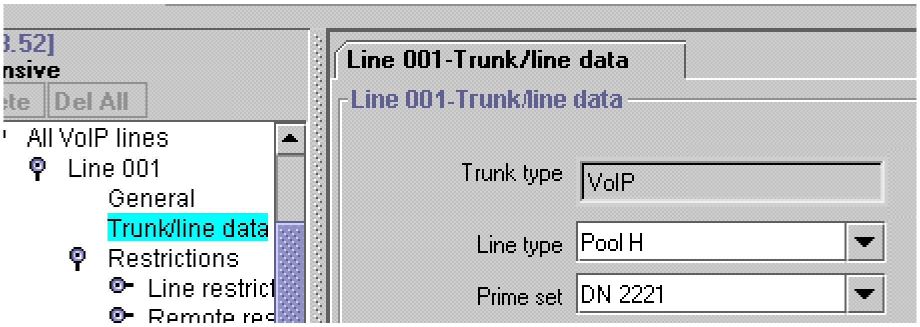
To put your lines into a line pool:

1 In Unified Manager, click on the keys beside **Services, Telephony Services**, **Lines**, **VoIP lines**, **Enabled VoIP lines**

2 Click on **Line XXX**, where XXX is the line number for the VoIP trunk you want to put in the line pool.

3 Click on **Trunk/Line Data**.
The Trunk/Line Data screen appears, as shown in the figure below.

Figure 18 Trunk/Line data



Trunk type: VoIP
Line type: Pool H
Prime set: DN 2221

4 In the **Line type** field, set a line pool that is not used by any non-VoIP lines.

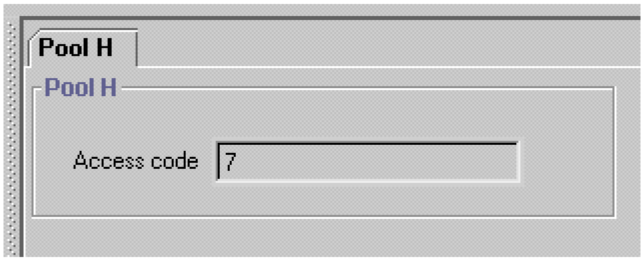
5 Repeat this procedure for as many trunk lines as you have keycodes for. You can use the same line pool for all VoIP lines.

6 On the navigation tree, click the keys beside **General Settings**, **Access Codes,** and **Line Pool Codes.**

Note: Set up an access code for the line pool only if you are NOT planning to use PSTN fallback. If you intend to use PSTN fallback, you must assign the line pool you create in this procedure to a route, and then you need to specify a destination code. Refer to "Configuring PSTN fallback" on page 80.

7 Click on the line pool that you selected as the VoIP line pool.
The Pool screen appears, as shown in the figure below.

Figure 19 Line pool access code setting



Access code: 7

8 Enter a unique access code for this line pool.

Ensure that no other line pools use this access code. Also ensure that this access code is not used for any other type of code, such as destination codes or DISA DNs.

Configuring telephones to access the VoIP lines

For each telephone that will be allowed to use the VoIP lines, you must add that line pool to the DN record:

1 In Unified Manager, open **Services**, **Telephony Services**, **System DNs, Active Set DNs**, **DN XXX**, **Line Access**. DN XXX is any DN that you want to allow to use VoIP trunking.

2 Click **Line Pool Access**.

3 Click **Add**.
The Add Line Pool Access dialog appears.

4 Type the letter of the VoIP line pool.

5 Click **Save**.

6 Repeat this procedure for every telephone you want to allow to use VoIP trunks.

Configuring a remote gateway

This section explains how to configure the Business Communications Manager to communicate with other Business Communications Managers and/or other VoIP gateways such as Meridian ITG. The remote gateway list must contain an entry for every remote system to which you want to make VoIP calls.

Note: Gatekeeper

If your system is controlled by a gatekeeper, you do not need to establish these gateways. Refer to “Using a gatekeeper” on page 103.

To add an entry to the remote gateway list:

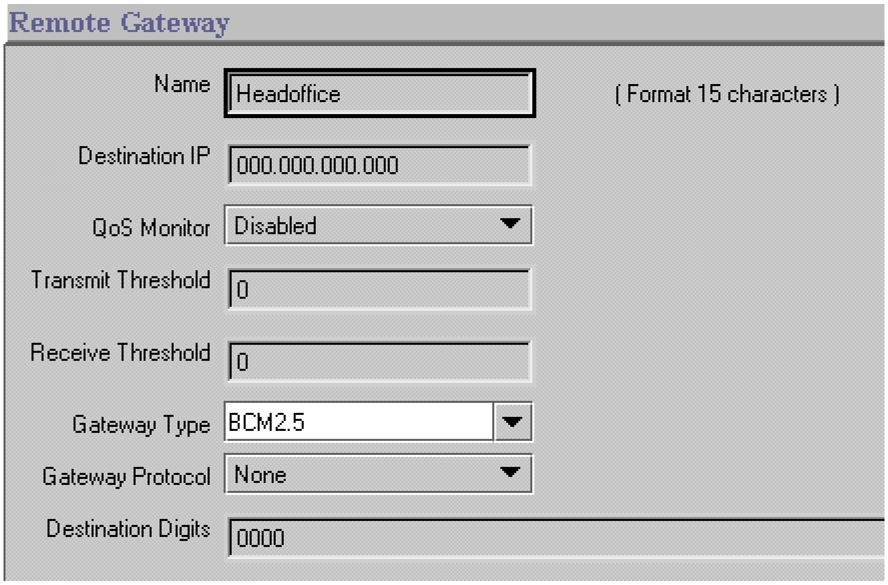
1 In Unified Manager, open **Services**, **IP Telephony**, **H.323 Trunks**, and click on **Remote Gateway**.

The remote gateway tab appears. The Remote Gateway screen shows all gateway records that have been added to the system.

2 On the top menu, click **Configuration**, and select **Add entry**.
If you are modifying an existing entry, select the entry, then, under **Configuration**, select **Modify entry**.

The Remote Gateway window appears as shown in the next figure.

Figure 20 Remote gateway dialog



Remote Gateway

Name: Headoffice (Format 15 characters)

Destination IP: 000.000.000.000

QoS Monitor: Disabled

Transmit Threshold: 0

Receive Threshold: 0

Gateway Type: BCM2.5

Gateway Protocol: None

Destination Digits: 0000

3 Use the information in the table below to set up the remote gateway information.

Table 17 Remote gateway record

Field	Value	Description
Name	<alphanumeric>	Enter an indentifying tag for the remote system
Destination IP	<ip address>	Enter the IP address of the remote system gateway.
QoS Monitor	Disabled Enabled	Choose Enabled, if you intend to use a fallback PSTN line. Ensure that QoS Monitor is also enabled on the remote system. Otherwise, choose Disabled. For information about enabling QoS, see “Turning on QoS monitor” on page 87
Transmit Threshold	read-only	
Receive Threshold	read-only	
Gateway Type	BCM3.0 BCM2.5 BCM2.0 ITG CSE 1000 CS 3000 IMS	Choose the type of system that is accessed through the remote gateway: BCM3.0: Business Communications Managers running 3.0 software *BCM2.5: Business Communications Managers running 2.5 or 2.5 FP1 or FP1 Maintenance Release software BCM 2.0: Business Communications Managers running 2.0 software, or Enterprise Edge systems running 2.0.x software. ITG: M1 Internet Telephony Gateway CSE 1000: CS3000/IMS: CS3000 is the previous version of IMS *If your gateway is set to BCMX.X and the other system is upgraded to 3.0, your system will automatically update this listing to BCM3.0 when the other system is contacted after the upgrade. If this does not occur, your original configuration may not be correct and you will have to set the change manually.

Table 17 Remote gateway record (Continued)

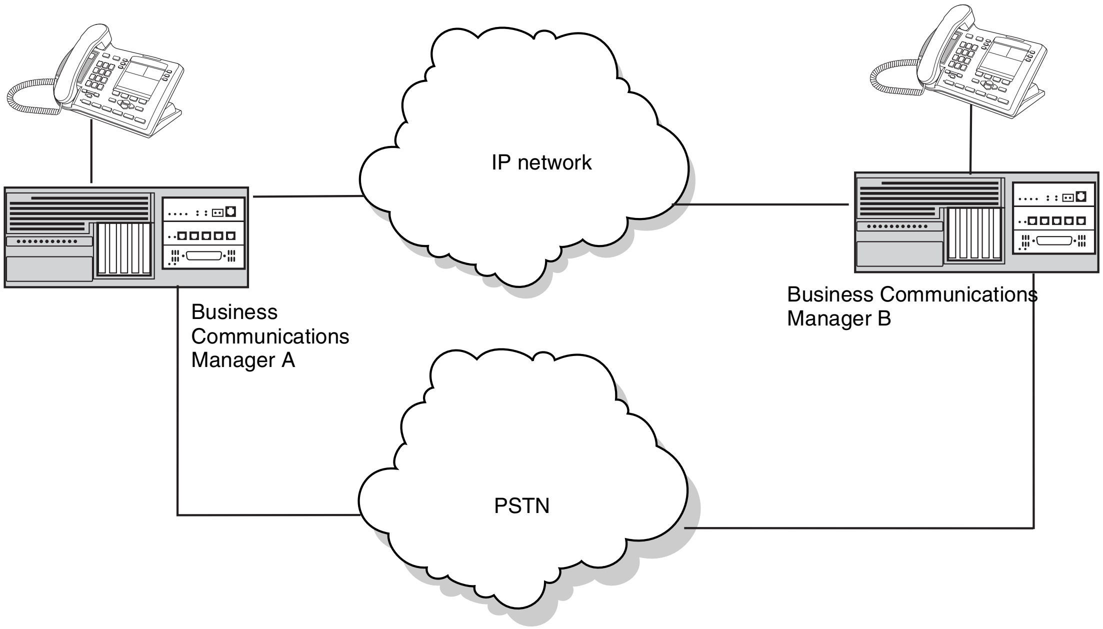
Field	Value	Description
Gateway Protocol	None SL-1 CSE	Select the gateway protocol that the trunk expects to use. None: No special features SL-1: MCDN protocol for gateways that provide MCDN over VoIP service CSE: Use this setting when using a CSE 1000 gateway.
Destination Digits	<numeric> (could be the same as the destination code for the route to this system)	Set the leading digits which callers can dial to route calls through the remote gateway. Ensure that there are no other remote gateways currently using this combination of destination digits. If multiple leading digits map to the same remote gateway, separate them with a space. For example, 7 81 9555. These numbers are passed to the remote system as part of the dialed number.

4 Click **Save**.

Configuring PSTN fallback

By enabling PSTN fallback, you allow the system to check the availability of suitable bandwidth for a VoIP call, then switch the call to a land line if the IP line is not available or cannot produce the expected quality. The following figure shows how a fallback network would be set up between two sites.

Figure 21 PSTN fallback diagram


IP network
Business Communications Manager A
Business Communications Manager B
PSTN

In a network configured for PSTN fallback, there are two connections between a Business Communications Manager and a remote system.

One connection is a VoIP trunk connection through the IP network.

The fallback line is a PSTN line, which can be the public lines or a dedicated T1, BRI, PRI or analog line (E&M), to the other system.

When a user dials the destination code, the system checks first to see if the connection between the two systems can support an appropriate level of QoS. If it can, the call proceeds as normal over the VoIP trunk. If the minimum acceptable level of QoS is not met, the call is routed over the second route, through the PSTN line.

For PSTN fallback to work, you must ensure that the digits the user dials will be the same regardless of whether the call is going over the VoIP trunk or the PSTN. In many cases, this involves configuring the system to add and/or absorb digits. This process is explained during the steps in "Configuring routes" on page 82 and "Creating destination codes for fallback" on page 84.

For detailed information about inserting and absorbing digits, see the *Business Communications Manager 3.0 Programming Operations Guide*.

Setting up PSTN fallback includes:

- Enabling PSTN fallback
- Setting up the VoIP schedule
- Configuring routes and dialing digits
- Creating destination codes for fallback
- Activating the VoIP schedule
- Turning on QoS monitor

Enabling PSTN fallback

To enable PSTN fallback:

1. Open **Services**, **IP Telephony** and click on **H.323 trunks**.
2. Click the **Fallback to Circuit-Switched** menu and select **Enabled-All** or **Enabled-TDM-only**. Enabled-TDM-only enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the Business Communications Manager network, because PSTN fallback is unlikely to result in better quality of service in that scenario.

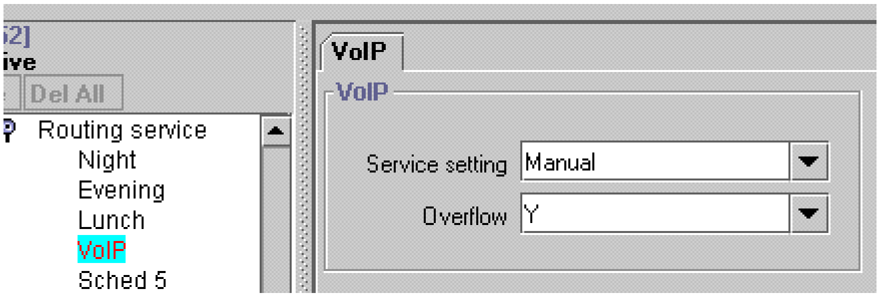
Setting up the VoIP schedule

You can determine which telephones/lines will choose the VoIP route as the prime route by setting up the VoIP schedule to allow you to manually activate the service from a control set. The PSTN route gets assigned to the Normal schedule, which runs on all telephones when no other schedule is activated.

Rename Schedule 4 (**Services, Telephony Services, Scheduled Services, Common Settings, Schedule Names**) to VoIP. Refer to the *Programming Operations Guide* for detailed instructions, if required. Then follow these steps to set up the VoIP schedule for routing services:

1 Open **Services**, **Telephony Services**, **Scheduled Services**, **Routing Service**, and click on **VoIP**. The VoIP schedule screen appears in the right frame.

Figure 22 VoIP Routing Service



Service setting: Manual

Overflow: Y

2 Change the **Service setting** to **Manual**.

3 Change the **Overflow** setting to **Y**.

Configuring routes

Configuring routes allows you to set up access to the VoIP and the PSTN line pools. These routes can be assigned to destination codes using schedules.

Note: If you have not already done so, remember to define a route for the local PSTN for your own system so users can still dial local PSTN numbers.

Ensure the PSTN and VoIP line pools have been configured before you continue with this section. For information about creating a VoIP line pool, see “Putting VoIP lines into a line pool” on page 76. You can create a PSTN line pool in the same manner, if such a pool does not already exist.

Note: If you already have routes for your PSTN or VoIP line pools configured, you do not need to configure new routes, unless you cannot match the dialed digits. For instance, you probably already have a PSTN route that uses 9 to access local PSTN numbers.

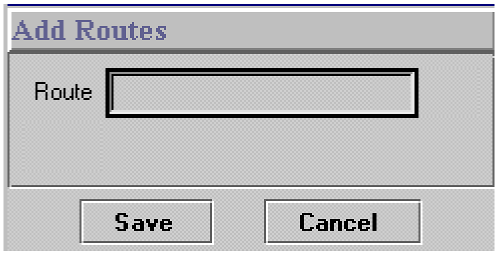
Follow these steps to configure the PSTN and VoIP routes:

1 Open **Services**, **Telephony Services**, **Call Routing,** and click on **Routes**.

2 Enter the route numbers for the PSTN and VoIP lines:
PSTN (to other system):

a Click the **Add** button. The Add Routes dialog appears.

Figure 23 Add route dialog


Add Routes

Route

b Type a number between 001 and 999 to define the PSTN route to the other system. Only numbers not otherwise assigned will be allowed by the system.

c Click Save.

PSTN (to local PSTN lines):

a Click the **Add** button.

b In the Add routes dialog Route field, type a number between 001 and 999 to define the PSTN route to your local PSTN.
Only numbers not otherwise assigned will be allowed by the system.

c Click Save.

VoIP:

a Click **Add** button.

b In the Add routes dialog Route field, type a number between 001 and 999 to define the VoIP route.

c Click **Save**.

3 Assign the line pools to routes.

PSTN line pool (to other system):

a On the navigation tree, click the route you created for the PSTN line.

b In the **Use Pool** box, type the letter of the line pool for the fallback lines.

c In the External # field enter the dial numbers that access the other system through the PSTN. For example: 1<area code> <local code>.

PSTN line pool: (to local PSTN lines)

a On the navigation tree, click the route you created for the PSTN line.

b In the **Use Pool** box, type the letter of the line pool for the fallback lines.

c Leave the External # field blank.

VoIP line pool

a On the navigation tree, click the route you created for the VoIP lines.

b In the **Use Pool** field, type the letter of the line pool for the VoIP lines.

c Leave the **External #** field blank unless the destination digit you entered for the remote gateway is different than the number you want to use for the destination code.

Creating destination codes for fallback

Create a destination code that includes the VoIP and PSTN routes that you created in "Configuring routes" on page 82 to respond to the same access number (destination code). When this code is dialed, the Business Communications Manager will select the VoIP line, if possible. If the line is not available, the call will fall back to the PSTN line.

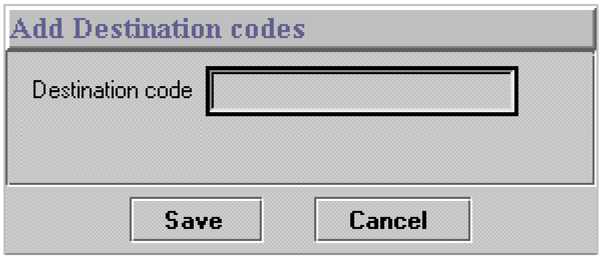
As well, you need to create, or ensure, that your destination code 9 includes a Normal and VoIP schedule that includes the route you created to the local PSTN.

➡ **Note:** If you already have a line pool access code defined as 9, you will need to delete this record before you create the destination code.

Follow these steps to create destination codes for your fallback route:

1 Open **Services**, **Telephony Services**, **Call Routing** and highlight **Destination Codes**.

2 Click **Add**.
The Add Destination codes dialog appears.



3 Type a one or more digits for this destination code.

Note: For example, if it is available, you might want to use the same number(s) that you used for the destination code of the gateway.

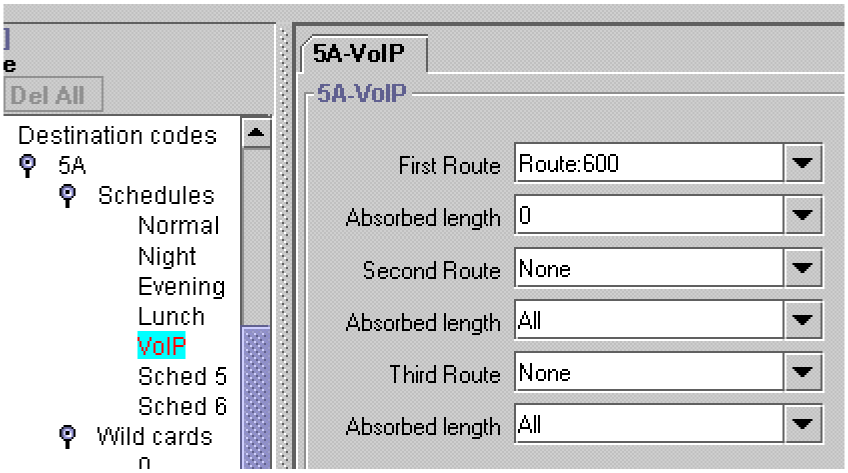
If you have multiple gateways, you could use a unique first number followed by the destination digits, to provide some consistency, such as 82, 83, 84, 85 to reach gateways with destinations digits of 2, 3, 4 and 5.

4 Click **Save** to close the dialog.

5 Click on the destination code heading for the destination code you just created.

6 Click on the key beside **Schedules**, and highlight **VoIP**.
The VoIP schedule appears, as shown in the next figure.

Figure 24 VoIP schedule



First Route: Route:600
Absorbed length: 0
Second Route: None
Absorbed length: All
Third Route: None
Absorbed length: All

a Change **Use Route** to the route you configured for your VoIP line.

b Set the **Absorbed length** to 0.

Note: In this case, the destination code and the gateway destination digit are the same.

Note that you can add up to three alternate routes.

Note: If the destination code is different from the remote gateway destination digits, and you entered an External # into the route record, set the absorbed length to the number of digits in the destination code. The system will dial out the External # you entered in front of the rest of the number that the user dialed.

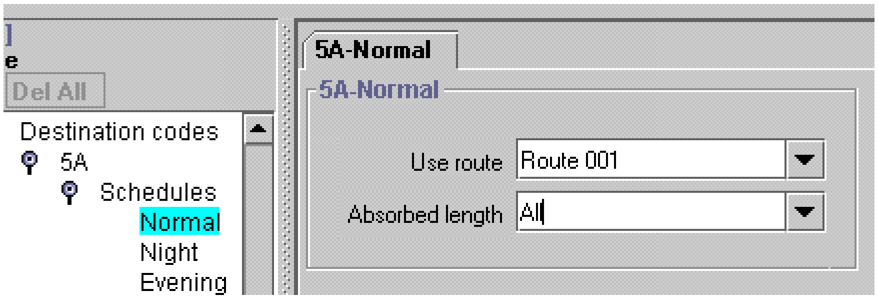
Or, you can use the destination digits as part of the destination code and set the absorbed length to 1, to absorb the destination code, but still dial the destination digits, so the system can find the gateway.

7 On the navigation tree, under the destination code schedule, click **Normal**.
The Normal schedule appears. It contains the same two fields as shown in the figure above.

a Change **Use Route** to the route you configured for your PSTN fallback line (the line to the other system).

b Set the **Absorbed length** to All.

Figure 25 Normal schedule routing information



Use route: Route 001

Absorbed length: All

In this case, the user dials the destination code plus the DN. The destination code is absorbed, but the system dials out the access number (1-XXX-XXX) before the DN digits.

Note: This same process will be necessary if you are part of a Universal Dialing Plan (UDP), where each system is assigned a private access code that is not part of the DN and you want your users to be able to just dial the DN of the telephone they are calling. In that case, you enter the private access code in the External # field, and that gets dialed out before the DN.

8 Repeat these steps for your destination code 9.

a Under the destination code, select the Normal schedule.

b Specify the route you created for the local PSTN.

c Set the absorb length to 0.

d Repeat these steps for the VoIP schedule.

Activating the VoIP schedule

Before activating the VoIP schedule, calls using the destination code are routed over the PSTN. This is because the system is set to use the Normal schedule, which routes the call over the PSTN. Once the VoIP schedule is activated, calls made with the VoIP destination code are routed over the VoIP trunk.

The VoIP line must be activated from the control set for the VoIP trunk, which is specified when the trunk is created (**Services, Telephony Services, Lines, VoIP lines, Enabled VoIP lines, Line XXX, General**). For information about control sets and configuring VoIP line records, refer to the *Business Communications Manager Programming Operations Guide*.

To activate the VoIP schedule:

1. Dial **FEATURE 873** from the control set for the VoIP trunk.
   The phone prompts you for a password.
2. Type the password.
3. Press OK.
   The first schedule appears.
4. Scroll down the list until VoIP is selected.
5. Press OK.
   The VoIP schedule stays active, even after a system reboot, and can only be deactivated manually.

To deactivate the VoIP schedule:

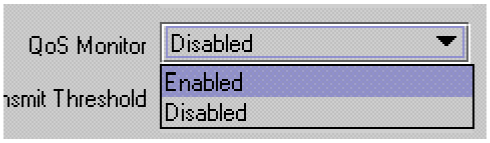
1. Dial **FEATURE #873**. The phone prompts you for a password.
2. Type the password.
3. Press OK. The system returns to the Normal schedule.

