Part No. P0609326 1.1
May, 2006

Business Communications Manager 3.6

Programming Operations Guide

NORTEL NETWORKS

Copyright © Nortel Networks 2003–2006

Trademarks

Software licensing

The Apache Software License, Version 1.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).”

   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Contents

Figures

Tables

Preface

This guide explains how to program your Business Communications Manager system. For more information about the Business Communications Manager document suite, refer to "Related publications" on page 56.

This issue of the document reflects the added functionality built into the Business Communications Manager 3.6 release. The hardware, and new and updated features described in this and other documentation from this suite requires that your Business Communications Manager system is running release 3.6.

This section includes the following general information:

Warning: Ensure that you make a complete backup of your data before attempting to upgrade your system. Refer to the upgrade guide that comes with the upgrade package for instructions about upgrading the Business Communications Manager software from one version to another.

Note: The section "Software licensing" on page 3 contains software licensing information.

Note: Hardware: BCM200 and BCM400 hardware is shipped with 3.0 or newer software, only.

Note: Network: All the Business Communications Managers in your private network should be running the same level of software to ensure that remote gateways and other networking protocols are compatible. Meridian 1 systems connected to your network using Voice Over IP (VoIP) trunks must be running the ITP software. Ask your Meridian distributor for details.
After you perform an upgrade, always check that your gateways are still correctly configured for local and remote connections.

Before you begin

This guide is intended for these audiences:

- the installer who performs the initial configuration of the system
- the operator who manages the overall telephony operations of the system
- the system administrator who manages the data and network operations of the system

This guide assumes the following:

- There is an existing plan outlining the telephony and data requirements for your Business Communications Manager system.
- The Business Communications Manager is installed and initialized, and all hardware appears to be working. External lines and wiring for terminals and sets are connected to the appropriate media bay modules on the Business Communications Manager. All required keycodes have been entered.
- That all operators have a working knowledge of the Windows operating system and graphical user interfaces.
- That operators managing the data portion of the system are familiar with network management and applications.

Symbols used in this guide

This guide uses symbols to draw your attention to important information. The following symbols appear in this guide:

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 Symbol
A Note alerts you to important information.

Tip: Tip Symbol
Alerts you to additional information that can help you perform a task.

Security Note: This symbol indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to 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	Indicates command names and options and text that you need to enter. Example: Use the **dinfo** command. Example: Enter **show ip** {**alerts**|**routes**}.
italic text	Indicates book titles
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: Set Trap Monitor Filters
FEATURE **HOLD** **RELEASE**	Indicates that you press the button with the coordinating icon on whichever set you are using. (Refer to About the buttons on your telephones.)

About the buttons on your telephones

This guide uses text designators to indicate key pad feature buttons, such as Feature, Hold and Release. The Business Series Terminals (BST) telephones and the IP telephones all use icons to label these buttons. Table 1 shows the icons that appear for each function on the different types of Nortel Networks digital telephones. Note that the T7316 and T7208 have a separate button for mute functions. The IP telephones and the T7316E have separate buttons for both mute and handsfree.

Table 1 Telephone buttons

Button Name	Business Series Terminal T-series: 7XXX IP telephones: i20XX	Legacy Norstar M-series telephones European Norion telephones
Feature[1]	, Feature (i20XX)	Feature, Fx
Handsfree[2]	(i2004, i2002); (7316E) 7208/7316 use assigned memory button.	Handsfree Mute
Mute[3]	(i20XX), (7208, 7316, 7316E)	Handsfree Mute

Table 1 Telephone buttons (Continued)

Hold[4]	,	Hold , ,
Release[5]	, (2001 has a Goodbye button	, Rls
Call button	(2001)	N/A

[1] This document uses FEATURE to indicate the action of pressing the feature button.
[2] This document uses HANDSFREE to indicate the action of pressing the handsfree or handsfree/mute button for handsfree functionality.
[3] This document uses MUTE to indicate the action of pressing the mute or handsfree/mute button for mute functionality.
[4] This document uses HOLD to indicate the action of pressing the hold button.
[5] This document uses RELEASE to indicate the action of pressing the release button.

You press the **FEATURE** key and then the feature code to use a feature.
For example: Press **FEATURE 70** to transfer a call.

Model 7100 and 7000 telephones

The 7100 and 7000 telephones work differently from other telephones on your system because they do not have line buttons. Where other telephones can require that you select a line or intercom button to answer a call, with these telephones you just pick up the handset. Where other telephones require you to select a line button to take a call on that line off hold, on these telephones, you press **HOLD**.

You answer a second call by pressing **HOLD**. Your active call is put on hold and you connect to the waiting call. You only can have two active calls at one time.

The 7100 and 7000 telephones do not have speakers, therefore, cannot use the handsfree feature.

Portable handsets

Companion, DECT, and the BST T7406 portable handsets all access system features in different ways. Each of these handsets comes with a user guide that explains the specific feature access for the handsets.

IP telephones

Nortel Networks IP telephones (i2001, i2002, i2004, i2050) have user cards that explain the buttons on each device, including the `Feature` button, which is a softkey located under the display on these telephones. The *Telephone Feature User Guide* can be used with these telephones, as most Business Communications Manager features can be accessed from these telephones. These telephones also have a display menu that provides quick access to listed features.

The Symbol NetVision wireless IP handsets have a separate feature card which provides a quick reference for accessing the system through the handset. The card also explains how to access the Business Communications Manager features allowed by the system. Features can be accessed either by entering the code on the dialpad or by using the menu on the handset display.

Information about configuring IP telephones and NetVision handsets is contained in the *IP Telephony Configuration Guide*.

Acronyms used in this guide

This guide uses the following acronyms:

AAL	Analog Access Lines
ACD	Automated Call Distribution
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Program Interface
ARP	Address Resolution Protocol
ASM	Analog station module
ATA (or ATA2)	Analog Terminal Adapter
AUI	Attachment Unit Interface
AWG	American Wire Gauge
BERT	Bit Error Rate Test
BC	committed burst
BE	excess burst
BIOS	Basic Input Output System
BKI	Break-in
BLF	Busy Lamp Field
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
BRU	Backup and Restore Utility
CAA	Centralized Auto Attendant
CAC	Equal Access Identifier Code (carrier code)
CAP	Central Answering Position (T7316E+KIM or M7324+CAP modules)
CDP	Coordinated Dialing Plan
CHAP	Challenge-Handshake Authentication Protocol
CIC	Carrier Identification Code
CIR	Committed Information Rate
CLID	Calling Line Identification
COPS	Common Open Policy Service

COS	Class of Service
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	Channel Service Unit
CTE	Connected Telecommunications Equipment
CVM	Centralized Voice Mail
DAL	Digital Access Lines
DASS2	Digital Access Signaling System Number 2
DCE	Data Communications Equipment
DCOM	Distributed Component Object Model
DECT	Digital enhanced cordless telecommunications or Digital European cordless telephone
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol.
DID	Direct Inward Dial
DiffServ	Differentiated Services
DIMM	Dual In-line Memory Module
DISA	Direct Inward System Access
DLCI	Data Link Connection Indentifier
DLCMI	Data Link Control Management Interface
DN	Directory Number
DNS	Domain Name Service (DNS)
DPNSS	Digital Private Network Signalling System
DRT	Delayed Ring Transfer
DSCP	Diff-Serv Code Point
DSP	Digital Signal Processor
DSS	Direct Station Set (also referred to as an auto dial key)
DTE	Data Terminal Equipment
DTM	Digital Trunk Module
DTMF	Dual Tone Multifrequency.
EBN	Egress Border Node
EDO	Extended Data-Out
EF	Expedited Forwarding
eKIM	enhanced Key Indicator Module
EN	Edge Node
ES	End Station

ESP	Encapsulated Security Payload
FDD	Full Double Density
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GATM	Global Analog Trunk Module
HDLC	High-level Data Link Control
HF	Handsfree
HLC	Home Location Code (UDP dialing)
HS	Hospitality services
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
IBN	Ingress Border Node
I/C	Intercom feature button
ICCL	ISDN Call Connection Limitation
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force.
IP	Internet Protocol
IF	Input Filter
IPCP	IP Control Protocol
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
IRQ	Interrupt Request
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
IVR	Interactive Voice Response
KIM	Key Indicator Module
LAN	Local Area Network
LCD	Liquid Crystal Display
LCP	Link Control Protocol
LM	LAN Manager
LQR	Link Quality Rate
MAC	Media Access Control

MAU	Media Access Unit
MCDN	Meridian Client Defined Network (PRI SL-1)
MD5	Message Digest algorithm
MLPPP	Multi-Link Point-to-Point Protocol
MPPC	Microsoft Point to Point Compression
MSC	Media Services Card
MS-PEC	Media Services Processor Expansion Card
MWI	Message Waiting Indicator
NAT	Network Address Translation
NBMA	Non Broadcast Multi-Access
NCRI	Network Call Redirection Information
NIC	Network Interface Card
NTLM	NT LAN Manager
NNTP	Network News Transfer Protocol
OPX	Off Premises Extension.
OSI	Open Service Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Procedure
PBX	Private Branch Exchange.
PCI	Peripheral Component Interconnect Slot
PDD	Partial Double Density
PDN	Public Data Network
PFS	Perfect Forward Secrecy
PHB	Per Hop Behavior
POF	Packet Output Filter
POP3	Post Office Protocol
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
QOTD	Quote of the day server
QSIG	Q reference point signalling

RAS	Remote access service
RIP	Routing Information Protocol
RLR	Receive Loudness Rating
RPC	Remote Procedure Call
RTP	Realtime Transport Protocol
SAP	Service Advertising Protocol
SAPS	Station Auxiliary Power Supply
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SLR	Send Loudness Rating
SMB	Server Message Block
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPID	Service Profile Identifier
SR	Static Route
SS	Static Service
SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
SUNNFS	SUN Network File System
TAPI	Telephony Application Program Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
TFTP	Trivial File Transfer Protocol
TOS	Type of Service.
TPE	Twisted Pair Ethernet
TTL	time-to-live
UNISTIM	Unified Networks IP Stimulus
UDP	User Datagram Protocol or Universal Dialing Plan
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Networks
WAN	Wide Area Network

WFQ	Weighted Fair Queuing
WINS	Windows Internet Name Service

Related publications

In addition to the *Programming Operations Guide*, the Business Communications Manager documentation suite contains the following documents:

- *Management User Guide*
- *Telephony Features Handbook*
- *Installation and Maintenance Guide* (BCM1000 and BCM400/200)
- *IP Telephony Configuration Guide*
- *CallPilot Manager Set Up and Operation Guide*
- *CallPilot Reference Guide*
- *CallPilot Quick Reference Guide*
- *CallPilot Programming Record*
- *CallPilot Message Networking Set Up and Operation Guide*
- *CallPilot Message Networking User Guide*
- *CallPilot Unified Messaging Installation and Maintenance Guide*
- *CallPilot Desktop (Unified) Messaging Quick Reference Guide*
- *Software Keycode Installation Guide*
- *Call Center Set Up and Operation Guide*
- *Call Center Agent Guide*
- *Call Center Supervisor Guide*
- *Call Center Reporting Set Up and Operation Guide*
- *LAN CTE Configuration Guide*
- *Personal Call Manager User Guide*
- *Call Detail Recording System Administrator Guide*
- *Analog Telephone User Guide*
- *CallPilot Fax Set Up and Operation Guide*
- *CallPilot Fax User Guide*
- *Interactive Voice Response Installation and Configuration Guide* (IVR)

From the Business Communications Manager 3.6 Documentation CD, you can also access a number of telephone and accessory quick reference cards.

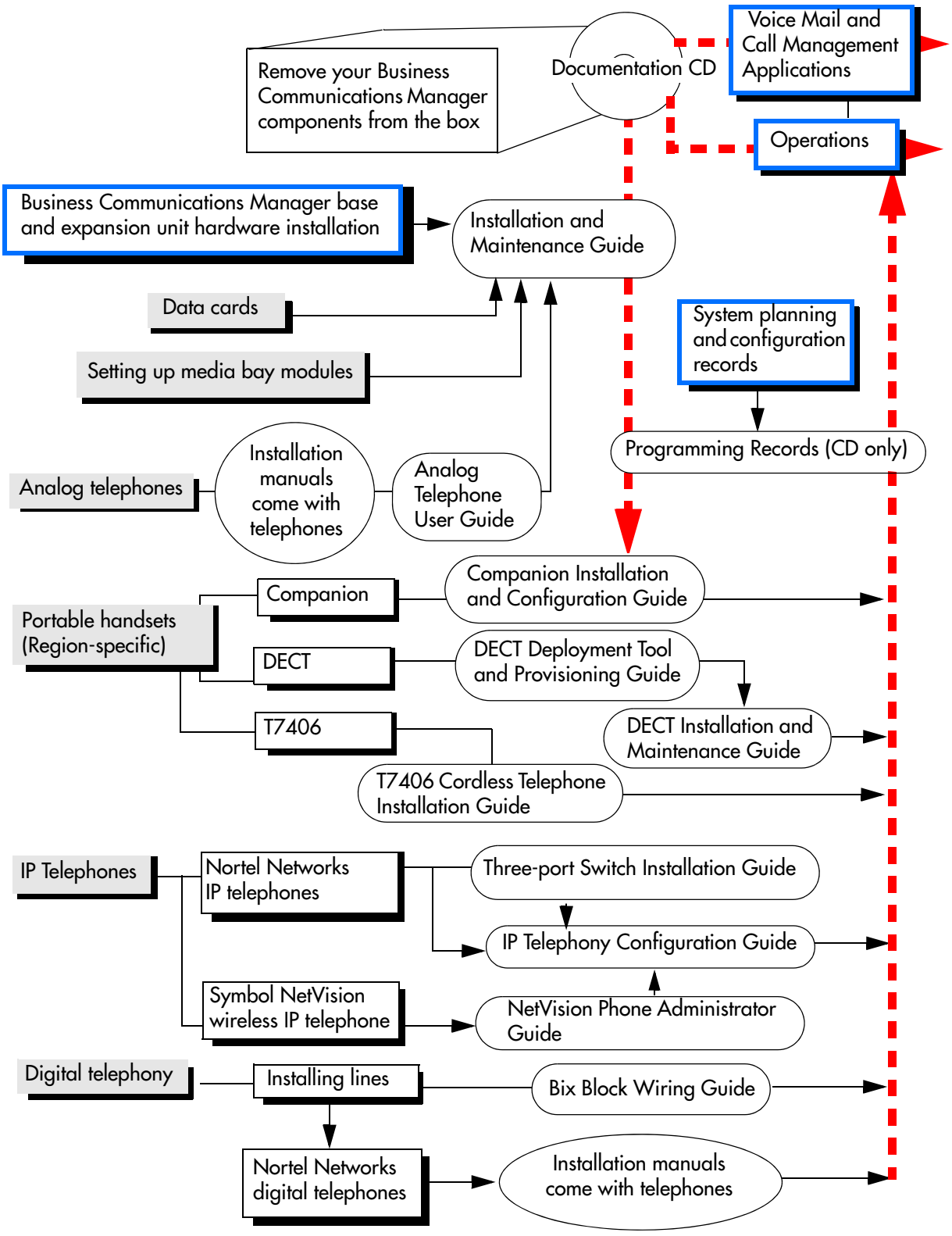
If you operate a multi-site Business Communications Manager network, you can use the Network Configuration Manager to provide centralized configuration and management operations. The documentation for this tool can be found on the Network Configuration Manager CD, which includes the software and the following documentation.

- *Network Configuration Manager Installation Guide*
- *Network Configuration Manager Administration Guide*
- *Network Configuration Manager Client Software User Guide*
- *Network Configuration Manager Reference Guide*

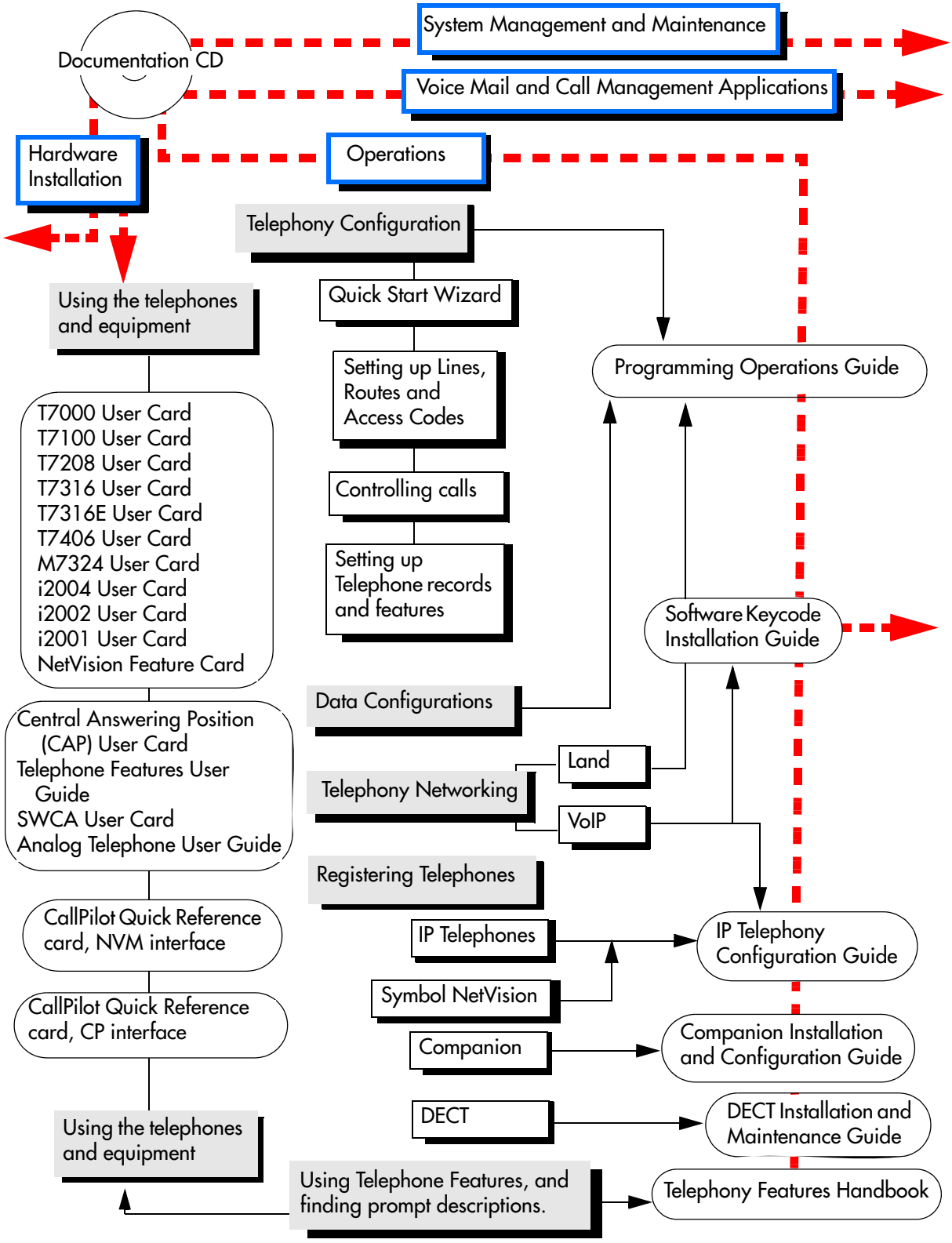
System documentation map

The following pages provide a map of the Business Communications Manager documentation CD. The map shows the overall task process of the system, and indicates which documentation deals with each section. All the documents describes are included on the documentation CD that came with your system.

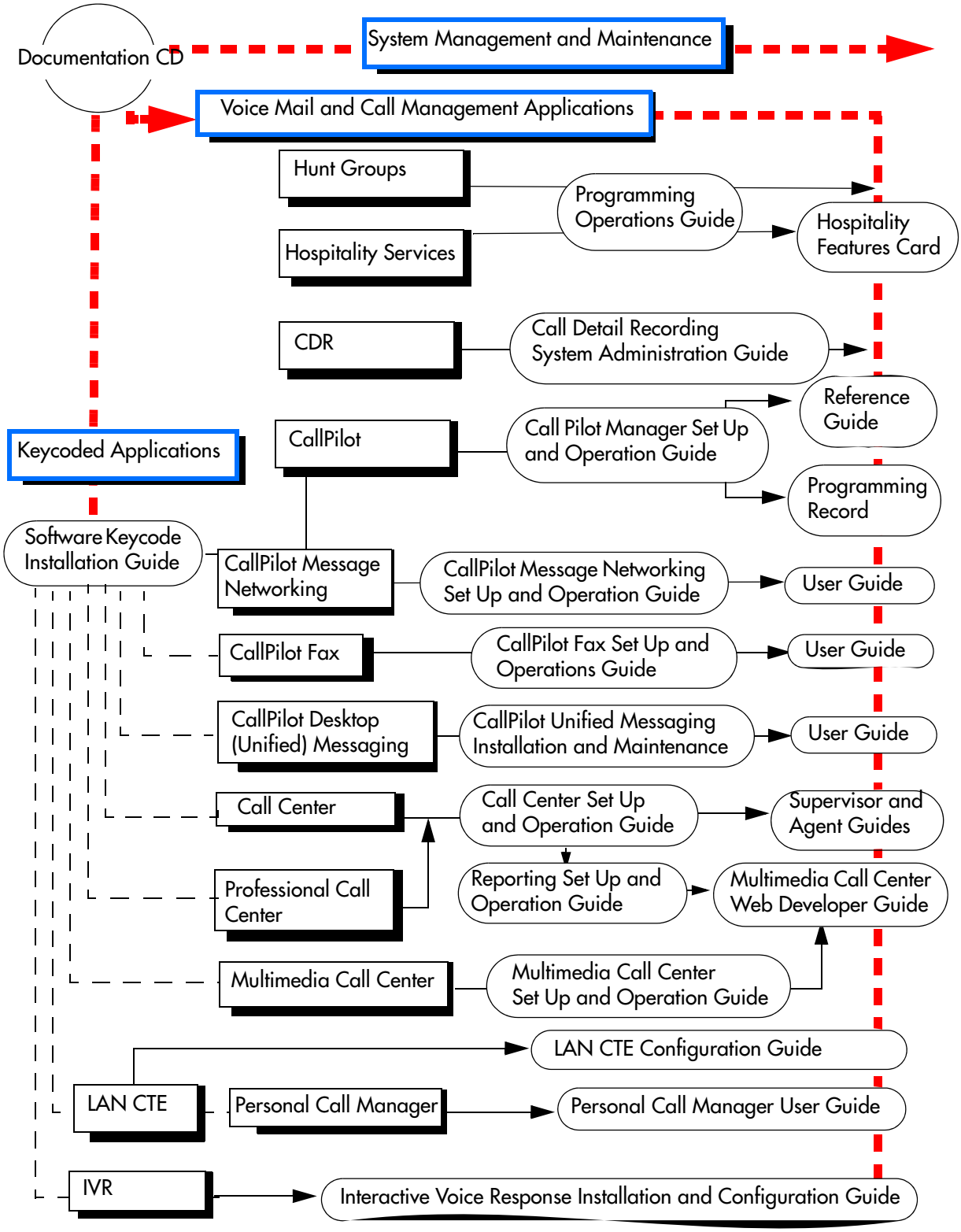
Installation documentation



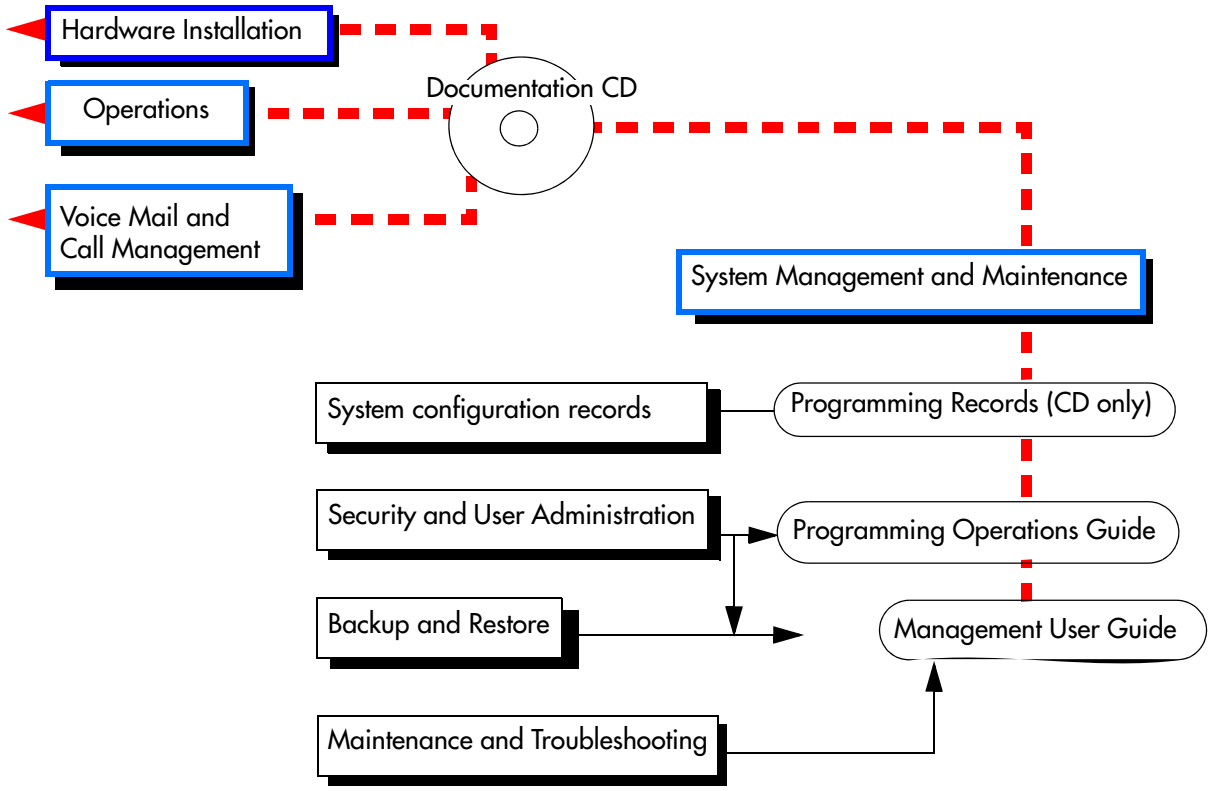
Operations documentation



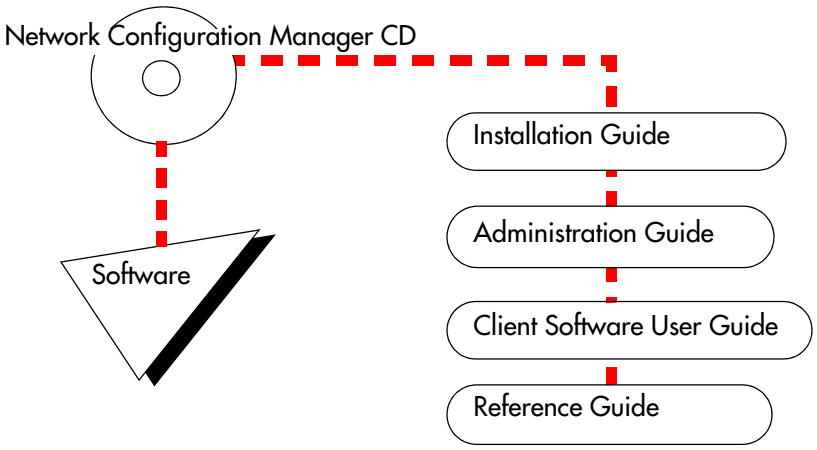
Call Management documentation



Unified Manager and hardware maintenance documentation



Multi-site Administration: Network Configuration Manager



How to get help

If you do not see an appropriate number in this list, go to *www.Nortelnetworks.com/support*.

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:

* European Freephone	00800 800 89009
European Alternative/	
United Kingdom	+44 (0)870-907-9009
Africa	+27-11-808-4000
Israel	800-945-9779

* Note: Calls are not free from all countries in Europe, Middle East or Africa

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: +61-2-870-8800

Fax: +61 388664644

email: asia_support@nortelnetworks.com

In-country toll free numbers

Australia 1800NORTEL (1800-667-835)

China 010-6510-7770

India 011-5154-2210

Indonesia 0018-036-1004

Japan 0120-332-533

Malaysia 1800-805-380

New Zealand 0800-449-716

Philippines 1800-1611-0063

Singapore 800-616-2004

South Korea 0079-8611-2001

Taiwan 0800-810-500

Thailand 001-800-611-3007

Service Business Centre & Pre-Sales Help Desk +61-2-8870-5511

Chapter 1
Introduction

The Business Communications Manager includes software and hardware components that provide telephony, voice messaging, interactive voice response (IVR), data networking, and IP telephony.

The web-based navigation tool, Unified Manager, provides easy access to all operations and maintenance programming on the Business Communications Manager system at a single site. For more information about Unified Manager, see "Using the Unified Manager" on page 82.

This section includes the following topics:

With the introduction of BCM version 3.5 software, there was an increase in the awareness of security in regards to access to the Unified Manager, both by administrative users and by client applications. The icon shown to the left, when used within this document, denotes points of security that you need to consider when setting up or using your system.

- This software includes a generic security certificate that provides an increased level of encryption ability. You can replace this certificate with a site-specific certificate. Since encryption levels have some dependencies to the version of Windows operating systems, the defaults are set at a mid-range level to allow for clients using earlier versions that do not support strict encryption requirements. You can reset these levels higher or lower.
- This version also provides more control over password policies, that allow you to determine the complexity of the passwords you want to assign to the users who do programming in the Unified Manager. You can also determine if you want the system to lockout users who have entered an incorrect password after a specified of times.
- Finally, a more secure front end application to the text-based interface is being introduced. The PuTTY application uses SSH to provide a secure connection to the text-based interface. The application is downloaded to a user's computer, rather than being resident on the Business Communications Manager, like Telnet.

The Network Configuration Manager provides multi-site network management. This process is described in a separate set of user guides.

Figure 2 on page 68, Figure 4 on page 70, Figure 5 on page 71, and Figure 3 on page 69 provide an overview of the processes for operating the Business Communications Manager system.

System configuration process maps

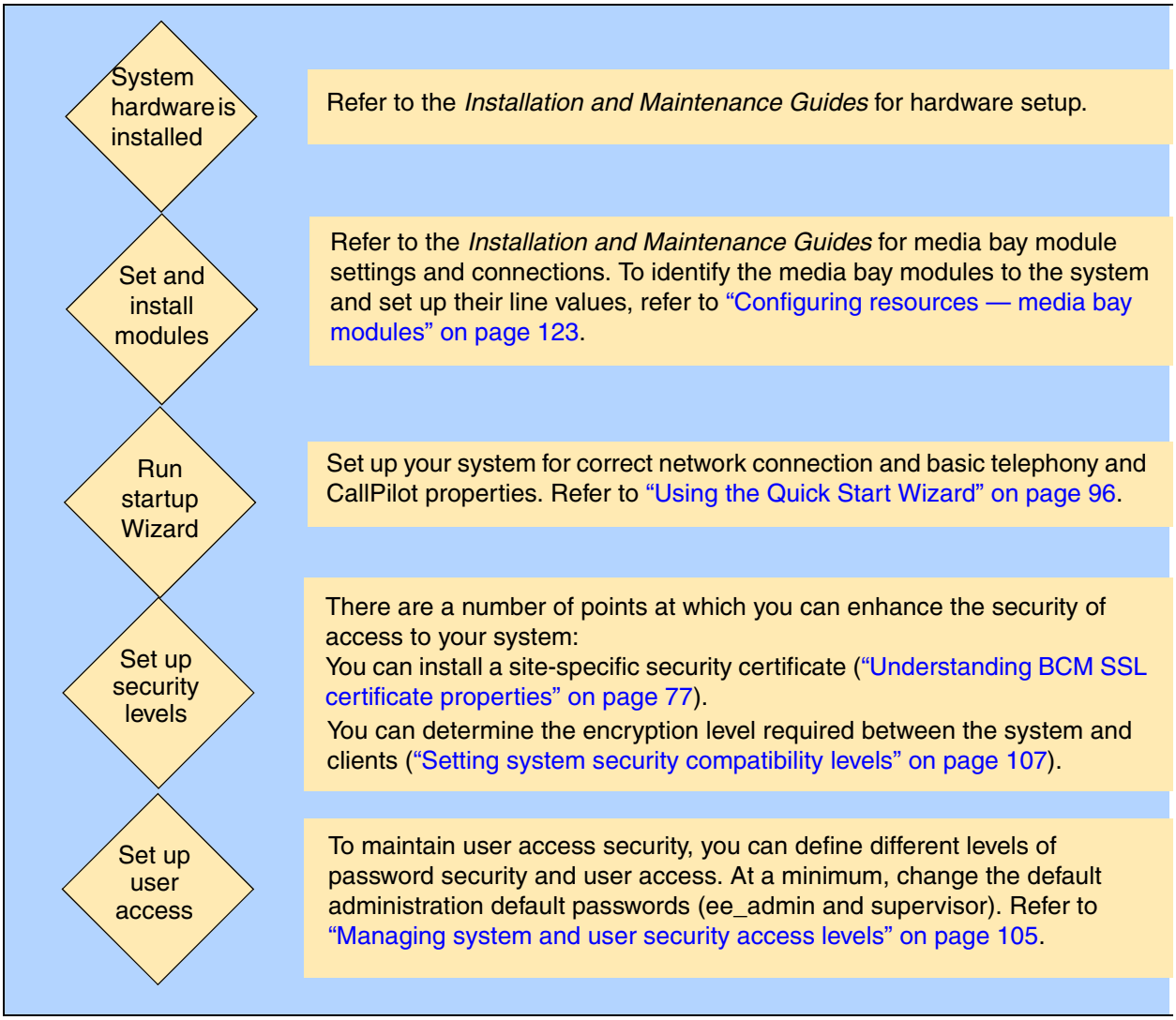
The following process maps show you the order in which your system is configured. Each section provides quick reference information about the step, plus a link to the process section.

- Initial system configuration
- “Configuring telephony components” on page 68
- “Optional keycoded features” on page 69
- “Data and IP telephony configuration” on page 70
- “Post-system setup features” on page 71

Caution: Programming affects system operation.
Only a qualified system administrator should perform startup, installation and maintenance programming. Many of the settings affect correct system operation.

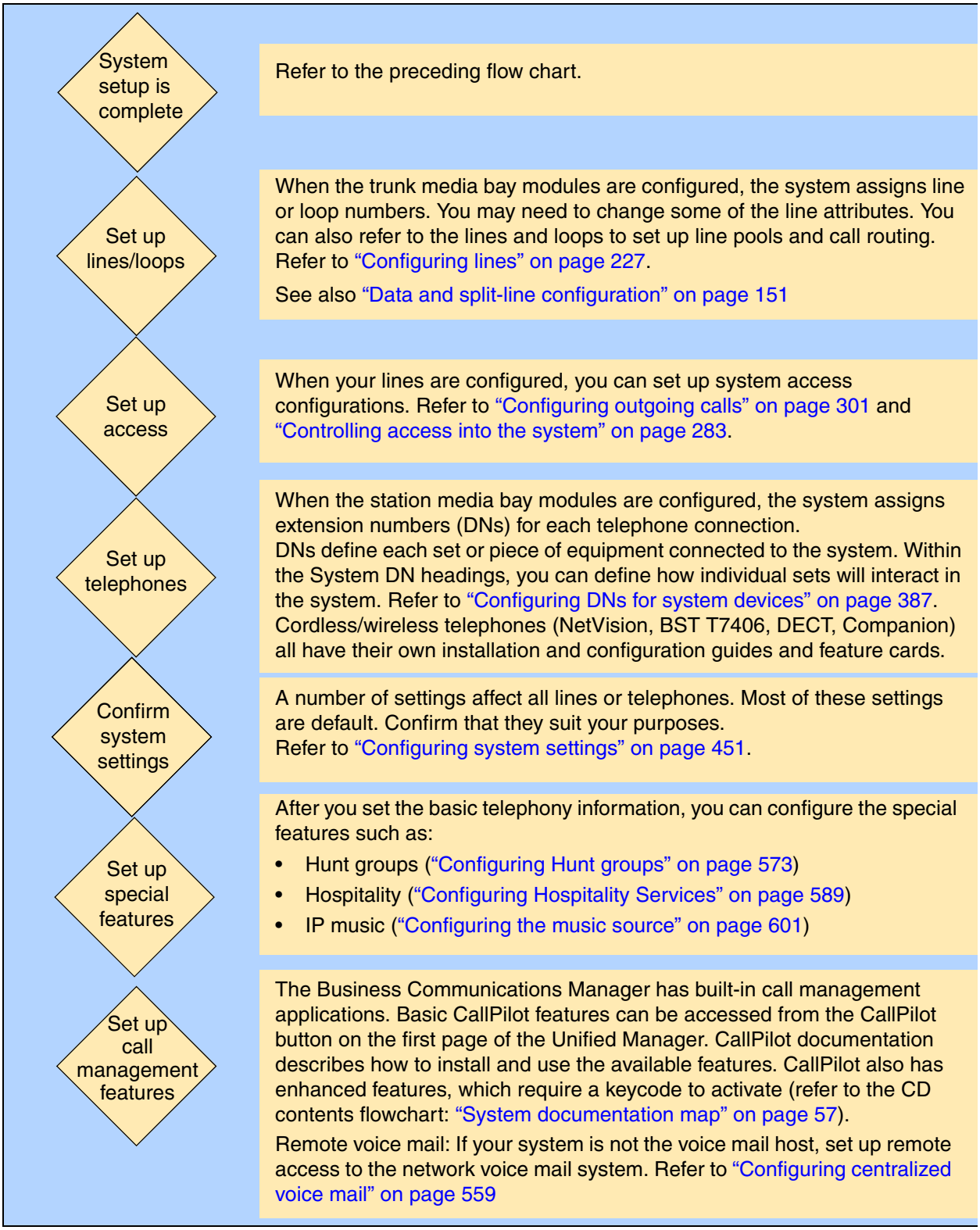
Initial system configuration

Figure 1 Process for initial system configuration



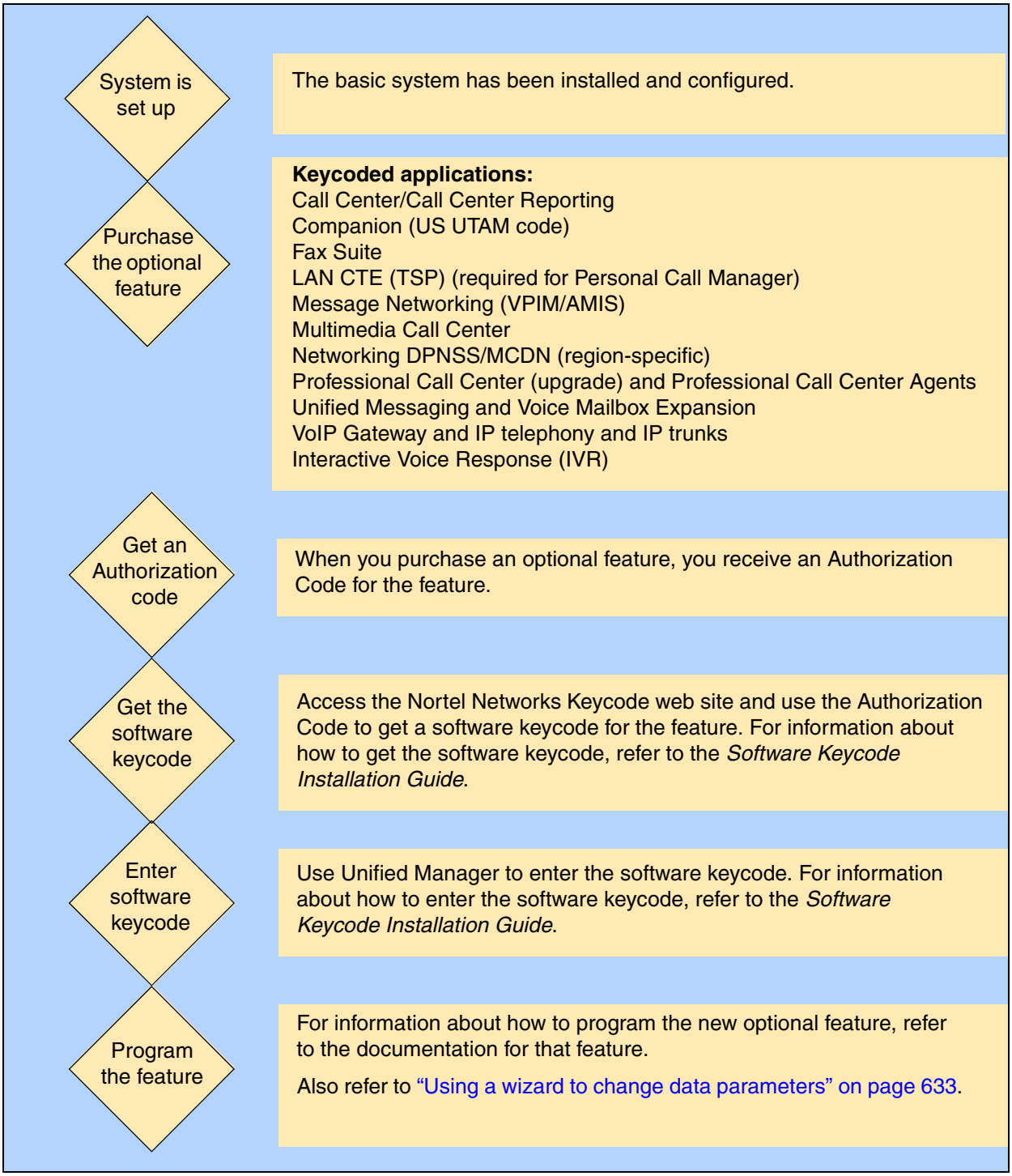
Configuring telephony components

Figure 2 Process for configuring the telephony components



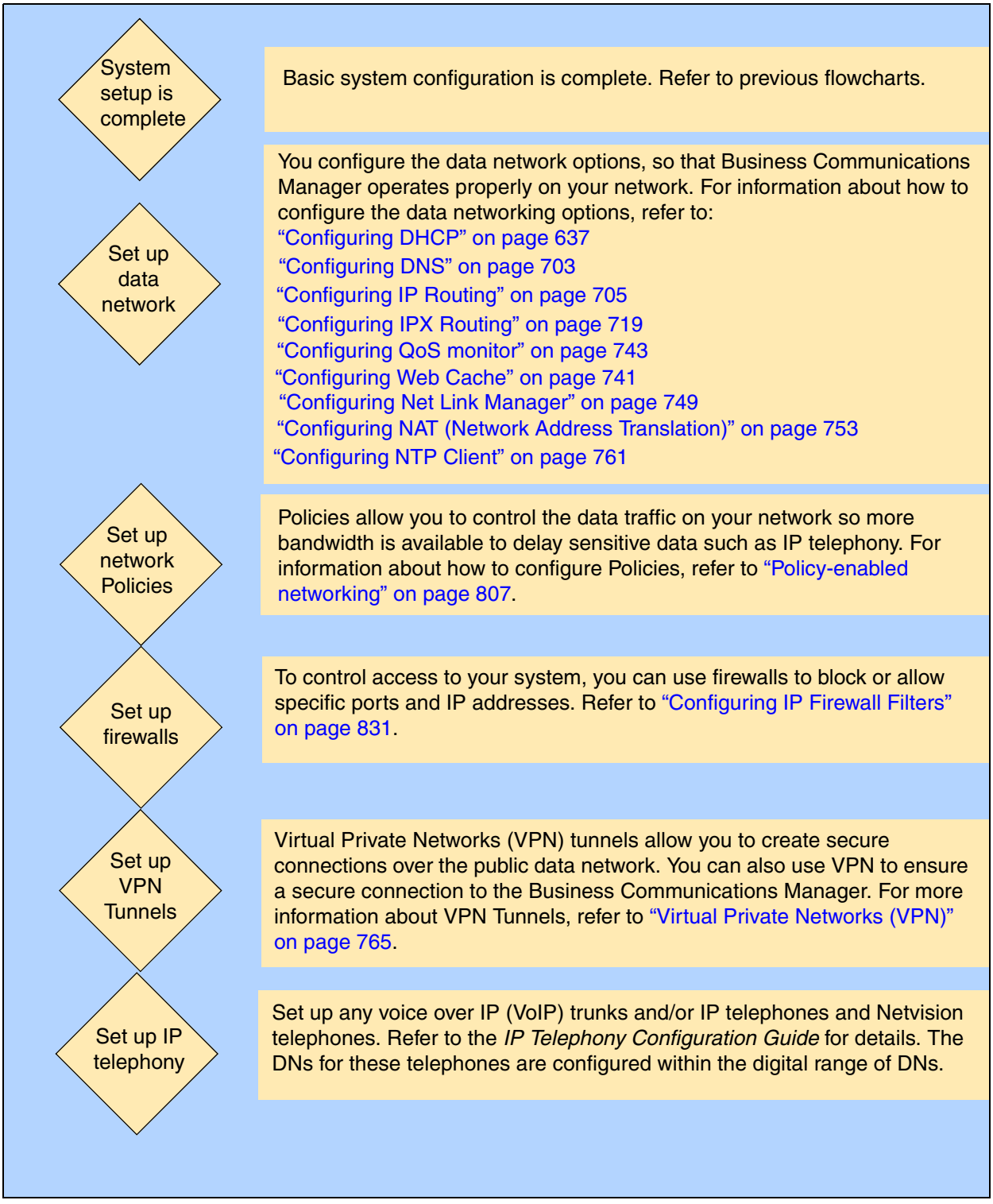
Optional keycoded features

Figure 3 Process for activating optional keycoded features



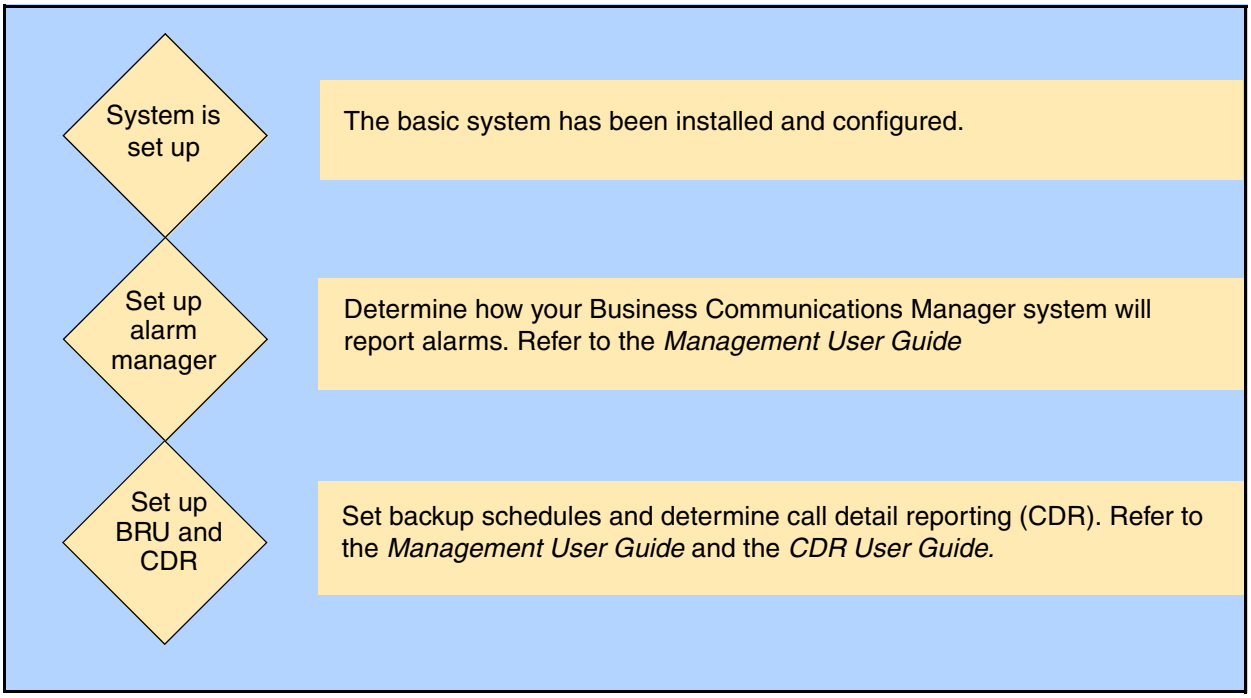
Data and IP telephony configuration

Figure 4 Process for configuring the data and IP telephony components



Post-system setup features

Figure 5 Post-setup processes



Finding your way around

The following sections provides you with quick links to the detailed configuration information:

Security and User Management

- Unified Manager access: "Getting started with Unified Manager" on page 77
- Security and user management: "Managing system and user security access levels" on page 105

Telephony programming quick access list

Configuration overviews and planning

- System configuration process overview: "System configuration process maps" on page 66
- Application overview: Getting started with Unified Manager on page 77
- Telephony Services overview: "Planning your telephony services" on page 188
- Quick reference section to telephony programming: "Telephony feature planning" on page 193

Lines and network configuration

- Configuring media bay modules: "Configuring resources — media bay modules" on page 123
- Configuring the PSTN lines: "Configuring lines" on page 227 and "Configuring BRI Loops" on page 265
- Configuring outgoing call programming: "Configuring outgoing calls" on page 301
- Configuring incoming and internal access: "Controlling access into the system" on page 283
- Configuring the public network access: "Configuring public networks" on page 499
- Configuring private network access: "Configuring private networks" on page 505, and "Configuring private networks with SL-1 MCDN" on page 519, or "Configuring ETSI QSIG and DPNSS network services" on page 543.
- Centralized Voice Mail (host or remote system and telephony settings): "Configuring centralized voice mail" on page 559
- ISDN general information: "ISDN overview" on page 869

Telephony configuration

- Using Wizards to configure telephones: “Configuring DNs using the Wizards” on page 369
- Using DN records to configure telephones: “Configuring DNs for system devices” on page 387
- Setting telephony system features: “Configuring system settings” on page 451
- Define telephony schedules: “Configuring schedules” on page 483
- Telephony features list: System Features on page 861

Special features

- Hunt groups: “Configuring Hunt groups” on page 573
- Hospitality Services: “Configuring Hospitality Services” on page 589

Reference material

- System profile tables: “Defining region-based defaults” on page 845
- Features available for programming on the telephone memory buttons: “Button programming features” on page 865

Data programming sections

- “Configuring the MSC resources” on page 609
- “Using a wizard to change data parameters” on page 633
- “Configuring DHCP” on page 637
- “Configuring the LAN resources” on page 663
- “Configuring the WAN resources” on page 669
- “Configuring the Dial Up resources” on page 685
- “Configuring DNS” on page 703
- “Configuring IP Routing” on page 705
- “Configuring IPX Routing” on page 719
- “Configuring QoS monitor” on page 743
- “Configuring Web Cache” on page 741
- “Configuring Net Link Manager” on page 749
- “Configuring NAT (Network Address Translation)” on page 753
- “Configuring NTP Client” on page 761
- “Virtual Private Networks (VPN)” on page 765 (tunnels)
- “Policy-enabled networking” on page 807
- “Configuring IP Firewall Filters” on page 831

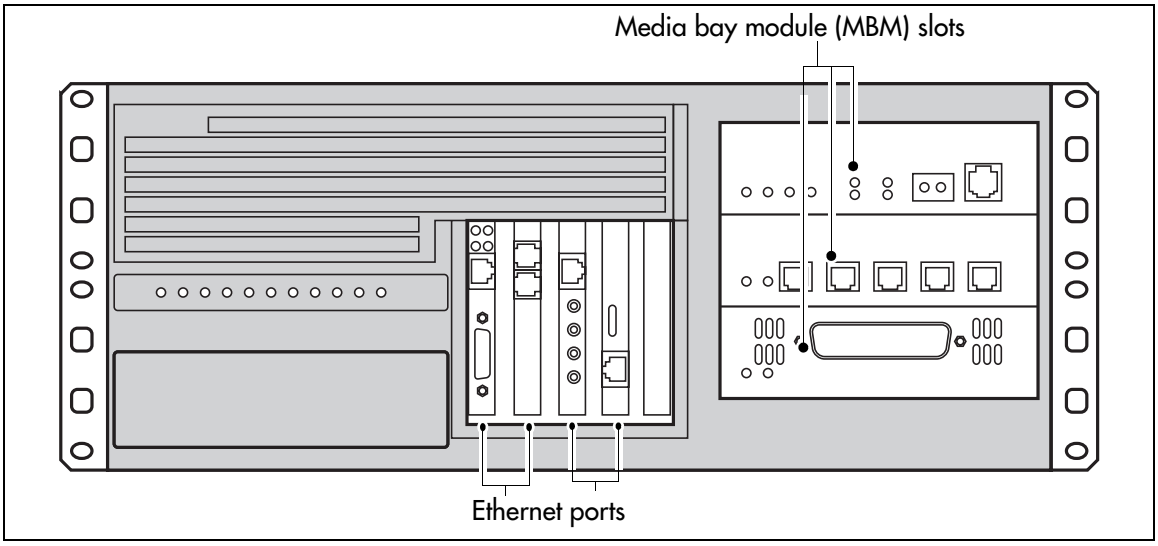
Business Communications Manager hardware

The main component of the Business Communications Manager system is the Business Communications Manager base unit. The Business Communications Manager base unit controls all tasks such as call processing, voice messaging, and data routing.

BCM1000 (legacy equipment)

If you have existing equipment, like the unit shown in the figure below (BCM1000), you can update the operating system with new Business Communications Manager software.