Turning on QoS monitor

For fallback to function, the QoS monitor must be enabled:

1. In Unified Manager, open **Services**, **IP Telephony**, **H.323 Trunks**, and click on **Remote Gateways**. The Remote Gateway screen appears.
2. Select the Remote Gateway listing for which you want to enable QoS Monitoring.
3. On the top menu, click **Configuration**, then click **Modify Entry**.
   The Remote Gateway dialog appears.
4. For the **QoS Monitor** field, select **Enabled**.

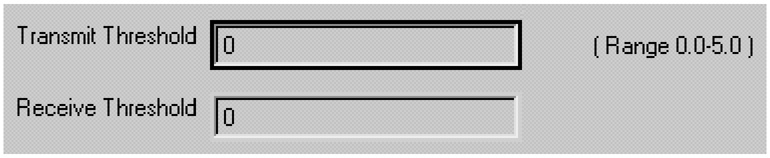
Figure 26 QoS Monitor field on the Remote Gateway screen



QoS Monitor: Disabled

5 Set the **Transmit Threshold** and **Receive Threshold** to a value between 0 and 5.

Figure 27 Threshold fields on the Remote Gateway screen



Transmit Threshold: 0 (Range 0.0-5.0)

Receive Threshold: 0

This marks the level of quality that the gateway must be able to support before transmitting a call. In most cases, the transmit threshold and receive threshold should be the same. On a line where communications in one direction are more important than in the other direction, you can set up asymmetrical thresholds.

Warning: QoS monitor must be turned on at both endpoints.

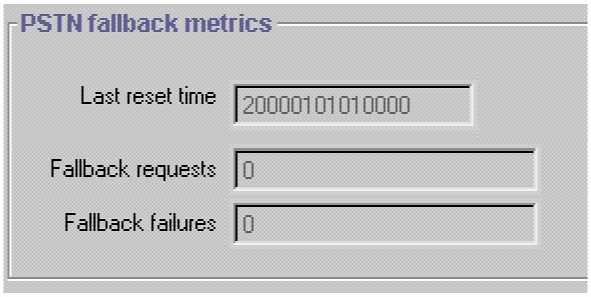
For information about using the QoS monitor, refer to "Quality of Service Monitor" on page 100.

PSTN fallback metrics

To view the metrics associated with VoIP calls that fallback to the PSTN network.

1 Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, and click the **PSTN fallback metrics** heading.
The Last reset time, Fallback requests and Fallback failures values appear.

Figure 28 Fallback Metrics fields



PSTN fallback metrics

Last reset time: 20000101010000

Fallback requests: 0

Fallback failures: 0

To reset the metric log, on the **Configuration** menu, click **Clear data and time**.

Incoming call configuration

To receive an incoming call directly to the telephone from a VoIP network, you need to ensure that the telephone is mapped to a target line

For information about setting up your Business Communications Manager to place outgoing VoIP calls, see "Outgoing call configuration" on page 76.

Assign a target line to the DN

A target line routes incoming calls to specific telephones (DNs) depending on the incoming digits. This process is independent of the trunk over which the call comes in.

Other options:

- You can assign the target line to a number of telephones, if you want the call to be answerable to a call group, for instance.
- If System-Wide Call Appearance (SWCA) keys are configured on memory buttons on the telephones, the incoming line acts the same way as any other incoming call, which depends on how SWCA has been set up to behave. Refer to the *Business Communications Manager 3.0 Programming Operations* Guide and the *Telephony Feature Handbook* for more information about setting up SWCA keys.
- You can assign the target line number to a Hunt Group DN if you want the call to appear on a group of telephones set up as a hunt group. Refer to the *Business Communications Manager 3.0 Programming Operations Guide* for more information about setting up Hunt groups.

Mapping target lines involves two steps:

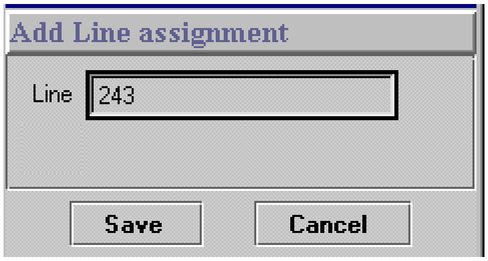
- The target line is mapped to a telephone (or Hunt group) by assigning a free target line (241 to 492) to the telephone (or Hunt group) DN record.
- The incoming digits (e.g. 3321) are mapped to a target line (the same one you assigned to the telephone) by setting the Received Number under that target line to the incoming digits.

If your system does not have target lines already assigned, use this procedure to assign target lines to individual telephones.

Note: You can also use the Add Users wizard if you need to create target lines for a range of telephones. Refer to the *Business Communications Manager 3.0 Programming Operations Guide* for detailed information about using the wizard.

1. In Unified Manager, open **Services**, **Telephony Services**, **System DNs**.
2. Under the Active Set DNs (or under the Inactive DNs, if you are preconfiguring DN records) choose the DN record of the telephone where you want the line to be directed.
3. Choose **Line Access**, **Line assignment** and click the **Add** button.

4 Enter the number of an available target line (241-492).



Line: 243

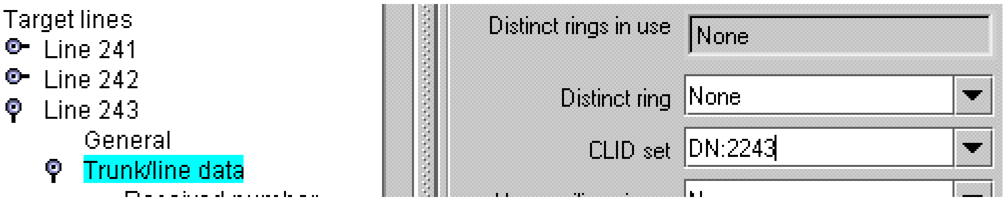
5 Click the **Save** button.

6 Click on the line number you just created and ensure that you have the line set to **Ring Only** if the telephone has no line buttons set for the line, or **Appearance and Ring**, if you are adding this to a DN that has line keys or which will be using SWCA keys.

7 Go to **Services**, **Telephony Services**, **Lines**, **Target Line** <*Target line number from step 4*>.

8 Click on the **Trunk/line data heading**.

9 In the **CLID set** field, enter the DN.



Distinct rings in use: None

Distinct ring: None

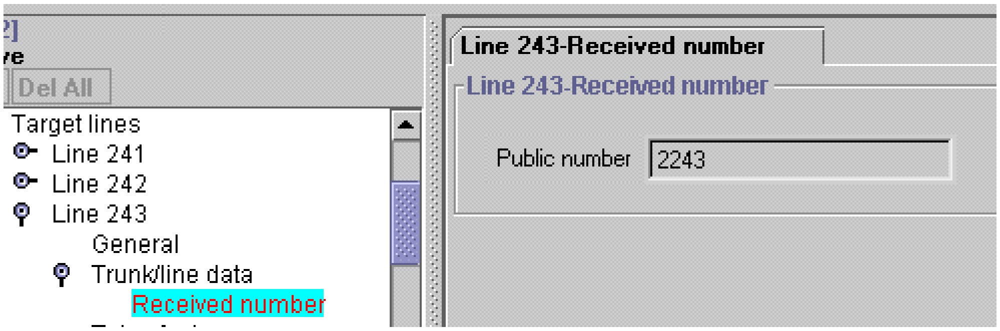
CLID set: DN:2243

This allows the caller ID to display at the set before the call is answered.

10 Click the key beside **Trunk/line data**.

11 Click on **Received number**.

12 In the **Public number** field, enter the DN.



Public number: 2243

The telephone assigned to that DN can now receive all calls with that DN number that come into the Business Communications Manager to which the telephone is connected.

For a detailed explanation about target lines, see the *Business Communications Manager 3.0 Programming Operations Guide*.

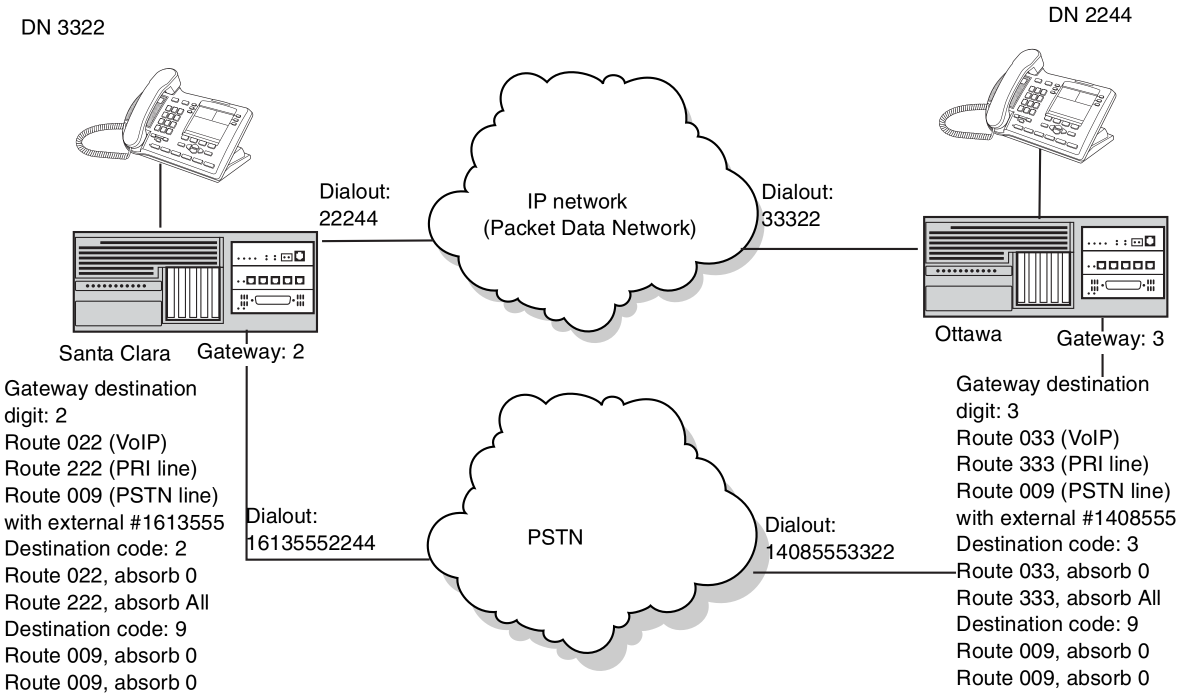
Example configuration, set to set

This section walks through a sample Business Communications Manager configuration, including:

- "On Business Communications Manager Ottawa" on page 92
- "On Business Communications Manager Santa Clara" on page 94
- "Making calls" on page 95
- "Connecting an i200X telephone" on page 96

In this scenario, shown in the following figure, two Business Communications Managers in different cities are connected to a WAN. One Business Communications Manager resides in Ottawa, the other resides in Santa Clara.

Figure 29 Example PSTN fallback



The systems already communicate through a PRI line, which will be configured to be used for fallback. Both systems already have all keycodes installed for eight VoIP lines, and resources properly allocated for VoIP trunking. For information about keycodes, see the *Business Communications Manager Keycode Installation Guide*. For information about Resource Allocation, see *Configuring the MSC Resources* in the *Business Communications Manager Programming Operations Guide.*

Each Business Communications Manager has 10 telephones that will be using VoIP lines. In this setup only eight calls can be sent or received at one time. If all 10 telephones attempt to call at the same time, two of the calls will be rerouted to the PSTN.

Business Communications Manager Ottawa	Business Communications Manager Santa Clara
• Private IP address: 10.10.4.1	• Private IP address: 10.10.5.1
• Public IP address: 47.62.54.1	• Public IP address: 47.62.84.1
• DNs 2000-2999	• DNs 3000-3999
• From this system, dial 9 to get onto PSTN	• From this system, dial 9 to get onto PSTN

On Business Communications Manager Ottawa

This procedure details actions that the installer performs to set up the Business Communications Manager Ottawa.

1. The installer sets up 2221 as the Control set for each VoIP line, so that the VoIP schedule can be manually activated. This setup is necessary for PSTN fallback.
2. The installer sets the published IP address.

   In this case, the public IP network is connected to the LAN 2 connection, therefore, the installer sets the published IP address to LAN 2. This is the address that devices on the Packet Data Network (PDN) will use to locate the system.
3. The installer configures the media for the system, using the following settings:
   - The first preferred codec is set to G.729. The installer chooses this setting due to the unique requirements of this installation.
   - Silence Compression is turned on.
   - Jitter Buffer is set to medium.
4. The installer puts eight VoIP lines into line pool O.

   Any line pool can be used as long as all of the lines in the pool are VoIP trunks. The installer does not set an access code for the line pool, because the access code does not work with fallback. Instead, the line pool will be accessed using destination digits after the installer sets up PSTN fallback.
5. For each telephone on the system, the installer gives the DN record access to line pool O.
6. The installer sets up a remote gateway for the Santa Clara Business Communications Manager, using the following settings:
   - Destination IP: **47.62.84.1** This is the published IP address of the Santa Clara Business Communications Manager.
   - QoS Monitor: **Enabled**
     This must be enabled for PSTN fallback to function.

- Transmit Threshold: **3.0**
  This is a Mean Opinion Score (MOS) value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
- Receive Threshold: **3.0**
  This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
- Destination Digits: **3**
  This number will also be used as part of the Destination code.

Note: In this case, because the systems are on a Coordinated Dialing Plan (CDP) network, and the 3 is included in the DN, this number will be absorbed before dialout.

7 The installer sets up the VoIP schedule with these settings:

- Service: **Manual**
- Overflow: **Y**

8 The installer ensures a route has been created to the line pool that accesses the local PSTN line, including the external # dialout.

9 The installer defines a new route called Route 003, and sets it to use line pool PRI-A. This is the line pool that contains the PRI fallback lines.

10 The installer defines a new route called Route 100, and sets it to use line pool O. This is the line pool that contains the VoIP lines.

11 The installer creates a destination code of 3.

- Under the Normal schedule, the installer assigns Route 003, which uses line pool PRI-A. The absorb digits is set to All.
- Under the VoIP schedule the installer assigns Route 100, which uses the VoIP lines in line pool O. The absorb digits is set to 0.

12 The installer creates a destination code of 9, which will be used to access the local line pool for the local PSTN access lines.

- Under the Normal schedule, the installer assigns the route created for the local PSTN access with absorb digits set to All.
- Under the VoIP schedule the installer assigns the route created for the local PSTN access with absorb digits set to All.

13 From the control set (2221), the installer dials **FEATURE 873** and selects the VoIP schedule. VoIP is now activated. At this point, the system is configured to make outgoing calls, but it is not set up to receive incoming calls.

14 If there are no target lines set up, the installer creates target lines for each DN or Hunt Group.

The Ottawa Business Communications Manager is now set to handle calls sent to and from a remote VoIP gateway. However, the Santa Clara Business Communications Manager must be set up before any calls can be made from that system.

On Business Communications Manager Santa Clara

This procedure details actions that the installer performs to set up the Business Communications Manager Santa Clara.

1. The installer sets up 3321 as the Control set for each VoIP line, so that the VoIP route can be manually activated.
2. The installer sets the published IP address.

   In this case the public data network (PDN) is connected to the LAN 2 connection, therefore, the installer sets the published IP address to LAN 2. This is the address that devices on the PDN will use to locate the system.
3. The installer configures the media for the system, using the following settings:
   - The first preferred codec is set to G.729.
   - Silence Compression is turned on.
   - Jitter Buffer is set to medium.
4. The installer puts the first eight VoIP lines into line pool O.

   Any line pool can be used as long as all of the lines in the pool are VoIP. The installer does not set an access code for the line pool, because the access code would not work with fallback. Instead, the line pool will be accessed using destination digits after the installer sets up PSTN fallback.
5. For each set on the system (DNs 3321 to 3331), the installer gives the set access to line pool O.
6. The installer sets up a remote gateway for the Santa Clara Business Communications Manager, using the following settings:
   - Destination IP: **47.62.54.1**
     This is the published IP address of the Ottawa Business Communications Manager.
   - QoS Monitor: **Enabled**
     This must be enabled for PSTN fallback to function.
   - Transmit Threshold: **3.0**
     This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
   - Receive Threshold: **3.0**
     This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
   - Destination Digits: **2**

   ➡ **Note:** In this case, because the systems are on a CDP network, and the 2 is included in the DN, this number will be absorbed before dialout.
7. The installer sets up the VoIP schedule with these settings:
   - Service: **Manual**
   - Overflow: **Y**

8 The installer sets up the routes, if they do not already exist.

- The installer ensures a route has been created to the line pool that accesses the local PSTN line, including the external # dialout.
- The installer defines a new route called Route 003, and sets it to use PRI-A. This is the line pool that contains the PRI fallback lines.
- The installer defines a new route called Route 100, and sets it to use line pool O. This is the line pool that contains the VoIP lines.

9 The installer creates a destination code of 2.

- Under the Normal schedule, the installer assigns Route 003, which uses line pool PRI-A. The absorb digits is set to All.
- Under the VoIP schedule the installer assigns Route 100, which uses the VoIP lines in line pool O. The absorb digits is set to 0.

10 The installer creates a destination code of 9, which is the line pool access code for the local PSTN access lines.

- Under the Normal schedule, the installer assigns the route created for the local PSTN access with absorb digits set to All.
- Under the VoIP schedule the installer assigns the route created for the local PSTN access with absorb digits set to All.

11 The installer dials FEATURE 873 and selects the VoIP schedule. VoIP is now activated. At this point, the system is configured to make outgoing calls, but it is not set up to receive incoming calls.

12 If there are no target lines set up, the installer creates target lines for each telephone record or Hunt group.

Making calls

From a set on Business Communications Manager Ottawa, a caller dialing a set on Business Communications Manager Santa Clara must dial the destination code, which includes the destination digits for the Business Communications Manager Santa Clara remote gateway, and the DN of the set. For example, dialing 33322 would connect as follows:

- 3 is the destination code. If a suitable level of QoS is available, the call is routed through the VoIP trunks and through the remote gateway with destination digits of 3. The call is sent across the PDN using the IP address of the Santa Clara Business Communications Manager.
- 3322 is linked to the target line associated with DN 3322.
- The call arrives at the phone with the DN 3322.

If a user in Santa Clara wanted to make a local call in Ottawa, they would dial 29, followed by the local Ottawa number. The digit 2 accesses the remote gateway for the VoIP line. The digit 9 accesses an Ottawa outside line.

Connecting an i200X telephone

This section takes the example above and uses it to demonstrate how an installer would configure an i2002 or i2004 telephone on the system. For information on configuring i200X telephones, see Chapter 3, “Installing IP telephones,” on page 39.

Note: IP clients require an IP network to reach the Business Communications Manager. However, they do not need to use VoIP trunks to communicate beyond the Business Communications Manager. They can use any type of trunk, just as any other phone on the Business Communications Manager can.

Connecting an i200X telephone on the LAN

In this case, the Santa Clara administrator wants to connect an i2004 phone using the LAN 1 network interface.

1. The installer sets up the Business Communications Manager to handle the IP telephone by turning Registration to ON, and Auto Assign DNs to ON.
2. The installer connects the telephone to the LAN, and sets it up using the following settings:
   - Set IP address: **10.10.5.10**
   - Default GW: **10.10.5.1**
     This is the IP address of the default gateway on the network, which is the nearest router to the telephone.
   - S1 IP address: **47.62.84.1**
     This is the published IP address of the Business Communications Manager.

   The Business Communications Manager automatically assigns the telephone the DN of 3348.
3. The installer configures DN record 3348 with the lines and attributes the IP telephone requires.
4. The installer sets up a target line for DN 3348, using the Received Digits 3348.

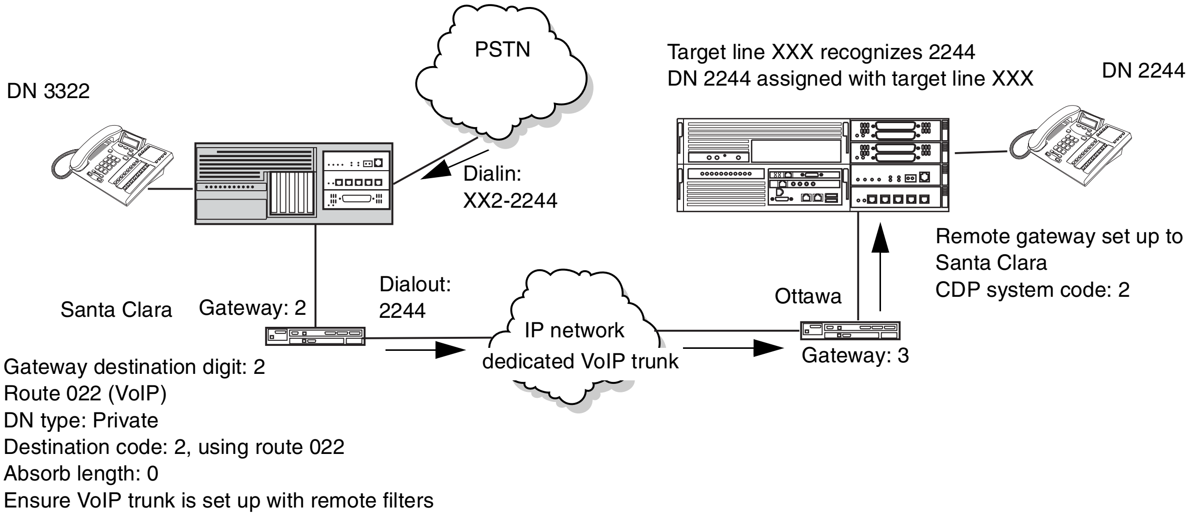
This phone would follow all of the same dialing rules as the other telephones on the Santa Clara Business Communications Manager. A caller could dial 3321 to connect with telephone 3321, dial 9 to access the PSTN, or dial 2<DN> to access a telephone on the Ottawa system.

Example, PSTN call to remote node

Programming for tandeming Business Communications Managers together using PRI SL-1 lines and MCDN protocol is described in detail in the *Programming Operations Guide*, *Private Networking* section. VoIP tandem trunks are configured in the same way, with the addition gateway programming required for IP trunks, which is covered in "Configuring a remote gateway" on page 78.

Making a call to a remote node requires that the receiving Business Communications Manager has the correct routing to pass the call on to the next node. When the call is received (system A), the system recognizes that the received number is not a system number. However, if it has a route and destination code that recognizes the received number, system A will then pass the call through. Further, the call is received as a public call on system A, the call then becomes a private call as it is passed through a dedicated trunk, in this case a VoIP trunk, to system B. On system B, the call is received over the VoIP trunk. System B recognizes the code as its own, and uses a local target line to route the call to the correct telephone.

Figure 30 Calling into a remote node from the PSTN



Remote access over VoIP trunks

You cannot program DISA or auto-answer for voice over IP (VoIP) trunks, therefore, your system cannot be accessed from an external location over a VoIP trunk. The exception to this is if the call comes into a tandemed system (system A) from a PSTN, and the call is then sent out across a VoIP trunk to system B. In this case, system A is controlling remote access before transferring the call to system B through private routing.Therefore, all call features except Page are available to the caller, depending on what the remote access package for the COS password allows.

Configuring Net Meeting clients

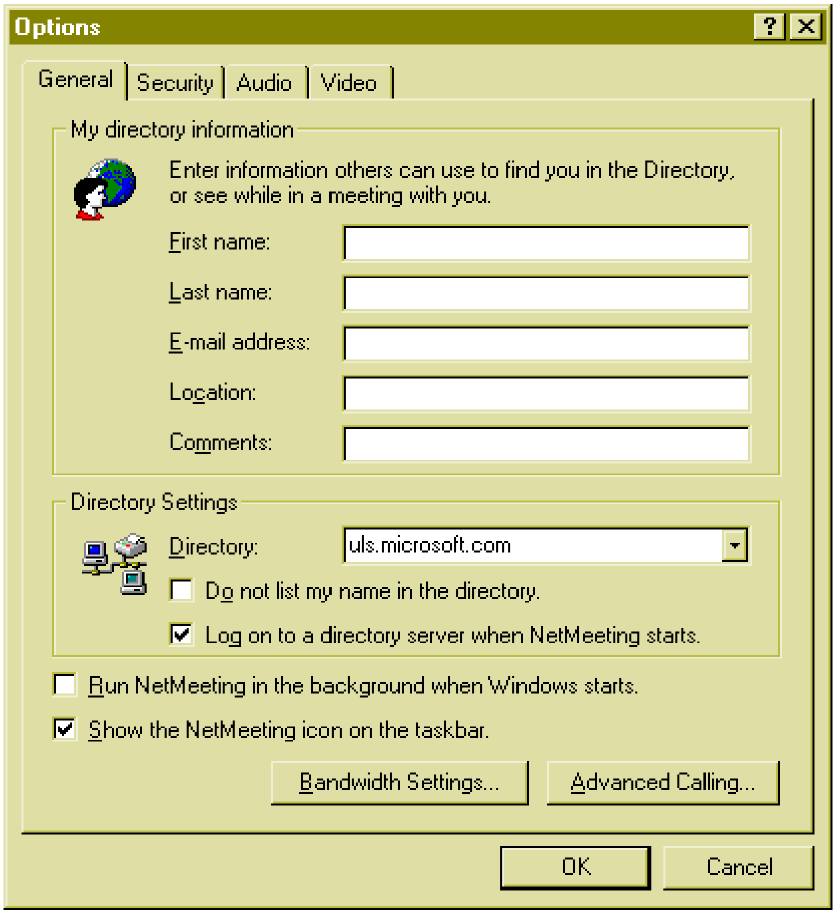
Net Meeting is an application available from Microsoft which uses the H.323 protocol.

To use Net Meeting:

1 Install Net Meeting on the client computer.

2 In the **Tools** menu, click **Options**.
The options dialog appears.

Figure 31 NetMeeting options



My directory information

Enter information others can use to find you in the Directory, or see while in a meeting with you.

First name:

Last name:

E-mail address:

Location:

Comments:

Directory Settings

Directory: uls.microsoft.com

□ Do not list my name in the directory.

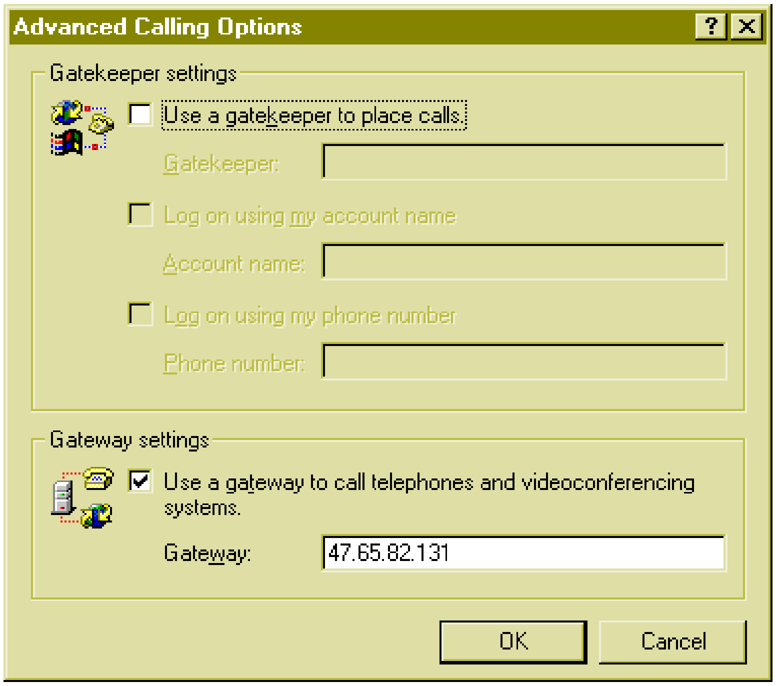
☑ Log on to a directory server when NetMeeting starts.

□ Run NetMeeting in the background when Windows starts.

☑ Show the NetMeeting icon on the taskbar.

3 Click **Advanced Calling**.
The advanced Calling Options dialog appears.

Figure 32 NetMeeting advanced options



Advanced Calling Options

Gatekeeper settings

□ Use a gatekeeper to place calls.

Gatekeeper:

□ Log on using my account name

Account name:

□ Log on using my phone number

Phone number:

Gateway settings

☑ Use a gateway to call telephones and videoconferencing systems.

Gateway: 47.65.82.131

4 Under **Gateway settings**, select the **Use a gateway...** option. In the **Gateway** field, type the published IP address of the Business Communications Manager.

5 Click **OK**.

6 Add a remote gateway to your system as explained in "Configuring a remote gateway" on page 78. When prompted for the IP address of the remote gateway, type the IP address of the client computer.

Repeat this procedure for every NetMeeting client you want to set up.

Quality of Service Monitor

The Quality of Service Monitor is an application that monitors the quality of the IP channels. It does this by performing a check every 15 seconds. The QoS Monitor determines the quality of the intranet based on threshold tables for each codec. If the QoS Monitor is enabled, and it determines that the quality of service falls below the set threshold, it will trigger fallback to PSTN. For information about setting up the system to use QoS and fallback to PSTN, see “Configuring PSTN fallback” on page 80.

Bandwidth required for QoS monitor: There are a total of 25 monitoring packets traveling in each direction every 15 seconds. Each of monitoring packages has 88 bytes in IP layer. These monitoring packets are equally spaced out in the 15-second interval. For example, if there are two Business Communications Managers, BCM-A and BCM-B, connected to each other with QoS Monitoring enabled. In every 15 seconds there are 25 monitoring packages going from BCM-A to BCM-B and then back to BCM-A. Similarly, the same occurs from BCM-B to BCM-A back to BCM-B. In other words, in this case the overhead in IP layer caused by these monitoring packets is about (2x25x88)/15= 293 bytes/second = 2346 bits/second in one direction.

Quality of Service Status

The QoS Status displays the current network quality described as a Mean Opinion Score (MOS) for each IP destination. A pull-down menu allows the administrator to view the MOS mapping. The table below shows a sample QoS Monitor.

Table 18 QoS status

IP	QoS Monitor	G.729		G.711		G.723.1 6.3 kbit/s		G.723.1 5.3 kbit/s	
		Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
47.192.5.2	Enabled	4.50	4.50	4.00	4.30	4.75	4.70	4.80	4.90
47.192.5.6	Disabled	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note: For the QoS monitor and PSTN fallback to function, both Business Communications Managers must list each other as a Remote Gateway and QoS Monitor must be enabled on both systems.

Updating the QoS monitor data

To update the table with the most current values:

From the **View** menu, select **Refresh**.

Viewing QoS monitoring logging

QoS monitor can be configured to log data. The process for setting up logging is described in detail in the Programming Operations Guide. The following steps explain how to view the log.

1. On the Unified Manager navigation tree, click the keys beside **Services** and **Qos Monitor**.
2. Click the **Mean Opinion Score** heading.
3. Click the **Logging** tab.
   The Logging screen appears.
4. On the **Tools** menu, click **Display Log**.
   The Mean Opinion Score Log File screen appears.
5. Close the browser window when you are finished viewing the log file.

Port settings

In some installations, you may need to adjust the port settings before the Business Communications Manager can work with other devices.

This section includes information about:

- "Using firewalls" on page 101
- "Port settings for legacy networks" on page 103

Using firewalls

Firewalls can interfere with communications between the Business Communications Manager and another device. The port settings must be properly configured for VoIP communications to function properly. Using the instructions provided with your firewall, ensure that communications using the ports specified for VoIP are allowed.

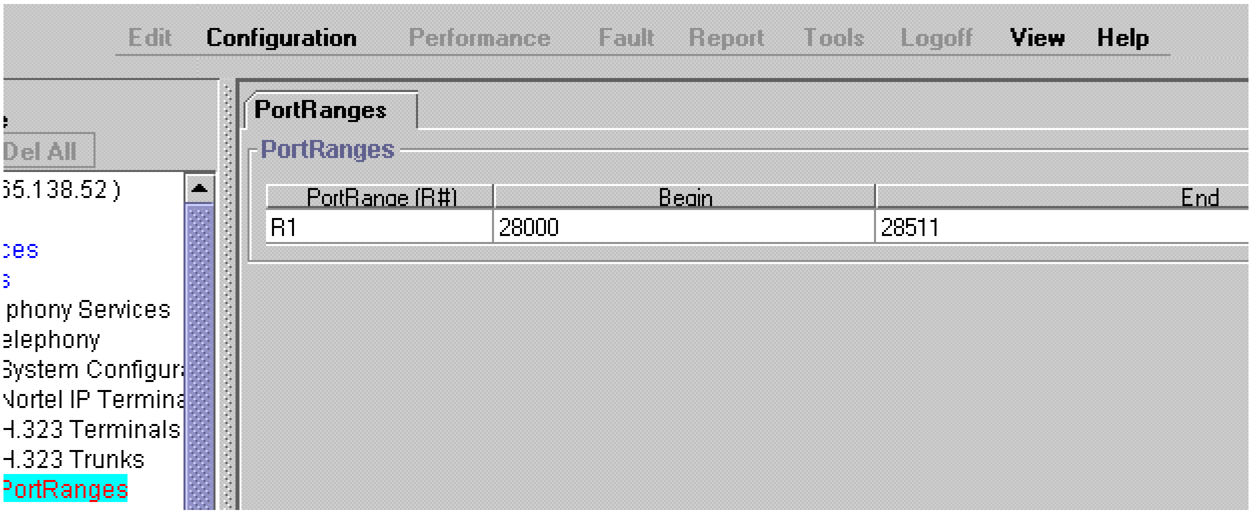
A Nortel Networks i2002 or i2004 telephone uses ports between 51000 and 51200 to communicate with the Business Communications Manager.

The Business Communications Manager, by default, uses ports 28000 to 28255 to transmit VoIP packets.

Follow these steps to modify these settings:

1 In Unified Manager, open **Services**, **IP Telephony**, **Port Ranges**.
The Port Ranges screen appears.

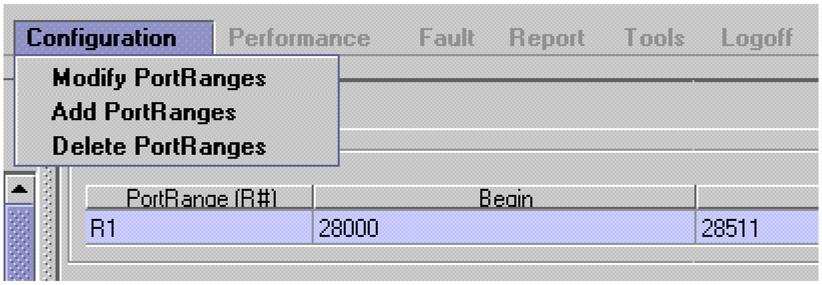
Figure 33 Port Ranges



PortRange (R#)	Begin	End
R1	28000	28511

2 Select the **Port Range** you want to modify.

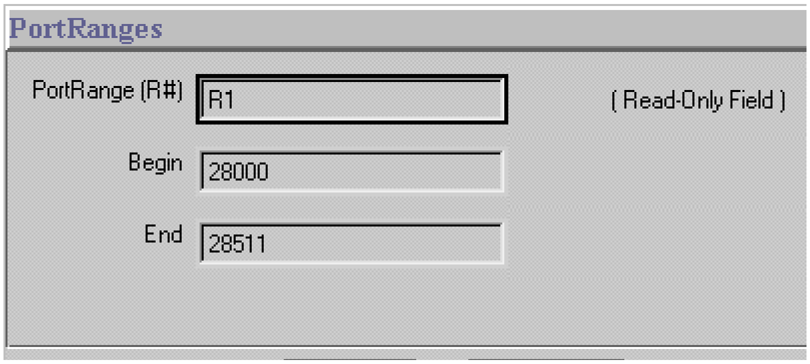
3 From the top menu, click **Configuration**, and then select **Modify PortRanges**.



PortRange (R#)	Begin	
R1	28000	28511

The Modify PortRanges dialog box appears. Refer to Figure 34.

Figure 34 Port ranges dialog box



PortRange (R#) R1 (Read-Only Field)

Begin 28000

End 28511

4 Change the port settings.

5 Click the **Save** button.

Port settings for legacy networks

Business Communications Manager 3.0 uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. You must reserve these same port ranges and set them to high priority on all routers that an administrator expects to have QoS support. You do not need to reserve port ranges on DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP Realtime Transfer Protocol (RTP) flow uses two ports for each direction. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

- Backbone routers reserve more ports than edge routers.
- The port ranges on edge routers are a subset of the backbone router port ranges.
- Include port number UDP 5000 in the reserved port ranges, for the QoS monitor.
- The port ranges reserved in a Business Communications Manager 3.0 system are also reserved by the remote router.
- You must reserve two ports for each voice call you expect to carry over the WAN link.
- You can reserve multiple discontinuous ranges. Business Communications Manager 3.0 requires that each range meet the following conditions:
  - Each range must start with an even number.
  - Each range must end with an odd number.
  - You cannot have a total of more than 256 ports reserved.

Using a gatekeeper

This section describes the use of a gatekeeper for your VoIP trunks.

- “Modifying the Local Gateway Settings” on page 104
- “Using Radvision ECS 2.1.0.1 as the gatekeeper” on page 108
- “Using CSE 1000 as a gatekeeper” on page 109
- “Gatekeeper call scenarios” on page 113

The Business Communications Manager supports the use of an ITU-H323 gatekeeper. A gatekeeper is a third-party software application residing somewhere on the network, which provides services such as:

- address translation
- call control
- admission control (ARQ)

- bandwidth control
- zone management

A single Gatekeeper manages a set of H.323 endpoints. This unit is called a Gatekeeper Zone. A zone is a logical relation that can unite components from different networks (LANS). These Gateway zones, such as the Business Communications Manager, are configured with one or more alias names that are registered with the gatekeeper. The gatekeeper stores the alias-IP mapping internally and uses them to provide aliases to IP address translation services. Later, if an endpoint IP address changes, that endpoint must re-register with the gatekeeper.

Refer to the gatekeeper software documentation for information about changing IP addresses.

Note: The Business Communications Manager has been tested by Nortel Networks to be compliant with RADVISION ECS 2.1.0.1 (http://www.radvision.com/) and CSE 1000 gateway applications.

Note: A gatekeeper may help to simplify IP configuration or the Business Communications Manager dialing plan, however it will not simplify the network dialing plan.

Modifying the Local Gateway Settings

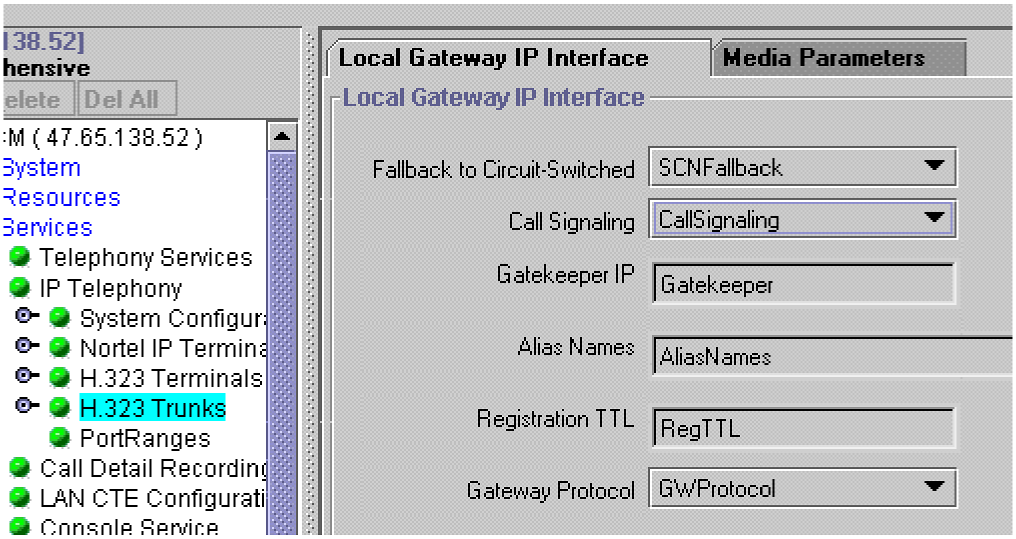
The call signaling method used by the local gateway defines how the Business Communications Manager prefers call signaling information to be directed. Call signaling establishes and disconnects a call.

If the network has a gatekeeper, The Business Communications Manager can request a method for call signaling, but whether this request is granted depends on the configuration of the gatekeeper. Ultimately, the gatekeeper decides which call signaling method to use.

To modify the settings for your local gateway:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **H.323 trunks**.
The Local Gateway IP Interface screen appears.

Figure 35 Local gateway IP interface



Local Gateway IP Interface

Fallback to Circuit-Switched: SCNFallback

Call Signaling: CallSignaling

Gatekeeper IP: Gatekeeper

Alias Names: AliasNames

Registration TTL: RegTTL

Gateway Protocol: GWProtocol

2 Use the information in the table below to set up the Local Gateway IP interface record..

Table 19 Local Gateway IP interface fields

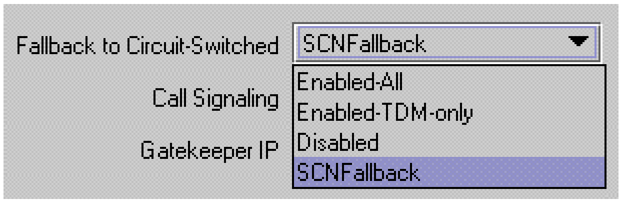
Field	Value	Description
Configuration note:	Refer to "Using Radvision ECS 2.1.0.1 as the gatekeeper" on page 108 and "Using CSE 1000 as a gatekeeper" on page 109 for specific information about configuring the gatekeeper for each application	
Fallback to Circuit-Switched	Enabled-All Enabled-TDM-only Disabled SCNFallback	Your choice determines how the system will handle calls if the IP network cannot be used. • **Enabled-All**: All calls will be rerouted over specified TDM trunks lines. • **Enabled-TDM-only**: All voice calls will be rerouted over specified TDM trunks lines. • **Disabled**: Calls will not be rerouted.  Fallback to Circuit-Switched: SCNFallback Call Signaling Gatekeeper IP Enabled-All Enabled-TDM-only Disabled SCNFallback

Table 19 Local Gateway IP interface fields (Continued)

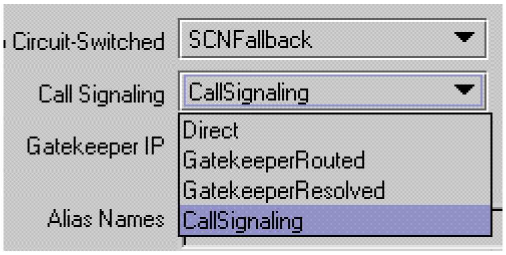
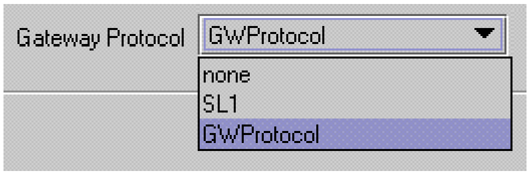
Field	Value	Description
*Call Signaling	Direct GateKeeperRouted GateKeeperResolved CallSignaling	• **Direct**: call signaling information is passed directly between endpoints. The remote gateway table in the Unified Manager defines a destination code (digits) for each remote system to direct the calls for that system to route. In each system, the Nortel IP Terminals and H.323 Terminals records map IP addresses to specific telephones. • **Gatekeeper Resolved**: all call signaling occurs directly between H.323 endpoints. This means that the gatekeeper resolves the phone numbers into IP addresses, but the gatekeeper is not involved in call signaling. • **Gatekeeper Routed**: uses a gatekeeper for call setup and control. In this method, call signaling is directed through the gatekeeper. • Call Signaling:  Circuit-Switched: SCNFallback Call Signaling: CallSignaling
*Gatekeeper IP	*<ip address>*	If **GateKeeperRouted** or **GateKeeperResolved** are selected under **Call Signaling**, type the IP address of the machine that is running the gatekeeper.
*Alias Names	<alphanumeric> Refer to example below.	If **GateKeeperRouted** or **GateKeeperResolved** are selected under **Call Signaling**, type one or more alias names for the gateway. One or more alias names may be configured for a Business Communications Manager. Alias names are comma delimited, and may be one of the following types: • **E.164** — numeric identifier containing a digit in the range 0-9. Identified by the keyword `TEL:` • **NPI-TON** — also referred to as a PartyNumber alias. Similar to E164 except that the keyword indicates the NPI (numbering plan identification), as well as the TON (type of number). Identified by one of the following keywords: `PUB` (Public Unknown Number); `PRI` (Private Unknown Number); `UDP` (Private Level 1 Regional Number (UDP)); `CDP` (Private Local Number (CDP)). Refer to "Notes about NPI-TON aliases" on page 107. • **H323Identifier** — alphanumeric strings representing names, e-mail addresses, etc. Identified by the keyword `NAME:`

Table 19 Local Gateway IP interface fields (Continued)

Field	Value	Description
	Example: In the following example, the Business Communications Manager is assigned an E.164 and an H323 Identifier: `Alias Names: TEL:76, NAME:bcm10.nortel.com` In the following example, the Business Communications Manager is assigned a public dialed number prefix of 76, a private DCP number of 45, and an H323 Identifier alias: `Alias Names: PUB:76, CDP:45, NAME:bcm10.nortel.com` **Note:** E164 or NPI-TON alias types are commonly used since they fit into dialing plans. A Business Communications Manager alias list should not mix these types. Also, the type of alias used should be consistent with the dialing plan configuration. Use the same alias on all Business Communications Managers within a networked system.	
**Registration TTL	Default: 60 seconds	This TimeToLive parameter specifies the intervals when the VoIP gateway sends KeepAlive signals to the gatekeeper. The gatekeeper can override this timer and send its own TimeToLive period.
**Gateway Protocol	None SL1 GWProtocol	If you are using an MCDN protocol on the IP trunk, select **SL1**. (Note: You require a keycode for this protocol.) Otherwise, use **None**.  Gateway Protocol GWProtocol
* These fields are mandatory when you use Radvision ECS 2.1.0.1. ** These fields are optional when you use Radvision ECS 2.1.0.1.		

Notes about NPI-TON aliases

NPI-TON aliases store dialed number prefixes as well as information about the type of number. A dialed number can be qualified according to its TON (type of Number), as well as its NPI (numbering plan identification). Nortel Networks recommends this format over the E.164 format, for encoding dialed numbers and aliases registered with a gatekeeper.

When using a gatekeeper, and attempting to place an outgoing VoIP trunk call, ensure that the route and dialing plan configuration matches the NPI-TON aliases registered, by the destination, with the gatekeeper. These requirements are summarized in the following table:

Table 20 Route and Dialing Plan configurations for NPI-TON

Route (DN type)	Dialing Plan used by calling gateway	Alias configured for calling gateway
Public	Public	PUB:<dialedDigitsPrefix>
Private	Private (Type = None)	PRI:<dialedDigitsPrefix>
	Private (Type = CDP)	CDP:<dialedDigitsPrefix>
	Private (Type = UDP)	UDP:<dialedDigitsPrefix>

Using Radvision ECS 2.1.0.1 as the gatekeeper

When you use Radvision ECS 2.1.0.1 as the gatekeeper with the Business Communications Manager, specifically with the FP1 Maintenance Release, use the configurations described in this section. For detailed information about Radvision, and how to open and use the application, refer to the documentation for the application.