Figure 6 Upgradeable BCM1000



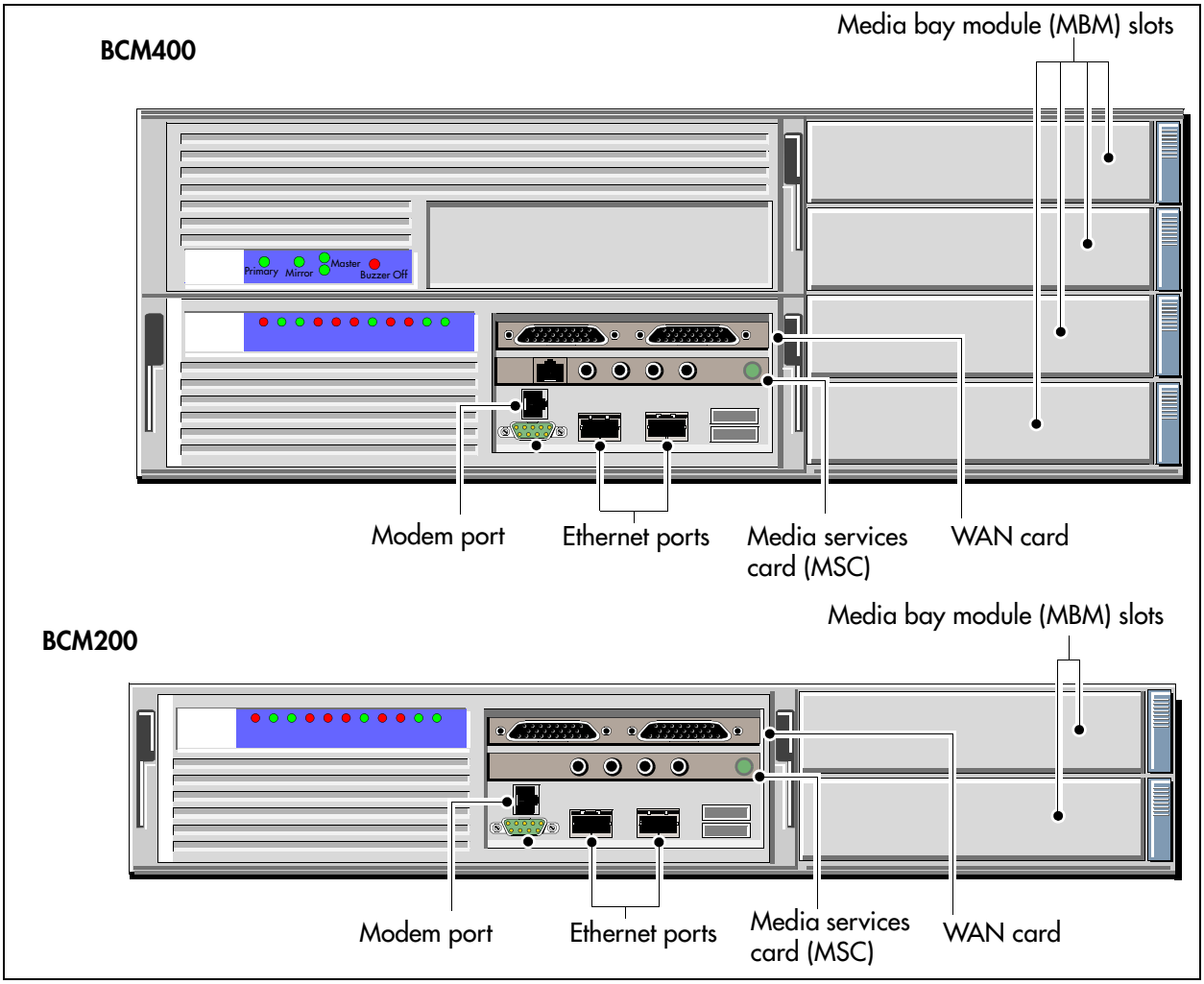
For a detailed description about maintaining these units, refer to the *Business Communications Manager BCM1000 Installation and Maintenance Guide*.

Note: Some of the components described in this section are not available in all areas. Ask your Nortel Networks Business Communications Manager supplier for information about the availability of components.

BCM200/BCM400 base units

In conjunction with the BCM version 3.0 system release, Nortel released two new base unit models to provide added flexibility for system planning. These systems come preloaded with the latest version of software. You cannot run versions previous to BCM 3.0 software on these units. However, you can reuse modules from previous versions of the system, if you are replacing old system hardware with the new BCM200 or BCM400 hardware (shown below). For a detailed description of this hardware, and how it is installed and maintained, refer to the *Business Communications Manager BCM200/BCM400 Installation and Maintenance Guide*.

Figure 7 BCM200 and BCM400 hardware



What do media bay modules do?

Media bay modules are key components of the system. They provide the link between the external lines (trunks), the Business Communications Manager applications, and the internal extensions (DNs), which connect to individual telephones.

The type of modules on your system depends on your set requirements and the type of lines available from your service provider. You need to determine this information before you order the system. For a detailed description of this hardware, and how it is installed and maintained, refer to the *Hardware Installation and Maintenance Guide*.

How does the system connect to the network?

The Business Communications Manager is designed to connect to your business network on a LAN and/or a WAN.

For data networking, the Business Communications Manager acts as a policy enabled router that optimizes data traffic and ensures consistent bandwidth for IP telephony, VoIP trunks, and mission critical data.

For telephony applications, the Business Communications Manager base unit acts as a switch and feature controller for the external lines and the internal extensions attached to the sets.

The IP telephone uses both data and telephony features to provide an network-based telephone that provides the call features of the telephony-based digital telephones.

Additional Business Communications Manager applications

The Business Communications Manager provides a number of software applications. Some applications work immediately after you install the Business Communications Manager system and access the Unified Manager. Refer to Chapter 2, “Getting started with Unified Manager,” on page 77 for a description of the Unified Manager interface.

To use other applications, you enable the application by entering software keycodes.

Keycodes are based on your system identification and an encrypted code that you obtain when you purchase the rights to an option. Refer to the *Software Keycode Installation Guide* for information about how to acquire a keycode and how to enter it. Each of these optional features has separate documentation which includes information keycodes and how to set up the application.

Refer to “Related publications” on page 56 for a list of the documentation for each of these applications. Also refer to “System documentation map” on page 57 for an overview of how these applications fit into the overall system.

Chapter 2
Getting started with Unified Manager

This section provides you with information about the Unified Manager, the tool you access on the Business Communications manager from your desktop and use to configure system information. This section describes the Unified Manager interface functions.

Warning: If the installer did not change the access password to the Unified Manager, you should do so at the earliest opportunity. Refer to "Managing access passwords" on page 109 for procedures for changing passwords and adding new users.

This section includes information about:

Security note: Multiple users logging on to the Business Communications Manager with the administrator account, from different client stations, can cause inconsistent or wrong configuration. Therefore, it is advisable to limit the number and distribution of administrator accounts.

Security note: The configuration section in the Unified Manager is not secured through SSL encryption. To provide security for this section, establish a VPN client tunnel. Refer to "IPSec Remote User configuration" on page 796.

Understanding BCM SSL certificate properties

When you first run the BCM version 3.6 software, you will note that the default Web access to the Business Communications Manager now utilizes SSL encryption for system security (BCM 3.5 and newer software). This includes the appearance of a security alert when you initiate a connection to the Unified Manager using SSL, which indicates site validation of the default certificate.

This security alert does not appear if you:

- add a site-specific certificate ("Uploading a certificate and a private security key" on page 78)
- suppress the message on your client browser ("Suppressing the security alert message" on page 79)
- use the non-SSL port (http:6800) ("Using the non-secure http:6800 port" on page 79)

The self-signed certificate that is included in the BCM version 3.6 software enables SSL encryption functionality, providing the necessary encryption keys. However, it does not address site authentication. Site authentication requires system-specific information such as an IP address, company name, and so on.

Note: Client applications do not need to install the certificate. The Business Communications Manager sends the certificate when it accesses the client application.

Uploading a certificate and a private security key

Obtain a site certificate for your Business Communications Manager from a CA (Certificate Authority) vendor. Certificate files must use the .PEM format. You will be provided with a certificate and a private security key. These are what need to be installed on the Unified Manager.

Security note: Ensure that you maintain a copy of your certificate and private security keys in a secure place, preferably offsite. This provides you with a backup if your system ever requires data re-entry.

1. Log on to the Business Communications Manager main screen.
2. Click on the **Maintenance** button.
3. You will be prompted to enter a system user name and password.
4. Click on **OK**.
   The main Business Communications Manager Product Maintenance and Support page appears.
5. On the left menu, click on the **Maintenance Tools** link.
   A web page showing a list of Maintenance Tools appears.
6. Under **Maintenance Tools**, **Security**, click the **Upload Certificate and Private Key** link.
   A web page displaying **Certificate** and **Private Key** fields appears.
7. Use the **Browse** button beside each field to locate the certificate and private key files.
   Both files must be uploaded at the same time.
8. Click the **Upload** button.
   Upload messages:
   - If the upload is successful:
     ```
     Certificate and Private Key Upload Was Successful!
     You must restart the Apache Service or Restart the BCM before the
     Settings will take Effect.
     ```
   - If the upload is unsuccessful:
     ```
     Certificate and Private Key Upload Was NOT Successful!
     The Certificate and Private Key do not match.
     Please upload a VALID Certificate and Private Key Combination!
     ```
9. Click on the **BCM** link beside **Your Location** to exit the maintenance pages.
10. To replace the default certificate with the new certificate and private key:

a Exit the Unified Manager.

b Log back into the Unified Manager.

Troubleshooting: Restoring the default certificate

If something happens to your private security certificate file, you cannot access the Unified Manager and you need to restore the default certificate. Contact your technical support team for assistance.

Suppressing the security alert message

If you do not want to add a site-specific security certificate, but you want to suppress the security alert message, you can use the Internet Explorer Security options to disable the warning.

1 Open Internet Explorer.

2 On the top menu bar, click **Tools** and select **Internet Options**.

3 Select the **Advanced** tab.
Note: Location of the following prompt may vary, depending on the version of Internet Explorer.

4 Scroll to the item **"Warn about invalid site certificates."**

5 If the check box has a check mark, click on the box to remove it. This disables this option.

6 Restart the browser.

Using the non-secure http:6800 port

If you choose not to use SSL on your system, you can disable the system prompt that forces secure web access. Refer to "Setting system security compatibility levels" on page 107. On the Security screen described in that section, choose **Disabled** for the **Force Secure Web Access** field.

Using the Unified Manager main page buttons

On the Business Communications Manager Unified Manager initial page, a number of buttons provide access to various parts of the Unified Manager. The purpose of each button is discussed in this section.

Security note: Ensure that you change the password after you first log on to Business Communications Manager. For information about how to change passwords, and how to define user profiles, refer to "Managing system and user security access levels" on page 105.

Locating Wizards

The Wizards are self-contained task applications that you can use to speed up some configuration tasks. The access icons for the Wizards are located on the Setup and Management Wizards page, which is accessed through the Wizards button on the start page of the Unified Manager.

These are the wizards that are available from this page:

- **Quick Start Wizard:** initializes the system and sets up your basic system information. This wizard is only run once, when your system is first set up. Refer to "Using the Quick Start Wizard" on page 96.
- **Add Users Wizard:** allows you to change the telephony settings for a set of DNs or for a single DN. You can define the settings in this Wizard, or you can use a pre-defined template, from a local site or from a remote site, created with the Edit DN Record Template wizard. Refer to "Creating telephone records with the Add Users Wizard" on page 375.
- **Edit DN Record Template Wizard:** allows you to select Telephony User Templates and change and define the user settings for telephones. The Telephony Template is stored in a file for use with the Add Users Wizard. Refer to "Editing DN Record Templates" on page 369.
- **DN Renumber Wizard**: renumbers a range of DNs. Refer to "Using a wizard to renumber telephone DNs" on page 367.
- **Network Update Wizard**: allows you to update your system data network settings any time after the Quick Start Wizard was run, which sets the initial network setup. Refer to "Using the Network Update Wizard" on page 634.
- **DECT Mobile Recording Wizard:** allows you to enable/disable mobile recording for one of the base station ports.
- **DECT Configuration Wizard:** allows you to easily configure a DECT module. It also turns on one of the base station ports to allow mobile recording (handset registration).

  Note: The DECT Wizards only appear on the Wizards page if there is a DECT module installed and identified to the system. These wizards are discussed in the *DECT Installation and Maintenance Guide*.

Navigating the wizards

These are some helpful hints about how the wizards work, and how to use them.

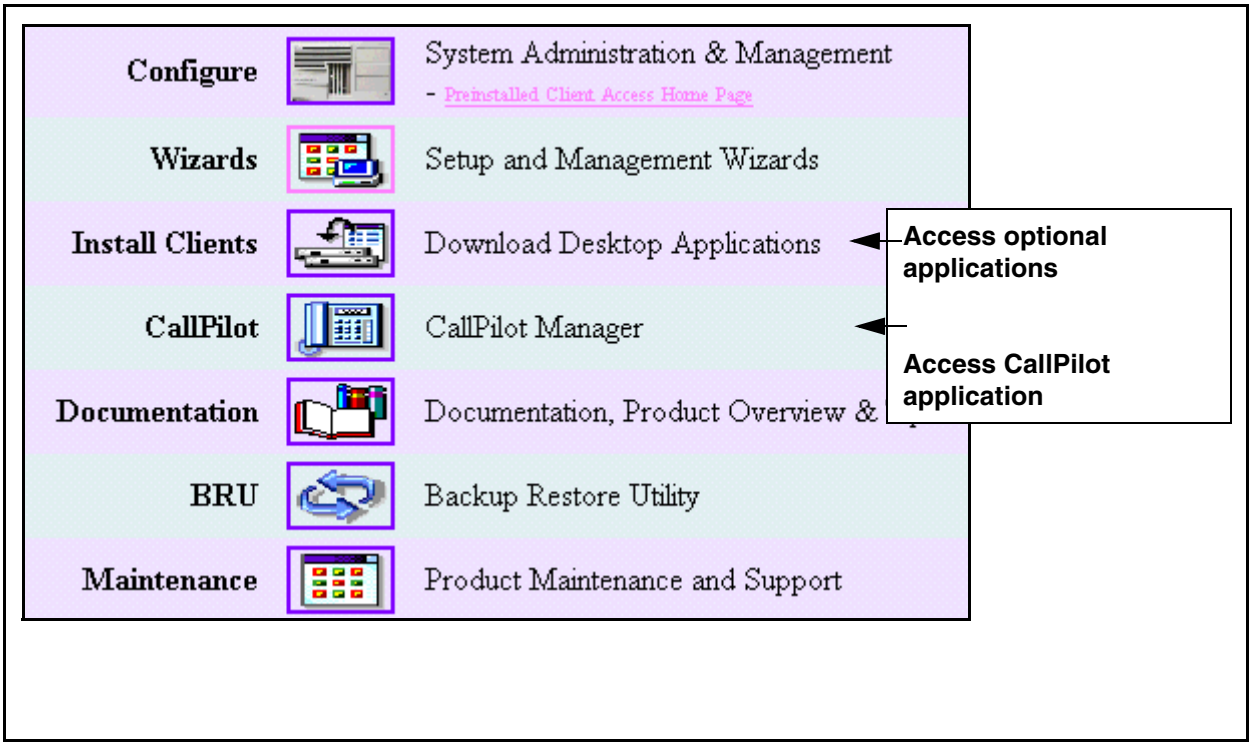
- To open the online help, from the Programming Wizards screen click the **Programming Wizards Help** link.
- You can move back and forth between screens in the wizards by clicking the Back and Next buttons.
- You can revise your choices and entries on any of the wizard pages until you click the Apply button. Once you click the Apply button, the system proceeds to apply the selected configurations. The user is presented with a confirmation box that provides the approximate timing of the process. To check the status of the configuration, press the Refresh button. When the process is complete, the title of the page has the word *completed* as part of the title.

Locating optional features from the main page

After you set up the system and it is operating, you can add the keycodes for any optional features you want to include.

You access the optional applications, including those which require keycodes, through the **Install Clients** button.

The program that manages CallPilot is accessed through the **Call Pilot** button.



For information about how to set up these optional features, refer to the documentation for each application.

Note: Basic CallPilot functions are standard on the Business Communications Manager and you define your region and basic settings when you run the Quick Start Wizard. Refer to "What you need to know before you use the wizard" on page 93. If you are using this call pilot as the voice mail host to other systems, you may need to set up areas of the Unified Manager, as well. Refer to "Configuring centralized voice mail" on page 559.

Finding documentation from the main page

Use the **Documentation** button to find the information you require to help you understand and configure your system to your specifications. The entire Business Communications Manager documentation suite, plus a number of training panels, are included on your Business Communications Manager computer, as well as on the CD that accompanied your system.

The Programming Records are on the CD only.

Using BRU from the main page

The **BRU** (Backup and Restore Utility) button, allows you to ensure the integrity of your system data by providing a way to back up your system data and configurations in the way that is most useful for your purposes. Backed up data can be restored to the Business Communications Manager should a system failure occur, such as a prolonged power outage. The *Management User Guide* describes how to use this feature.

Accessing maintenance information from the main page

The **Maintenance** button accesses a number of maintenance tools that allow you to determine the current status of the various aspects of your Business Communications Manager system. The *Management User Guide* describes how to use these tools.

Using the Unified Manager

Most changes made with Unified Manager become part of current Business Communications Manager programming when you select an item from the menu options. However, some changes take effect after you exit the screen. If a programming error occurs, you must reenter the original programming.

This section describes the various parts of the configuration main screen:

- Business Communications Manager system access
- Unified Manager screen display
- “Understanding the dynamic menu” on page 84
- “Understanding the navigation tree headings” on page 85
- “Understanding tabbed pages” on page 87

Business Communications Manager system access

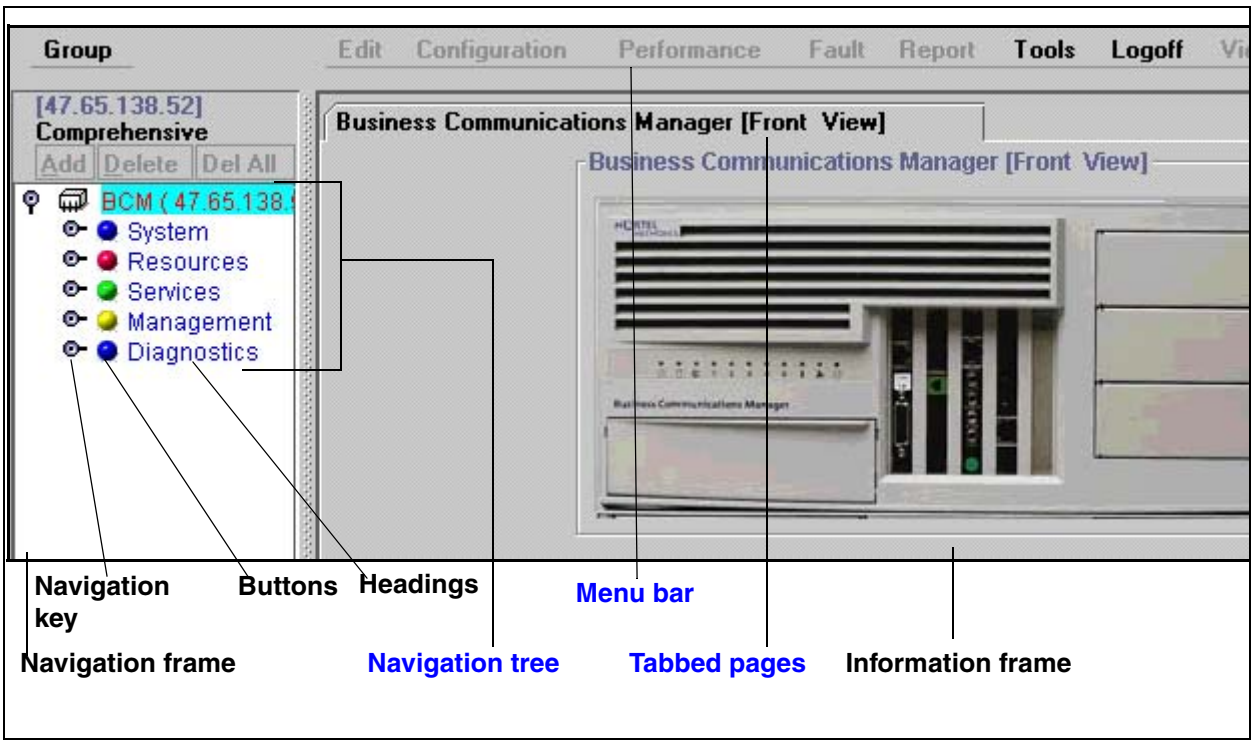
You must control system access by providing one user id, the administrator, with read-write privileges. Give all other users selected access privileges to control the possibility of concurrent configuration of the Business Communications Manager system. For information about defining user profiles and passwords, see “Managing system and user security access levels” on page 105.

Unified Manager screen display

The Unified Manager screen display, shown in the figure below, consists of:

- a menu bar, where users access configuration commands
- a navigation frame that displays the navigation tree you use to navigate through Business Communications Manager programming headings
- an information frame that displays the windows related to the headings you select in the navigation frame

Figure 8 Main display of the Unified Manager



The menu bar contains configuration management options. When you select the different headings in the navigation tree, these options are enabled. If an option appears dimmed, it is not available for the heading you have selected.

The navigation tree contains headings that allow you to access specific areas of the Business Communications Manager system. The key symbol (⚲) beside each heading indicates that the heading can be expanded to show sub-headings. To display sub-headings, double-click the item or just click on the key itself. As you select various headings in the navigation tree, the heading changes color and Unified Manager displays the appropriate information frame.

Note: If you receive the error message `Telephony programming is currently not available. Please try again later.` when you click on one of the headings, this means that the part of the system that handles MSC is doing a reset. Wait about one-and-a-half minutes and try again.

The information frame can contain configuration windows or dialog boxes indicating the appropriate action or showing system messages or warnings.

Understanding the dynamic menu

You access some of the Business Communications Manager functions using the top menu bar. This menu bar is dynamic. Commands become active or inactive depending on the heading you select from the navigation tree in the left frame. The following table defines the menu bar top-level items.

Table 2 Menu bar items

Menu item	Description
Group	View the system, resources, services, and management.
Edit	Edit parameters.
Configuration	Access configuration dialog boxes and screens.
Performance	Access performance graphs and tables.
Fault	Access fault management settings.
Report	Generate a report.
Tools	Use Business Communications Manager tools.
Logoff	Log off, reboot or shutdown the Business Communications Manager base unit.
View	Refresh the information window to reflect configuration changes.
Help	Access online help.

Refer to the figure in "Unified Manager screen display" on page 83.

Understanding the navigation tree headings

The Unified Manager navigation tree contains five main headings that allow you to access specific areas of the Business Communications Manager system. These headings are described in the following table.

Table 3 Navigation tree menu functions

Heading	Programming
System	Provides access to **Licensing**, **Identification** and **Security** subheadings. This includes a form to enter keycodes, and a list of current supported services. The Security heading provides screens that allow you to determine the level of security within and entering the system. Refer to "Managing system and user security access levels" on page 105. When you select the **System** heading, you can view system information such as your system name and a description about which resources and services are available. Selecting the **System** heading also enables the following menu options: **Configuration**, **Performance**, **Fault**, **Logoff**, **View** and **Help**. These menu options provide access for you to: • enable/disable services • access CPU and memory status • access to the alarm banner, which displays totals of alarms • access or refresh a system inventory list • perform system reboot or shutdown operations Also refer to the Management User Guide.
Resources	Provides access for configuring data and telephony resources for Business Communications Manager hardware setup. This information is included in "Configuring resources — media bay modules" on page 123, "Data and split-line configuration" on page 151, "Configuring the LAN resources" on page 663, "Configuring the WAN resources" on page 669, "Configuring the Dial Up resources" on page 685, and "Configuring the MSC resources" on page 609, as well as in the *DECT Installation and Maintenance Guide*.

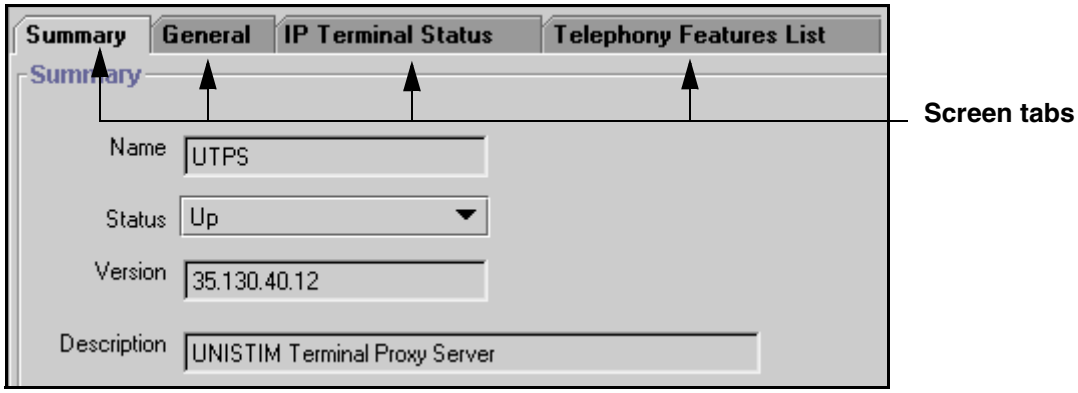
Table 3 Navigation tree menu functions (Continued)

Heading	Programming
Services	Provides access for configuring telephony and data networking services and various other related services. Telephony information is discussed from Chapter 7, "Telephony Services overview," on page 183 to Chapter 31, "Configuring the Dial Up resources," on page 685 and in the *IP Telephony Configuration Guide*. / Doorphone configuration is located in separate documentation. System data configuration is discussed from Chapter 32, "Configuring DNS," on page 703 to Chapter 42, "Configuring IP Firewall Filters," on page 831. This section also supports the information found in the CallPilot documentation, and the documents for CDR Recording, LAN CTE, IVR, Doorphone, Network administration, universal power supply, UPS) document, and *DECT Installation and Configuration Guide*. The Management User Guide provides information about SNMP, Alarm Service, and NetIQ. To manually enable or disable the Telnet service, refer to "Manually activating Telnet" on page 90.
Management	Provides access to the User Manager, which you use to manage the users who have access to the Unified Manage ("Managing system and user security access levels" on page 105), and to the Alarm Manager, which is used to define why types of alarms get reported by the system. The latter information is discussed in the *Management User Guide*.
Diagnostics	Provides access to items that allow you to generate and access statistics on different system components. Business Communications Manager provides statistics, metrics and event logs on resources and services to help you carry out system maintenance activities. For more information about using diagnostics tools, refer to the *Management User Guide*. System metrics information is contained in the programming section to which they apply. Refer to "Viewing CbC limit metrics" on page 343, "Using Hunt group metrics" on page 587, and the *IP Telephony Guide*. Split DS30 configuration and double density configuration are located under the Configuration menu of the MSC heading. These system features are discussed in the section that discusses MSC configuration. Refer to "Changing the DS30 Split" on page 629 and "Configuring Double Density" on page 630.

Understanding tabbed pages

Some headings display records that have more than one level. Each level is accessed by clicking the appropriate tab at the top of the screen.

Figure 9 Tabbed page example



Using Unified Manager Help

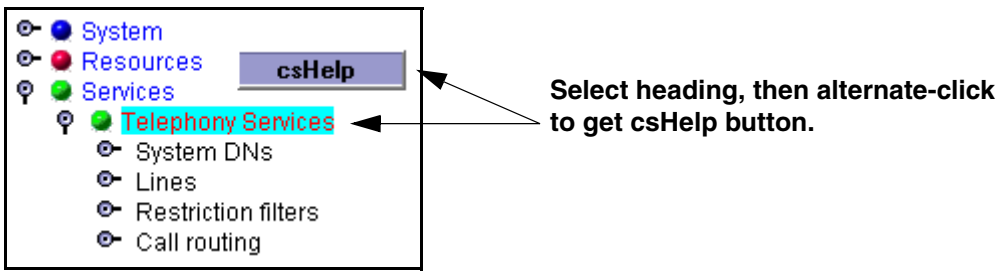
As noted in "Understanding the dynamic menu" on page 84, the dynamic menu has a Help heading. This heading allows you to access help topics relevant to active navigation tree headings and screens. Each navigation tree heading and tab also has an alternate-click help link.