1 Open the Radvision application.

2 On the viaIP Administrator screen, select the **Settings** tab, then click on the **Basics** button.

3 Beside the **Who can register** field, choose **Everyone**.

4 In the left frame, click the **Calls** button.

Ensure the following fields are set:

Table 21 Radvision Calls screen required settings

Field	Value	Description
Accept calls	check box	Box must be checked.
Routing Mode	Direct Setup(Q.931) (not supported) Call Control (H.245)	Set to **Direct**. (Nortel recommends that you always use Direct mode.)
Check that call is active every	check box	Leave box UNCHECKED. Enabling this feature will result in dropped calls.

5 In the left frame click the **Advanced** button.

Ensure the following fields are set:

Table 22 Radvision Advanced screen required settings

Field	Value	Description
Check that the endpoint is online every ___	check box	Leave box checked. This setting controls the intervals when Radvision checks if the Business Communications Manager is still on line.
Enable TTL	check box	Box must be checked. This is the only mechanism currently supported that allows the gatekeeper to determine if the end point (the Business Communications Manager) is active.
Force Direct for Service Calls	check box	Check this box if you selected the **Routing Mode: Direct** on the **Calls** screen.

Gatekeeper support for interoperability

6 Create a service configuration for ITG.

a Select the **Services** tab.

b Click on the Add button.

c In the Prefix field, enter the unique telephone number that identifies the Meridian ITG system in the Business Communications Manager dialing plan.

7 Define the ITG as a predefined endpoint.

a Select the **Endpoints** tab.

b Click the Add predefined button.
The Predefined Endpoint Properties dialog displays.

c Ensure the following fields are set:

Table 23 Radvision Predefined Endpoints Properties settings

Field	**Value**	**Description**
Endpoint Type	Gateway	
Force Online Status	check box selected	
Registration IP	<ip address>	This is the IP address of the Meridian ITG system.
Aliases	Add: Name Phone Number	Name: The name of the ITG that will be displayed. Phone Number: The number assigned to the ITG. Radvision uses this number to identify calls to be routed to this ITG.
Allowed Services	Allowed Disallowed	Ensure the ITG service is on the list, and is **Allowed**.

8 Close the application.

9 Run system tests to ensure the gatekeeper is routing calls correctly.

Using CSE 1000 as a gatekeeper

Both the Business Communications Manager and the CSE 1000 must be set to the parameters described in this section for the gatekeeper to work effectively.

The CSE 1000 GK Admin tool is obtained from *http://<Gatekeeper IP>/gk/*.

Before an endpoint registers with the CSE 1000 gatekeeper it must first be added to the gatekeeper configuration. Before a registered endpoint may make calls, it must have its numbering plan information assigned within the gatekeeper configuration. Before any of these configuration changes become part of the gatekeeper active configuration, they must be committed to the active database. Configuration and activation information is described in the following sections.

Business Communications Manager requirements

Set the Business Communications Manager Local Gateway IP interface to the following:

- **Set Call Signaling Method** to either GatekeeperResolved or GatekeeperRouted, depending on your system requirements.
- Set **Gatekeeper IP** to the IP address at which the CSE 1000 gatekeeper operates.
- Set **Alias Names** to a single H.323 identifier that is unique across all endpoints registered with the gatekeeper. For example: “NAME:BCM-OTTAWA”. This H.323 identifier must exactly match that in the CSE 1000 gatekeeper configuration. This entry is case-sensitive.

CSE 1000 configuration, adding an H.323 endpoint

In the Gatekeeper Admin tool, perform the following:

1. Select GK standby DB admin.
2. Select H.323 Endpoints.
3. Select Add H.323 Endpoint
4. Ensure the following fields are set:

Table 24 CSE 1000 H.323 endpoints

Field	**Value**	**Description**
H323AliasName	<unique name>	This is the unique name that identifies your Business Communications Manager as an H.323 endpoint.
CDP Domain Name	<choose name from list>	If your system is using a CDP dialing plan, choose the CDP domain name for the Business Communications Manager.
Tandem Endpoint	<choose name from list>	This is the name of another H.323 endpoint. Picking a name in this field provides a tandem endpoint.

5. Click Create H323.

Setting the H.323 Endpoint Dialing Plan

All dialing plan information must be identical on all H.323 endpoints using the gatekeeper.

Follow these steps to set the dialing plan into the Gatekeeper Admin tool:

1. Select GK Standby DB Admin.
2. Select NumberPlanEntries.
3. Select Create.
4. Ensure that the Endpoint you select is the one for which you want to create a numbering plan entry.
5. Click Select.

6. Ensure that the following fields are set:

Table 25 CSE 1000 H.323 dialing plans

Field	Value	Description
Number	<digits>	This is the unique number that identifies the Business Communications Manager.
Type	<choose from list>	This is the TON (Type of Number) or NPI (Numbering Plan Identifier) for the endpoint.
EntryCost	<digits (1-255)>	This value determines which destination the gatekeeper will deliver to if the leading digits are the same for more than one endpoint. The gatekeeper will select the endpoint with the lowest EntryCost value.

7. Click Create.

Committing Gatekeeper Configuration Changes

Gatekeeper changes occur in the standby database. For these settings to be used by the active gatekeeper, you must commit them to the active database from the Gatekeeper Admin tool, as describe below:

1. Select GK Standby DB Admin.
2. Select Database Actions.
3. Select Single Step Commit and Crossover.

Configuring Codec Compatibility

The default codec settings for a CSE1000 are not compatible with those used by a Business Communications Manager system. In order to successfully make IP trunk calls between a Business Communications Manager and the CSE 1000, the codec configuration on both the Business Communications Manager and the CSE 1000 must coincide, as shown in the table below. As well any configured codecs on the CSE 1000 must have their payload size set to 30 ms.

Caution: The CSE 1000 can only register five codecs at once. This can include: G-711 mu-law, G.711 a-law, T.38.G.711CC, and either G.729A, G729AB, or G.723.1. It is important to that you disable the unused codecs. This ensures that the required codecs get registered with the DSP. Failure to disable unused codecs could result in the wrong codecs being registered with the DSP, which would create call failures.

Table 26 CSE1000 codec compatibility with endpoints

Business Communications Manager preferred codec **Refer to "Configuring media parameters" on page 74.**	**CSE 1000 codec configuration**
G.729 silence suppression is enabled G.729 silence suppression is disabled.	G.729 AB is enabled G.729A, and G.723 are disabled G.729A is enabled G.729AB, and G.723 are disabled
G.723 silence suppression is enabled	Not supported on CSE 1000.
G.723 silence suppression is disabled G.711 ulaw, or G.711 alaw silence suppression has no effect	G.723 is enabled G.729A and G.729AB are disabled G.711 is always part of the CSE 1000 configuration, and cannot be removed.

Setting Codecs on the CSE 1000

Use the Element Manager tool to set the codec information for the CSE 1000. This tool can be accessed at *http://<SignalingServerIP>/*.

1 In the tool, select Configuration.

2 Select IP Telephony.

3 In the Node Summary Window, select the node to be configured, and click on Edit.

4 Click on DSP Profile.

5 On the list of codecs, enable or disable each by clicking on the check box beside the codec name.

6 To view or change the codec configuration, click on the codec name.

7 Ensure the following fields are set:

Table 27 CSE 1000 codec configuration

Field	**Value**	**Description**
Codec Name	<codec name>	Name of the codec you selected.
Voice Payload Size	<msec per frame>	Choose the payload size for the codec. Use 30 ms for interoperability with the Business Communications Manager.
Voice Playout (Jitter Buffer) Nominal Delay	<digits>	Choose the minimum jitter buffer value you want to allow.
Voice Playout (Jitter Buffer) Maximum Delay	<digits>	Choose the maximum jitter buffer value you want to allow.
VAD	<checkbox enabled/disabled>	Check or uncheck box to enable or disable silence suppression for the codec.

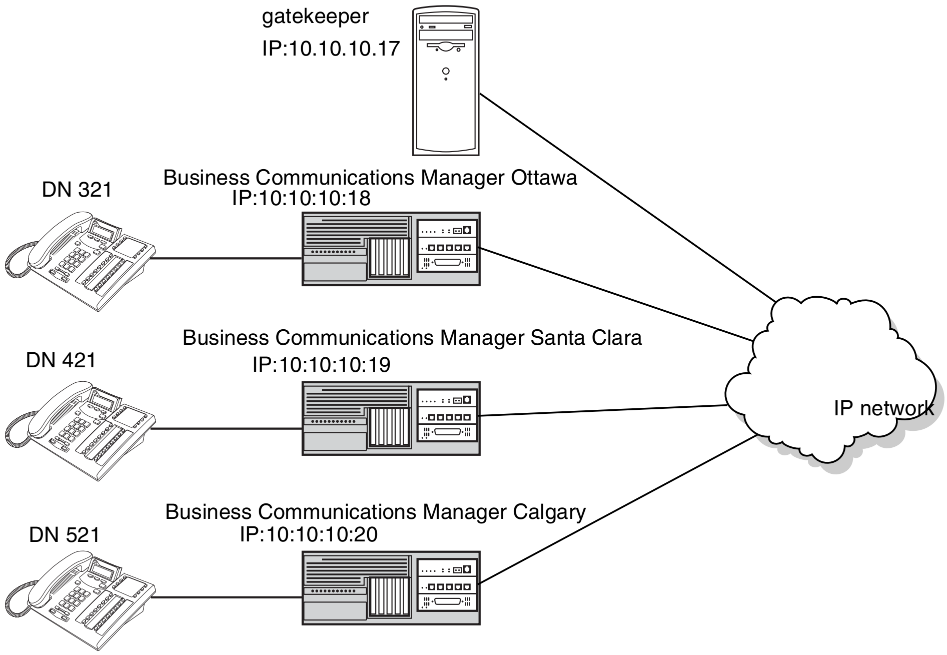
8 Click Submit.

9 Click Transfer for the node that you modified.

Gatekeeper call scenarios

This section explains what must be set up, and how a call would be processed for the two types of gatekeeper configurations. The following figure shows a network with three Business Communications Managers and a gatekeeper.

Figure 36 Business Communications Manager systems with a gatekeeper


gatekeeper
IP:10.10.10.17
DN 321
Business Communications Manager Ottawa
IP:10:10:10:18
DN 421
Business Communications Manager Santa Clara
IP:10:10:10:19
IP network
DN 521
Business Communications Manager Calgary
IP:10:10:10:20

This example explains how a call from DN 321 in Ottawa would be made to DN 421 in Santa Clara. It assumes that call signaling is set to Gatekeeper Resolved and no pre-granted ARQ has been issued:

1. Business Communications Manager Ottawa sends an AdmissionRequest (ARQ) to the gatekeeper for DN 421.
2. The gatekeeper resolves DN 421 to 10.10.10.19 and returns this IP in an AdmissionConfirm to the Business Communications Manager Ottawa.
3. Business Communications Manager Ottawa sends the call Setup message for DN 421 to the gateway at 10.10.10.19, and the call is established.

If call signaling is set to Gatekeeper Routed and no pre-granted ARQ has been issued:

1. Business Communications Manager Ottawa sends an AdmissionRequest to the gatekeeper for DN 421.
2. The gatekeeper resolves DN 421 to 10.10.10.17.
3. Business Communications Manager Ottawa sends the call Setup message for DN 421 to the gatekeeper (10.10.10.17), which forwards it to the gateway at 10.10.10.19.
4. The call is established.

Chapter 6
Typical network applications using MCDN

This section explains several common installation scenarios and provides examples about how to use VoIP trunks and IP telephony to enhance your network.

Information in this section includes:

Setting up MCDN over VoIP with fallback

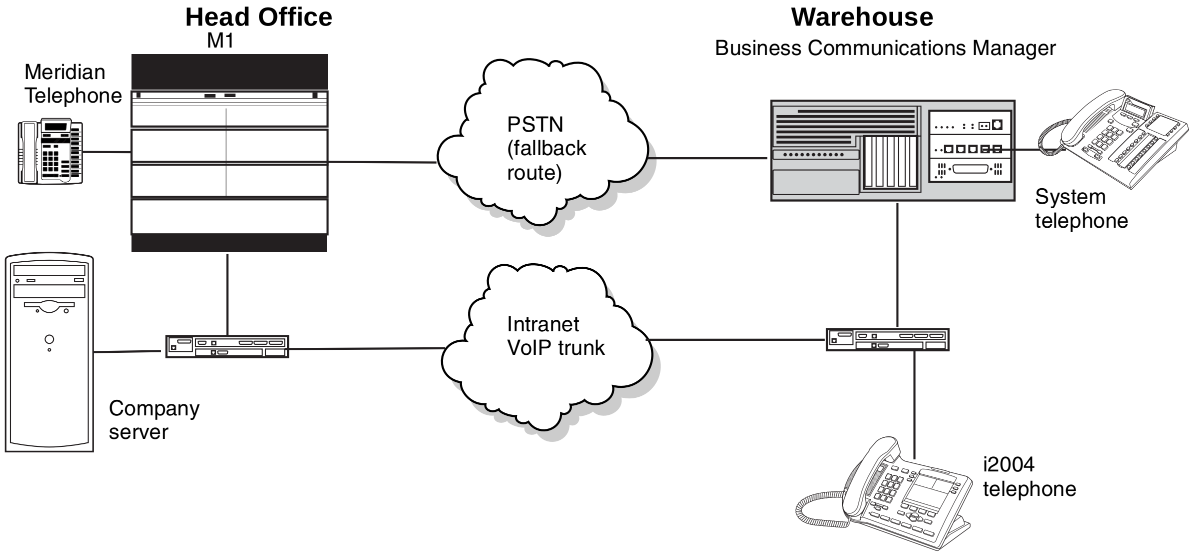
The MCDN networking protocol between a Meridian 1 and one or more Business Communications Managers works the same way as it does over PRI lines. You still require the MCDN and IP telephony software keys and compatible dialing plans on all networked systems.

The one difference between MCDN over PRI and MCDN over VoIP is that the VoIP trunks require specific Remote Gateway settings. Under **Services**, **IP Telephony**, **H.323 Trunks**, **Remote Gateway**, ensure that **Gateway Protocol** is set to **SL-1** for the VoIP connection to the Meridian system. The **Gateway Type** would be set to **ITG** (M1 Internet Telephony Gateway), as it would for any non-MCDN VoIP connection to a Meridian system. For details about setting up MCDN networks, refer to the *Private Networking* chapter in the *Business Communications Manager 3.0 Programming Operations Guide.*

➡ **Note:** If you use MCDN over VoIP, ensure that your fallback line is a PRI SL-1 line, to maintain MCDN features on the network.

One application of this type of network might be for a company, which has an M1 at Head Office, who want to set up a warehouse in another region. This would allow the warehouse to call Head Office across VoIP lines, bypassing long-distance tolls. This type of network also provides the possibility of having common voicemail off the M1. Refer to the following figure for an example.

Figure 37 M1 to Business Communications Manager network diagram



To set up this system:

1 Make sure the M1 ITG meets the following requirements:

- ITG 2.X.26
- Rls25.30 or higher
- S/W Packages 57, 58, 59, 145, 147, 148, 160

2 Ensure that the M1 ESN programming (CDP/UDP) is compatible. For information on this, refer to your M1 documentation.

3 On the Business Communications Manager 3.0 Unified Manager:

- Set up outgoing call configuration for the VoIP gateway.
- Set up a remote gateway for the Meridian 1.
- Ensure the dialing rules (CDP or UDP) are compatible with the M1. For information on CDP and UDP, refer to the *Programming Operations Guide*.
- Configure the PSTN fallback, and enable QoS on both systems.
- If target lines have not already been set up, configure the telephones to receive incoming calls through target lines.

MCDN functionality on fallback PRI lines

To be able to use MCDN functionality over PRI fallback lines, set up:

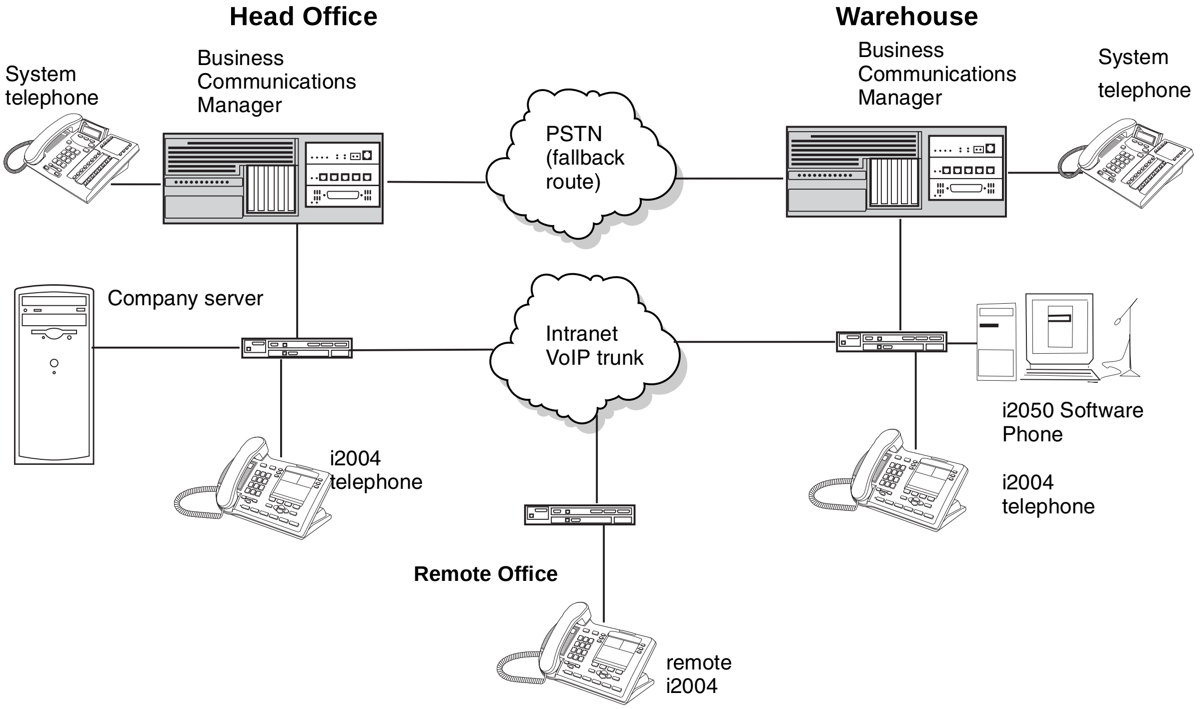
- Check MCDN PRI settings on the M1. For information on this, refer to the M1 documentation.
- Ensure SL-1 (MCDN) keycodes are entered on the Business Communications Manager 3.0 and the PRI line is set up for SL-1 protocol.

For a detailed description of setting up fallback, refer to Chapter 5, “Configuring VoIP trunks,” on page 73.

Networking multiple Business Communications Managers

The system shown in the following diagram allows multiple offices with Business Communications Manager systems to connect across the company Intranet. This installation allows for CallPilot to direct calls throughout the system. Full toll bypass occurs through the tandem setup, meaning that any user can call any DN without long distance charges being applied. Users have full access to system users, applications, PSTN connections, and Unified Messaging. The network diagram shows two Business Communications Managers, but additional base units can be added.

Figure 38 Multiple Business Communications Manager systems network diagram



To set up this system:

1. Ensure that the existing network can support the additional VoIP traffic.
2. Coordinate a Private dialing plan between all the systems.
3. On each Business Communications Manager 3.0 system:
   - Set up outgoing call configuration for the VoIP gateway.
   - Set up a remote gateway for the other Business Communications Managers or NetMeeting users.

- Set telephones to receive incoming calls through target lines.
- Configure the PSTN fallback and enable QoS on both systems.

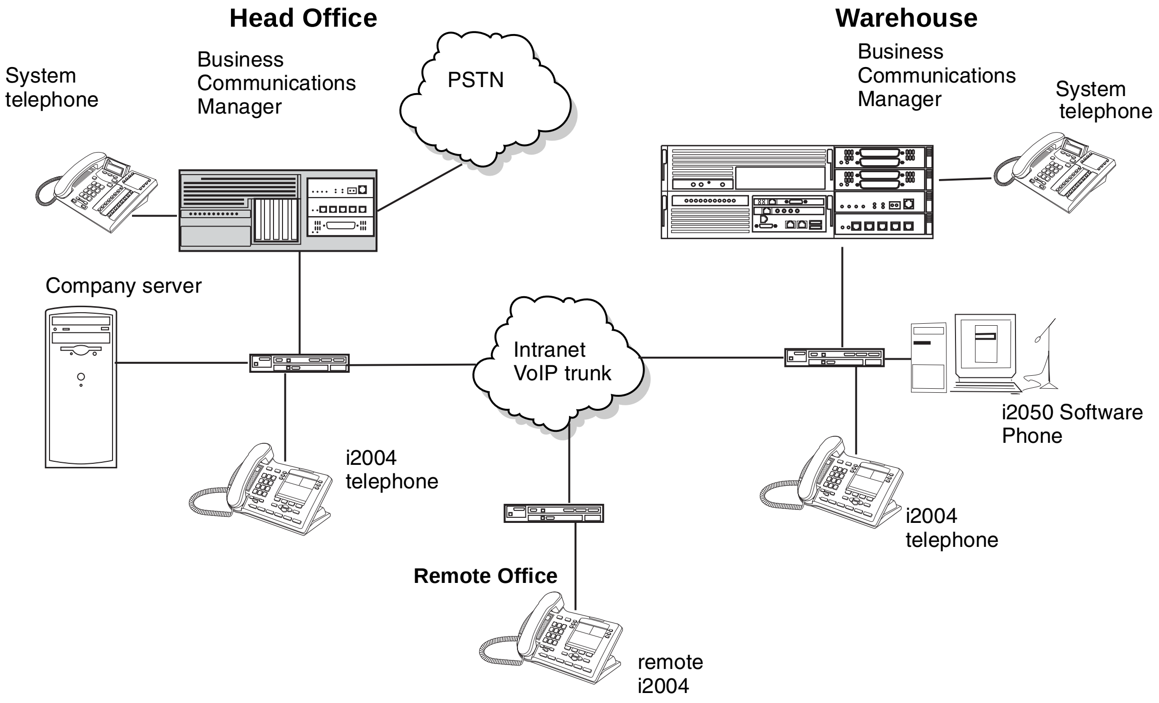
4 Reboot each system.

This system uses fallback to PSTN so calls can be routed across the PSTN connection if VoIP traffic between the Business Communications Manager systems becomes too heavy.

A similar system is shown below, except that only one of the Business Communication Managers has a line to the PSTN network. In this case, all public calls from both systems are funneled through the system with the PSTN connection and all communication between the systems occurs over IP trunks. To facilitate this system, you need to ensure that the routing codes on the non-PSTN system point to the system connected to the PSTN, and then, to the PSTN. On the PSTN-connected system, the system and routing codes must be configured to recognize and pass public calls from the other system out into the PSTN network.

This also means that if the VoIP trunks are inaccessible between the systems, there is no provision for a fallback route.