The help pages open in a new web-based window. Each help page also have navigation tools that allow you to move back or forward to find other help topics.

Viewing help for navigation tree headings

1. Highlight the heading for which you want to view help.
2. Alternate-click anywhere in the left pane to get the **csHelp** button.
3. Then click normally on the **csHelp** button to open the help web page.

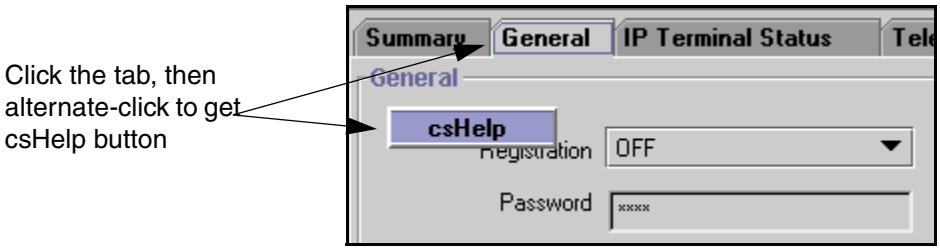
Figure 10 Accessing navigation tree heading help



Viewing help for tabs

1. Click on the tab to make it the active screen.
2. Alternate-click anywhere in the right pane to get the **csHelp** button.
   Note: Some tabs may have other headings as well.
3. Then click normally on the **csHelp** button to open the help web page.

Figure 11 Accessing navigation tree heading help



Logging off

When you have finished a session on the Unified Manager, you need to log off correctly to protect the integrity of the information you entered.

1. Choose **BCM (<*IP address*>)** at the top of the navigation tree.
   The **Logoff** menu is enabled.
2. Click **Logoff**, then select **Logoff**.
   A message appears that asks you to confirm your request to log off.
3. Click **Yes** to continue.
4. A second message appears reminding you to close your browser window after the system has logged out. Click **Yes** to continue.

   A Logoff progress bar appears. When it the logoff is complete, the browser display will revert to the Login screen.
5. Click the Windows exit icon (top, right corner).
6. Click the Windows exit icon on the browser window displaying the Business Communications Manager main menu.

   Note: Exit both Unified Manager browser windows, even if you want to re-log on to the Configuration area. Once you have exited both windows, you can re-establish a connection with the Business Communications Manager and log on as usual.
   Failure to log out of both browser windows could result in a failed attempt to re-enter the Unified Manager Configuration section.

Using the SSH client to access the text-based interface

Some operations for the Business Communications Manager, such as initializing a new hard disk, use a text-based interface. In previous versions, the Telnet application was used to access the Business Communications Manager text menus. BCM version 3.6 software introduces the ability to securely access the Business Communications Manager through a network connection using SSH server software. SSH service software is from SSH Communications Security (www.ssh.com). The SSH client application, called PuTTY, can be downloaded from a link under the Install Clients button on the Business Communications Manager first page. Refer to Installing PuTTY. Refer to "Using PuTTY" on page 89 for detailed information about using the client to access the Unified Manager text-based menus.

Users require an administrator-level password to use either PuTTY or Telnet.

Security note: You can still use Telnet for direct connections through a crossover cable, since network security is not an issue in this case.
If you want to use Telnet over the network, you need to manually start the service. Refer to "Manually activating Telnet" on page 90.

Installing PuTTY

The PuTTY application resides on your computer. It provides an access interface that allows you to connect to the text interface used by the Business Communications Manager.

1. On the Unified Manager front page, click the Install Clients button.
2. On the resulting web page, go to the bottom of the left column.
3. Under **Administrative Tools**, click **SSH client**.
4. On the SSH Client page, click the button beside **Download SSH Client**, at the bottom of the right pane.
   The application downloads to your computer.
5. On your computer desktop, double click **Putty.exe**.
6. Follow the steps in the install Wizard to install the application.

Using PuTTY

1. Click the shortcut PuTTY icon.
   The PuTTY Configuration screen appears.
2. Click on the radio box beside **SSH**.
3. In the **Host Name (or IP address)** box enter the IP address or the Fully Qualified Domain Name for the Business Communications Manager you want to connect with.
4. Click **Open**.

5 The first time you enter the application you may receive a security notice. Click **OK**. The PuTTY text screen appears.

6 At the login prompt, enter an administrator-level user name.

7 Press <**Enter**>.

8 At the next prompt, enter the corresponding password.

9 Press <**Enter**>.

10 The Business Communications Manager Main Menu appears.

11 Refer to the specific tasks that require this menu for details about using this it.

Manually activating Telnet

If you choose to continue operating the text-based menus with Telnet, rather than using the PuTTY client, you can manually activate the service from the Unified Manager.

Security note: Using the Telnet interface poses a security risk since the Telnet protocol is not encrypted.

Note: If you are using a cross-over cable to make a direct connection, Hyperterminal is still enabled, regardless of the status of Telnet on the system.

1 Click the key beside **Services**.

2 Click on **Telnet**.

3 On the Telnet screen, change **Status** to **Enabled**.

Chapter 3
Configuring system parameters

This section describes how to configure the basic programming information onto your new Business Communications Manager system using the Quick Start Wizard. This wizard allows you to choose the network and default telephony information that you want to use as the basic parameters for your system. This includes choosing a system software and companding law protocol.

Refer to the *Installation and Maintenance Guides* for information about installing Business Communications Manager hardware.

Warning: If you are installing this Business Communications Manager as a replacement for an existing system, you must ensure that the system has been re-initialized and the Region is correct.
This is especially important if you have a DECT system that requires the µ-law companding law protocol. Refer to the *DECT Installation and Maintenance Guide* for information about setting up a DECT system that requires the µ-law protocol.
Once the system is re-initialized using the Quick Start Wizard, you can restore system programming from the latest backup file taken from your old Business Communications Manager.

This section also describes how to change some of the system settings after the Quick Start Wizard has been run.

Information in this section includes:

Wizard Warnings
Read the Warnings in this chapter before you attempt to use any of the wizards.

Accessing the Wizards

You can access all the Business Communications Manager wizards through the Wizards button that appears on the first page of the Unified Manager.

If the Quick Start Wizard button does not appear, it means the Wizard has already been run on this system. You can allow the button to appear again by clicking the **Enable Quick Start** link. However, if you run the Wizard again, you will wipe out all system settings and data.

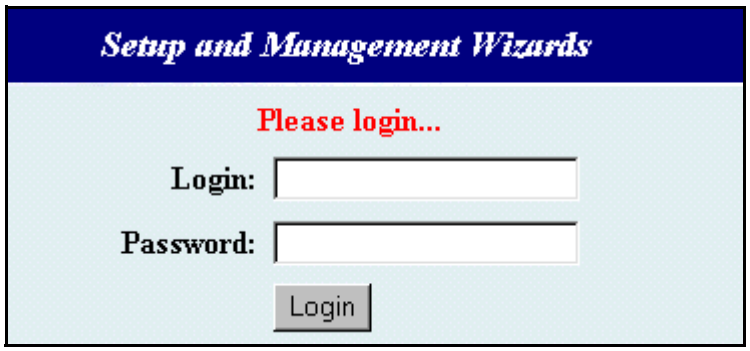
Refer to "Locating Wizards" on page 80 for a description of the function of the other wizards which are accessed through the icons on the Setup and Management Wizards page.

1 Open up the Unified Manager.

Refer to "Getting started with Unified Manager" on page 77 if you need instructions.

2 Click the **Wizards** button.

A login dialog box appears.



3 In the **Login** field, type your login name.
The default login name is `ee_admin`.
Note: You must have administrator-level privileges to use the wizards.

4 In the **Password** field, type your password.
The default password is `PlsChgMe!`.

5 Click on the **Login** button.
The Wizards page appears with all the Wizards icons.

READ first: "Wizard Warnings".

Then refer to these sections for details about "What you need to know before you use the wizard" on page 93, "Using the Quick Start Wizard" on page 96, and "Entering information into the Quick Start Wizard" on page 97.

Wizard Warnings

Read the following Warnings before you attempt to use any of the Wizards.

Warning: Users

Unified Manager allows multiple users to log on to the Business Communications Manager system. If more than one user logs on to configure the same or related subsystems, the most recent modification remains in effect and overwrites changes previously made.

Maintain one user profile with system administrator privileges. If you have more than one system administrator, you must plan configuration changes carefully. Refer to "Managing system and user security access levels" on page 105.

Warning: Wizard timeouts

When the `Wizard Instance Timeout` message appears, it indicates that the wizard was inactive for 30 minutes, the wizard has already been applied, or the Business Communications Manager or the server-side wizard component was restarted.

Warning: Operations during Wizard application

Do not use Windows NT login sessions while you are using the wizards or while there are wizards being applied.

What you need to know before you use the wizard

Use the following table to enter information that you want to enter into the wizard.

Screen 1, General information	
• What do you want to call your Business Communications Manager?	(System Name)
• What region do you want to use for the Business Communications Manager CallPilot system? Refer to "CallPilot regions" on page 859 for a description of the available choices. If you do not specify a region, the system defaults to North America.	(CallPilot Region)
• What time zone is your system in?	(Time Zone)
Screen 2, Data information (which fields appear will depend on your current data hardware configuration)	
• LAN settings	
IP address	LAN 1: LAN 2:
Subnet mask	LAN 1: LAN 2:

Primary Wins Address	LAN 1: LAN 2:
Secondary Wins Address	LAN 1: LAN 2:
• WAN settings	
IP address	WAN 1: WAN 2:
Subnet mask	WAN 1: WAN 2:
Port (read-only)	WAN 1: T1 WAN 2: V.35
Link Protocol	WAN 1: WAN 2:
• Default Next Hop Router What is the IP address of the next router or link on the network?	(Next Hop on Primary Link)
• DNS What is the domain name of the DNS server?	(IP Domain)
What are the IP addresses (primary and secondary) for the server? Note: Use a space to separate the groups of numbers.	<xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
Screen 3, Telephony information	
• What is the mobility protocol your system requires? For more information, refer to "Mobility services by region" on page 848.	(Mobility protocol) CT2+ Etiquette DECT
• What is the carrier profile that your system requires? **TIP:** most North American systems use a T1 protocol, while most European-base systems use E1 Refer to "Core software and regions" on page 846.	(Carrier protocol) E1 T1
• What is the telephony Region where your system is located? Refer to "Core software and regions" on page 846 if you do not know your region.	(Region)
• Software Version (determined by choice of Region)	read-only
• What system template do you want to use for your system?	(Default template) PBX DID
• How many digits will you be using for your system extensions (DNs)? Remember, if your system is part of an MCDN or tandem network, this must be the same length as in all the other nodes if you are using a Uniform dialing plan (UDP).	(Start DN Length)

• What extension (DN) do you want to start at for your sets? Note: the number of digits must agree with the Start DN Length. Default: 221.	(Start DN)
Received # length This setting determines how much of an incoming public telephone number the system reads to identify a telephone in the system. **Notes:** • The fields default to the number entered in the Start DN length field. When you manually change the value for one or both of these fields, the system does not attempt to update the field. • If the Template field is set to DID, these fields are read-only	(Public length)
• What is the received number length for the Private network?	(Private length)
• What is the received number length for the network? The default is equal to the number of digits entered in the Start DN length field.	(Public length (max))
Ignore the following questions if you do not have IP telephones on your system.	
• Are you planning to deploy a large number of IP telephones? The field beside **3/5 DS30 Split to increase IP telephony capacity** determines how many voice channels the Business Communications Manager provides. If you need more information to help you decide, click the **help** link. You can also refer to Chapter 26, "Configuring the MSC resources," on page 609.	No = 2/6 split (default) Yes = 3/5 split
• Do you want to be able to immediately start registering Nortel IP terminals on the system?	(Registration) On Off
• Do you want to change the default IP telephone access password? This is the password that installers will need to enter before they can configure an IP telephone in the field.	(Password)
• Do you want the system to automatically assign extension numbers (DNs) to your IP telephones when you install them?	(Auto Assign DNs) On Off
Screen 4, CallPilot Initialization (complete this section if you intend to use CallPilot on your system.	
• Do you want to initialize CallPilot on your system?	(Call Pilot System Initialization) Yes No
• Do you want to create a new System Administrator password? (Default: 0000)	(System Administrator Password)
• If you create a new password, retype it in this field.	(System Administrator Password Confirmation)

• Do you want to specify an Attendant DN length? This DN must be the same length as the DN length you specified on the Telephony page.	Attendant DN
• Which system are you going to use for your primary interface?	(Primary UI Style) NVM CallPilot
• In which language do you want your system prompts to appear? The wizard will enter a choice, based on your selection of the CallPilot Region on the General Page. You can change that default choice here.	(Primary Language)
• Do you want to initialize Auto-attendant?	(Auto-attendant Initialize?) Yes No
• If you choose to initialize Auto-attendant, enter the line and ring information. First line in the range you want to assign to the Auto-attendant. Last line in the range you want to assign to the Auto-attendant. Number of rings before Auto-attendant answers.	**from line:** **to line:** **number of rings:**

Using the Quick Start Wizard

Use the Quick Start Wizard to set the basic capabilities of your system, such as the name of your system, the CallPilot profile, basic data setup, and the telephony region and template.

Do not use this wizard until you have read and complied with the warnings printed in "Wizard Warnings" on page 93.

You can access a Quick Start Wizard from either a serial port connection or a LAN connection. The appearance will be slightly different, but the information required is the same. If you have not already connected your computer to the Business Communications Manager base unit, refer to the *Installation and Maintenance Guide* for details. To use the Unified Manager wizard, refer to "Entering information into the Quick Start Wizard" on page 97

To help you fill out the wizard, you can print out or copy the pages in "What you need to know before you use the wizard" and collect all the information that you need before you run the wizard.

Warning: Running the Quick Start Wizard

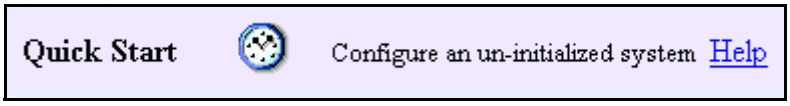
Run the Quick Start Wizard only to configure uninitialized systems. When you click the **Apply** button, Business Communications Manager erases the telephony programming and disables the telephony system temporarily. During application of the Wizard, the Business Communications Manager base unit reboots several times.

Security note: Disable the Quick Start Wizard once it has run successfully. This can be performed from the Programming Wizards page. On this page, click the **Disable Quick Start** link. The Quick Start Wizard button icon disappears from the page.

Entering information into the Quick Start Wizard

This section describes how to use the Quick Start Wizard to set up your system with information that is unique to your system. Refer to "What you need to know before you use the wizard" on page 93 for a list of the fields contained in this wizard:

1 On the Wizards page, click the **Quick Start** icon.



The General page for the Quick Start wizard appears.

2 Enter your system information on the **General** page, **Network** page, **Telephony** page and **CallPilot** page.

Refer to the information you entered in the table under "What you need to know before you use the wizard" on page 93.
Refer to "Navigating the wizards" on page 80 if you do not understand how to move from page to page.

3 When you reach the **Summary** page, review all the information you entered.

If required, go back and make changes, then return to the Summary page.

4 On the Summary page, click the **Apply** button.

A warning dialog box appears, indicating the system changes that will occur if you continue.

Figure 12 Quick Start Wizard application warnings

5 Press **OK** to continue, or **Cancel** to exit the Wizard.

If you press **OK**, a login dialog appears.

6 Enter an administration-level user name and password in the login box.

7 Click **OK**.

The wizard starts the initialization process and displays a progress screen. This screen does not automatically update. Click the **refresh this page** link after 20 minutes to check that the Status line indicates that the change is Complete.

8 Click the **close this window** link to exit the wizard.

Changing system identification parameters

There are some identification parameters you may choose to change after the Quick Start Wizard has set up your system.

Warning: Running the Quick Start Wizard a second time will delete any changes you entered to the default telephony settings, including any telephony data.

The following sections provide information about changing your system identification parameters through the Unified Manager.

Identifying your system and software version

The System heading has a tab that allows you to find or change the name assigned to your system and to view the current version of BCM software that is running on your system.

This section provides information about:

Changing the system name

The system name identifies the Business Communications Manager system on the network.

To change the system name:

1 On the navigation tree, click on **System**.
The Item screen appears.

2 Click the **System Name** box.

3 Enter the new system name.

4 Press the **Tab** key to save your change.

After you change the System Name, restart the Business Communications Manager system. If you change the System Name and do not restart the Business Communications Manager system, Scheduled tasks will not run.

Note: The System Name is the NetBIOS name of Business Communications Manager.

Viewing the system software version

The system software version determines which features are available to your system, and, sometimes, how they work. Each version has a number of new features that only work with that version and newer versions. If you are having a problem running a feature, this may be one area where your service technician will ask you to look.

1. Click on the **System** heading.
   The **Item** screen appears.
   The **Description** box displays a read-only statement about the version of BCM software that the system is running.

Changing the Business Communications Manager time and date

To change the time, date and time zone for the Business Communications Manager system:

1. Click the key beside **System**.
2. Click the **Identification** heading.
   The Identification screen appears.
3. Click the **Date** box and enter the current date.
4. Click the **Time** box and enter the current time at the site where the Business Communications Manager system is located.
5. Click the **Time Zone** box and then click the time zone at the site where the Business Communications Manager system is located.
6. Press the **Tab** key to save your changes.

Changing the system domain

The system domain is the domain in which the Business Communications Manager system resides. If you do not know the domain for the Business Communications Manager system, contact your network administrator.

To change the system domain, add the Business Communications Manager system to a new domain. This section describes:

- Assigning a workgroup
- Assigning a domain
- Assigning a Windows 2000 domain

Assigning a workgroup

1. Click the key beside **System**.
2. Click the **Identification** heading.
   The Identification screen appears.
3. Click the **Change Domain Membership** tab.
   The Change Domain Membership screen appears.
4. Click the **Add To** box and click **Workgroup**.
5. Click the **New Workgroup** box and enter the name of the workgroup to which you want to add the Business Communications Manager system.
6. Press the **Tab** key to save your change.
7. Restart the Business Communications Manager system.

Assigning a domain

1. Click the key beside **System**.
2. Click the **Identification** heading.
   The Identification screen appears.
3. Click the **Change Domain Membership** tab.
   The Change Domain Membership screen appears.
4. Click the **Add To** box and click **Domain**.
5. Click the **New System Domain** box and enter the name of the domain to which you want to add the Business Communications Manager system.
6. Press the **Tab** key to save your change.
7. Restart the Business Communications Manager system.

Assigning a Windows 2000 domain

1. Click the key beside **System**.
2. Click the **Identification** heading.
   The Identification screen appears.
3. Click the **Change Domain Membership** tab.
   The Change Domain Membership screen appears.
4. Click the **Add To** box and click **Win2000Domain**.
5. Click the **Domain User ID** box and enter the User ID that the system uses to access this domain.
6. Click the **Password** box and enter the password that the system uses to access this domain.
7. Click the **New Win 2000 Domain** box and enter the name of the domain to which you want to add the Business Communications Manager system.
8. Press the **Tab** key to save your change.
9. Restart the Business Communications Manager system.

Changing the CallPilot region

The CallPilot region defines some call-management-related system defaults. For information about the CallPilot regions, refer to "BRI and PRI line types" on page 857.

To change the CallPilot region:

1. Click the key beside **System**.
2. Click the **Identification** heading.
   The Identification screen appears.
3. Click the **CallPilot Region** box.
4. Click the region in which the Business Communications Manager system resides.
5. Press the **Tab** key to save your change.

Delayed system restart

There may be times when you perform a procedure that requires a system restart, but you want to delay the restart for a low-activity time.

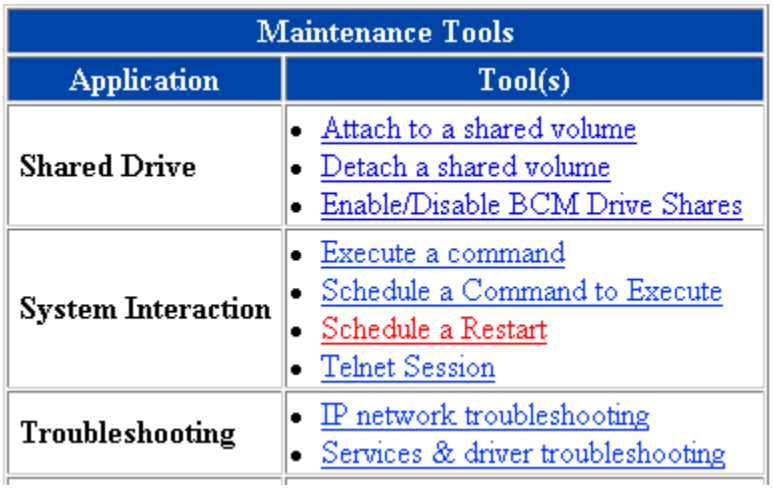
For instance, some keycodes require a cold start to become effective. You can add the keycode at any time, then use this procedure to delay the system restart until early morning, when there is no traffic on your system.

1 On the first page of the Unified Manager, click the **Maintenance** button.

2 You will be prompted to enter your system ID and password.
These are the same ID and password you use to sign into the Unified Manager.

3 On the left menu, under Maintenance, click on **Maintenance Tools**.
The Maintenance Tools screen appears in the right frame.

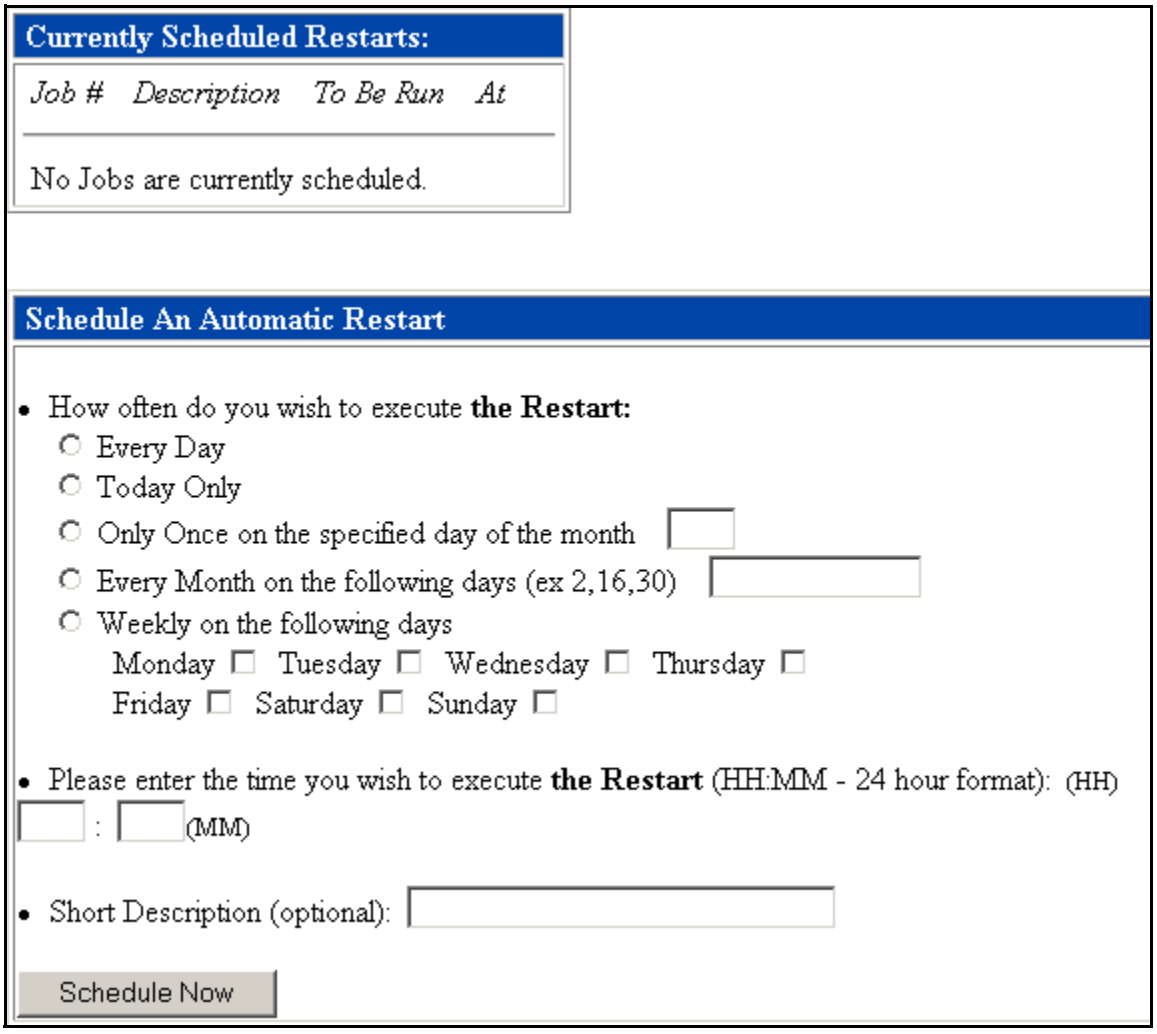
Figure 13 Maintenance Tools screen



4 Beside **System Interaction**, click **Schedule a Restart**.

The schedule screens appear in the right frame.

Figure 14 Job scheduling window



5 Under the first bullet, choose how often you want to schedule a restart.

Example: If you are activating a keycode, click the **Today Only** radio button.

6 Under the next bullet, enter the time you want the restart to occur.

Example: for a 3 a.m. restart, type in 03:00.

7 Under the next bullet, type in a short note about why you want the restart to occur.

8 Click the **Schedule Now** button to activate the schedule.

9 Exit the Maintenance pages.

Chapter 4
Managing system and user security access levels

This section provides information about how you can set up and maintain the access security to your system by users and client applications.

Security note: This symbol will be used throughout this section to indicate areas of possible security concern, primarily in regard to default settings that could pose a security risk if they are not changed.

To define security parameters for the system and for users, you need to consider what level of security you need to achieve to meet your network security standard. Note that the default security settings are not set to their maximum secure settings and can be changed to suit your specific requirements. If you change the default settings, ensure that you understand the interoperability implications between your system and client applications, the computer you use to access the system, and network impacts. For instance, some levels of security are not compatible with clients running Windows© 95©, 98©, or ME©.

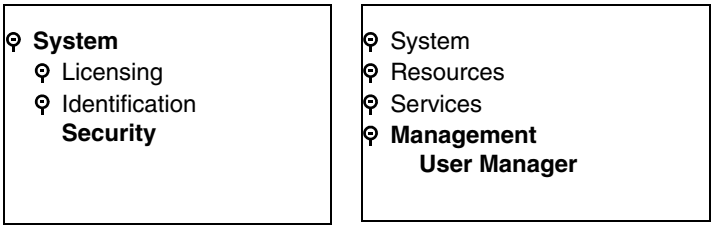
Security note: Minimum configuration should include changing all default system passwords.

Unified Manager security considerations include:

- How long you want the Unified Manager to remain open if there is no input from the user. Refer to “Setting the interface timeout” on page 106.
- If you want to use secure web access to Unified Manager through SSL (Secure Sockets Layer). Note that SSL encryption does not secure the Configuration Menu. To secure communication with the Configuration Menu, a VPN client connection is required. Refer to “Setting system security compatibility levels” on page 107 and “Virtual Private Networks (VPN)” on page 765.
- How much access to the Unified Manager interface users are allowed. Access is based on user privileges defined through user group membership.There are two default administrator accounts, *ee_admin* and *supervisor,* which both also have default dial-in access privileges. Refer to “Managing access passwords” on page 109. This section also contains information about determining password and lockout policies.