Figure 39 Routing all system-wide public calls through one Business Communications Manager

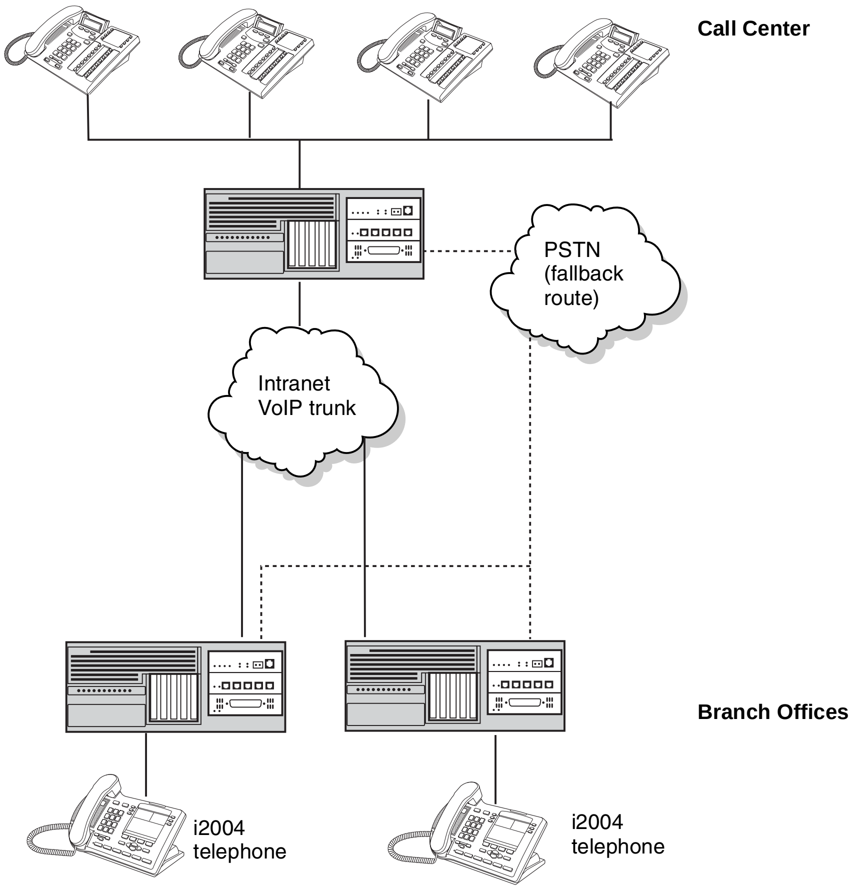


The *Programming Operations Guide* provides a detailed description of the configurations required for tandeming a system over PRI lines. Except for the VoIP trunk requirements, the system and routing configurations would be similar.

Multi-location chain with call center

In the installation shown in the following diagram, one Business Communications Manager runs a Call Center and passes calls to the appropriate branch offices, each of which use a Business Communications Manager. A typical use of this would be a 1-800 number that users world-wide can call, who are then directed to the remote office best able to handle their needs.

Figure 40 M1 to Business Communications Manager network diagram



To set up this system:

1 Ensure that the existing network can support the additional VoIP traffic.

2 Coordinate a Private dialing plan between the systems.

3 On each Business Communications Manager 3.0 system:

- Set up outgoing call configuration for the VoIP gateway.
- Set up a remote gateway for other Business Communications Managers.
- Set phones to receive incoming calls through target lines.
- Configure the PSTN fallback and enable QoS on both systems.

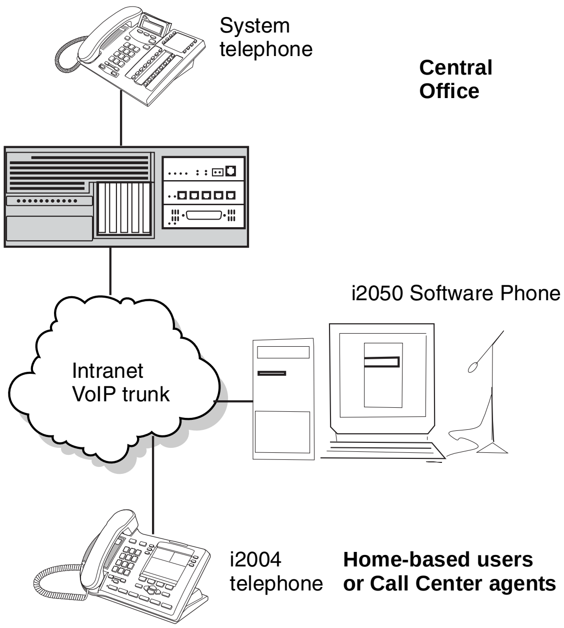
4 Reboot each system.

5 Set up a Call Center on the central Business Communications Manager.

Business Communications Manager to IP telephones

The system shown in the following figure allows home-based users or Call Center agents to use the full capabilities of the Business Communications Manager, including access to system users, applications, and PSTN connections. This system does not require VoIP trunk configuration. This system functions in a similar manner to the system described in "Multi-location chain with call center" on page 119. This system is less expensive and on a smaller scale. However, it does not offer PSTN fallback.

Figure 41 Connecting to IP telephones



Setting up a remote-based IP telephone

To set up this system:

1 Ensure that each remote user has a network connection capable of supporting VoIP traffic, such as DSL or cable.

2 On the Business Communications Manager, set up the system to support IP telephones.

3 At the remote location, install and configure an IP telephone.

4 Register each telephone and provide it with a DN.

5 Set up the DN record with the required lines and services.

Appendix A
Efficient Networking

This section provides information about making your network run more efficiently.

Determining the bandwidth requirements

The IP network design process starts with the an IP telephony bandwidth forecast. The bandwidth forecast determines the following:

- LAN requirements: LAN must have enough capacity for the number of calls plus the overhead
- WAN requirements: WAN must have enough capacity for the number of calls plus the overhead

Determining WAN link resources

For most installations, IP telephony traffic travels over WAN links within the intranet. WAN links are the highest recurring expenses in the network and they are often the source of capacity problems in the network. WAN links require time to receive financial approval, provision and upgrade, especially inter-LATA (Local Access and Transport Area) and international links. For these reasons, it is important to determine the state of WAN links in the intranet before installing IP telephony.

Link utilization

This procedure explains how to determine and adjust link utilization:

1 Get a current topology map and link utilization report of the intranet. A visual inspection of the topology can indicate the WAN links anticipated to deliver IP telephony traffic.

2 Record the current utilization of the links that will be handling IP telephony traffic. For example, the link utilization can be an average of a week, a day, or one hour. To be consistent with the considerations, get the peak utilization of the trunk.

3 Determine the available spare capacity. Business Communications Manager intranets are subject to capacity planning controls that ensure that capacity use remains below a determined utilization level.
For example, a planning control can state that the utilization of a 56 kbit/s link during the peak hour must not exceed 50%. For a T1 link, the threshold is higher, at 85%. The carrying capacity of the 56 kbit/s link can be 28 kbit/s, and for the T1, 1.3056 Mbit/s. In some

organizations the thresholds can be lower than those used in this example. In the event of link failures, spare capacity for rerouting traffic is required.

Some WAN links can exist on top of layer 2 services, such as Frame Relay and Asynchronous Transfer Mode (ATM). The router-to-router link is a virtual circuit, which is subject not only to a physical capacity limits, but also to a logical capacity limit. The installer or administrator needs to obtain the physical link capacity and the QoS parameters. The important QoS parameters are CIR (committed information rate) for Frame Relay, and MCR (maximum cell rate) for Asynchronous Transfer Mode (ATM).

The difference between the current capacity and the acceptable limit is the available capacity. For example, a T1 link used at 48% during the peak hour with a planning limit of 85% has an available capacity of approximately 568 kbit/s.

Network engineering

This section describes some network engineering criteria that you need to consider for your system:

- "Bandwidth requirements on half duplex links" on page 124
- "Bandwidth requirements on full duplex links" on page 125
- "LAN engineering examples" on page 126
- "WAN engineering" on page 126
- "QoS Monitoring Bandwidth Requirement" on page 127

Engineer the network for worst-case numbers to indicate the spare bandwidth a LAN must have to handle peak traffic. It is important to plan so that the LAN/WAN can handle the IP telephony traffic using the defined codec without delay or packet loss. The installer or administrator must select one configuration and then set up the LAN/WAN so there is more bandwidth than the IP telephony output.

The following table provides bandwidth characteristics for the transmission of voice over IP for various link types given codec type and payload sizes. The bandwidths provided in this table explain the continuous transmission of a unidirectional media stream.

Table 28 VoIP Transmission Characteristics for unidirectional continuous media stream

Codec Type	Payload Size		IP Packet	Ethernet B/W[2]	PPP B/W	FR B/W
	ms	Bytes	Bytes	kbit/s	kbit/s	kbit/s
G.711 (64 kb/s)	10	80	120	116.8	97.6	103.2
	20	160	200	90.4	80.8	83.6
	30	240	280	81.6	75.2	77.1

Table 28 VoIP Transmission Characteristics for unidirectional continuous media stream (Continued)

Codec Type	Payload Size		IP Packet	Ethernet B/W[2]	PPP B/W	FR B/W
	ms	Bytes	Bytes	kbit/s	kbit/s	kbit/s
G.729 (8 kb/s)	10	10	50	60.8	41.6	47.2
	20	20	60	34.4	24.8	27.6
	30	30	70	25.6	19.2	21.1
G.723.1 (6.3 kb/s)	30	24	64	24.0	17.6	19.5
G.723.1 (5.3 kb/s)	30	20	60	22.9	16.5	18.4

Notes:

1) Gray background indicates payload sizes used by Business Communications Manager 3.0 for transmission. Other values listed indicate payload sizes that the Business Communications Manager 3.0 can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12-byte inter-frame gap.

The peak bandwidth and average bandwidth requirements for a normal two-way call must take into account the affects of full and half duplex links and the affects of silence suppression. Refer to the tables in the next two sections, below, and to Table 30 on page 125 for voice Gateway bandwidth requirements.

Peak bandwidth is the amount of bandwidth that the link must provide for each call. Considering voice traffic only, the number of calls a link can support is:

Number of Calls = Usable Link Bandwidth / peak Bandwidth per call

The average bandwidth takes into account the affects of silence suppression, which, over time, tends to reduce bandwidth requirements to 50% of the continuous transmission rate. The affects of silence suppression on peak bandwidth requirements differ depending on whether the link is half-duplex or full-duplex. See Appendix B, “Silence compression,” on page 135 for more information.

When engineering total bandwidth requirements for LANs and WANs, additional bandwidth must be allocated for data. Refer to standard Ethernet engineering tables for passive 10BaseT repeater hubs. Refer to the manufacturer’s specification for intelligent 10BaseT layer switches. WAN links must take into account parameters such as normal link utilization and committed information rates.

Bandwidth requirements on half duplex links

The following table provides bandwidth requirements for normal two-way voice calls on a half-duplex link for a variety of link protocols, codec types and payload sizes.

Table 29 Bandwidth Requirements per Gateway port for half-duplex links

Codec Type	**Payload Size**	**Ethernet B/W[2]**			**PPP B/W**			**FR B/W**		
		No SP	Silence Suppression		No SP	Silence Suppression		No SP	Silence Suppression	
	ms	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)
G.711 (64 kb/s)	10	233.6	233.6[3]	233.6[3]	195.2	195.2[3]	195.2[3]	206.4	206.4[3]	206.4[3]
	20	180.8	180.8[3]	180.8[3]	161.6	161.6[3]	161.6[3]	167.2	167.2[3]	167.2[3]
	30	163.2	163.2[3]	163.2[3]	150.4	150.4[3]	150.4[3]	154.2	154.2[3]	154.2[3]
G.729 (8 kb/s)	10	121.6	60.8	60.8	83.2	41.6	41.6	94.4	47.2	47.2
	20	68.8	34.4	34.4	49.6	24.8	24.8	55.2	27.6	27.6
	30	51.2	25.6	25.6	38.4	19.2	19.2	42.2	21.1	21.1
G.723.1 (6.3 kb/s)	30	48.0	24.0	24.0	35.2	17.6	17.6	39.0	19.5	19.5
G.723.1 (5.3 kb/s)	30	45.8	22.9	22.9	33.0	16.5	16.5	36.8	18.4	18.4

Notes:

1) Gray background indicates payload sizes used by Business Communications Manager 2.5 for transmission. Other values listed indicate payload sizes that BCM can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12 byte inter-frame gap.

3) G.711 does not support silence suppression.

With no silence suppression, both the transmit path and the receive path continuously transmit voice packets. Therefore, the peak bandwidth requirement per call on half-duplex links is:

Peak Bandwidth per call = 2(Continuous Transmission Rate)

(Half Duplex links, No Silence Suppression)

On half-duplex links with silence suppression enabled, the half-duplex nature of normal voice calls allows the sender and receiver to share the same bandwidth on the common channel. While the sender is talking, the receiver is quiet. Since only one party is transmitting at a time, silence suppression reduces the peak bandwidth requirement per call on a half-duplex link to:

Peak Bandwidth per call = 1(Continuous Transmission Rate)

(Half Duplex links, With Silence Suppression)

Bandwidth requirements on full duplex links

The following table provides bandwidth requirements for normal two-way voice calls on a full-duplex link for a variety of link protocols, codec types and payload sizes. Bandwidths for full-duplex links are stated in terms of the individual transmit and receive channels. For instance, a 64 kbits full duplex link (e.g. a DS0 on T1 link) has 64 kbits in the transmit direction and 64 kbits in the receive direction.

Table 30 Bandwidth Requirements per Gateway port for Full-duplex links

		Ethernet B/W[2]			**PPP B/W**			**FR B/W**		
	Payload Size	**No SP**	Silence Suppression		**No SP**	Silence Suppression		**No SP**	Silence Suppression	
Codec Type	ms	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)
G.711 (64 kb/s)	10	116.8	116.8	116.8[3]	97.6	97.6	97.6[3]	103.2	103.2	103.2[3]
	20	90.48	90.4	90.4[3]	80.8	80.8	80.8[3]	83.6	83.6	83.6[3]
	30	81.6	81.6	81.6[3]	75.2	75.2	75.2[3]	77.1	77.1	77.1[3]
G.729 (8 kb/s)	10	60.8	60.8	30.4	41.6	41.6	20.8	47.2	47.2	23.6
	20	34.2	34.4	17.2	24.8	24.8	12.4	27.6	27.6	13.8
	30	25.6	25.6	12.8	19.2	19.2	9.6	21.1	21.1	10.6
G.723.1 (6.3 kb/s)	30	24.0	24.0	12.0	17.6	17.6	8.8	19.5	19.5	9.8
G.723.1 (5.3 kb/s)	30	22.9	22.9	11.5	16.5	16.5	8.3	18.4	18.4	9.2

Notes:

1) Gray background indicates payload sizes used by Business Communications Manager 3.0 for transmission. Other values listed indicate payload sizes that Business Communications Manager can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12 byte inter-frame gap.

3) G.711 does not support silence suppression. Therefore the average bandwidth is the same as the peak bandwidth.

4) Bandwidths stated per channel (Rx or Tx).

With no silence suppression, both the transmit path and the receive path continuously transmit voice packets. Enabling silence suppression on full-duplex links reduces the average bandwidth. However, since transmit and receive paths use separate channels, the peak bandwidth per call per channel does not change. Therefore, peak bandwidth requirements per channel (Rx or Tx) per call on a full-duplex link is:

Peak Bandwidth per channel per call = 2(Continuous Transmission Rate)

(Full Duplex links, With or Without Silence Suppression)

The bandwidth made available by silence suppression on full-duplex links with continuous transmission rate – average bandwidth requirement, is available for lower priority data applications that can tolerate increased delay and jitter.

LAN engineering examples

Example 1: LAN engineering - voice calls

Consider a site with four Business Communications Manager IP telephony ports. Assume a preferred codec of G.729, which uses a voice payload of 20 ms. Silence compression is enabled. The Ethernet LAN is half-duplex. Ethernet LAN may also be full duplex.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on the LAN?

From the table under "Bandwidth requirements on half duplex links" on page 124, the following figure shows the peak transmission bandwidth for G.729 with silence suppression enabled on a half-duplex link is 34.4 kbit/s per call or 137.6 kbit/s for all four calls.

Figure 42 LAN engineering peak transmission

		Ethernet B/W[2]		
		No SP	**Silence Suppression**	
		peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)
G.729 (8 kb/s)	10			
	20		34.4	34.4
	30			

WAN engineering

Wide Area Network (WAN) links are typically full-duplex links - both talk and listen traffic use separate channels. For example, a T1 link uses a number of 64 kbit/s (DS0) duplex channels allowing *64 kbit/s for transmit path and n*64 kbit/s for the receive path.

(WAN links may also be half-duplex.)

Example 1: WAN engineering - voice calls

Consider a site with four IP telephony ports and a full-duplex WAN link using PPP. The preferred codec is G.729 kbit/s, which uses a voice payload of 20 ms. Silence compression is enabled.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on the WAN?

From the table under "Bandwidth requirements on full duplex links" on page 125, the following figure shows the peak transmission rate for G.729 is 24.8 kbit/s per call or 99.2 kbit/s in each direction for all four calls. In other words, in order to support four G.729 calls, the WAN link must have at least 99.2 kbit/s of usable bandwidth (in each direction).

The average bandwidth for each call is 12.4 kbit/sec per channel or 49.4 kbit/s for all four calls for each channel. Low priority data applications can make use of bandwidth made available by silence suppression.

Figure 43 Peak traffic, WAN link

		PPP B/W		
		No SP	**Silence Suppression**	
		peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)
G.729 (8 kb/s)	10			
	20		24.8	12.4
	30			

QoS Monitoring Bandwidth Requirement

The VoIP Quality-of-Service (QoS) Monitor periodically monitors the delay and packet-loss of IP networks between two peer gateways, e.g., Business Communications Manager to Business Communications Manager, by using a proprietary protocol. The main objective of the QoS Monitor is to allow new VOIP calls to fall back to the PSTN if the IP network is detected as *bad* in terms of delay and packet-loss. For more details about configuring QoS Monitoring, refer to the *Programming Operations Guide*.

The monitoring packets are delivered at UDP port 5000. If you use QoS Monitoring in your gateway setting, please refer to the following paragraph for a description of bandwidth requirement of QoS Monitoring.

There are a total of 25 monitoring packets traveling in each direction every 15 seconds. Each of monitoring packages has 88 bytes in IP layer. These monitoring packets are equally spaced out in the 15-second intervals. For example, if there are two Business Communications Managers, BCM-A and BCM-B, connected to each other with QoS Monitoring enabled, then in every 15 seconds there are 25 monitoring packets going from BCM-A to BCM-B and then back to BCM-A. Similarly, 25 packets go from BCM-B to BCM-A, then back to BCM-B.
In other words, in this case the overhead in IP layer caused by these monitoring packets is about (2x25x88)/15= 293 bytes/second in one direction.

Additional feature configuration

This section contains additional information about configuring your network to run efficiently.

- “Setting Non-linear processing” on page 128
- “Determining network loading caused by IP telephony traffic” on page 128
- “Implementing the network, LAN engineering” on page 131

Setting Non-linear processing

Non-linear processing should normally be enabled.

To set non-linear processing:

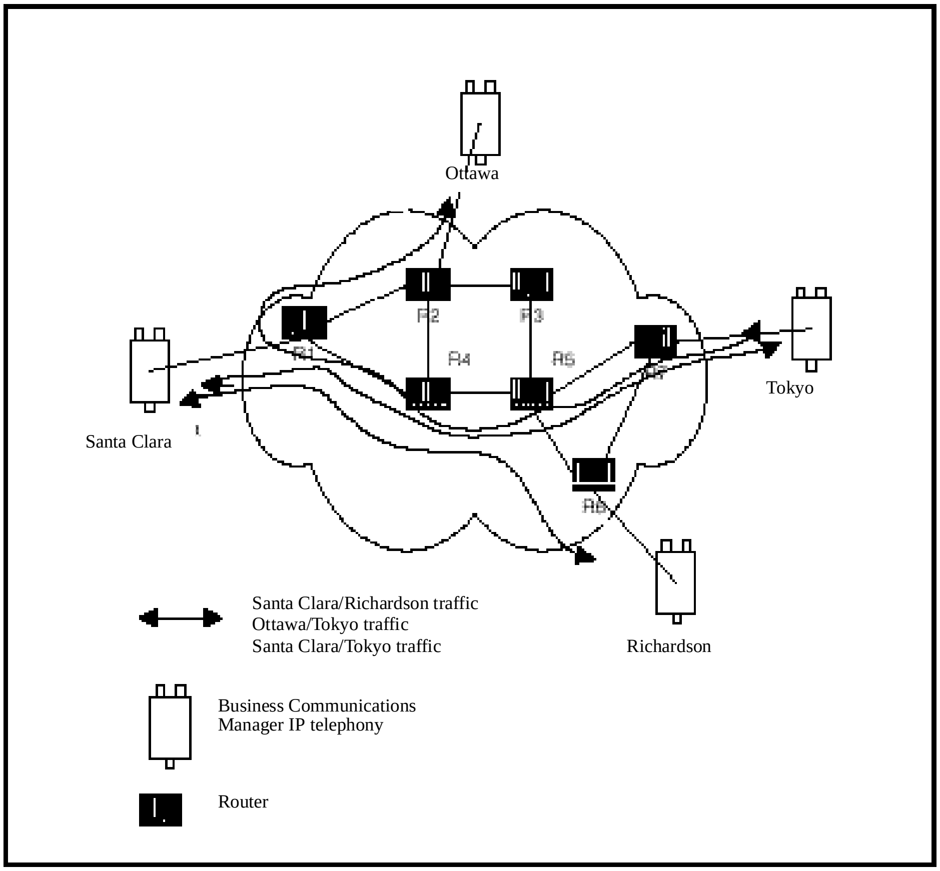
1. In Unified Manager, open **Services, IP Telephony**, and click on **H.323 settings**. The H.323 parameters appear in the right window.
2. Click the **Non-linear processing** drop-down menu, and select either **Enabled** or **Disabled**.

Determining network loading caused by IP telephony traffic

At this point, the installer or administrator has enough information to load the IP telephony traffic on the intranet.

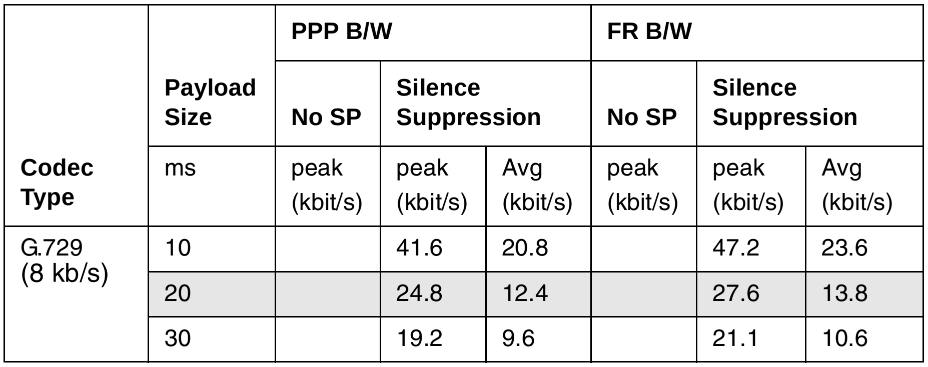
Consider the intranet has the topology as shown in the figure below, and the installer or administrator wants to know, in advance, the amount of traffic on a specific link, R4-R5.

Figure 44 Calculating network load with IP telephony traffic



Each site supports four VoIP ports. Assume the codex is G.729 Annex B, 20 ms payload. Assuming full-duplex links, peak bandwidths per call are between 24.8 kbit/s and 27.6 kbit/s peak transmission or approximately 28 kbit/s. This is shown in the following figure, taken from the table under “Bandwidth requirements on full duplex links” on page 125.