The figure below displays the Unified Manager headings under which security and user information is configured. The SSH client access application is installed on your desktop. The **Install Clients** button on the first Unified Manager page provides a download path.

Figure 15 Security and user access headings



Setting the interface timeout

Set the amount of time the Unified Manager stays open if there is no input activity. When the timeout period completes, the program automatically returns to the log-in window. This prevents unauthorized users from accessing the system.

Security note: This is especially important if a password-protected screen saver is not installed on the client PC.

1 On the navigation tree, click on the **Management** heading.
A screen with two tabs appears in the right frame.

2 Click on **Unified Manager Management** tab.

Figure 16 Unified Manager Timeout setting

3 In the **Unified Manager Timeout** field, enter the period of inactivity the program will allow before it closes the application and returns to the log-in window.

Note: If you do not want the Unified Manager to time out, enter 0 in this field.

Setting system security compatibility levels

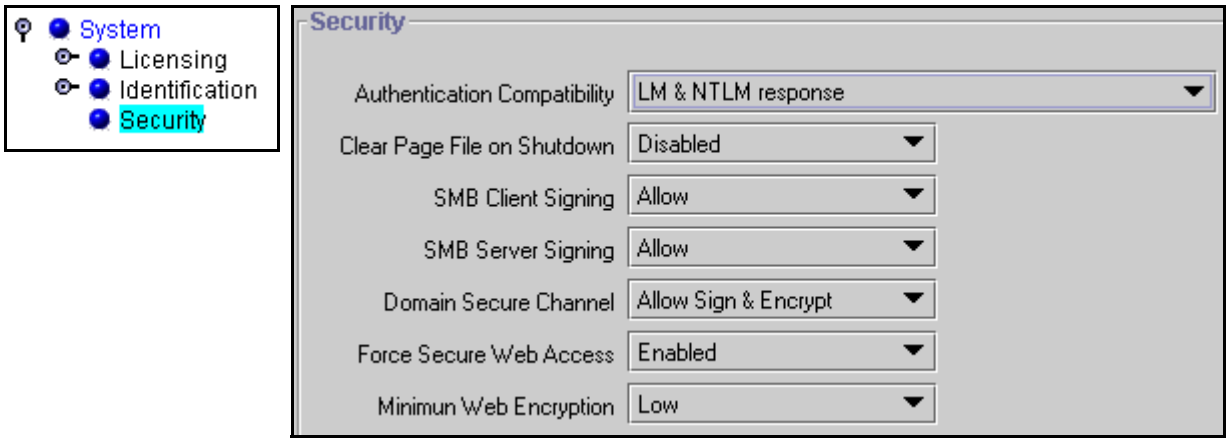
Use the Security screen to set authentication, signing, encryption, and other security-related settings. Some of these settings depend on the Windows operating system used by client workstations.

Security note: The default settings define a mid-level of security which accommodates Windows 95/98/Me operating systems. If you would like to set a higher level of security, ensure that all the computers that will be used for client access have upgraded to at least Windows NT4, 2000 or XP.

1 Click the keys beside **BCM** and **System**.

2 Click on **Security**.
The Security screen appears in the right frame.

Figure 17 System security level settings



3 The following table describes the fields. Set the fields to the values that best fit your system requirements and that accommodate compatibility issues with interconnecting users or services.

Table 4 Security settings

Attribute	Value	Description
Authentication Compatibility	LM&NTLM response - refuse NTLMv2 session security LM & NTLM response NTLM response only NTLMv2 response only NTLMv2 response only - refuse LM	**Default: LM & NTLM response** This setting determines the type of authentication protocol required by your system during interactions with client applications. The default, LM & NTLM response, maintains compatibility with all Windows OS versions. Any of the other settings enforce a more secure authentication protocol, and will prevent access from computers running Windows 95/98/Me, unless you install the directory services client on the client computer.

Table 4 Security settings (Continued)

Attribute	Value	Description
Clear Page File on Shutdown	Disabled Enabled	**Default: Disabled** If Enabled, this setting prompts the system to clear the virtual memory swap file on shutdown. When enabled, this option extends system shutdown by about two minutes.
SMB Client Signing	Allow Disabled Require	**Default: Allow** Determine what level of signing you require from SMB clients. Disabled: None required. Allow: Tries to perform the digital signature whenever a compatible client platform is detected. This setting also supports clients running with Windows 95/98/Me. Require: Always secures the connection with a digital signature. However, this setting prevents access from clients running with Windows 95/98/Me. Applicable applications: BRU and Archlog
SMB Server Signing	Allow Disabled Require	**Default: Allow** Determine what level of signing you require from SMB client servers. Disabled: None required. Allow: Tries to perform the digital signature whenever a compatible client platform is detected. This setting also supports clients running with Windows 95/98/Me. Require: Always secures the connection with a digital signature. However, this setting prevents access from clients running with Windows 95/98/Me unless you install the directory services client on the client computer. Applicable applications: BCM monitor.
Domain Secure Channel	Disabled Allow Sign Allow Sign & Encrypt Require Sign or Encrypt	**Default: Allow Sign & Encrypt** Define what level of channel security you require. Disabled: No special security. Allow Sign or Allow Sign & Encrypt: Tries to perform the digital signature and/or encryption whenever a compatible client platform is detected. This level needs to be aligned with your Domain controller setting. Require Sign & Encrypt: Always secures the connection with a digital signature and/or encryption. Clients running with Windows 95/98/Me are not supported. Applicable applications: CDR and TAPI.
Force Secure Web Access	Enabled Disabled	**Default: Enabled** If enabled, SSL is used for all web access to the Business Communications Manager. In that case, the https://<*IP address*> must be used. As well, old bookmarks will be rerouted to that interface. If disabled, the http URL references will not automatically redirect to the SSL-based https interface. Both the unencrypted http://<*IPaddress*>:6800 and the encrypted https://<*IP address*> interfaces can be used.
Minimum web encryption	Low Medium High	Set the encryption strength of the web interface. Low: all low strength ciphers Medium: all ciphers with 128 bit encryption High: all ciphers with 3DES encryption.

4 Click outside the window to set the changes.

Managing access passwords

You can grant or restrict specific access within the Unified Manager by assigning new users into user groups using the User Management screens.

Core system configuration, such as resources and network management should be restricted to an administrator-level account.
Use the group profiles to define other levels of users with access to the headings that are specific to their task.
This also helps to prevent overlap programming if more than one person is using the interface at the same time.

Dial-in access: Restrict this user group to users who require this interface. If modem access is not required, the modem interface can be disabled to provide further security. Refer to "Enabling and disabling the V.90 modem interface" on page 686.

This section includes information about the viewing and configuring the user profiles and groups:

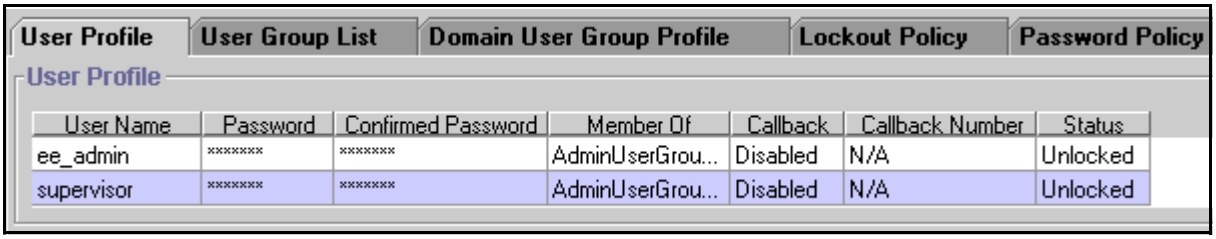
Callback security
If a user is connecting to the system using a V.90 modem, you can enhance your access security by assigning that person a specific user account that prompts the system to acknowledge the user, then hang up and dial back the user at a designated telephone number, before allowing the person to have access to the system.

The information in this section is found under the **Management**, **User Manager** heading.

Viewing the User Manager tabs

The various tabs under User Manager allow you to define user and group profiles and the parameters that define security levels for user accounts. This heading is located under the **Management** heading on the navigation tree.

- The **User Profile** tab appears showing the current user profile information.



Business Communications Manager comes with these default administrator user profiles:

— **ee_admin (cannot be deleted)**: Default password: `PlsChgMe!`. Access privilege: Read-Write, dial-up access

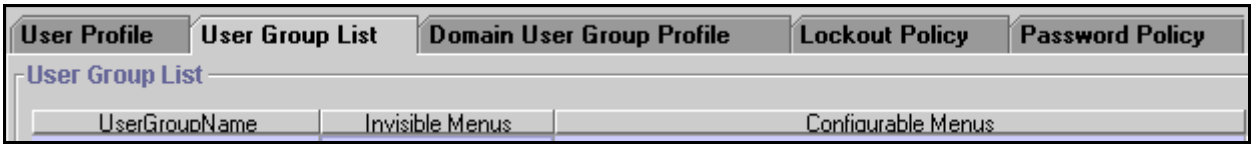
— **supervisor**: Default password: `PlsChgMe!`. Access privilege: Read-Write, dial-up access

Security note: Change the default passwords on the ee_admin and supervisor account after you initialize your system. The ee_admin account cannot be deleted, but the group membership can be modified for both accounts.

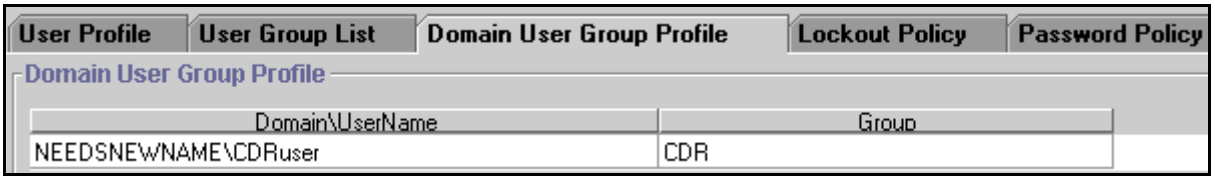
Remote support: In order for the Nortel Networks support organization to assist you, dial-in access has been granted to both default administrator accounts. If dial-in access is removed, then remote access by support organizations may be impacted. It is recommended that the administrator accounts and dial-in access rights be restricted to select personnel. Callback capability increases the dial-in security.

- **ISDN note:** When you enter an ISDN dial up user interface, the user name shows up on this list. If you plan to use the secure callback properties for an ISDN user, you need to specify a static IP address for that interface. Refer to "Configuring an ISDN interface" on page 691.

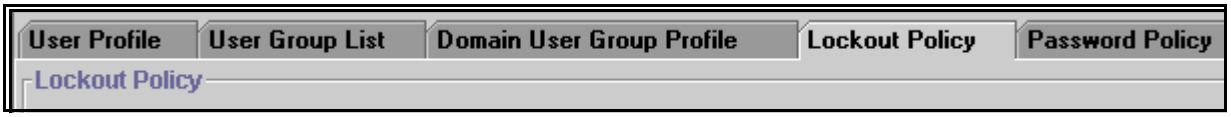
- The **User Group List** tab shows all the user groups defined in your system.
The system comes with a set of default User Groups that have various access privileges.



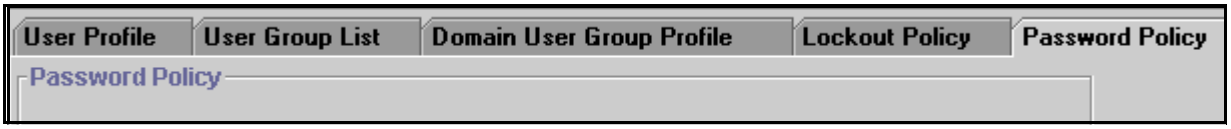
- The **Domain User Group Profile** tab lists the domains for all the user group profiles.



- The **Lockout Policy** tab provides settings to determine the parameters for locking users out of the Unified Manager if the lockout policy is enabled.



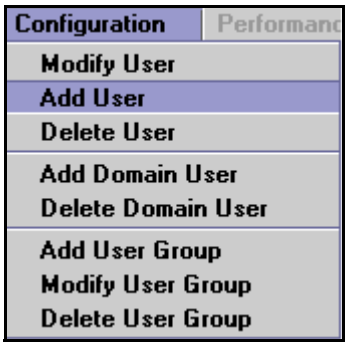
- The **Password Policy** tab allows you to define the complexity policies you want to use for your system passwords.



Adding or modifying a user profile

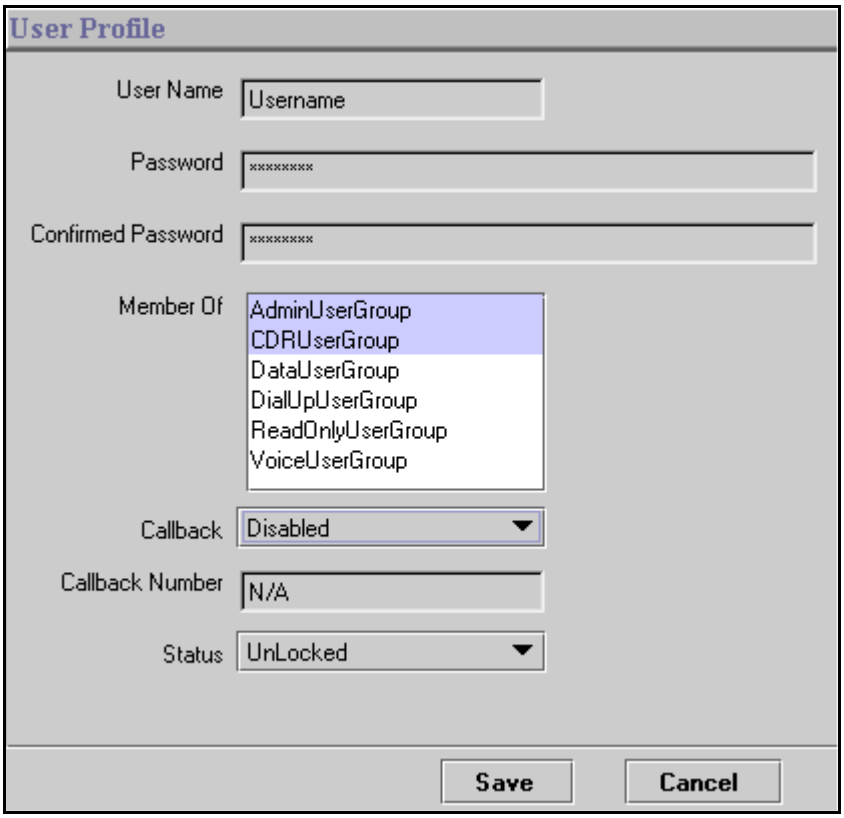
To add or modify the profile for a single user, follow these steps:

1. Click the key beside **Management.**
2. Click on **User Manager**.
   The User Profile screen appears showing the current user profile information.
3. Access the **User Profile** dialog:
   - If you are adding a new user: from the **Configuration** menu, select **Add User**.
   - If you are editing an existing user: select the user name on the list, then from the **Configuration** menu, select **Modify User**.



The User Profile dialog box appears.

Figure 18 User Profile screen to add or modify a user profile



4 Use the following table to determine what information you need to add or change:

Table 5 User Profile settings

Attribute	Value	Description
User Name	*<maximum of 20 characters>*	Allows you to enter the user name. The User Name is case-sensitive and cannot exceed 20 characters in length. **Edit note:** You cannot modify a user name. You must delete the complete User Profile row from the User Profile window and add a profile with the new name. **ISDN note:** When you enter an ISDN dial up user interface, the user name shows up on this list. If you plan to use the secure callback properties for an ISDN user, you need to specify a static IP address for that interface. Refer to "Configuring an ISDN interface" on page 691.

Table 5 User Profile settings (Continued)

Attribute	Value	Description
Password	*<maximum of 14 characters long>*	Allows you to assign a password for the user. The password is case-sensitive and can be a maximum of 14 characters long. **Note:** • Password length is determined by the Minimum Password Length setting in the Password policy table. • Passwords must contain elements from three of the four following character sets. This requirement can change, if you change the default password policy complexity setting ("Setting password policy" on page 122): — upper case alphabet — lower case alphabet — westernized Arabic numerals — nonalphanumeric characters ($, !, %, ^) • A user who fails to enter the correct password can be locked out of the system after a defined number of retries (account lockout threshold). For information about setting the lockout threshold, refer to "Setting password lockout policy" on page 120.
Confirmed Password		Requires you to enter the same password again to validate the new or modified password.
Member of	AdminUserGroup CDRUserGroup DATAUserGroup DialUpUserGroup ReadOnlyUserGroup VoiceUserGroup	Allows you to select the level of access associated with the user name. The following levels of access are default settings: **AdminUserGroup:** Can see and change any menu items (default). **CDRUser Group:** Can see everything but cannot make changes. This user is restricted to accessing the CDRs. **DATAUserGroup:** Can only configure pre-defined data fields (default). **DialUpUserGroup:** All menus are invisible, and no menus are configurable (default). This group allows the user to access the system through a dial-up connection. **ReadOnlyUserGroup:** Can see everything but cannot make changes (default). **VoiceUserGroup:** Can only configure pre-defined voice fields (default). Note: You cannot modify default user groups. **Dial-up note:** If any of the users will be using a dial-up connection to access the system, they must be assigned to the DialUpUserGroup. For information about adding new groups, refer to "Adding or modifying a group profile" on page 116.
Callback	Disabled/Enabled	If this user is going to use a dial-up connection to connect to the system and the user requires callback, ensure that Callback is enabled. If the user is configured as an ISDN interface, ensure that a static IP address has been specified for the interface. Refer to "Configuring an ISDN interface" on page 691. If this user is not using a dial-up connection or does not require callback, set Callback to Disabled. Note: The system supports one dial-up connection at a time.
Callback Number		This is the number the system uses to call back to the user's dial-up location. Ensure that the appropriate routing codes are added to the dial string.

Table 5 User Profile settings (Continued)

Attribute	Value	Description
Status	Unlocked Unlock	This field indicates the current state of the user's password. If the password becomes locked and the user does not want to wait the lock-out time, the Administrator can choose **Unlock** on the user's password record to release the password.

5 Click the **SAVE** button to save your settings.
The new user profile information is added to the list on the User Profile window.

Security note: An integral part of your system security is password management. This includes changing default passwords after the system is installed.
Also, to further increase access security, minimize the number of user accounts, especially the administrator accounts, and change them frequently.

Deleting a user profile

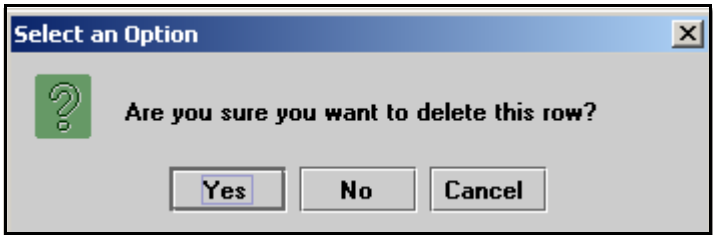
To delete a user profile:

1 Select **Management, User Manager**.
The User Profile window appears showing a list of the current user profiles.

2 Click the line for the user you want to delete.

3 From the **Configuration** menu, select **Delete User**.
A confirmation dialog will ask you to confirm that you want to delete the user record.

Figure 19 User Manager delete confirmation dialog



4 Click the **YES** button to delete the user profile.

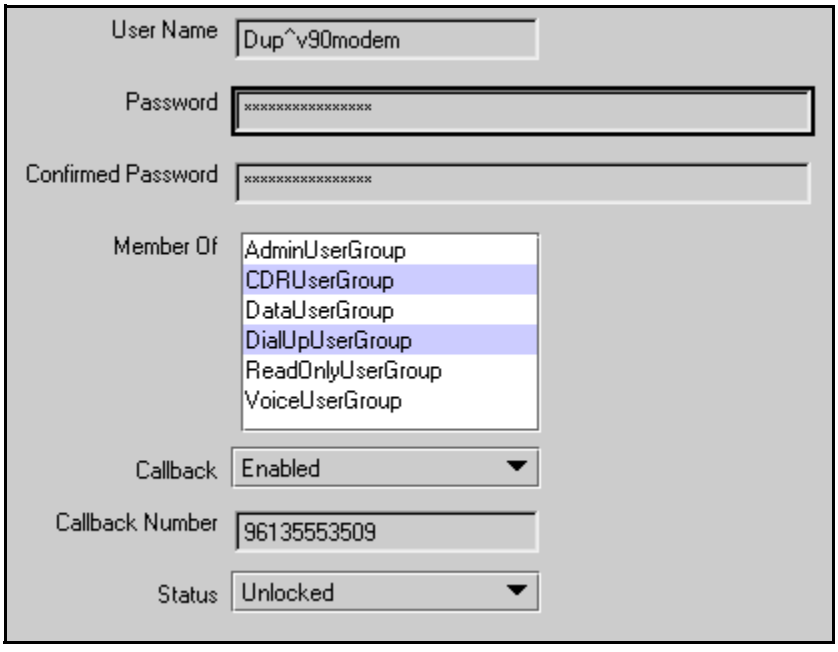
Security note: You cannot delete the ee_admin user.

Setting up callback for a user

If the user will be accessing the system through a dial-up connection, you need to add that group to the user account. As well, in this case, callback will be enabled to ensure that the system security is maintained.

1. Select **Management, User Manager**.
   The User Profile screen appears showing the current user profile information.
2. Access the User Profile screen:
   - If you are adding a new user: from the **Configuration** menu, select **Add User**.
   - If you are editing an existing user: select the user name on the list, then from the **Configuration** menu, select **Modify User**.
3. Enter a **User Name**, if one does not already exist.
4. Enter and confirm a password, if one has not already been specified.
5. Click to highlight the DialUpUserGroup name. Then, hold the **<Ctrl>** key down and click on any other groups to which you want to assign the user.
6. Select **Enabled** from the **Callback** menu.
7. Enter the number the system will dial to contact the client modem. Ensure you include the correct routing codes.
8. Click **OK** at the bottom of the screen to save the settings.

Figure 20 User profile for dial-up user



Adding or modifying a group profile

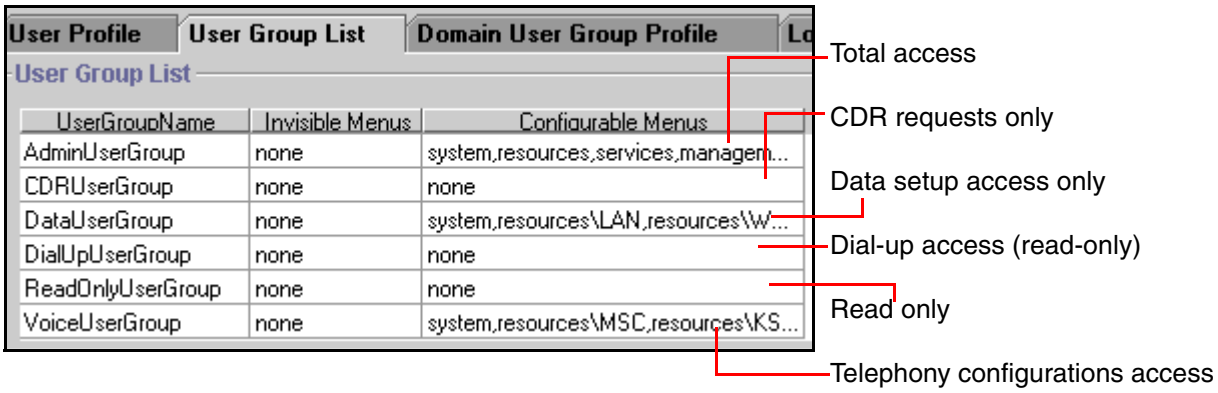
The access privileges inherent in the various predefined group profiles control user access within the Unified Manager interface. The administration group maps to administrator privileges on the Business Communications Manager host system. The other group profiles map to non-administration groups.

To add or modify the profile for a group, follow these steps:

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

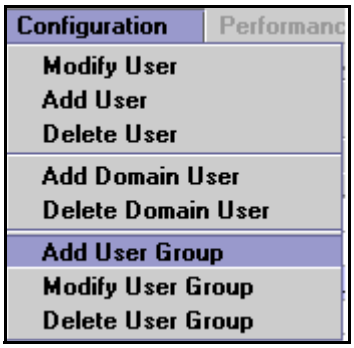
2 Click the **User Group List** tab, to view the existing groups.

Figure 21 Default user groups



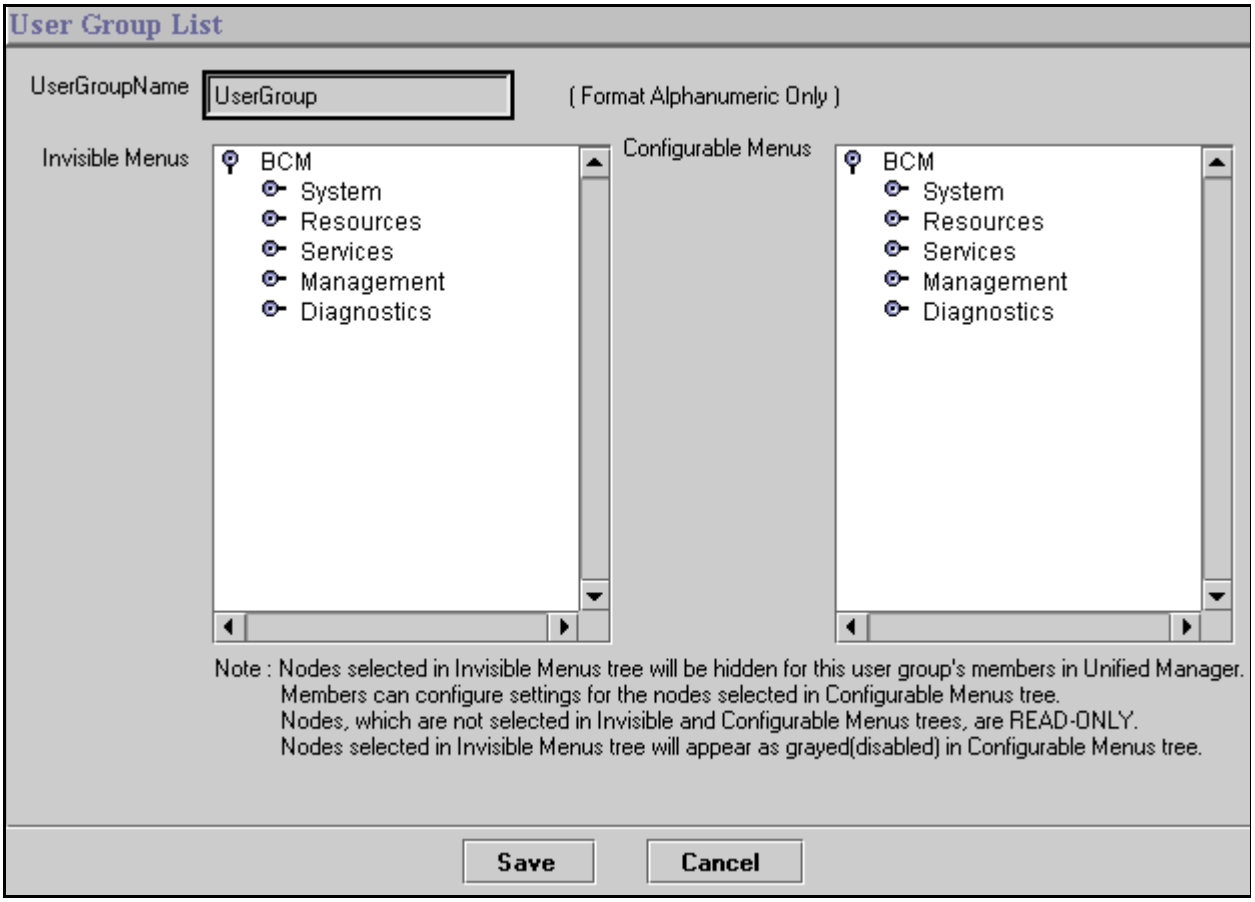
3 Add or change a user group:

- If you are adding a new group: from the **Configuration** menu, select **Add User Group**.
- If you are editing an existing group: select the user group name on the list, then from the **Configuration** menu, select **Modify User Group**.