Figure 45 Network loading bandwidth



		PPP B/W			**FR B/W**		
	Payload Size	**No SP**	**Silence Suppression**		**No SP**	**Silence Suppression**	
Codec Type	ms	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)	peak (kbit/s)	peak (kbit/s)	Avg (kbit/s)
G.729 (8 kb/s)	10		41.6	20.8		47.2	23.6
	20		24.8	12.4		27.6	13.8
	30		19.2	9.6		21.1	10.6

Route R1-R2 needs to support four VoIP Calls. R4-R5 needs to support eight VoIP calls. The incremental peak bandwidth for VoIP traffic is therefore:

R1-R2 peak VoIP Load = 4(28 kbit/s) = 112kbit/s

R4-R5 peak VoIP Load = 8(28kbit/s) = 224kbit/s

With Business Communications Manager VoIP gateway bandwidth requirements and `Traceroute` measurements, the R4-R5 link is expected to support the Santa Clara/Richardson, Santa Clara/Tokyo and the Ottawa/Tokyo traffic flows. The other IP telephony traffic flows do not route over R4-R5. A peak of eight calls can be made over R4-R5 for the four IP telephony ports per site. R4-R5 needs to support the incremental bandwidth of 8 x 12 = 96 kbit/s.

To complete this exercise, the traffic flow from every site pair needs to be summed to calculate the load on each route and loaded to the link.

Enough link capacity

The following table sorts the computations so that for each link, the available link capacity is compared against the additional IP telephony load. For example, on link R4-R5, there is capacity (568 kbit/s) to allow for the additional 96 kbit/s of IP telephony traffic.

Table 31 Link capacity example

Link		**Utilization (%)**		**Available capacity kbit/s**	**Incremental IP telephony load**		**Enough capacity?**
End Points	**Capacity kbit/s**	**Threshold**	**Used**		**Site pair**	**Traffic kbit/s**	
R1-R2	1536	85	75	154	Santa Clara/ Ottawa Santa Clara/ Tokyo	15.5	Yes
R1-R3	1536						
R2-R3	1536						
R2-R4	1536						
R4-R5	1536	85	48	568	Santa Clara/ Richardson Ottawa/Tokyo Santa Clara/ Tokyo	24	Yes

Some network management systems have network planning modules that determine network flows. These modules provide more detailed and accurate analysis because they can include correct node, link and routing information. They also help to determine network strength by conducting link and node failure analysis. By simulating failures, re-loading network and re-computed routes, the modules indicate where the network can be out of capacity during failures.

Not enough link capacity

If there is not enough link capacity, consider one or more of the following options:

- Use the G.723.1 codec. Compared to the default G.729 codec with 20 ms payload, the G.723.1 codecs use 29% to 33% less bandwidth.
- Upgrade the bandwidth for the links.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources do not occur often. For a more complete evaluation, consider the impact of incremental IP telephony traffic on routers and LAN resources in the intranet where the IP telephony traffic moves across LAN segments that are saturated, or routers whose central processing unit (CPU) utilization is high.

Implementing the network, LAN engineering

To minimize the number of router hops between the systems, connect the gateways to the intranet. Ensure that there is enough bandwidth on the WAN links shorter routes. Place the gateway and the LAN router near the WAN backbone. This prevents division of the constant bit-rate IP telephony traffic from bursty LAN traffic, and makes easier the end-to-end Quality of Service engineering for packet delay, jitter and packet loss.

Further network analysis

This section describes how to examine the sources of delay and error in the intranet. It also discusses several methods for reducing one-way delay and packet loss.

The key methods are:

- “Components of delay” on page 131
- “Reduce link delay” on page 132
- “Reducing hop count” on page 132
- “Routing issues” on page 134

Components of delay

End-to-end delay is the result of many delay components. The major components of delay are:

- Propagation delay: Propagation delay is the result of the distance and the medium of links moved across. Within a country, the one-way propagation delay over terrestrial lines is under 18 ms. Within the U.S., the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and trans-oceanic circuits, use the rule of thumb of 1 ms per 100 terrestrial miles.
  If a circuit goes through a satellite system, estimate each hop between earth stations adds 260 ms to the propagation delay.
- Serialization delay: The serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is the result of the following formula:

  serialization delay in ms = 8(IP packet size in bytes/link bandwidth in kbit/s)

- Queuing delay: The queuing delay is the time it takes for a packet to wait in the transmission queue of the link before it is serialized. On a link where packets are processed in a first-come first-served order, the average queuing time is in milliseconds and is the result of the following formula:

  queuing time in ms = 8(average IP packet size in bytes/(1-p)(link bandwidth in kbit/s))

  The average size of intranet packets carried over WAN links generally is between 250 and 500 bytes. Queueing delays can be important for links with bandwidth under 512 kbit/s, while with higher speed links they can allow higher utilization levels.
- Routing and hop count: Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design.

Reduce link delay

In this and the next few sections, the guidelines examine different ways of reducing one-way delay and packet loss in the network.

The time taken for a voice packet to queue on the transmission buffer of a link until it is received at the next hop router is referred to as the link delay. Methods to reduce link delays include:

- Upgrade link capacity to reduce the serialization delay of the packet. This also reduces the utilization of the link, reducing the queueing delay. Before upgrading a link, check both routers connected to the link for the upgrade and ensure correct router configuration guidelines.
- Change the link from satellite to terrestrial to reduce the link delay by approximately 100 to 300 ms.
- Put into operation a priority queueing rule.
- Identify the links with the highest use and the slowest traffic. Estimate the link delay of these links using Traceroute. Contact your service provider for help with improving your QoS.

Reducing hop count

To reduce end-to-end delay, reduce hop count, especially on hops that move across WAN links. Some of the ways to reduce hop count include:

- Improve meshing. Add links to help improve routing, adding a link from router1 to router4 instead of having the call routed from router1 to router2 to router3 to router4, reducing the hop count by two.
- Router reduction. Join co-located gateways on one larger and more powerful router.

Adjust the jitter buffer size

The parameters for the voice jitter buffer directly affect the end-to-end delay and audio quality. IP telephony dynamically adjusts the size of the jitter buffer to adjust for jitter in the network. The network administrator sets the starting point for the jitter buffer.

Lower the jitter buffer to decrease one-way delay and provide less waiting time for late packets. Late packets that are lost are replaced with silence, decreasing quality. Increase the size of the jitter buffer to improve quality when jitter is high.

Reduce packet errors

Packet errors in intranets correlate to congestion in the network. Packet errors are high because the packets are dropped if they arrive faster than the link can transmit. Identify which links are the most used to upgrade. This removes a source of packet errors on a distinct flow. A reduction in hop count provides for less occurrences for routers and links to drop packets.

Other causes of packet errors not related to delay are as follows:

- reduced link quality
- overloaded CPU
- saturation
- LAN saturation
- limited size of jitter buffer

If the underlying circuit has transmission problems, high line error rates, outages, or other problems, the link quality is reduced. Other services such as X.25 or frame relay can affect the link. Check with your service provider for information.

Find out what the router threshold CPU utilization level is, and check if the router conforms to the threshold. If a router is overloaded, the router is continuously processing intensive tasks. Processing intensive tasks prevents the router from forwarding packets. To correct this, reconfigure or upgrade the router.

A router can be overloaded when there are too many high-capacity and high-traffic links configured on it. Ensure that routers are configured to vendor guidelines.

Saturation refers to a situation where too many packets are on the intranet. Packets can be dropped on improperly planned or damaged LAN segments.

Packets that arrive at the destination late are not placed in the jitter buffer and are lost packets. See “Adjust the jitter buffer size” on page 133.

Routing issues

Routing problems cause unnecessary delay. Some routes are better than other routes. The Traceroute program allows the user to detect routing anomalies and to correct these problems.

Possible high-delay differences causes are:

- routing instability
- wrong load splitting
- frequent changes to the intranet
- asymmetrical routing

Post-installation network measurements

The network design process is continuous, even after implementation of the IP telephony and commissioning of voice services over the network. Network changes in regard to real IP telephony traffic, general intranet traffic patterns, network controls, network topology, user needs and networking technology can make a design invalid or non-compliant with QoS objectives. Review designs against prevailing and trended network conditions and traffic patterns every two to three weeks at the start, and after that, four times a year. Ensure that you keep accurate records of settings and any network changes on an ongoing basis.

Ensure that you have valid processes to monitor, analyze, and perform design changes to the IP telephony and the corporate intranet. These processes ensure that both networks continue to conform to internal quality of service standards and that QoS objectives are always met.

Appendix B
Silence compression

This section describes using silence compression on half duplex and full duplex links:

- “Silence Compression on Half Duplex Links” on page 136
- “Silence compression on Full Duplex Links” on page 138
- “Comfort noise” on page 140

Silence compression reduces bandwidth requirements by as much as 50 per cent. This section explains how silence compression functions on a Business Communications Manager network. For information about enabling silence compression in VoIP gateways, refer to “Configuring media parameters” on page 74.

G.723.1 and G.729, Annex B support Silence compression.

A key to VoIP Gateways in business applications is reducing WAN bandwidth use. Beyond speech compression, the best bandwidth-reducing technology is silence compression, also known as Voice Activity Detection (VAD). Silence compression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36% to 40% of a full-duplex conversation is active. When one person talks, the other listens. This is half-duplex. There are important periods of silence during speaker pauses between words and phrases. By applying silence compression, average bandwidth use is reduced by the same amount. This reduction in average bandwidth requirements develops over a 20-to-30-second period as the conversation switches from one direction to another.

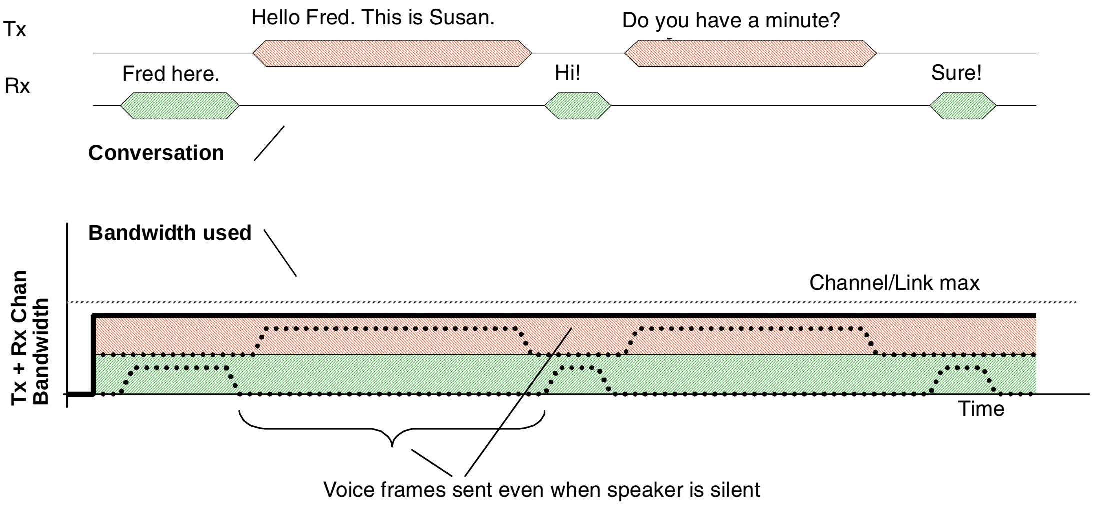
When a voice is being transmitted, it uses the full rate or continuous transmission rate.

The effects of silence compression on peak bandwidth requirements differ, depending on whether the link is half-duplex or full duplex.

Silence Compression on Half Duplex Links

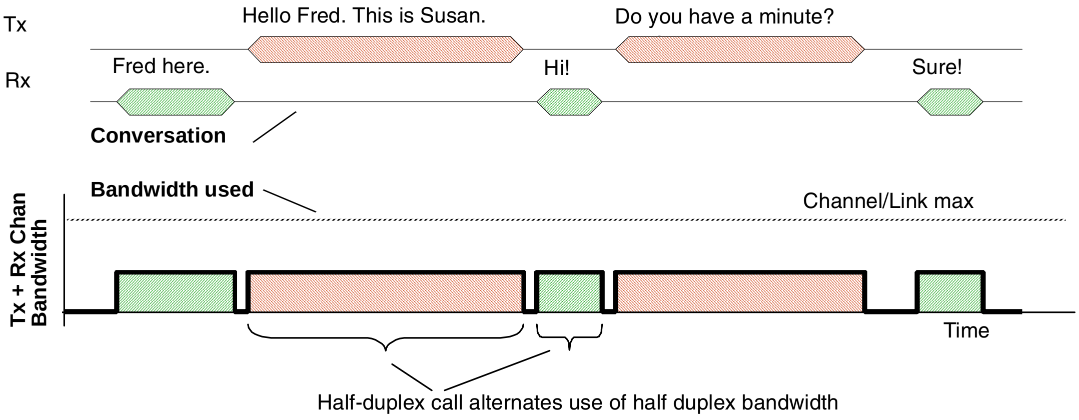
The following figure shows the bandwidth requirement for one call on a half-duplex link without silence compression. Since the sender and receiver share the same channel, the peak bandwidth is double the full transmission rate. Because voice packets are transmitted even when a speaker is silent, the average bandwidth used is equal to the full transmission rate.

Figure 46 One call on a half duplex link without silence compression



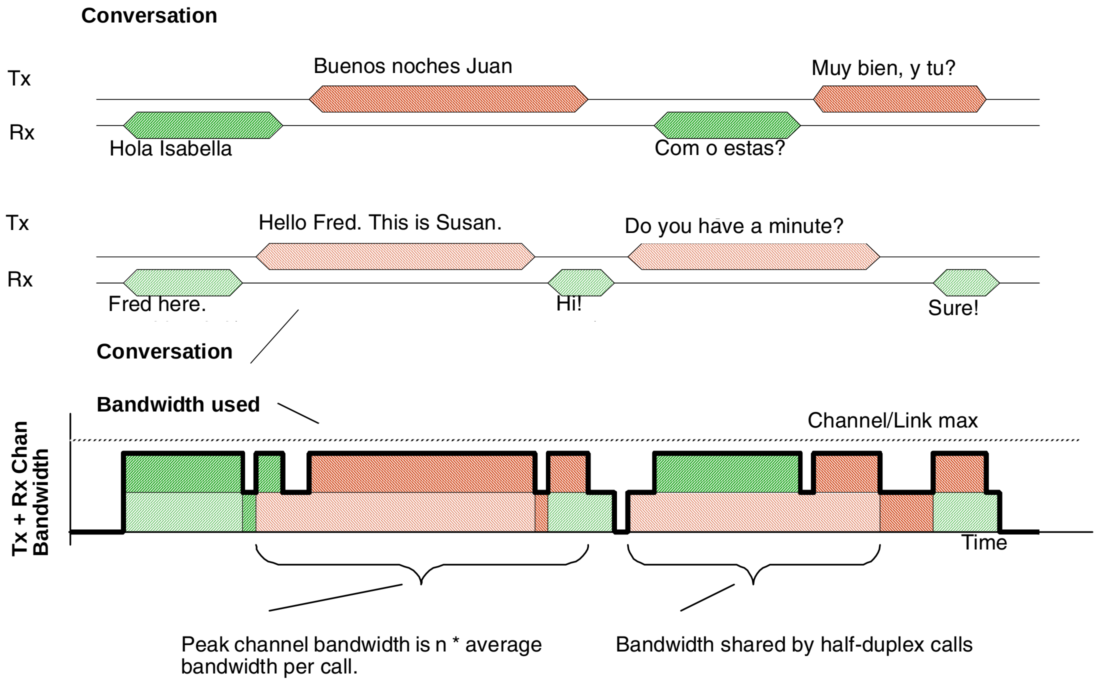
When silence compression is enabled, voice packets are only sent when a speaker is talking. In a typical voice conversation, while one speaker is talking, the other speaker is listening – a half duplex conversation. The following figure shows the peak bandwidth requirements for one call on a half-duplex link with silence compression enabled. Because the sender and receiver alternate the use of the shared channel, the peak bandwidth requirement is equal to the full transmission rate. Only one media path is present on the channel at one time.

Figure 47 One call on a half duplex link with silence compression



The effect of silence compression on half-duplex links is, therefore, to reduce the peak and average bandwidth requirements by approximately 50% of the full transmission rate. Because the sender and receiver are sharing the same bandwidth, this affect can be aggregated for a number of calls. The following figure shows the peak bandwidth requirements for two calls on a half-duplex link with silence compression enabled. The peak bandwidth for all calls is equal to the sum of the peak bandwidth for each individual call. In this case, that is twice the full transmission rate for the two calls.

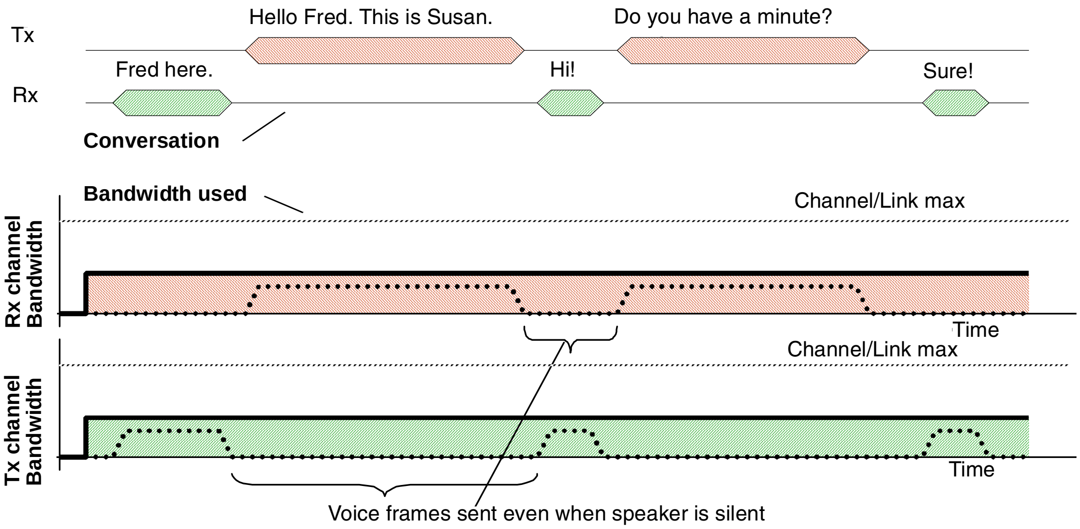
Figure 48 Two calls on a half duplex link with silence compression



Silence compression on Full Duplex Links

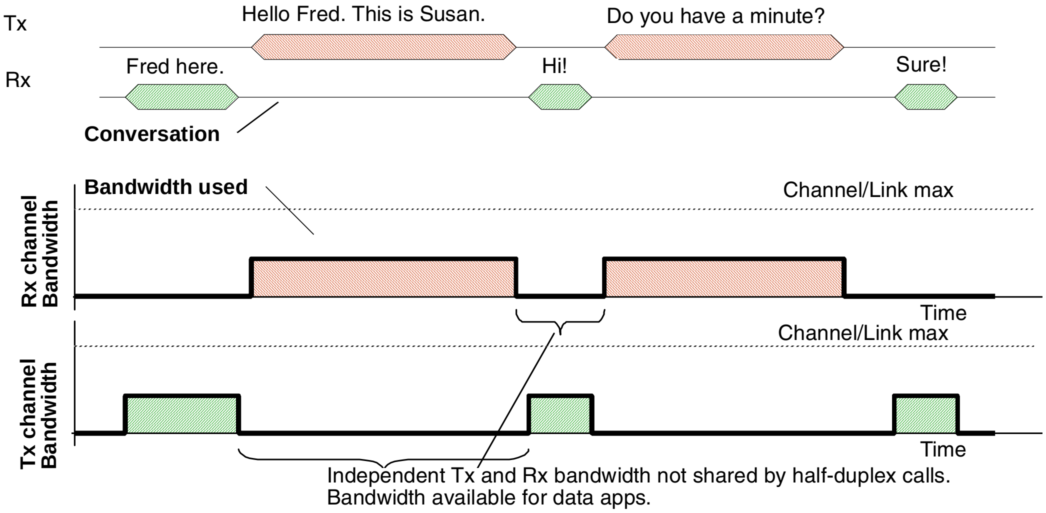
On full duplex links, the transmit path and the receive path are separate channels, with bandwidths usually quoted in terms of individual channels. The following figure shows the peak bandwidth requirements for one call on a full-duplex link without silence compression. Voice packets are transmitted, even when a speaker is silent. Therefore, the peak bandwidth and the average bandwidth used equals the full transmission rate for both the transmit and the receive channel.

Figure 49 One call on a full duplex link without silence compression



When silence compression is enabled, voice packets are only sent when a speaker is talking. When a voice is being transmitted, it uses the full rate transmission rate. Since the sender and receiver do not share the same channel, the peak bandwidth requirement per channel is still equal to the full transmission rate. The following figure shows the peak bandwidth requirements for one call on a full-duplex link with silence compression enabled. The spare bandwidth made available by silence compression is used for lower priority data applications that can tolerate increased delay and jitter.

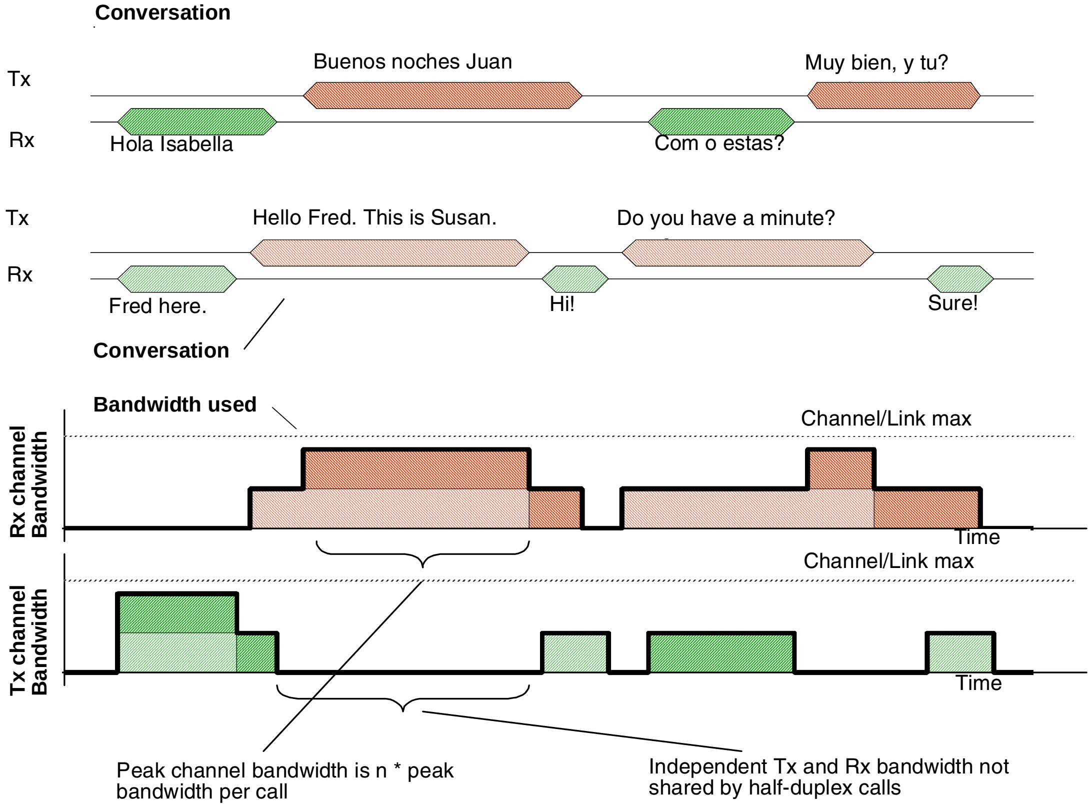
Figure 50 One call on a full duplex link with silence compression



When several calls are made over a full duplex link, all calls share the same transmit path and they share the same receive path. Since the calls are independent, the peak bandwidth must account for the possibility that all speakers at one end of the link may talk at the same time. Therefore, the peak bandwidth for n calls is n * the full transmission rate. The following figure shows the peak bandwidth requirements for two calls on a full duplex link with silence compression. Note that the peak bandwidth is twice the full transmission rate, even though the average bandwidth is considerably less.