The User Group List dialog box appears.

Figure 22 User Group List add/modify screen



4 Use the following table to determine the user profile information that needs to be added or changed:

Table 6 User Group Profile settings

Attribute	Description
UserGroupName	This is the name of the user group. If you are modifying an existing record, you will not be able to change this field.
Invisible menus	This box allows you to choose which menus you want to keep hidden from the user group. The Configurable Menus box shows these fields covered by a grey box.
Configurable menus	For the headings not covered by grey boxes, select the ones for which you want the users to be able to change settings. All headings that are left white will appear on the menu, but will be read-only for this group.

5 Click the **SAVE** button to save your settings.
The new user group information is added to the list on the User Group List window.

Deleting a Group profile

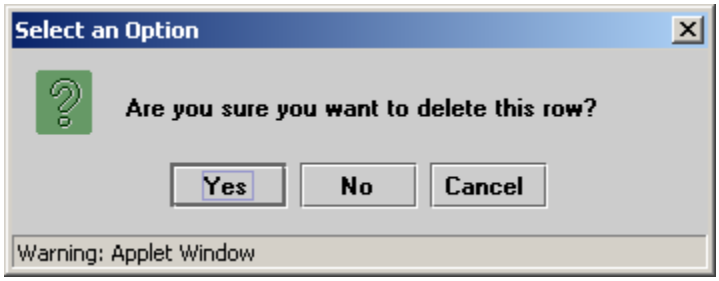
If you want to delete a group profile, follow these steps:

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

2 Click the **User Group List** tab, to view the existing groups.

3 From the **Configuration** menu, select **Delete User Group**.
A confirmation dialog will ask you to confirm that you want to delete the record.

Figure 23 User Manager delete confirmation dialog



4 Click the **YES** button to delete the user group profile.

Adding a Domain User Group profile

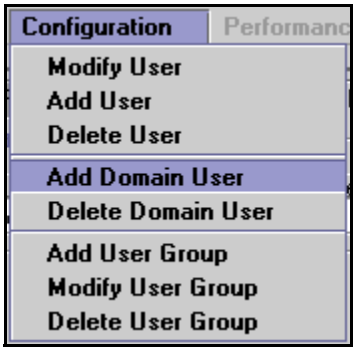
The Domain User Group Profile screen displays a table of members of the Windows NT CDR User group. This screen is used to add external domain users into a CDR User group. Members of CDR user group have the sole ability to download CDR files from this Business Communications Manager system. For details about Call Detail Report processes, refer to the CDR documentation.

You can only add valid users currently assigned to CDR user groups. Refer to "Adding or modifying a user profile" on page 111. When you add local users, the user name is automatically added to this list. If you are entering an external user, they must be members of a domain that recognizes this Business Communications Manager, and you add their user name.

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

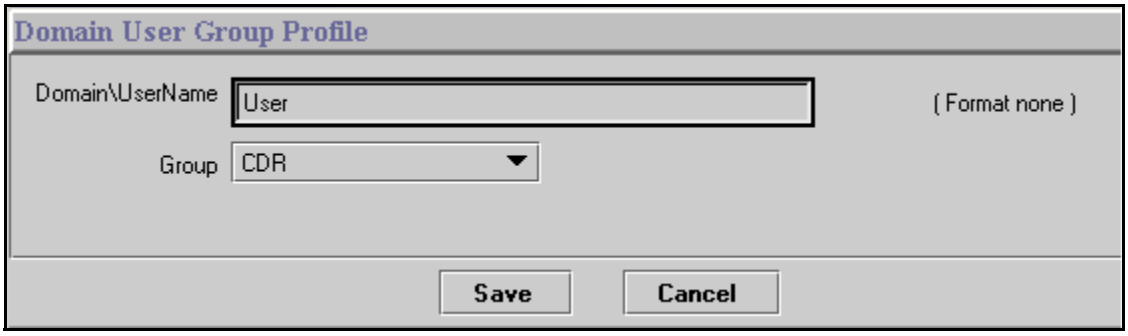
2 Click the **Domain User Group Profile** tab, to view the existing groups.

3 From the **Configuration** menu, select **Add Domain User**.



The Domain User Group Profile dialog box appears.

Figure 24 Domain User Group Profile add/modify screen



4 Use the following table to add the new Domain user Group profile name:

Table 7 Domain User Group Profile settings

Attribute	Description
Domain\User Name	Enter the user name.
Group	CDR (only choice)

5 Click the **SAVE** button to save your settings.
The new user group information is added to the list on the Domain User Group Profile screen.

Deleting a Domain User Group profile

If you want to delete a Domain user Group, follow these steps:

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

2 Click the **Domain User Group Profile** tab, to view the existing groups.

3 From the **Configuration** menu, select **Delete Domain User**.
A confirmation dialog will ask you to confirm that you want to delete the record.

4 Click the **YES** button to delete the Domain User Group profile.

Setting password lockout policy

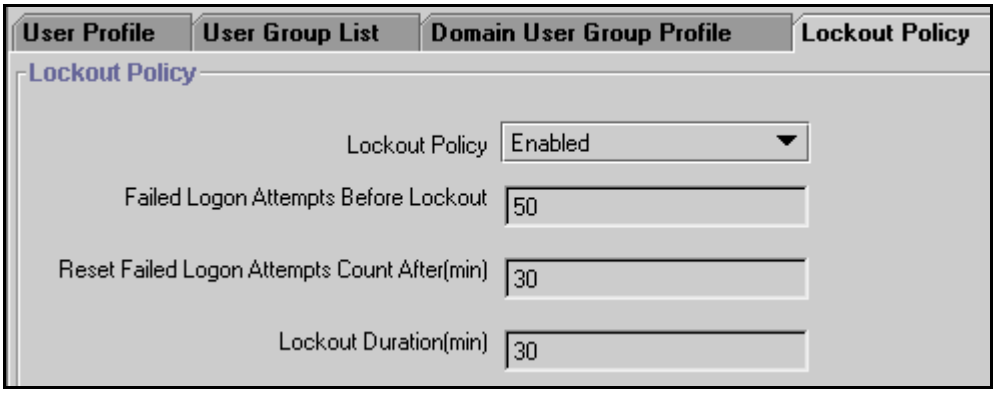
If you have Lockout Policy enabled, you can choose the parameters that will determine when a user will be locked out of the system if an incorrect password is entered repeatedly.

Security note: Lockout policy is enabled as the default setting. This policy is particularly important to stop unauthorized logon attempts to your Business Communications Manager system.
You can further tighten the access security to the system by setting the account lockout threshold to a recommended value of 5.

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

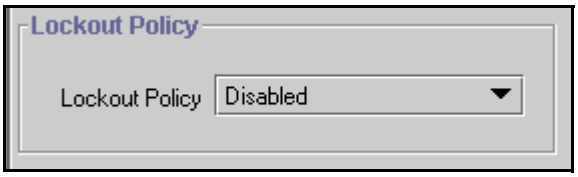
2 Click the **Lockout Policy** tab.
The default is to have Lockout Policy enabled.

Figure 25 Lockout Policy screen



3 Use the information provided in the following table to determine the lockout policy for your system. The settings are effective as soon as they are entered.

Table 8 Lockout policy settings

Attribute	Value	Description
Lockout Policy	Enabled Disabled	The **Enabled** setting allows you to set the following three parameters. If you choose **Disabled**, no configurable parameters display. 
Failed Logon Attempts Before Lockout	<digits>	Default: 50 Enter the number of times the user can attempt to enter a password before the user is locked out.
Reset Failed Logon Attempts Count after (min)	<minutes>	Default: 30 The amount of time before the lockout counter is reset. Note: This does not necessarily mean the user was locked out.
Lockout Duration (min)	<minutes>	Default: 30 The amount of time that passes after the user is locked out and before they are allowed to try to log in again, and the Reset count is set back to zero.

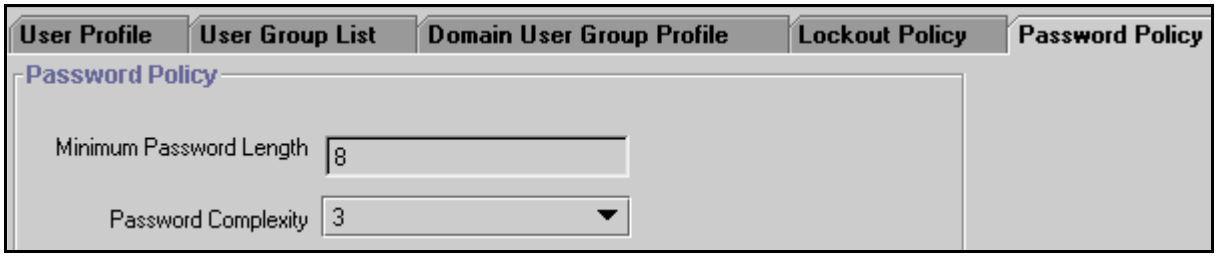
Setting password policy

You can define the system parameters for the passwords that you assign to users by determining the length, age and history that the passwords must meet.

1 Select **Management, User Manager**.
The User Profile screen appears showing the current user profile information.

2 Click the **Password Policy** tab.

Figure 26 Password Policy tab



3 Use the information provided in the following table to determine the lockout policy for your system.

Table 9 Password policy settings

Attribute	Value	Description
Minimum Password Length	1 to 8	Default: 8 Determines the minimum number of characters that must be entered for a new password. Passwords can be a maximum of 14 characters long.
Password Complexity	0 2 3	Default: 3 Define the level of complexity for the system user passwords. 0 (zero): none of the Password policies are required 2: at least two different types of characters are required 3: at least three different types of characters are required.
	At highest complexity, passwords must contain elements from three of the four following character sets: • upper case alphabet (English) • lower case alphabet (English • westernized Arabic numerals • non-alphanumeric characters ($, !, %, ^)	
Network note: If you are using Network Configuration Manager, password policies will be applied, regardless of the Unified Manager settings.		

Chapter 5
Configuring resources — media bay modules

This chapter describes the Unified Manager headings that define and control the settings for the media bay modules installed on your system.

Task:

Check settings for the media bay modules installed in the system.

Trunk modules:

- Confirm that the DIP switch setting matches the intended DS30 bus placement.
- Verify module type and programmed bus type settings under intended DS30 bus are correct for the type of module installed
- Configure the module parameters of individual modules installed on each DS30 bus

Station modules:

- Confirm that the DIP switch setting matches the intended DS30 bus placement.
- Verify module type and programmed bus type settings under intended Bus # are correct for the type of module installed

Note: Data and split-telephony/data module configuration are described in the section "Data and split-line configuration" on page 151.

This section contains information about:

Media bay modules provide the Business Communications Manager with physical interfaces to trunk (CO) lines and your system telephones, which are defined by directory number (DNs) records. When media bay modules are first installed in your system you need to configure them using the procedures described in this section. Media bay module DIP switch settings and installation procedures are described in the *BCM1000 Installation and Maintenance Guide* and the *BCM200/400 Installation and Maintenance Guide*.

The *Installation and Maintenance Guide* also describes the concept of the 2/6 and 3/5 split, which determines how many channels are available for media bay modules. When to choose to change the DS30 split is discussed in the MSC section of this guide, refer to Chapter 26, "Configuring the MSC resources," on page 609.

The *Installation and Maintenance Guide* also describes the concept of partial double density (PDD) and full double density (FDD). If your system is set to PDD (the default), and you have installed a media bay module that supports double density, the system can support 32 lines on

whatever buses from 02 to 05 have the module installed. If your system was changed to FDD, the system supports double density on all six buses. Refer to Chapter 26, “Configuring the MSC resources,” on page 609.

Explaining the Media Bay Modules headings

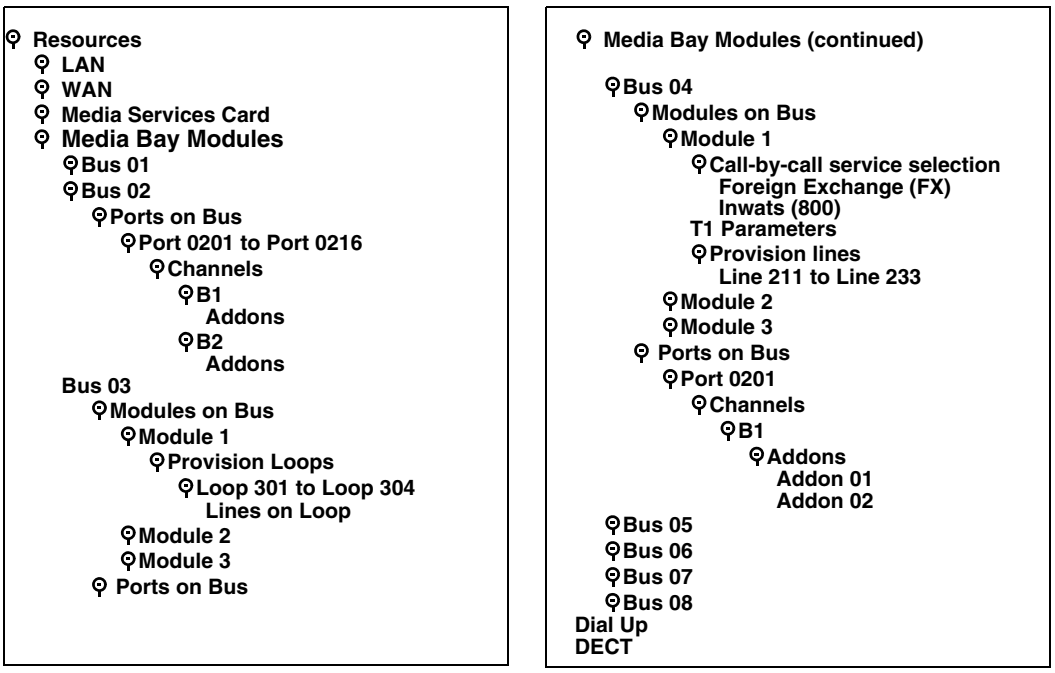
The **Resources, Media Bay Modules** heading allows you to view and change settings for each media bay module installed in Business Communications Manager.

When you choose a region during your system startup, the Business Communications Manager installs a default set of media bay module settings under **Resources, Media Bay Modules**. However, these may not be the settings that you want for the modules you install. Therefore, when you install a module, you must go to the appropriate **Resources, Media Bay Modules, Bus ##** record and verify the settings for the module you installed.

This section includes information about:

The following figure illustrates the headings found under **Resources, Media Bay Modules** heading on the navigation tree. The exact items displayed below the Bus XX headings depends on the type of module configured for that DS30 number.

Figure 27 Resources, Media Bay Modules menus



Tips: Some modules are region-based. If your system does not have the correct region installed during setup, the modules will not work. Refer to "Media bay module availability by region" on page 849.

Note: Dimmed fields are read-only and cannot be changed.

Note: If you receive the error message `Telephony programming is currently not available. Please try again later.` when you click on one of the headings, this means that the part of the system that handles MSC is doing a reset. Wait about 1-1/2 minutes and try again.

Media bay module Bus numbers

Under the headings for DS30 02 to 07 (or 02 to 06 if your system has a 3/5 DS30 split):

- Station or analog station modules ("Viewing station module information" on page 143) display the **Ports on Bus** heading.
- Trunk modules ("Defining trunk module types and settings" on page 130) display from one to four **Module <#>** headings. These modules correspond to the offset configured on the module. A **Ports on Bus** heading also appears for some types of modules (DTM set to PRI, and the BRI modules).
- If you have a WAN board installed in the base unit, DS30 08 does not appear. Bus 08 and Bus 01 are used for internal media channels. ("Internally-driven channels" on page 146). If you system is set to a 3/5 split, DS30 07 is also used for media channels.

Identifying the module

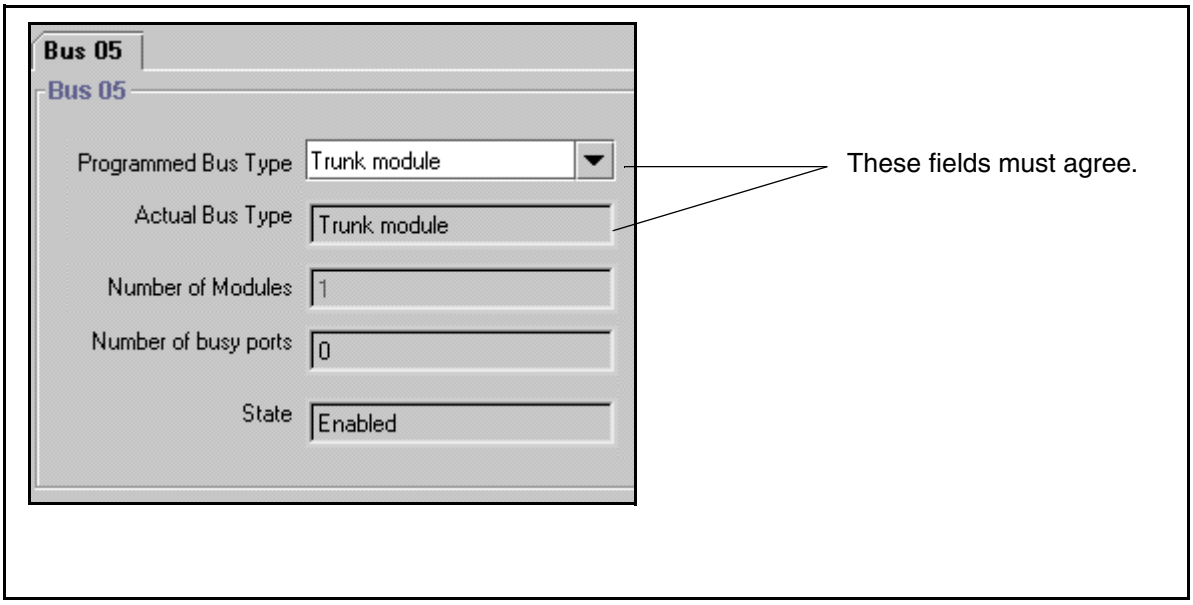
Use these steps to define a Programmed Bus Type. This setting notifies the Unified Manager about what type of module is installed on the DS30 bus.

1. Click on the keys beside **Resources**, and **Media Bay Modules**.
2. Click a **Bus** (Bus 02 to 07).

   Tips: Bus number is determined by the DS30 number set on the DIP switches of the module before it was installed.

   The Bus screen appears.
3. Ensure the entry in the **Programmed Bus Type** field agrees with the **Actual Bus Type** of module that is installed for the DS30 bus, as shown in the following figure. Refer also to "Module types and capacities" on page 128.

Figure 28 Confirming the Programmed Bus Type



Programming tips: If the **Actual Bus Type** reads **None**, choose the correct setting in the **Programmed Bus Type** field. After the system initializes to the module, the **Actual Bus Type** should change to the correct module type. You may also have to disable, then re-enable the module to force the system to re-initialize (under the **Configuration** menu). Refer to "Viewing Media Bay Module status" on page 147 for details about enabling and disabling modules.

Some modules take a few minutes to reinitialize.

If these actions do not cause the fields to display correctly, you may have a damaged module or backplane. Try installing the module in a different media bay and retry the configuration. Refer to the *Installation and Maintenance Guide* for your hardware for information about removing and installing media bay modules.

4 The other headings on the Bus screen describe the current status of the modules, as described in the following table.

Table 10 Bus XX record settings

Heading	Value	Description
Station module		
Number of sets	<digit>	This setting indicates the number of sets that are currently attached to the module.
Number of busy sets	<digit>	This setting indicates the number of sets that are currently using the module.
State	Enabled Disabled	This setting indicates the state of the module. Use the **Configuration** menu item to change this setting.

Table 10 Bus XX record settings (Continued)

Heading	Value	Description
Trunk module, Analog Station Module or Data Module		
Number of busy ports	<digit>	This setting indicates how many ports on the module are currently being used.
State	Enabled Disabled	This setting indicates the current state of the module. Use the Configuration menu item to change this setting.

5 Your next steps depend on which type of module you are configuring:

- If you are configuring a station or analog station module, ensure that the bus type is correct and the Programmed Bus Type field displays the correct module type. The **State** field displays **Enabled**, indicating that the module is active and ready to have telephones connected. Refer to "Module types and capacities" on page 128.
- If you are configuring trunk modules, you must now ensure each module associated with the DS30 bus is set up. This process is described in the next section, "Defining trunk module types and settings" on page 130.

Module types and capacities

Refer to the following table for a description of the Bus types settings.

Table 11 Programmed Bus Types

Programmed Bus Type	Hardware unit	Capacity	Available line types (some line types are region-dependent)
Station module	• Digital Station Media Bay Module (DSM 16/16+ or DSM 32/32+)	Single density • DSM16/16+ = 1 per bus/16 digital sets per module • DSM 32/32+ = 2 buses/32 digital sets per module Double density • DSM16+ = 2 per bus/16 digital sets per module • DSM 32+ = 1 per bus/32 digital sets per module	N/A
	• 4X16 Media Bay Module (4X16) (counts as one DSM 16)	• 4X16 = 1 offset (trunk) and additional bus/16 digital sets	
	• Norstar station module (SM) connected to a FEM	• SM = 1 bus/16 digital sets	
Analog station module	• Analog Station Media Bay Module (ASM 8)	Single density • ASM8 = 2 per bus/8 analog sets for each module Double density • ASM8 = 4 per bus/16 analog sets for each module	N/A
	• (Global) Analog Station Media Bay Module (ASM8+)	Single density • 2 per bus/8 analog sets for each module Double density • 4 per bus/8 analog sets for each module	North America: Provides CLID passthrough, Message Waiting Indication and Disconnect Supervision UK: Provides Message Waiting Indication
	• Norstar analog station module (ASM) connected to a FEM	• FEM = 1 per bus/16 digital sets	N/A
Trunk module	• Digital Trunk Media Bay Module (DTM)	• DTM = 1 per bus/16 lines (max. three DTMs on a system)	• DTMs can be set to module types: Loop, E&M, DID, T1, PRI (NI or ETSI are region-specific)
	• CLID Trunk Media Bay Module (CTM4 or CTM8) • Global Analog Trunk Module (GATM4 or GATM8) (released with BCM version 3.5)	• CTM4/GATM4=1 per offset/4 lines per module • CTM8/GATM8= 2 per bus/8 lines per module	• CTMs/GATMs can be set to module types: Loop

Table 11 Programmed Bus Types (Continued)

Programmed Bus Type	Hardware unit	Capacity	Available line types (some line types are region-dependent)
Trunk module (continued)	• 4X16 Media Bay Module (4X16) (counts as one CTM)	• 4X16=1 per offset (4 lines) and additional bus (station)	• 4X16s can be set to module types: Loop
	• BRI Media Bay Module (BRI)	• BRI=3 per bus, 4 loops (8 lines) per module	• BRI can be set to module types BRI S/T, BRI U2, BRI U4 (setting must match physical module type). U2 and U4 are region-specific
Data/trunk module*	• Digital Drop and Insert (DDI) Mux module	• Universal T1=1 per two buses, supports 24 lines * Also refer to the section that describes the UTWAN, which provides the data connections through a WAN card.	• T1
Specialized modules	• DECT Media Bay Module (DECT)	• DECT=1 per bus, 4 loops, supports 36 handsets	• DECT (region-specific)* *This module type only appears when a DECT module is present on the system. If the DIP switches are set incorrectly, the setting appears, but the module displays as *unequipped*.
	• Norstar trunk expansion modules, with Analog Trunk cards, connected to a FEM	• FEM=1 per bus, can support up to three analog trunk cards (in one trunk expansion unit)/4 lines each	• Norstar analog trunk cards: Loop, E&M, DID
	• Norstar trunk expansion modules with BRI cards, connected to a FEM	• FEM=1 per bus, can support up to three BRI cards (in one trunk expansion unit)/4 loops each	• Norstar BRI cards: BRI S/T, BRI U2, BRI U4 (setting must match physical module type). U2 and U4 are region-specific
Data module	Refer to the data section of this book ("Configuring a data module" on page 178) for details about setting up a data module on DS30 08. This process includes any Norstar Data Modules connected to a FEM.		

GATM (Global Analog Trunk module)

These trunk modules can be adjusted to have static trunk parameters (pre-BCM 3.5 software), or to allow the system to download new parameters when they become available (BCM 3.5 and newer software). If the trunk is set to the latter state, trunk parameters are downloaded every time the module boots up, or when the parameters change while the module is working. You can also set line and telephone impedance to either 600ohm or 900ohm for modules with downloadable parameters. The impedance settings are located under **Lines** and **Telephone Services**, respectively. Refer to the installation guides for details about the module.

Ports on Bus

Both types of modules have a **Ports on bus** heading. This heading shows the state of the port that connects the module to the trunk line or system device.

- Trunk modules, each port maps to an incoming line. Trunk port status is either idle or active. Refer to “Trunk module ports programming” on page 142.
- Station modules, each port maps to a connection to a system device (telephones, fax machines, doorphone). For station modules, port status is either equipped (device connected) or unequipped (no device connected). You can also determine what type of device is attached to the port. Refer to “Viewing station module information” on page 143.

Bus 01 and 08 note: Bus 01 and 08 ports on bus are really virtual ports, since they connect to services supported by the MSC. These ports are used for such devices and services as IP telephones and Symbol NetVision handsets and voice mail traffic.

Defining trunk module types and settings

MSC bus numbers assigned to a trunk module display module numbers under the Bus heading that correspond to the offset number set on the module DIP switches. For instance any trunk module that has an offset of 0, will display under the heading Module 1, and so on to a maximum of four modules (CTM4s/GATM4s).

The Module menu, which appears only under a Bus record that is configured for trunk modules, allows you to configure line or loop provisioning for the module associated with a particular bus. This record shows the number of lines or loops assigned to the module. It also provides the first and last loop or line number. These settings are read-only.

The fields that appear on the module screen vary, depending on the module type you specify. Trunk lines can also require configuration of settings such as the protocol type/version, frame structure, clocking, and timers. These parameters depend on how the interface of the service provider that the module connects to has been configured.

This section refers to these topics:

- “Configuring the trunk module to line type” on page 131
- “Determining Clock Sources for DTMs or BRIs” on page 135
- “T1 interface parameters (region-specific)” on page 136
- “E1 parameters (region-specific)” on page 138
- “PRI Call-by-Call service selection” on page 138
- “Provisioning lines (PRI, T1, DASS2)” on page 140
- “PRI B-channel provisioning” on page 142
- “Trunk module ports programming” on page 142

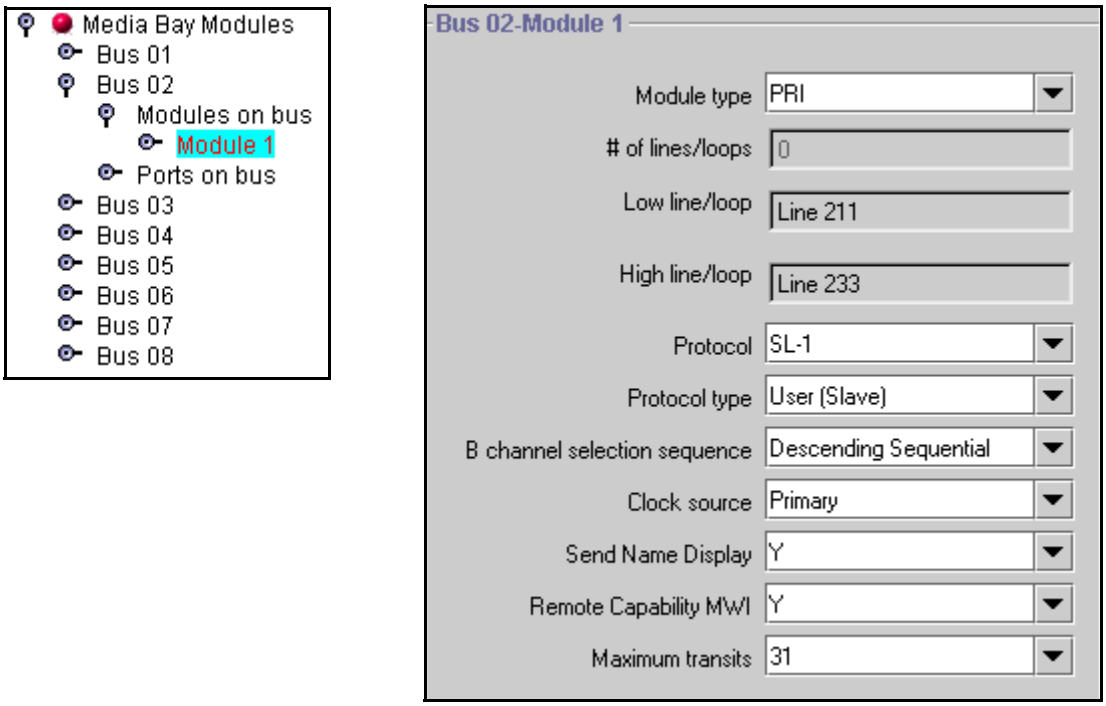
Configuring the trunk module to line type

Follow these steps to define the modules to the system:

1. Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <*number*>**, and **Modules on Bus**.
2. Click on the **Module <*number*>** you want to program.

   The Bus <*number*>-Module: <*number*> screen appears. The following figure shows an example of the fields that display for a PRI module type.

Figure 29 Example of PRI module settings



3. Click on the arrow beside the **Module type** field and choose the correct setting that defines the type of lines for the module.

   The module installed in the system and Module Type must match the defined type of loop or trunk and associated services provided by the central office line that you intend to be connected to the module.

   Note: When you configure a media bay module for PRI, BRI, or DECT, the system may download new software to the module. This takes a couple of minutes to complete. Allow the download to finish before continuing to program the module.

4. Press **<TAB>** on your keyboard to update the record.

   Tips: To refresh the record, you may need to click on another navigation tree heading and then re-enter the module record you were working on.

5 Check the settings to ensure they reflect the line requirements. Note that only some of the fields appear for all module types.
Refer to the following table for a description of each field.

Table 12 Module record values

Attribute	Value	Module/line type
Module mode	DS/CLID, Global, Legacy	**Loop**
	• DS/CLID: displays for old North American LS/DS or CLID analog trunk modules, the old analog MBM, or the GATM with North American DIP switch settings. • Global: displays for the GATM MBM with no regional DIP switches set. • Legacy: displays for all other (old) analog trunk modules	
# of lines/ loops	<digits>	**Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4**
	The total number of lines or loops provided by the loops or trunks on this module.	
Low/line loop	View only	**Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4**
	The lowest line or loop number assigned by the system to the module based on the Bus number, module type, and the module position on the Bus (offset on module DIP switch).	
High/line loop	View only	**Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4**
	The highest line or loop number assigned by the system to the module based on the Bus number, module type, and the module position on the Bus (offset on the module DIP switch).	
Disconnect timer	60, 100, 260, 460, or 600 milliseconds	**Loop T1**
	Specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO). You must enable disconnect supervision by changing the **Trunk mode** attribute. Under the Telephony Services sub-heading, choose Lines and Line/trunk Data. See "Assigning Trunk/line data" on page 236 for more information. Note: Available to all supported countries for BCM 3.6 and newer software.	
Answer timer	1, 2, 3, 4, or 5 sec.	**E&M PRI**
	Set the minimum duration of an answer signal before a call is considered to be answered.	

Table 12 Module record values (Continued)

Attribute	Value	Module/line type
Protocol	NI, DMS100, DMS250, AT&T4ESS, SL-1, Euro, ETSI Q-Sig	**PRI**
	Choose the trunk protocol used by your service provider. The supported protocols are: **PRI-T1:** NI (NI-1 and NI-2), DMS100, DMS250, AT&T4ESS, SL-1 **PRI-E1:** ETSI QSIG, Euro, SL-1 **Note:** SL-1 and ETSI QSIG require an MCDN keycode to display. **BRI:** Protocol can also be selected on BRI T-loops under the **Services/Telephony/Loops** heading. **Note:** Always check the line protocol with the central office.	
Protocol type	User, Network	**PRI**
	When you select SL-1 protocol, an additional setting, Protocol type, appears. SL-1 protocol is a private networking protocol. This allows you to designate a Business Communications Manager node as a Network (Master). The default setting is User (Slave). In public network configurations, the CO is generally considered the Network side or Master. Applies to SL-1 protocol only.	
NSF Extension	None, WATS, ALL	**PRI**
	The Network Specific Facilities (NSF) information element is used to request a particular service from the network. Settings are based on the type of switch to which the line connects. Suggested settings: DMS100/250: NONE Siemens ESWD, Lucent 5ESS: WATS GTD5, DMS10: ALL When you select **NONE**, the NSF extension bit is not set for any service. When you select **WATS**, the NSF extension bit is set for unbanded OUTWATS calls. When you select **ALL**, the NSF extension is always set for all CbC services. Appears only for NI protocol.	
B-channel selection sequence	Ascending Sequential Descending Sequential	**PRI**
	Defines how B-channel resources are selected for call processing. For more information, see “PRI B-channel provisioning” on page 142.	

Table 12 Module record values (Continued)

Attribute	Value	Module/line type
Clock Source	Primary, Secondary, Timing Master	**T1** **PRI** ***BRI S/T** ***BRI U2** ***BRI U4** **DASS2**
	Designates whether the DTM/BRI acts as a primary or secondary timing slave or as a Timing Master. **Note:** A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be Timing Master if a DTM exists on the system to be the Primary clock source. *BRI clock source is set on the Services, Loops, Loop XXX screen. Refer to "Identifying BRI T-loops (T1 profiles)" on page 267 or "Identifying BRI T-loops (ETSI, QSIG)" on page 271. For more information, see "Determining Clock Sources for DTMs or BRIs" on page 135.	
Send Name Display	Y, N	**PRI** ***BRI QSIG**
	When set to Y, the system sends a specified outgoing name display (OLI) from the calling telephone. Appears only for Protocols: SL-1, NI, DMS100, DMS250, or PRI QSIG. *BRI QSIG Send Name Display is set on the Services, Loops, Loop XXX screen. Refer to "Identifying BRI T-loops (ETSI, QSIG)" on page 271.	
Remote Capability MWI	Y, N	**PRI**
	This setting allows you to indicate MWI compatibility on the specific loop(s) that you are using to connect to the central voice mail system on a Meridian 1 which has the MWI package installed, with the RCAP setting set to MWI. Appears only for SL-1 protocol.	
Max Transits	Default: 31	**PRI**
	Indicate the maximum number of times that a call will be transferred within the SL-1 network before the call is dropped. Protocol must be set to SL-1 to display this field.	
Host node	M1, Embark, IDPX, DSM	**DNPSS**
	DPNSS cards connected to Embark switches have a different way of handling call diversion, therefore, when you provision a DTM for DPNSS, you must indicate what type of switch the lines are connected to. When you select the Embark switch, calls are diverted using the Call Forwarding feature instead of call diversion.	

Programming Tips - DECT module: The Module Type for the DECT module is DECT. Refer to "Configuring DECT resources" on page 149 for a description of the Resources headings for DECT, and to the *DECT Installation and Maintenance Guide* for details about setting up the DECT system.

6 Press **<TAB>** to save the settings.

7 If your module is set to T1, PRI, or DASS2, refer to "PRI Call-by-Call service selection" on page 138 to continue with the configuration.

8 After you have completed your module configurations, refer to Chapter 9, "Configuring lines," on page 227 to set up the lines the trunk modules will use.

Determining Clock Sources for DTMs or BRIs

Clock Source allows you to designate the DTM or BRI on the system that obtains the timing reference for synchronization from the network.

Systems with digital interfaces need to synchronize to the network in order to function. Synchronization follows a hierarchical path. Each device (switch) obtains the network clock from the device above it in the synchronization hierarchy. The device then passes the network clock to the device below it in the synchronization hierarchy. The synchronization levels are referred to as strata.

Business Communications Manager systems are stratum 4E equipment and are usually used as termination points in a network.

For each DTM and BRI, choose one of the following settings: **Primary**, **Secondary**, or **Timing Master**:

- Primary reference —The DTM/BRI obtains the timing reference from the network and the system synchronizes to it. This is the default value for the first DTM in Business Communications Manager. Note that there should only be one defined Primary clock source on a System.
  Private network: If this system is in a private network and is intended to provide the master clock for that private network, the system must have one and only one Primary clock reference on a DTM or BRI. If this system is intended to act as clock master in a private network, then all clock sources should be set to Timing Master on this system.

- Secondary reference —The DTM/BRI acts as a standby reference. If there are excessive errors on the Primary reference link, or the DTM/BRI designated as Primary reference fails, the Secondary DTM/BRI obtains the timing reference from the network to be used for system synchronization. This is the default value for the second DTM in a Business Communications Manager.
  Private network: If this system is in a private network and is intended to provide the Master clock for that private network, then there should be no Secondary reference defined on any DTM/BRI. Note that there should only be one defined Secondary clock source on a system.

- Timing Master —The DTM/BRI does not obtain timing from the network, but transmits the internally-generated system timing, which is derived from the Primary/Secondary source, to equipment connected to it.
  Note that while in the absence of a DTM Primary clocking source a BRI module can be used for the primary timing reference, it is always recommended that, when possible, DTM(s) be used as primary (and secondary) clock sources and that any remaining DTMs/BRIs be set to Timing Master.

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

Timing within networks

In most T1/E1 network configurations, you need one DTM or BRI configured as Primary to act as a primary reference and obtain clocking from the network.

The only application where you might not have a DTM/BRI designated as a primary reference is in a private DTM/BRI network where your Business Communications Manager system is connected to other equipment using T1/E1/BRI interface(s) that require a clock source and your system had been designated as the source of clocking for that private network.

- If the other switches are to be clocked to your Business Communications Manager system, *all* your DTMs/BRIs should be designated as Timing Master.
- If your Business Communications Manager system has two DTMs, you cannot assign both DTMs as primary reference or both DTMs as secondary reference.
  You can have one Primary reference and one Secondary reference per system.
- A T1, PRI(T1), PRI(E1), or BRI can act as the clock source.

T1 interface parameters (region-specific)

The **T1 parameters** heading appears for module types that have been configured as T1 or PRI. It allows you to define a number of settings that are dependent on your T1 service provider settings.

1. Click the keys beside **Resources**, **`Media Bay Modules`**, **Bus <*number*>**, **Modules on Bus,** and **Module <*number*>**.
2. Click on **T1 Parameters**.
3. Configure the T1 parameters according to the information in the following table.

Table 13 TI parameters

Attribute	Value	Description
CO fail	TIA-547A or TR62411	Select the carrier failure standard used by your T1 or PRI service provider. Consult your T1 or PRI service provider for the proper setting.
Interface levels	ISDN or PSTN	Define a loss plan setting. For more information, see “Interface levels” on page 137.
Framing	ESF or SF	Select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.)

Table 13 TI parameters (Continued)

Attribute	Value	Description
Internal CSU	On or Off	Turn the internal T1 channel service unit (CSU) on or off. For more information, see "Internal CSU" on page 137.
CSU line build	0, 7.5, or 15 dB	Set the gain level of the transmitted signal. This setting appears only when the Internal CSU is set to On.
DSX1 build	000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet	Set the distance between Business Communications Manager and an external channel service unit. This setting only appears when the Internal CSU is set to Off. Contact your service provider for the proper settings.
Line coding	B8ZS or AMI	Define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting.

Interface levels

The default Interface levels are the ISDN loss plan settings.

Check with your telecommunications service provider to determine if your Business Communications Manager system is connected to a central office (CO) with digital network loss treatment (ISDN I/F levels) or analog network loss treatment (PSTN I/F levels).

The ISDN setting requires digital access lines (DAL) that have digital network loss treatment. On a DAL network, the PBX system administers the dB loss not than the CO. DALs may have ISDN signaling or digital signaling (for example, T1). The loss plan follows the Draft TIA-464-C loss plan, which uses a send loudness rating (SLR) of 8 dB. You must contact your service provider to get DAL network loss treatment on a line with digital signaling.

The PSTN setting requires analog access lines (AAL) that have analog network loss treatment and digital signaling. On an AAL(D) network, the CO administers the dB loss.

The loss plan follows the Draft TIA-464-C loss plan. The ISDN loss plan uses a send loudness rating (SLR) of 8 dB and a receive loudness rating (RLR) of 2 dB. The PSTN loss plan uses an SLR of 11 dB and an RLR of -3 dB. If you choose the wrong setting, the voice signal can be too loud or too soft.

Internal CSU

Internal CSU allows you to turn the internal T1 channel service unit on or off. The channel service unit gathers performance statistics for your T1 lines or PRI with public interface. Contact your service provider for the correct settings.

Note: You must disable the DTM before you can change this setting. See "Disabling/enabling a single module" on page 147 for details.

You can view the performance statistics for your T1 lines in Maintenance under the CSU stats heading. Before you set the internal CSU to off, you must ensure there is an external CSU connected to your T1 lines.

E1 parameters (region-specific)

The E1 Parameters command appears for modules that have been configured as PRI in an E1 region. There is only one setting in the E1 Parameters menu - the CRC4 setting. CRC4 checking is enabled at the other end.

1 Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <*number*>**, **Modules on Bus,** and **Module <*number*>**.

2 Click on **E1 Parameters**.

3 Configure the E1 CRC4 parameter as being On or Off to correspond to the CRC4 setting at the far end of the E1 interface.

PRI Call-by-Call service selection

This section provides information about how to configure the PRI Call-by-call Service Selection, which is region-specific to North America, for a DTM set to a PRI Module type.

By default, incoming calls on a PRI are routed based on the Called Party Number information within the call request. The last number of digits of the called party number which matches the Received Number Length setting, are used as Receive Digits to find a target line.

For example, assume an incoming called party number is 800-555-1234. The received digit number length is 4, and the result is 1234. These last four digits are used to route the call.

In North American PRI, the Call-by-Call services allows alternate routing maps to be defined in various ways, depending on the protocol defined for this PRI.

Use this process to define call-by-call services:

1 Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <*number*>**, **Modules on Bus,** and **Module <*number*>**.

2 Click on **Call-by-call service selection**.
The following table lists the applicable services for the protocol defined on the Module <number> record.

Table 14 Services available for each PRI protocol

Protocol	Services Available				
	Foreign Exchg	**Inwats (800)**	**Intl-800**	**Switched Digital (SDS)**	**Nine Hundred (900)**
NI	SID or All	By number or All	N/A	N/A	N/A
DMS-100	SID or All	SID, By number, or All	N/A	N/A	N/A
DMS-250	SID or All	SID, By number, or All	N/A	N/A	SID, or By number, or All
4ESS	N/A	By number or All	By number or All	By number or All	By number or All

3 Select the service you want to change.
A configuration screen appears in the right frame. The Translation mode default is None.

4 The following table shows the possible settings for the services.

Table 15 Module record values

Attribute	Value	Description
Translation Mode	None All By SID By Number	Define how the system maps incoming digits for this service type to the line number within the system. In all cases, the received digits are used to find a target line or to activate remote access.
Translation mode value definitions:		**None:** No mapping is applied. The last digits of the Called Party Number which match the Received Number Length setting are used as received digits. Note that if there is no called party number (may occur with some FX calls) the call will ring at the incoming trunk prime set.
		All: Allows you to define the received digits used for all calls with this service type, regardless of the called party number or service identifier (SID). For this option, all calls with this service type on this PRI will ring the same target line. Depending on the service type and the protocol, you may be able to map the called party number (By number) and the service identifier (SID).
		By SID: Allows you to associate different received digits with different calls of this service type based on the service identifier. **By Number:** Allows you to associate different received digits with different calls of this service type based on party number.
		NOTE: Any calls that do not match any entry defined in the map table will ring at the prime set.
Map Table	Select **Add** on the Map Table screen to create a new map entry From *digits* To *digits*	Enter the incoming line number to the internal line number, such as the target line.

Provisioning lines (PRI, T1, DASS2)

The **Provision lines** heading allows you to provision and deprovision lines associated with a T1 PRI, E1 (DASS2), or BRI ST/U interface.

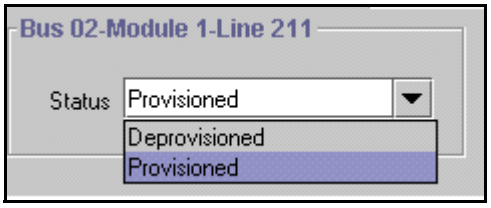
Provisioning a line or loop makes it available for system use. A deprovisioned line/loop is not available for use. If you are purchasing a partial PRI trunk, the lines that have not been assigned must be set to Deprovisioned.

The line number listed in each **Line <*number*>** entry corresponds to the line numbers listed under the **Services, Telephony Services, Lines, Physical Lines, Enabled Physical Lines** menu heading.

Provisioning a line

Note that all PRI lines are provisioned by default.

1. Click the keys beside **Resources,** and **Media Bay Modules**.
2. Choose the a bus number (Bus 02 to 07) associated with the trunk module you want to provision.
3. Click the key beside the **Modules on Bus** heading.
   The single DTM module on this bus appears.
4. Choose the module.
   Expand **Provision lines**.
   All the available lines appear as **Line <*number*>** headings.
5. Click the line you want to provision.
6. From the **Status** box, click **Provisioned**.



Provisioning BRI loops/lines

In order to provision lines on a BRI module you must first provision the loop on which the lines exist.

1. Click the keys beside **Resources** and **Media Bay Modules**.
2. Click the key beside the bus number (Bus 02 to 07) associated with the trunk module you want to provision.
3. Click the key beside **Modules on Bus**.
4. Choose the BRI module where you want to provision loops.
5. Expand **Provision Loops**.
   All the available loops appear as **Loop <*number*>** headings.
6. Click the **Loop <*number*>** you want to provision.
7. In the **Status** box, click **Provisioned**.
8. After provisioning one or more loops on the module:
   a. Refresh the **Loop <*number*>** entry and you will see two **Line <*number*>** entries under this loop.
   b. Click on the **Line <*number*>** you wish to provision.
   c. In the **Status** box, click **Provisioned**

Deprovisioning a line/loop

When you are not using a line/loop, or when you want to cancel it, you can deprovision that line or loop.

Follow these steps to deprovision a line/loop:

1. Click the keys beside **Resources** and **Media Bay Modules**.
2. Click the key beside the bus number (Bus 02 to 07) associated with the module you want to provision.
3. Click the key beside **Modules on Bus**.
   A list of the modules assigned to the Bus appears.
4. Choose the module you want to provision.
   For example, click on Module 1.
5. Click the key beside **Provision lines or Provision Loops**.
   All the available lines/loops appear.
6. Choose the line/loop you want to deprovision.
7. From the **Status** box, click **Deprovisioned**.

Use this procedure if your system configuration requires/receives fewer than the standard number of channels delivered from the PRI line. This is called Fractional T1/PRI. Your service provider might offer you Fractional T1/PRI service to address specific needs on your system.

You should only have as many lines provisioned on a T1/PRI as you have B-channels being delivered on the T1/PRI from your service provider. Having more lines provisioned and assigned to users may occasionally result in the attempt to perform calls over a line failing because of a lack of B-channel resources being available.

Provisioning notes:

- Deprovisioning all of the lines on a DTM does not disable the module.
- BRI loops/lines are deprovisioned by default in the N1 ISDN protocol regions, otherwise they are provisioned by default.

PRI B-channel provisioning

When you purchase PRI from your service provider, you can request the number of B-channels that are allocated for you to use. For example, you may want to use only 12 B-channels instead of 23 B-channels. If you do not have all of the PRI B channels, you should disable all the B-channels that you do not need.

It is recommended that the number of lines that are deprovisioned on an DTM (configured as PRI) be the same as the number of B-channels that are disabled. For example, If the DTM is on bus 07, when B-channels 13-23 are disabled, you should deprovision lines 73 to 83.

1 Choose **Diagnostics**, **Trunk Modules**.

2 Choose a bus, and then choose a module.

3 Choose **B channels**.
A list of the B channels on this module appears.

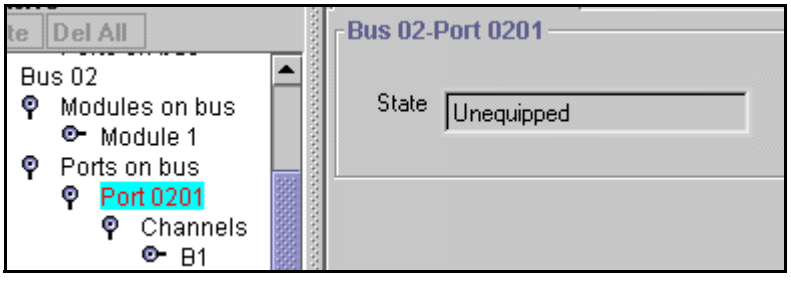
4 Click a channel, for example, **B 01**
The display shows the status of the PRI channel.

5 On the **Configuration** menu, click **Enable** or **Disable** to change the setting for the channel.

Trunk module ports programming

Click on the Port XXX (where XXX is a port number) heading, located under **Ports on Bus**, to access information about the state of the module ports. Each port maps to an incoming line.

Figure 30 Finding state of port on Bus



PRI version information

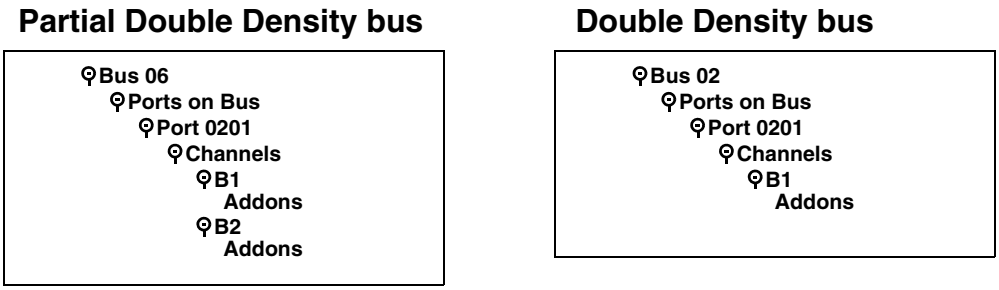
DTM modules that are set to PRI and BRI modules display additional PRI information under **Ports on bus, Port <*number*>, Channels, B1/B2, Addons**. By clicking on the **Addon 01** heading, you can view information about the version of the downloadable firmware component being used in this module. By clicking on the Addon 02 heading, you can view information about the version of the downloadable protocol component being used on this module.

You can enable or disable any port. Refer to "Disabling or enabling a port channel setting" on page 148.

Viewing station module information

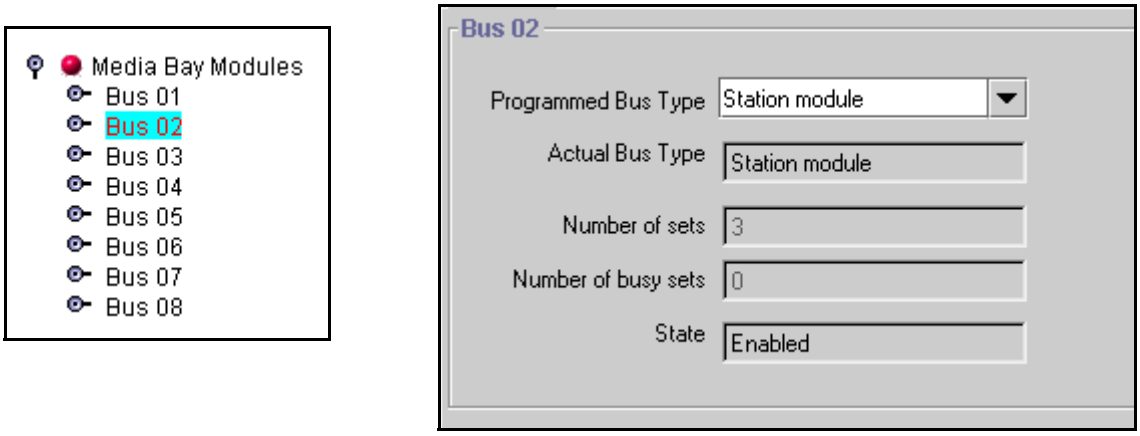
The following figure shows a typical example of the headings for a station media bay module.

Figure 31 Station media bay module Bus headings



When you click on a bus that has a station module installed, you will see a screen that indicates the type of module, the number of ports that are busy on the module, and the operational state of the module.

Figure 32 Bus assigned to a station module



Programming Note: If the **Actual Bus Type** reads **None**, choose the correct setting in the **Programmed Bus Type** field. After the system initializes to the module, the **Actual Bus Type**

should change to the correct module type. You may also have to disable, then re-enable the module to force the system to re-initialize (under the **Configuration** menu). Refer to "Viewing Media Bay Module status" on page 147 for details about enabling and disabling modules.

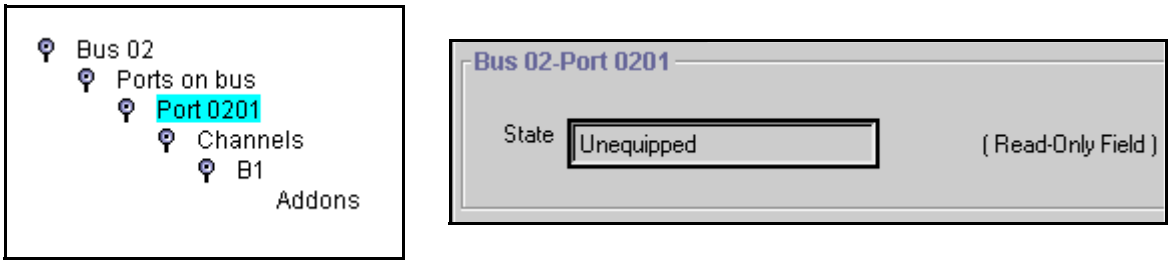
Some modules take a few minutes to reinitialize.

If these actions do not cause the fields to display correctly, you may have a damaged module or back plane. Try installing the module in a different media bay and retry the configuration. Refer to the *Installation and Maintenance Guide* for your hardware for information about removing and installing media bay modules.