The spare bandwidth made available by silence compression is available for lower priority data applications that can tolerate increased delay and jitter.

Figure 51 Two calls on a full duplex link with silence compression



Comfort noise

To provide a more natural sound during periods of silence, comfort noise is added at the destination gateway when silence compression is active. The source gateway sends information packets to the destination gateway informing it that silence compression is active and describing what background comfort noise to insert. The source gateway only sends the information packets when it detects a significant change in background noise.

Appendix C
Network performance utilities

There are two common network utilities, **Ping** and **Traceroute**. These utilities provide a method to measure quality of service parameters. Other utilities used also find more information about VoIP Gateway network performance.

Note: Because data network conditions can vary at different times, collect performance data over at least a 24-hour time period.

This section also describes the Sniffer utility.

- Ping
- Traceroute
- Sniffer

Ping

Ping (Packet InterNet Groper) sends an ICMP (Internet Control Message Protocol) echo request message to a host. It also expects an ICMP echo reply, which allows for the measurement of a round trip time to a selected host. By sending repeated ICMP echo request messages, percent packet loss for a route can be measured.

Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. Instead, a router discards the packet and returns to the originating IP address an ICMP `time exceeded` message.

Traceroute sends an IP datagram with a TTL of 1 to the selected destination host. The first router to handle the datagram sends back a `time exceeded` message. This message identifies the first router on the route. Then Traceroute transmits a datagram with a TTL of 2.

Following, the second router on the route returns a `time exceeded` message until all hops are identified. The Traceroute IP datagram has a UDP Port number not likely to be in use at the destination (normally > 30,000). The destination returns a `port unreachable` ICMP packet. The destination host is identified.

`Traceroute` is used to measure round trip times to all hops along a route, identifying bottlenecks in the network.

Sniffer

Sniffer is not provided with the Business Communications Manager, but it is a useful tool for diagnosing network functionality. It provides origin, destination, and header information of all packets on the data network.

Appendix D
Interoperability

This section discusses interoperability between the Business Communications Manager and other networks, including:

- "Speech path setup methods" on page 144
- "Media path redirection" on page 144
- "Gatekeeper" on page 145
- "Asymmetrical media channel negotiation" on page 145
- "Setting up Remote Routers for IP Telephony Prioritization" on page 146
- "Using VLAN on the network" on page 148
- "Symbol NetVision telephones" on page 150
- "Software interoperability restrictions and limitations" on page 150

Business Communications Manager 3.0 IP Telephony adheres to the ITU-T H.323v2 standards. Such endpoints include the Nortel Networks M1-ITG and Microsoft NetMeeting. As well, the Business Communications Manager is backward compatible, and interoperates with the Nortel Networks i2002, i2004 telephones, and i2050 Software Phone, and with the Symbol NetVision IP Phones. The following table summarizes this information:

Table 32 Business Communications Manager 3.0 Product Interoperability Summary

Vendor	Product	Version
Nortel Networks	Business Communications Manager	2.0 or greater
Nortel Networks	i2002/i2004	3002B20 (or greater)
Nortel Networks	i2050 Software Phone	1.0.x
Nortel Networks	M1-ITG	ITG2.X.26
Microsoft	NetMeeting	3.0
Symbol	NetVision Telephone	03.50-12/01.00-24 (or greater)

Business Communications Manager IP Telephony interoperates with the Gatekeeper applications Radvision ECS 2.1.0.1 and CSE 1000, which conform to the specifications in the following tables.

Table 33 Engineering specifications

Capacity	1 to 8 ports
Voice compression	G.723.1 MP-MLQ, 6.3 kbit/s or ACELP, 5.3 kbit/s G.729 CS-ACELP, 8 kbit/s (supports plain, Annex A and Annex B) G.711 PCM, 64 kbit/s u/A-law
Silence compression	G.723.1 Annex A G.729 Annex B

Table 33 Engineering specifications

Capacity	1 to 8 ports
Echo cancellation	48 ms tail delay
In-band signaling	DTMF (TIA 464B) Call progress
Speech path setup methods	Call Initiator: • H.323 fastStart Call Terminator: • H.323 slowStart • H.323v2 fastStart
End-to-end DTMF signaling	digits 0-9, # and *, fixed-duration tones only

Table 34 Supported voice payload sizes

Codec	Receive/transmit to M1-ITG	Receive/transmit to others
G.711	Highest supported by both ends, up to 30 ms in 10 ms increments.	20 ms
G.723.1	30 ms	30 ms
G.729	Highest supported by both ends, up to 30 ms in 10 ms increments.	20 ms

Speech path setup methods

Business Communications Manager 3.0 currently initiates calls using H.323 fastStart methods. The Business Communications Manager will accept and set up calls that have been initiated by another endpoint using H.323v2 fastStart methods, as well as H.323 slowStart methods.

Media path redirection

Media path redirection occurs after a call has been established, when an attempt is made to transfer to or conference in another telephone. Business Communications Manager 3.0 does not support codec re-negotiation upon media path redirection.

To ensure that call transfers, and conference works correctly, the following rules must be followed:

- The first preferred codec for VoIP Trunks must be the same on all Business Communications Managers. (See “Configuring media parameters” on page 74). If this codec is G.729, or G.723, the Silence Suppression option must be the same on all Business Communications Managers involved.

- If interworking with a Meridian 1-ITG, the profile on the Internet Telephony Gateway (ITG) must be set to have the same first preferred codec as on the Business Communications Manager, the Voice Activity Detection (VAD) option must be set to the same value as the Silence Suppression on the Business Communications Manager and the ITG payload size must be set to 30 ms. If these rules are not adhered to, simple calls will still go through, but some transfer scenarios will fail.

Gatekeeper

The Business Communications Manager is designed to interoperate with Radvision ECS 2.1.0.1 and CSE 1000 gatekeepers. As part of this, the Business Communications Manager supports both Direct (GatekeeperResolved) and Routed (GatekeeperRouted) call signaling in this mode of operation. Note that if the call signaling method is changed, the Business Communications Manager must be restarted before it functions properly. Refer to "Using a gatekeeper" on page 103 for specific configuration instructions.

Asymmetrical media channel negotiation

By default, the Business Communications Manager IP Telephony gateway supports the G.729 codec family, G.723.1, G.711 mu-law and G.711 A-law audio media encoding. Because NetMeeting does not support the H.323 fastStart call setup method, NetMeeting can choose a different media type for its receive and transmit channels. However, Business Communications Manager IP Telephony gateway does not support calls with different media types for the receive and transmit channels and immediately hangs up a call taken with asymmetric audio channels. In this case, the party on the Business Communications Manager switch hears a treatment from the switch (normally a reorder tone). The party on the NetMeeting client loses connection.

To solve this problem, in NetMeeting, under the **Tools**, **Options**, **Audio**, **Advanced**, check **Manually configure compression settings**, and ensure that the media types are in the same order as shown in the Business Communications Manager media parameters table. The following table lists the names used by the Business Communications Manager local gateway table and the matching names in NetMeeting.

Table 35 Name comparison

Business Communications Manager media parameters table	MS NetMeeting
G.723.1 6.3 Kbit/s	MS G.723 6400 bit/s
G.723.1 5.3 Kbit/s	MS G.723 5333 bit/s
G.711 µ-law	CCITT µ-law
G.711 A-law	CCITT A-law

No feedback busy station

The Business Communications Manager VoIP gateway provides call progress tones in-band to the user. If a busy station is contacted through the gateway, the gateway plays a busy tone to the user. However, as NetMeeting does not support fastStart, no speech path is opened to the user before the call connects. Because of this, the user on the NetMeeting station does not hear a busy signal from the gateway.

Setting up Remote Routers for IP Telephony Prioritization

This section includes information about setting up earlier version of BayStack routers and how to set up a range of UDP as a high priority.

➡ **Note:** The information in this section is not required for recent versions of the Nortel Networks routers, such as BayRS release 15, that support prioritization based on the DiffServ Code Point (DSCP).

Creating an outbound traffic filter

To create an outbound traffic filter:

1. In the Configuration Manager window, click **Circuits** and then click **Edit Circuits**.
   The Circuit List window appears.
2. Select a circuit.
3. Click the **Edit** button.
   The Circuit Definition screen appears with the circuit you selected highlighted.
4. On the **Protocol** menu, click **Add**.
5. Select the protocol priority from the list.
6. Click the **OK** button.
7. Click **Protocols**, **Edit Protocol Priority,** and then click **Priority/Outbound Filters**.
   The Priority/Outbound Filters window appears.
8. Click **Template**.
   The Filter Template Management window appears.
9. Enter the template name and click **Create**.
   The Create Priority/Outbound Template window appears.
10. Type a descriptive name in the Filter Name field.
11. Click **Criteria**, **Add**, **Datalink**, **IP,** and then click **Criterion**.
    The Add Range window appears. If you choose the User-Defined criterion, the Add User-Defined Field window appears first.

12 Type a minimum and maximum value to specify the range, and then click the **OK** button.
The Add Range window closes. The new criterion and ranges now appear in the Filter Information field of the Create Priority/Outbound Template window.

13 Click **Action**, **Add** and then click **action**.

14 Click the **OK** button.
The Filter Template Management window opens. The new template appears in the templates list.

15 Click **Done**.
The Priority/Outbound Filters window opens.

16 Click **Create**.
The Create Filter window opens.

17 Select a circuit in the Interfaces field.

18 Select a template in the Templates field.

19 Type a descriptive name in the Filter Name field.

20 Click **OK**.
The Priority/Outbound Filters window opens.

21 Click **Apply**.
The filter is applied to the circuit.

Sample criteria, ranges, and actions for UDP filtering

The filtering goal is to place all VoIP H.323 traffic leaving a particular interface in the high priority queue. From the BayRS Site Manager:

- Use a criteria path of **Criteria**, **Add**, **IP**, **IP**, **UDP Destination Port**
- The range is 28000 to 28255.
- The action path is: **Action**, **IP**, **Add**, **High Queue**.

Note: This example shows how to give H.323 traffic priority over other protocols on the interface.

Using VLAN on the network

A virtual LAN (VLAN) is a logical grouping of ports, controlled by a switch, and end-stations, such as IP telephones, configured so that all ports and end-stations in the VLAN appear to be on the same physical (or extended) LAN segment even though they may be geographically separated. VLAN IDs are determined by how the VLAN switch is configured. If you are not the network administrator, you will have to ask whoever manages the switch what the VLAN ID range is for your system.

VLANs aim to offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of move, add, and change in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- For IP telephony, VLANs provide a useful technique to separate and prioritize the telephony traffic for L2 switches.
- VLAN also provide a shield from malicious traffic that may be targeted at the IP phone in order to steal or disrupt service.
- Reuse IP address in different VLANs.
- As far as possible, VLANs maintain compatibility with existing bridges and end stations.
- If all bridge ports are configured to transmit and receive untagged frames, bridges will work in plug-and-play ISO/IEC 15802-3 mode. End stations will be able to communicate throughout the Bridged LAN.

Choosing DHCP for VLAN

If you use a DHCP server remote to your Business Communications Manager, you must enter any VLAN IDs manually on i2004 telephones.

By using the Business Communications Manager DHCP server, you can configure DHCP to auto-assign a VLAN ID to each IP telephone that registers. With this configuration, you can also choose to manually enter VLAN IDs, if you choose. The Business Communications Manager DHCP server becomes the default VLAN that everyone can reach. The server provides the network configuration information in the default VLAN, and it also provides the VLAN information for the network. Refer to the *Programming Operations Guide* for the DHCP settings for VLAN. Refer to “Configuring the i2002 or i2004 telephone to the system” on page 44 for information about configuring VLAN on the i2002 or i2004 telephone.

Assigning VLANs becomes important if you have multiple devices connected to the same switch port, such as when you use a 3-port-switch to connect a computer and IP phone on the same network cable. In this case, the system needs to apply the correct VLAN for each device.

Specifying the site-specific options for VLAN

The Business Communications Manager DHCP server resides in default VLAN and is configured to supply the VLAN information to the IP phones. The DHCP server will supply site-specific option in the DHCP offer message.

The following definition describes the Nortel i2004 specific, Site Specific option. This option uses the **reserved for site specific use** DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the i2004 to accept these messages as valid. The i2004 will pull the relevant information out of this option and use it to configure the IP phone.

Format of field is: Type, Length, Data.

`Type (1 octet):`

Five choices 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251).

Providing a choice of five types allows the i2004 to work in environments where the initial choice may already be in use by a different vendor. Pick only one TYPE byte.

`Length (1 octet):`

(variable depends on the message content)

`Data (length octets):`

- ASCII based
- format: `VLAN-A:XXX,YYY.ZZZ.`

where,

`VLAN-A:` uniquely identifies this as the Nortel DHCP VLAN discovery.

- `-A` signifies this version of this spec. Future enhancements could use `-B`, for example.
- ASCII `,` (comma) is used to separate fields.
- ASCII `.` (period) is used to signal end of structure.
- `XXX`, `YYY` and `ZZZ` are ASCII-encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN Ids. A maximum of 10 VLAN Ids can be configured. `NONE` means no VLAN (default VLAN).

The DHCP Offer message carrying VLAN information has no VLAN tag when it is sent out from the DHCP server. However, a VLAN tag will be added to the packet at the switch port. The packet will be untagged at the port of the IP phone.

Symbol NetVision telephones

In order to make calls between Symbol telephones and Business Communications Manager 3.0, each must be configured to have at least one common codec. The following codecs are supported by the NetVision telephones.

- G.711 u-law
- G.711 A-law
- G.729 Annex A and Annex B

Software interoperability restrictions and limitations

The following tables provide a brief overview of the IP telephony H.323 compatibility issues, including NetVision handset restrictions, and Gatekeeper restrictions. The tables are organized by Business Communications Manager software release numbers.

Table 36 Software interoperability restrictions and limitations

Software release	Description of restriction/limitation
All versions	ITG payload sizes should be set to 30 ms.
All versions	Silence suppression should be configured to the same value on both Business Communications Manager and ITG (for example: both on or both off). Silence suppression is called Voice Activity Detection on ITG.
2.03 GA 2.5 GA	M1/ITG interaction with more than one ITG: when transferring, conferencing, working with two or more ITG cards, they must be on the same subnet. If they are not on the same subnet, one-way speech path situations can occur.
2.5 FP1 2.5 FP1 MR1.1 3.0	The profile on the ITG must be set to the same first preferred codec as that of the Business Communication software. Software on the ITG trunk card must be 2.X.25 release. In order for features such as Transfer and Conference to operate correctly between all Business Communications Managers and ITGs in a network, these are the rules: • The First Preferred Codec for VoIP Trunks must be the same on all Business Communications Managers. This is configured in Unified Manager under **Services, IP Telephony, H.323 Trunks, Media Parameters**. • In addition, if the first preferred codec is G.729 or G.723, the Silence Suppression option on that page must be the same on all Business Communications Managers in the network. The Business Communications Manager supports only basic call to/from NetMeeting.(S/W version FP1 GA)
2.5 GA, 2.5 FP1, 3.0	FAX over IP is not supported.
2.5 FP 2.5 FP1 MR1.1 3.0	Long tones do not work over IP trunks.
2.5 FP1 2.5 FP1 MR1.1 3.0	Firewall Default Rules, when enabled, block call processing and signaling. You must add an additional rule to pass Protocol TCP\UDP, Destination Port H.323 for speech path to initialize.

Table 36 Software interoperability restrictions and limitations

Software release	Description of restriction/limitation
2.5 FP1 2.5 FP1 MR1.1 3.0	If an IP Telephony Remote Gateway IP address is pointed at a Wan Link Interface, which is a Published IP address, the ISDN WAN Backup Feature will not support VoIP Traffic from any set type to that Published IP Address in some Network Topologies.
2.5 FP1 2.5 FP1 MR1.1 3.0	**Symbol portable IP handsets** • Login by Extension is login option offered by the telephone, but is not currently supported by Business Communications manager. The work-around is to administer the extension as the username in Unified Manager. • The NetVision handsets do not support G.723, so they will be unable to negotiate a call on a VoIP trunk if the trunk is set to G.723 only. • Call Center (ACD) FEATURE 909 is not supported. This is an unworkable feature on single line display sets, including the M7100, and especially on Symbol. • Calls between Symbol sets do not support the Call Record feature. • There is sometimes significant echo heard on the Symbol set during ringback on outgoing calls over analog lines. • Business Communications Manager does not support remote registration for symbol sets if these sets are behind another device, for example, another Business Communications Manager, or a third-party router, which has NAT turned on. • Each H323 Terminal configured utilizes one IP Client Resource, whether the H323 Terminal is being used or not. • Firewall Default Rules, when enabled, block Symbol Registration and call processing. You must add two additional rules. (1) Pass Protocol TCP\UDP, Destination Port H.323 and (2) Pass Protocol UDP, Destination port 1719. • Ring cadence on Symbol handsets does not distinguish between Internal and External callers. • Symbol sets work fine as members of hunt groups, but when they are answer DN twinned with other sets, they do not ring under some circumstances. • When configured with an answer DN for a set in a hunt group, Symbol sets sometimes do not ring, or ring but do not display CLID information, and cannot answer the incoming call. It is recommended that the Symbol set be added to the hunt group before the answer DN set, or that the Symbol set be designated as the prime DN, with the answer DN for it applied to the twinned desk set. This does address most of the functionality problems. There still appears to be a problem for calls routed by CCR.
2.5 FP1 MR1.1	**Gatekeeper** • Officially Business Communications Manager supports only ECS 2.1.0.1 gatekeeper. Business Communications Manager does not support Call Setup (Q.931) routing mode. • Business Communications Manager does not support the Radvision Dialing plan package. • ECS option **Check that call is active every XXX seconds** must be unchecked. • Radvision ECS 2.1.0.1 gatekeeper limitations: ECS does not support fast start in the Call Setup (Q.931) and Call Control (H.245) routing mode.

Table 36 Software interoperability restrictions and limitations

Software release	Description of restriction/limitation
3.0 GA	**Gatekeeper** • Officially Business Communications Manager supports RadVision ECS 2.1.0.1 and CSE 1000 as gatekeepers. It does not support the Radvision Dialing plan package. • Radvision ECS 2.1.0.1 gatekeeper limitations: ECS does not support fast start in the Call Setup (Q.931) and Call Control (H.245) routing mode. **Call signaling** By selecting **GatekeeperRouted** or **GatekeeperResolved** you switch Business Communications Manager to gatekeeper mode, which means your Remote Gateway table will no longer be a part of your call routing plan. Choosing one of the modes will advertise a Business Communications Manager preference. The Gatekeeper is the final decisionmaker. It will select the mode (routed or resolved) based on its configuration. • GatekeeperRouted routes the Call Setup Channel and Control Channel through the ECS. In ECS terminology this mode is called Call Setup Q.931 and Call Control h.245 • GatekeeperResolved routes the Call Setup Channel and Control Channel directly to the far-end without ECS intervention. In ECS terminology this mode is called **Direct**. By using this method you will speed up you call setup time. This is the recommended configuration for the Business Communications Manager. **ECS Configuration:** • Accept calls – this must be enabled so that calls pass through the ECS Gatekeeper. • Routing Mode – it is recommended that you set this to **Direct** to minimize call setup time. The Business Communications Manager also supports routing of Setup(Q.931) and Call Control(H.245). **Important:** The Business Communications Manager does NOT support the second option – the routing of Setup(Q.931). The option, **Check that call is active every XXX seconds,** must be unchecked. • Force Direct For Service Calls – this setting (on the Settings, Advanced tab) should be enabled if the ECS Gatekeeper has been configured to use Direct call routing. ITG version 26.26 does not include support for gatekeeper interaction. To be able to establish calls between Business Communications Manager 3.0 and ITG through a gatekeeper, follow the configuration steps found in the "Using a gatekeeper" on page 103.

The following table shows which networking applications are supported for each Business Communications Manager software release.

Table 37 Software network communications application compatibility

BCM version	Application compatibility								
	BCM 2.03	**BCM 2.5**	**2.5 FP1**	**2.5 FP1 MR1**	**Net Meeting**	**ITG v. X.X**	**Symbol**	**GK**	**CSE1K**
BCM 2.03	X				basic call to/from	ITG v. 25.24			
BCM 2.5	X	X			basic call to/from	ITG v. 25.25			
BCM 2.5 FP1	X	X	X		X	ITG 25.25	X		
FP1 MR 1.1		X	X	X	X	ITG 25.25	X	X	
BCM 3.0			X	X	X	ITG 26.26	X	X	X

Appendix E
Quality of Service

The users of corporate voice and data services expect these services to meet a level of quality of service (QoS). This, in turn, affects network design. The purpose of planning is to design and allocate enough resources in the network to meet user needs. QoS metrics or parameters help in meeting the needs required by the user of the service.

This section provides information about:

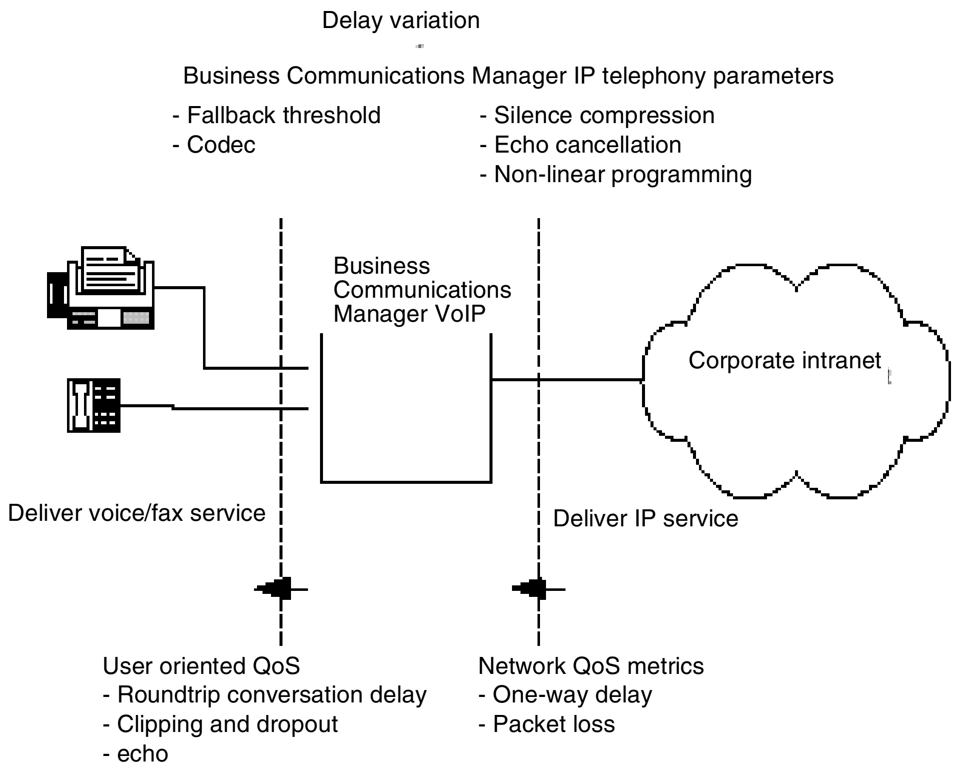
- "Setting QoS" on page 153
- "Measuring Intranet QoS" on page 155
- "Implementing QoS in IP networks" on page 159
- "Network Quality of Service" on page 161

Setting QoS

There are two interfaces that must be considered when you set up QoS on the network, as shown in the figure below:

- IP telephony interfaces with the end users: voice services made available need to meet user QoS objectives.
- The gateways interface with the intranet: the service provided by the intranet is "best-effort delivery of IP packets," not guaranteed QoS for real-time voice transport. IP telephony translates the QoS objectives set by the end users into IP adjusted QoS objectives. The guidelines call these objectives the intranet QoS objectives.

Figure 52 Relationship between users and services



The IP gateway can monitor the QoS of the Intranet. In this mode, two parameters, the receive fallback threshold and the transmit fallback threshold, control the minimum QoS level of the intranet. Fallback thresholds are set on pair-per-site basis.

The QoS level is aligned for user QoS metrics to provide an acceptable Mean Opinion Score (MOS) level. The administrator can adjust the fallback thresholds to provide acceptable service to the users.

The settings in the following table indicate the quality of voice service. IP telephony periodically calculates the prevailing QoS level per site pair based on the measurement of the following:

- one-way delay
- packet loss
- codec

Table 38 Quality of voice service

MOS Range	Qualitative Scale
4.86 to 5.00	Excellent
3.00 to 4.85	Good
2.00 to 2.99	Fair
1.00 to 1.99	Poor

When the QoS level of any remote gateway is below the fallback threshold, all new calls are routed over the standard circuit-switched network, if fallback is enabled.

The computation is taken from the ITU-T G.107 Transmission Rating Model.

Measuring Intranet QoS

Measure the end-to-end delay and error characteristics of the current state of the intranet. These measurements help to set accurate QoS needs when using the corporate intranet to carry voice services.

This section provides information about:

- "Measuring end-to-end network delay" on page 155
- "Measuring end-to-end packet loss" on page 156
- "Recording routes" on page 156
- "Adjusting Ping measurements" on page 157
- "Measurement procedure" on page 158
- "Other measurement considerations" on page 158

Measuring end-to-end network delay

The basic tool used in IP networks to get delay measurements is the Ping program. Ping takes a delay sample by sending a series of packets to a specified IP address and then returning to the originating IP address. Ping then displays statistics for the packets. High packet times can indicate network congestion. If the packets time out, then the remote device is unreachable.

The round trip time (rtt) is indicated by the time field

So that the delay sample results match what the gateway experiences, both the Ping host and target must be on a functioning LAN segment on the intranet.

Set the size of the Ping probe packets to 60 bytes to approximate the size of probe packets sent by IP telephony. This determines if new calls need to fall back on the circuit-switched voice facilities.

Notice from the Ping output the difference of rtt. The repeated sampling of rtt allows you to receive a delay characteristic of the intranet. To get a delay distribution, include the Ping tool in a script which controls the frequency of the Ping probes, which timestamps and stores the samples in a raw data file.

The file can be analyzed by the administrator using spreadsheets and other statistics packages. The installer can check if the intranet network management software has any delay measurement modules which can cause a delay-distribution measurement for specific site pairs.

Delay characteristics vary depending on the site pair and the time of day. The evaluation of the intranet includes taking delay measurements for each site pair. If there are important changes of traffic in the intranet, include some Ping samples during the peak hour. For a more complete evaluation of the intranet delay characteristics, get Ping measurements over a period of at least a week.

Measuring end-to-end packet loss

The `Ping` program also reports if the packet made its round trip correctly. Use the same `Ping` host setup to measure end-to-end errors. Use the same packet size.

Sampling error rate, require taking multiple `Ping` samples (at least 30). An accurate error distribution requires data collection over a greater period of time. The error rate statistic from multiple `Ping` samples is the packet loss rate.

Recording routes

As part of the network evaluation, record routing information for all source destination pairs. Use the Traceroute tool to record routing information. A sample of the output of the Traceroute tool follows:

```
C:\WINDOWS>tracert 10.10.10.15

Tracing route to 10.10.10.15 over a maximum of 30 hops:

1 3 ms 1 ms <10 ms tftzraf1.ca.nortel.com [10.10.10.1]
2 1 ms 1 ms 1 ms 10.10.10.57
3 7 ms 2 ms 3 ms tcarrbf0.ca.nortel.com [10.10.10.2]
4 8 ms 7 ms 5 ms bcarha56.ca.nortel.com [10.10.10.15]

Trace complete.
```

The Traceroute program checks if routing in the intranet is symmetric for each source destination pairs. Also, the Traceroute program identifies the intranet links used to carry voice traffic. For example, if Traceroute of four site pairs gets the results shown in the following table, you can calculate the load of voice traffic per link, as shown in the second table.

Table 39 Site pairs and routes

Site pair	Intranet route
Santa Clara/Richardson	R1-R4-R5-R6
Santa Clara/Ottawa	R1-R2
Santa Clara/Tokyo	R1-R4-R5-R7
Richardson/Ottawa	R2-R3-R5-R6

Table 40 Computed load of voice traffic per link

Links	Traffic from
R1-R4	Santa Clara/Richardson Santa Clara/Tokyo
R4-R5	Santa Clara/Richardson Santa Clara/Tokyo
R5-R6	Santa Clara/Richardson Richardson/Ottawa
R1-R2	Santa Clara/Ottawa
R5-R7	Santa Clara/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Adjusting Ping measurements

The Ping statistics are based on round-trip measurements. While the QoS metrics in the Transmission Rating model are one-way. To make the comparison compatible, the delay and packet error `Ping` statistics are halved.

Adjustment for processing

The `Ping` measurements are taken from `Ping` host to `Ping` host. The Transmission Rating QoS metrics are from end user to end user, and include components outside the intranet. The `Ping` statistics for delay requires additional adjustments by adding 140 ms to explain the processing and jitter buffer delay of the gateways.

No adjustments are required for error rates.

If the intranet measurement barely meets the round trip QoS objectives, the one-way QoS is not met in one of the directions of flow. This state can be true when the flow is on a symmetric route caused by the asymmetric behavior of the data processing services.

Late packets

Packets that arrive outside of the window allowed by the jitter buffer are discarded. To determine which `Ping` samples to ignore, calculate the average one-way delay based on all the samples. Add 300 ms to that amount. This amount is the maximum delay. All samples that exceed this one-way delay maximum are considered late and are removed from the sample. Calculate the percentage of late packets, and add that percentage to the packet loss statistics.

Measurement procedure

The following procedure is an example of how to get delay and error statistics for a specific site pair during peak hours.

Program a script to run the Ping program during the intranet peak hours, repeatedly sending a series of 50 Ping requests. Each Ping request generates a summary of packet loss, with a granularity of 2%, and, for each successful probe that made its round-trip, that many *rtt* samples.

For a strong network there must be at least 3000 delay samples and 60 packet loss samples. Store the raw output of the `Ping` results in a file. Determine the average and standard deviation of *one-way delay* and *packet loss.*

Repeat this for each site pair. At the end of the measurements, the results are as shown in the following table.

Table 41 Delay and error statistics

Destination pair	**Measured one-way delay (ms)**		**Measured packet loss (%)**		**Expected QoS level**	
	Mean	**Mean+σ**	**Mean**	**Mean+σ**	**Mean**	**Mean+σ**
Santa Clara /Richardson	171	179	2	2.3	Good	Good
Santa Clara /Ottawa						
Santa Clara /Tokyo						
Richardson/ Ottawa						
Richardson/Tokyo						
Ottawa/Tokyo						

Other measurement considerations

The Ping statistics described above measure the intranet before IP telephony installation. The measurement does not take into consideration the expected load provided by the IP telephony users.

If the intranet capacity is tight, and the IP telephony traffic is important, the installer or administrator must consider making intranet measurements under load. Apply load using traffic generator tools. The amount of load must match the IP telephony offered traffic estimated in the Business Communications Manager VoIP Gateway Bandwidth requirements.

Decision: does the intranet meet IP telephony QoS needs?

The end of the measurement and analysis is a good indicator of whether the corporate intranet can deliver acceptable voice and fax services. The Expected QoS level column in the table under “Measurement procedure” on page 158 indicates to the installer or administrator the QoS level for each site pair with the data.

To provide voice and fax services over the intranet, keep the network within a Good or Excellent QoS level at the Mean+σ operating area. Fax services must not travel on routes that have Fair or Poor QoS levels.

If QoS levels of some or all routes fall short of being Good, evaluate options and costs for upgrading the intranet. The evaluation often requires a link upgrade, a topology change, or implementation of QoS in the network.

To maintain costs, you can accept a Fair QoS level for the time for a selected route. A calculated trade-off in quality requires the installer or administrator to monitor the QoS level, reset needs with the end users, and respond to user feedback.

Implementing QoS in IP networks

This section describes information about implementing QoS in IP networks:

- “Traffic mix” on page 160
- “TCP traffic behavior” on page 160
- “Business Communications Manager router QoS support” on page 161

Corporate intranets are developed to support data services. Accordingly, normal intranets are designed to support a set of QoS objectives dictated by these data services.

When an intranet takes on a real-time service, users of that service set additional QoS objectives in the intranet. Some of the targets can be less controlled, compared with the targets set by current services, while other targets are more controlled. For intranets not exposed to real-time services in the past, but which now need to deliver IP telephony traffic, QoS objectives for delay can set an additional design restriction on the intranet.

One method of determining requirements is to subject all intranet traffic to additional QoS restrictions, and design the network to the strictest QoS objectives. An exact plan for the design improves the quality of data services, although most applications cannot identify a reduction of, say, 50 ms in delay. Improvement of the network results in a network that is correctly planned for voice, but over planned for data services.

Another plan is to consider using QoS in the intranet. This provides a more cost-effective solution to engineering the intranet for non-homogenous traffic types.

Traffic mix

This section describes QoS works with the IP telephony, and what new intranet-wide results can occur.

Before putting into operation QoS in the network, determine the traffic mix of the network. QoS depends on the process and ability to determine traffic (by class) so as to provide different services.

With an intranet designed only to deliver IP telephony traffic, where all traffic flows are equal priority, there is no need to consider QoS. This network can have one class of traffic.

In most corporate environments, the intranet supports data and other services. When planning to provide voice services over the intranet the installer must determine the following:

- Is there existing QoS? What kind? IP telephony traffic must take advantage of established mechanisms if possible.
- What is the traffic mix? If the IP telephony traffic is light compared to data traffic on the intranet, then IP QoS can work. If IP telephony traffic is heavy, data services can be affected if QoS is biased toward IP telephony traffic.

TCP traffic behavior

Most of corporate intranet traffic is TCP-based. Different from UDP, which has no flow control, TCP uses a sliding window flow control mechanism. Under this design, TCP increases its window size, increasing throughput, until congestion occurs. Congestion results in packet losses, and when that occurs the throughput decreases, and the whole cycle repeats.

When multiple TCP sessions flow over few congestion links in the intranet, the flow control algorithm can cause TCP sessions in the network to decrease at the same time, causing a periodic and synchronized surge and ebb in traffic flows. WAN links can appear to be overloaded at one time, and then followed by a period of under-utilization. There are two results:

- bad performance of WAN links
- IP telephony traffic streams are unfairly affected

Business Communications Manager router QoS support

With a Business Communications Manager system, the VoIP gateway and the router are in the same box. The Business Communications Manager router performs QoS and priority queuing to support VoIP traffic. The router supports VoIP in the following two ways:

- In a DiffServ network, the Business Communications Manager system acts as a DiffServ edge device and performs packet classification, prioritization, and marking. The router performs admission control for H.323 flows based on the WAN link bandwidth and utilization. When received, the WAN link marks the H.323 flows as Premium traffic and places the flows in the high priority queue.

Note: Differentiated Service (DiffServ) is a QoS framework standardized by the Internet Engineering Task Force (IETF).

- In a non-DiffServ or a legacy network, the router manages the WAN link to make sure Premium VoIP packets have high priority in both directions when crossing a slow WAN link.

Network Quality of Service

This section discusses the quality of service aspects of networking.

- "Network monitoring" on page 162
- "Quality of Service parameters" on page 162
- "Fallback to PSTN" on page 163

Business Communications Manager VoIP Gateway uses a method like the ITU-T Recommendation G.107, the E-Model, to determine the voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating "R" for the network transmission quality. The packet loss and latency of the end-to-end network determine "R". The model correlates the network objective measure "R", with the subjective QoS metric for voice quality, MOS or the Mean Opinion Score.

This model provides an effective traffic building process by activating the Fallback to Circuit-Switched Voice Facilities feature at call set up to avoid quality of service degradation. New calls fall back when the configured MOS values for all codecs are below the threshold.

The model is the reason for compression characteristics of the codecs. Each codec delivers a different MOS for the same network quality.

Network monitoring

The VoIP Gateway network monitoring function measures the quality of service between the local and all remote gateways on a continuous basis. The network monitoring function exchanges UDP probe packets between all monitored gateways to collect the network statistics for each remote location. All the packets make a round trip from the Sender to Receiver and back to the Sender. From this information, you can calculate the latency and loss in the network for a distinct location.

Note 1: Quality of Service monitoring is supported only on Business Communications Manager, M1 with ITG card, and i20xx.

Note 2: The Quality of Service threshold is configurable per remote gateway.

Note 3: Fallback starts for all new originating calls if the QoS of any monitored gateway is below its threshold.

Note 4: The fallback decision is made only at the originating gateway using the QoS thresholds monitored at the originating gateway for the destination gateway.

VoIP Gateway allows for manual configuration of QoS thresholds, depending on the customer preference between cost and voice quality.

Quality of Service parameters

Quality of Service depends on end-to-end network performance and available bandwidth. A number of parameters determine the VoIP Gateway QoS over the data network. The VoIP Gateway monitoring function can take about three minutes to respond to marginal changes in the network condition.

Packet loss

Packet loss is the percentage of packets that do not arrive at their destination. Transmission equipment problems and high delay and congestion can cause packet loss. In a voice conversation, gaps in the conversation represent packet losses. Some packet loss, less than 5%, can be acceptable without audible degradation in voice quality.

Packet delay

Packet delay is the period between when a packet leaves and when a packet arrives at the destination. The total packet delay time includes fixed and variable delay. Variable delay is the more manageable delay, while fixed delay depends on the network technology. The distinct network routing of packets are the cause of variable delays. To minimize packet delay and increase voice quality, the gateway must be as close as possible to the network backbone (WAN) with a minimum number of hops.

Delay variation (jitter)

The amount of variation in packet delay is otherwise known as delay variations, or jitter. Jitter affects the ability of the receiving gateway to assemble voice packets received at irregular intervals into a continuous voice stream.

Fallback to PSTN

If the measured Mean Opinion Score (MOS) for all codecs is below the configured threshold for any monitored gateway, the Fallback to PSTN activates. This feature reroutes calls to different trunks such as the Public Switched Telephone Network (PSTN) until the network QoS improves. When the QoS meets or exceeds the threshold, calls route over the IP network.

Fallback can be caused by any of the following reasons:

- bad network conditions
- remote gateway is out of service
- no network connection
- not enough DSP resources available

The fallback feature can be in the Local Gateway Configuration. With the fallback feature disabled, calls move across the IP telephony trunks no matter what level of Quality of Service. The fallback feature is active only at call setup. A call in progress does not fall back if the quality degrades.

Calls fallback if there is no response from the destination, an incorrectly configured remote gateway table, or if there are not enough DSP resources available to handle the new call.

Glossary

access point (802.11b)

This is a piece of hardware using either IEEE 802.11 (1 or 2 M-bits/sec, Frequency Hopping Spread Spectrum) or IEEE 802.11B (11 M-bits/sec, Direct Sequence Spread Spectrum) technology, that connects to the internet and acts as a wireless gateway for devices to connect to the internet. In the context of the Business Communications Manager, this is the device that the NetVision handset uses to connect to the LAN to which the Business Communications Manager is connected.

backbone

The major transmission path of a network, handling high-volume, high-density traffic.

bandwidth

A measure of information carrying capacity available for a transmission medium, shown in bits per second. The greater the bandwidth, the more information sent in a given amount of time.

bridge

LAN equipment providing interconnection between two networks using the same addressing structure. A bridge filters out packets that remain on one LAN and forwards packets for other LANs.

codec

Equipment or circuits that digitally code and decode voice signals. Software that provides compression/decompression algorithms for voice traffic over IP networks and VoIP trunks.

communications protocol

A set of agreed-upon communications formats and procedures between devices on a data communication network.

data communications

Processes and equipment used to transport signals from a data processing device at one location to a data processing device at another location.

default gateway

For IP telephony, this refers to the router that closest to the IP telephone.

DS30 split

This term refers to the allocation of media resources by the media services card (MSC) on the Business Communications Manager. The default setting is a 2/6 split, meaning that DS 01 and DS 08 are automatically used internal media processing, including IP telephony. If you plan to have a maximum number of IP telephones, you may need to set your system so that it uses DS30 bus 07 (DS30 3/5 split) as a processor for internal media traffic, including IP telephony, instead of for digital traffic through a media bay module.

enbloc

All dialed digits sent in a single expression. The system waits for all digits to be dialed before processing the call.

ESSID

This is the code that identifies the access point that a NetVision handset uses to connect to the internet and the Business Communications Manager.

fallback to PSTN

Your VoIP trunks can be configured to revert to land lines processed over the PSTN (public switched telephony network) if the IP network experiences quality issues. This process occurs during call setup. QoS must be active on the network to use this feature.

FEATURE *900

This feature code accesses a display menu on Nortel IP telephones. You use the directional arrows on the telephone to access menu items, which, when selected, perform as if you had entered that feature code. This menu can also be accessed through the Services button (default).

FEATURE *999 (hot desking)

This feature allows you to transfer the telephone and call features temporarily from one IP telephone to another. The originating IP telephone cannot be used during this period.

feature labels

The names that appear beside the four/six soft keys on Nortel IP telephones can be adjusted to better reflect local requirements. Label changes are performed through the Unified Manager.

firewalls

Firewalls are server security devices on a network that block or allow IP traffic into node networks or devices. When configuring IP telephony, you need to ensure that the port settings are correctly configured to pass through any network firewalls between the telephone and the Business Communications Manager.

full-duplex transmission

Simultaneous two-way separate transmission in both directions.

G.711

A codec that delivers toll quality audio at 64 kbit/s. This codec is best for speech because it has small delay, and is very resilient to channel errors.

G.729

A codec that provides near toll quality at a low delay. Uses compression to 8 kbit/s (8:1 compression rate).

G.723.1

A codec that provides the greatest compression, 5.3 kbit/s or 6.3 kbit/s. Normally used for multimedia applications such as H.323 videoconferencing. Allows connectivity to Microsoft-based equipment.

gatekeeper

A gatekeeper is server application on a network that tracks IP addresses of specified devices to provide authorization for making and accepting calls for those devices. The Business Communications Manager supports RadVision and CSE 1000 gatekeeper applications.

H.323

The ITU standard for multimedia communications over an IP network. Business Communications Manager IP Telephony supports H.323.

hop count

This is the number of routers the signal must go through to reach the destination device. The more hops that are required, the more potential there is for voice quality issues to arise.

hot desking

See Feature *999.

hub

Center of a star topology network or cabling system.

IEEE802 ESS

This is the LAN and switch standard used to define the connection between the access point and the NetVision handset onto the network. The handset is given the ID code of the device(s) with this standard so the access points recognize them.

i2050 Software Phone

This is a computer-based version of an IP telephone. Once installed, it acts, and is programmed, as you would the i2004 telephone. You must have a sound card and a USB headset to use this application.

interoperability

Interoperability refers to how compatible Business Communications Manager data configuration is with the rest of the network. Business Communications Manager IP Telephony adheres to the ITU-T H.323v2 standards, and is compatible with any H.323v1 or H.323v2 endpoints.

This also refers to IP compatibility issues between released versions of the Business Communications Manager. Business Communications Managers on the network with earlier versions of the software will not have the same operability for VoIP trunks as systems with 3.0 software.

IP server

On the Business Communications Manager, this is the server that registers IP telephones.

IP telephone

In this book, this term refers to any internet-based telephone that works with the Business Communications Manager system. For this release, this includes the Nortel Networks IP telephones, i2002, i2004 and i2050 Software Phone, as well as the Symbol NetVision sets and NetVision data handsets. These telephones all interface to the Business Communications Manager LAN or WAN card through an internet or intranet link

ITG

This is the internet telephony gateway protocol for the Meridian 1 to Business Communications Manager IP trunk connections. VoIP trunks require compatible configuration at both endpoints. The Business Communications Manager must be set to recognize that the other end of the trunk is an M1-ITG system.

jitter buffer

This is the process of collecting and organizing data frames at the receiving end to provide balanced voice quality.

kbit/s

kilobits per second. Thousands of bits per second.

keycodes

These are software codes that release feature applications on the Business Communications Manager, such as VoIP trunks, IP telephony ports, and MCDN.

latency

The amount of time it takes for a discrete event to occur.

Mbit/s

Megabits per second. Millions of bits per second.

MCDN

This is a specific network protocol used on private networks between Business Communications Manager systems or between Business Communications Manager systems and Meridian systems. The protocol only works on PRI SL-1 lines and on VoIP trunks. The protocol is activated with a keycode.

modem

Device that converts serial data from a transmitting terminal to an analog device for transmission over a telephone channel. Another modem converts the signal to serial digital Noise.

network diagram

This is a physical drawing/description of how the local network works to which your Business Communications Manager will be connected. It also includes information about the Business Communications Manager requirements, such as public and/or private IP addressing, DHCP requirements, and quality of service availabilities. Where possible, it should include information about the public networks and any changes or adjustments required by the network or the Business Communications Manager for compatibility.

Nortel NetVision Phone Administrator (NVPA)

This is the Business Communications Manager-specific application that is used to configure features and system information into the NetVision handsets. This application is included on the Business Communications Manager database. The latest application can be obtained at: http://www.symbol.com/services/downloads/nvfirmware2.html. The serial cable required to update the programming of the handset can be purchased from Purchased from Symbol at <http://symbol.com> (part number: 25-20528-01)

packet

Group of bits transmitted as a complete package on a packet switched network.

packet switched network (PSTN)

A telecommunications network based on packet switching technology. A link is busy for the duration of the packets.

Ping

This utility is used to echo messages to a host over an IP network. This allows you to find out if the other point is available. Ping also can include statistics about how long it took from end to end, which provides information about routing.

prioritization

This refers to how a voice data packet is set up in the Business Communications Manager so that external routers recognize it as having a high priority, thus shortening delay times and increasing the perception of voice quality over VoIP trunks.

published IP address

The IP address that both the IP telephones and the Symbol NetVision telephones use to access the Business Communications Manager. NetVision uses the H.323+ RAS protocol.

QoS (quality of service) routing

To minimize voice jitter over low bandwidth connections, the Business Communications Manager programming assigns specific DiffServ Marking in the IPv4 header of the data packets sent from IP telephones. During the packet journey through the network, including any routers on that network, the header specifies a level of priority service. This is quality of service routing. For QoS to be successful for IP telephony, it must be end-to-end on the network.

silence compression/silence suppression

This is the utility that omits the data packets that occur when no one is talking during the IP trunk calls, thus reducing the bandwidth load required for IP calls.

Symbol NetVision handsets

These IP telephones connect to the system through wireless access points connected to the same network to which the Business Communication Manager is connected.

target lines

These are internal channels on the Business Communications Manager that allow you to direct incoming calls to specific telephones, call groups/Hunt groups, or system devices. System telephones require target lines (if they have not already been configured) when receiving VoIP trunk calls, so the call knows where to go.

terminal

Device capable of sending or receiving data over a data communications channel.

throughput

Indicator of data handling ability. Measures data processed as output by a computer, communications device, link, or system.

topology

Logical or physical arrangement of nodes or stations.

Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine router hops to a specific IP address.

UNISTIM Terminal Proxy Server (UTPS)

This is a Nortel-designed protocol for IP telephony applications. The i2004 and i2002, for instance, use this protocol to communicate with the Business Communications Manager.

voice compression

Method of reducing bandwidth by reducing the number of bits required to transmit voice.

Voice over IP (VoIP) trunks

VoIP trunks are virtual telephone lines that the Business Communications Manager uses instead of wired lines to transfer IP traffic to other compatible systems with VoIP trunks. Both digital and IP telephones can use these channels.

Index