Determining station port state

Click on the **Port <*number*>** heading, located under **Ports on Bus**, to access information about the state of the device (media bay module).

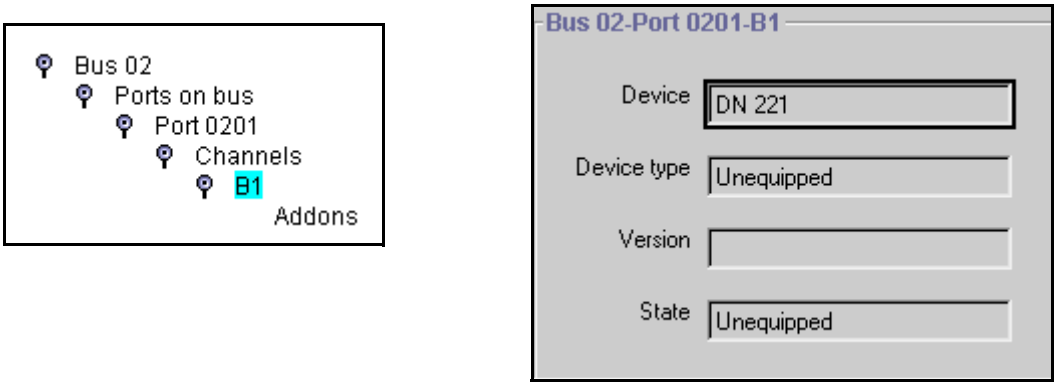
Figure 33 Finding state of port on Bus



Viewing port device information

Under the **Port** heading, the **Channels** heading provides access to device information about the B1 (and B2 for Bus 06 and 07 on PDD systems) media channels. Clicking on the **B1** heading displays the information about the device assigned to that media channel, including the DN of the device, the type of device (model), the version of the firmware on the device, and the state of the device, as set on the Port XXXX screen.

Figure 34 Ports on Bus, B1 screen



You can enable or disable any port. Refer to "Disabling or enabling a port channel setting" on page 148.

Station module line deployment

The MSC presents 32 physical ports for each bus number assigned to a station or analog station module. The DIP switch settings on the module determine which ports support telephone connections. The first 16 ports are based on the B1 channel; the second 16 ports are based on the B2 channel. Therefore, if a single-density DSM 16 module is used, only the first 16 DNs are available for system telephones. Any module that was installed on a BCM version 2.5 or earlier system is single density, which means it would support some of the first 16 ports, depending on the type of module.

On systems running BCM version 3.0 and newer software, if you install DSM 16+ or DSM32+ modules, you can set them to be either single density or double density. An ASM8+ installed on a double density bus can populate all four offsets. If a DSM16+ or DSM32+ are set to double density 32 ports are available, depending on the module and the dip switch settings. Example: A DSM16+ set to double density accesses either the first 16 ports or the second 16 ports, depending on the offset setting. A DSM32+ set to double density accesses the first 16 ports on the lower connector and the second 16 ports on the upper connector.

Partial Double Density systems (PDD), which is the default system setting for BCM version 3.0 and newer software, retain a single-density identity for buses 06 and 07, to allow support for Companion installations which support two handsets for each B1/B2 port. Each port in single density configurations are assigned a B1 and a B2 channel. If you set your system to fully-deployed double density (FDD), both bus 06 and 07 are configured as double density and are no longer available for applications that require both B1 and B2 ports.

You can change your system density from PDD to FDD under the Configuration menu in the MSC programming. (**Services**, **Diagnostics**, **MSC**)

Upgraded systems: BCM version 2.5 systems upgraded to BCM version 3.0 or newer systems have a different DN deployment than newly-deployed BCM version 3.0 systems. In upgraded systems, the first 16 DNs are assigned to DS30 02, the next 16 are assigned to DS30 03, and so on, down to DS30 07. Then the first 16 DNs following this list is assigned to the second 16 lines (B2) on DS30 02, and so on down the list again.

New BCM version 3.0 and newer systems: The DN deployment in these systems is sequential. That is, the first 32 DN numbers are assigned to DS30 02, the second 32 DN numbers are assigned to DS30 03, and so on.

DN numbering for each type of system is displayed in tables in "DN mapping for digital telephones" on page 355

Internally-driven channels

You cannot change headings for buses that are used for internal processing. This section describes how these buses fit into the system.

Bus 01 and Bus 08 provide access to telephony operations for internal processing, applications, and IP sets on the Business Communications Manager system. These two buses are commonly referred to as virtual buses since they have no external physical connections.

Bus 01 has 32 virtual ports. Bus 08 has 28 virtual ports. Each of these ports has one media channel associated with it. These channels are labeled as B1 on the configuration menu. When IP telephones are assigned to the system, they will appear on these ports. The ports are allocated sequentially as telephones are added.

Bus 08 can also be used for a virtual data module (NA only) when a Business Communications Manager data service such as WAN service is activated. Refer to "Configuring a data module" on page 178 for further programming. Note that Bus 08 does not display when there is a WAN active on the system.

By default, Bus 07 is used for a media bay module connection (2/6 channel split). However, if your system was set to a 3/5 DS30 split, then Bus 07 becomes a virtual bus with 32 ports. The headings under Bus 07 become invalid in this configuration. Refer to the "Configuring the MSC resources" on page 609 for further details.

Working with the modules

When you need to find out information about a module, you can determine the status of any of the settings under the media bay modules headings. To correct a problem, or change a module setting, you may need to enable or disable a port, a module, or an entire bus. This section provides the procedures got:

Viewing Media Bay Module status

Media Bay Modules selection allows you to view the status of all the modules as well as identify any device or lines connected to the system. This allows you to isolate any malfunctioning part of the system. In addition, you can use the **Media Bay Module** selection to disable and enable modules and devices. For more information, refer to one of the following procedures.

Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module state:

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
   The window displays **Bus 02** through to **08**.
2. Click heading of the bus you want to view. For example, **Bus 02**.
   The **Configuration** menu is enabled and the status information of the module associated with that bus appears.

Disabling/enabling a DS30 bus

The following procedure describes the process for enabling or disabling a bus. This means that if there is more than one module assigned to the DS30 bus, all modules will be disabled.

1. Click the keys beside **Resources** and **Media Bay Modules**.
   Buses 01 to 07 are displayed.
2. Click on the bus number of the module you wish to enable/disable (Bus 02 to 07).
3. On the top menu, click **Configuration**, and then, click **Enable** or **Disable**.
   The system prompts you to confirm your request.
4. Click the **OK** button.

   Programming reminder: If your system has a 3/5 DS30 split, BUS 07 will not have a module assigned to it.

Disabling/enabling a single module

The following procedure describes the process for enabling or disabling a single module if there is more than one module assigned to a DS30 bus.

1. Click the keys beside **Resources** and **Media Bay Modules**.
   Buses 01 to 07 are displayed.
2. Click on the key beside the Bus number of the module you wish to disable (Bus 02 to 07).
3. Click on the Module number of the media bay module you want to enable/disable.
4. On the top menu, click **Configuration**, and then, click **Enable** or **Disable**.
   The system prompts you to confirm your request.

5 Click the **OK** button.

Programming reminder: If your system has a 3/5 DS30 split, bus 07 will not have a module assigned to it.

Disabling or enabling a port channel setting

If you need to isolate a problem or block access from the module, you may need to turn off individual port channels, rather than the entire module.

To turn off a channel:

1 Click on the keys beside **Resources**, **Media Bay Modules,** and beside the Bus number where the module is located.

2 Click the key beside **Ports on bus**.

3 Click the key beside the port that contains the channel you want to disable.

4 Click the key beside **Channels**.

5 Click on the B channel you want to disable (**B1** or **B2**).

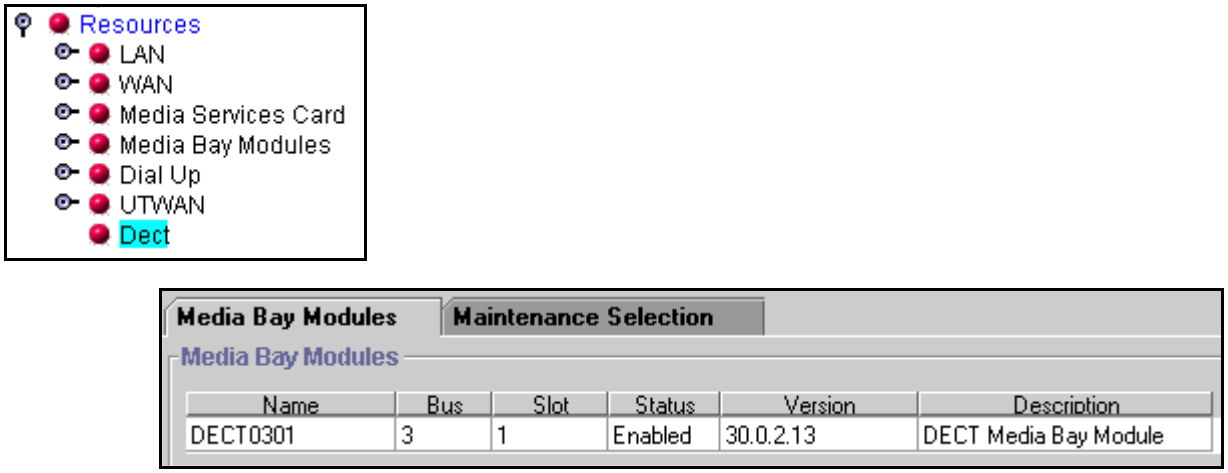
6 On the top menu, click **Configuration** and select **Disable** or **Enable**.
If you are disabling the channel, you will be prompted by a dialog box to confirm your action. The **State** field indicates the mode of operation for the port, as shown in the figure below. If the port is enabled, this field is blank unless a device is physically connected.

Configuring DECT resources

There are three areas on the Unified Manager that you need to program or look for DECT module information:

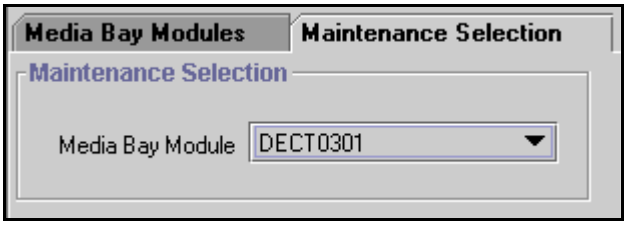
- The DECT module is enabled on the system through the **Resources, Media Bay Module, Bus <*number*>** record, as with all other modules. The difference is that you set the Module Type to **DECT**.
- The **Resources, DECT** menu allows you to view the identification information for the DECT media bay module installed in Business Communications Manager. Refer to the following figure.

Figure 35 DECT media bay module description



- The **Maintenance Selection** tab opens a screen from which you select the DECT module. This allows you to collect maintenance information that can be viewed through the maintenance console under **Services, DECT**. Refer to the following figure.

Figure 36 DECT maintenance selection



The entries on this screen fill automatically when a DECT module is plugged into the Business Communications Manager and the system is powered up. The DIP switch settings on the DECT module define the bus and the slot (offset, always set to 0). The information on the module provides the Version and Description information. The status information is obtained from the **Provision Lines** heading found under **Resources, Media Bay Modules, Bus <*number*>**.

The DECT module contains four internally-accessible BRI loops. These loops are also automatically populated when the module is installed.

Note: The module BRI loops are defined within the module to act as a line pool. DNs are assigned to the loops from within the DECT module interface. This also occurs if you configure your system using the DECT wizards. Refer to the *DECT Installation and Maintenance Guide* for details.

Chapter 6
Data and split-line configuration

This section discusses configuration for modules and applications that require data or combination data/telephony line configuration.

- DDI MUX modules require two DS30 bus positions. This module supports combinations of data channels and T1 lines. A DTM (digital trunk module) contained within the module is programmed using normal DTM line configuration. The data portion of the lines are configured under the second DS30 bus as data lines. The DDI MUX supports using either the internal router or an external router. Refer to "Configuring the DDI Mux module" on page 151.
- The UT-WAN application, performs a similar function as the DTM module, only without using a physical data module. This feature uses an installed DTM for lines and the internal router for data. Refer to "Universal T1 WAN (UTWAN)" on page 159
- Data modules used to configure channels on a WAN interface are always configured under DS30 Bus 08. Refer to "Configuring a data module" on page 178.

Configuring the DDI Mux module

The Digital Drop and Insert (DDI) Mux media bay module enables a Business Communications Manager system to share its connection to a Universal T1 network with a local area network (LAN). A DDI Mux allows you to make more efficient use of your digital network resources and reduces the amount of equipment needed to support your voice and data networks. This module is currently available only for North American installations.

This section contains the following information:

DDI Mux features

The DDI Mux performs the following services:

- provides the functionality of a DTM media bay module (T1 digital lines only)
- splits the incoming T1 line so that some of the lines are used for voice traffic and some of the lines are used for data traffic
- provides either the CSU (Channel Service Unit) or DSU (Data Service Unit) functionality to support connections to data terminal equipment (DTE), such as a router or a bridge
- connects to network devices that support V.35 interfaces

- provides end-to-end transparent bit service
- supports loopbacks between the DDI Mux and the internal Business Communications Manager components, and between the DDI Mux and digital terminal equipment

Note: The DTE cable that connects the Business Communications Manager to the router is ordered separately from the module. If you do not have this cable, ask your customer service representative about how to obtain one.

The following figures provide examples that use internal and external routers with the DDI Mux.

Figure 37 Network overview: DDI MUX connected to 2.5 hardware internal router

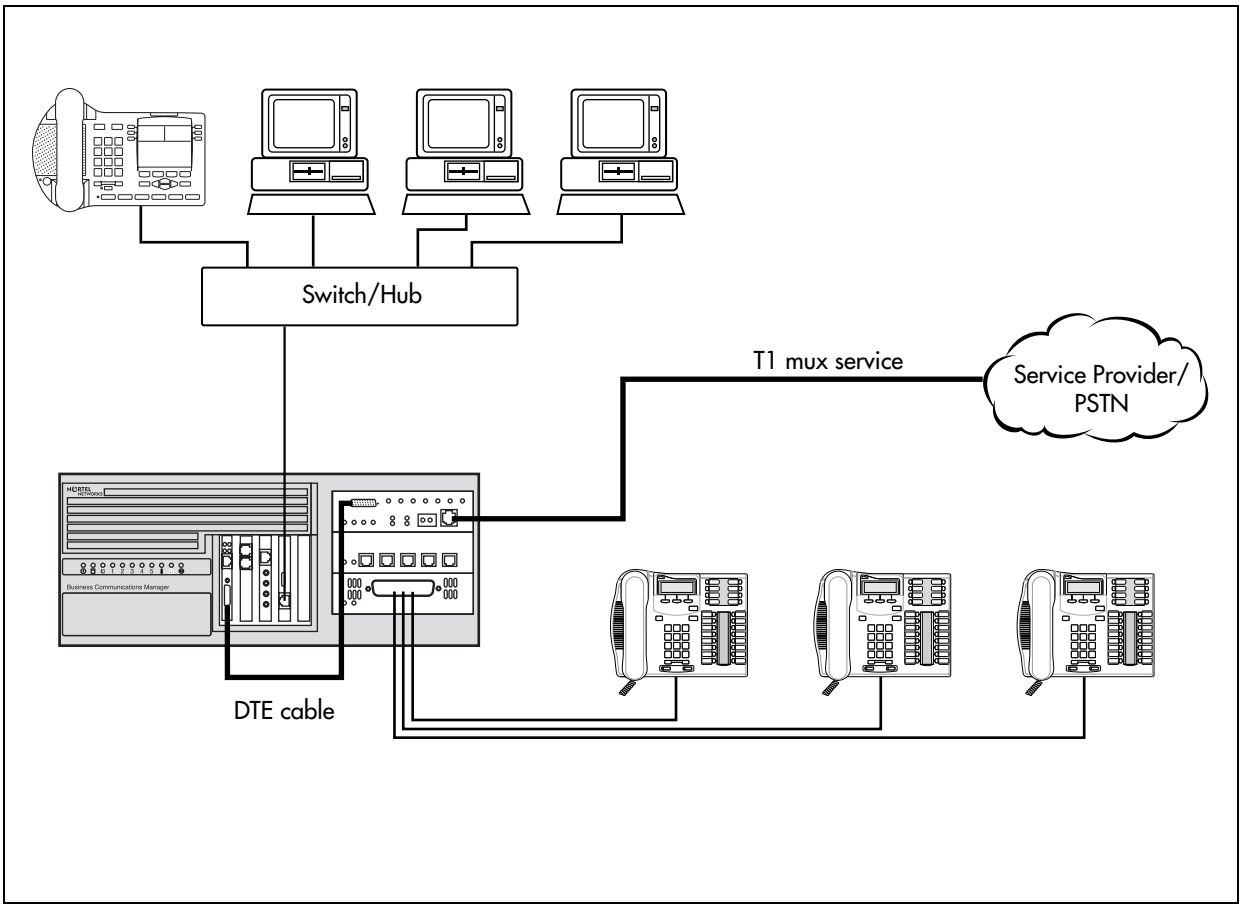


Figure 38 Network overview: DDI MUX connected to BCM400 internal router

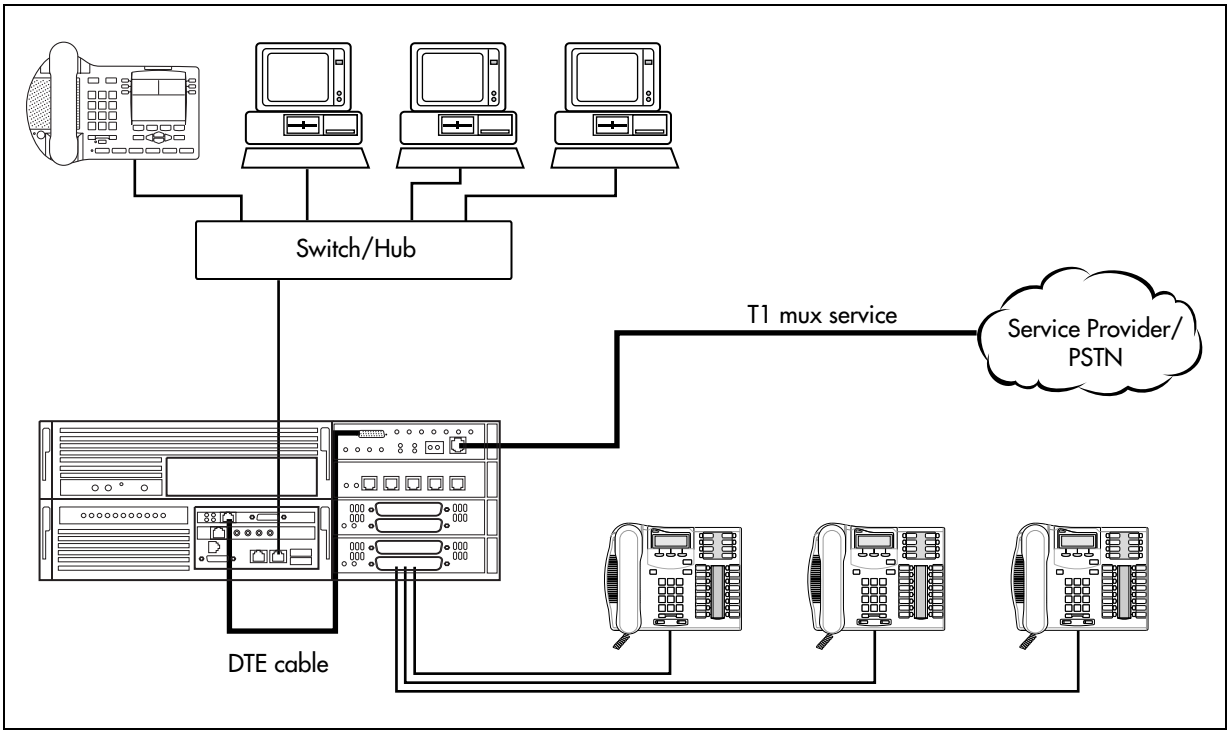
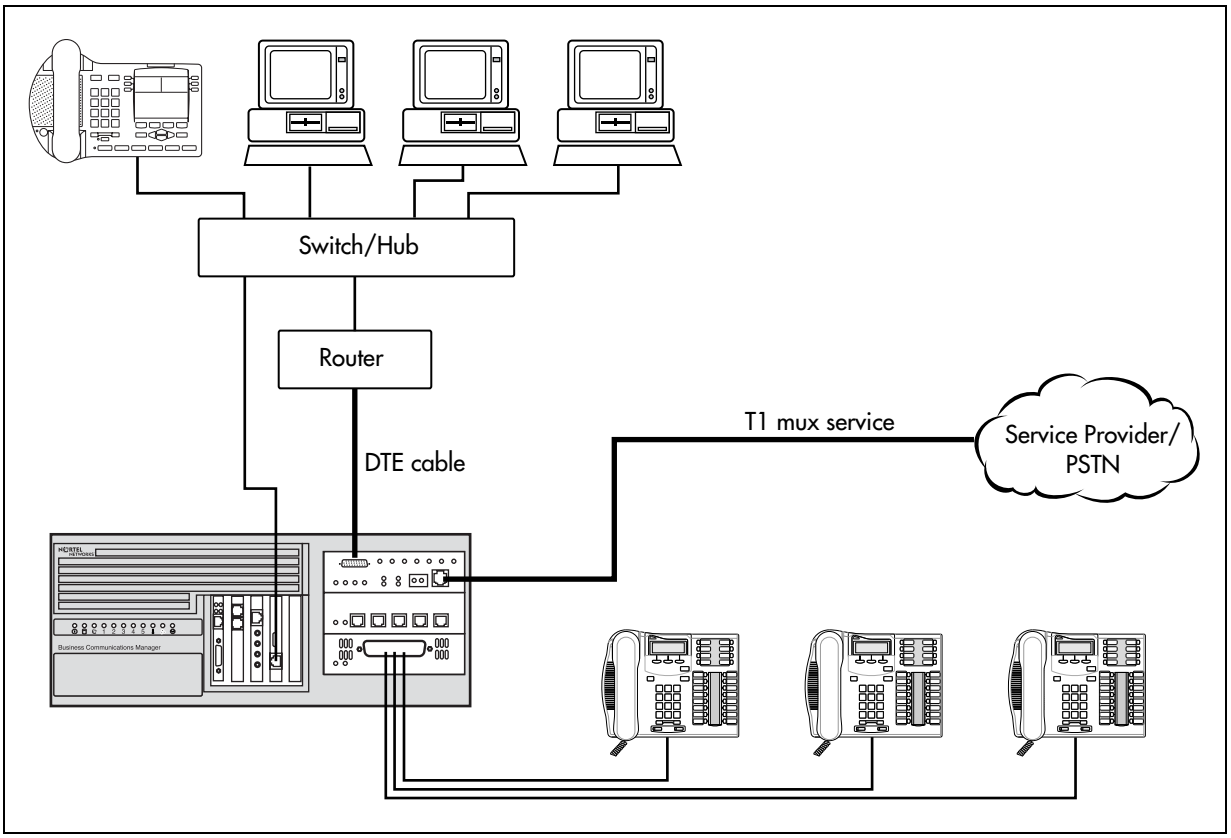


Figure 39 Overview of network using DDI Mux module with an external router



Configuring DDI Mux connections

After you have installed the DDI Mux, configure the module settings in the Unified Manager.

To configure the DDI Mux, you need to:

- assign the DDI Mux modules under Resources, Media Bay Modules
- assign the lines for voice traffic under Services, Telephony Services, Lines
- assign lines to the Data Module portion of the module
- configure the DDI Mux to work with the DTE

Before you start, record the settings for the DDI Mux in the form provided in the Programming Records. At the very least, you need the following configuration information:

Table 16 Configuring DDI Mux connections

Protocol	V.35 ❑	Loopback state:	**Off** ❑ Manual DTE ❑ Manual DS30 ❑ Automatic DTE ❑
Fixed Access			
	Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____		Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____
	Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____		Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____
	Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____		Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____
	Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____		Line ____ Channel ____ Line ____ Channel ____ Line ____ Channel ____

Assigning the DDI mux modules

1. Click the keys beside **Resources** and **Media Bay Modules**.
2. Click the DS30 Bus heading that was assigned to the DDI Mux.
   This Bus is the same as the DS30 bus you assigned to the DDI Mux using the DIP switches on the module.
3. Make sure the option in the **Programmed Bus Type** drop list is **Trunk module**.
4. Click the heading of the next DS30 Bus.
   This Bus is the DS30 bus automatically assigned to the Data Module portion of the DDI Mux.
5. Click the **Programmed Bus Type** drop list, then click **Data module**.

Assigning lines for voice traffic

A digital T1 line has up to 24 telephone lines available for use. On the DDI Mux, you can assign some of these lines to telephony traffic and some to data traffic.

For the lines that you want to use for telephony traffic, configure the lines in the same manner as you configure lines for a DTM. For information about how to configure digital lines on a DTM, refer to "Provisioning lines (PRI, T1, DASS2)" on page 140.

Assigning lines to the data module

The number of lines you assign to the data module determines the bandwidth of your data networking connection. The following table shows the allocated bandwidth for the DDI Mux according to the number of lines assigned. The allocated bandwidth also depends on the line data rate indicated by the B-channel data rate parameter.

Table 17 List of all the multiples of 56000 and 64000 bits/s

Number of lines selected	56000 bits/s	64000 bits/s
1	56000	64000
2	112000	128000
3	168000	192000
4	224000	256000
5	280000	320000
6	336000	384000
7	392000	448000
8	448000	512000
9	504000	576000
10	560000	640000
11	616000	704000
12	672000	768000

Number of lines selected	56000 bits/s	64000 bits/s
13	728000	832000
14	784000	896000
15	840000	960000
16	896000	1024000
17	952000	1088000
18	1008000	1152000
19	1064000	1216000
20	1120000	1280000
21	1176000	1344000
22	1232000	1408000
23	1288000	1472000
24	1344000	1536000

To assign a line to the data module, you must change the line type to Fixed Data Channel and then assign the line to the data module.

Changing the line type

1. In the Unified Manager, click the keys beside **Services** and **Telephony Services**.
2. Click the **Lines** key and then click the **Physical lines** key.
3. Click the **All physical lines** key.
4. Click the key of one of the line numbers assigned to the Data Module.

5 Click the **Trunk/line data** heading.

6 Click the **Trunk type** drop list and then click **Fixed data channel**.

7 Repeat steps 5 to 7 for each line you want to assign to the Data Module.

Assigning the line

1 Click the **Resources** key and then the **Media Bay Modules** key.

2 Click the key beside the Bus number assigned to the Data Module.
In this release of Business Communications Manager, the Data Module is always Bus 08.

3 Click the **Data module** key and click the **Interfaces** key.

4 Click the key beside the Interface to which you want to add a line. For example, click the key beside **Interface 02**.

Note: You can add all of the lines to the single Interface, or you can the lines to multiple interfaces.

5 Click the **Line assignment** heading below you Interface to which you are adding lines.

6 Click the **Add** button.
The Add Fixed line assignment dialog box appears.

7 In the **Line** box, enter the line number of one of the lines assigned to the Data Module.

Note: You can assign up to 24 lines to the DDI Mux.
You can assign only Fixed lines.

8 Click the **Save** button.

9 If you are adding all of the lines to a single Interface, repeat steps 6 to 8 for each line you want to assign to the Data Module.
If you are adding the lines to multiple Interfaces, repeat steps 4 to 8 for each line you want to assign to the Data Module.

Removing a line assignment

If you decide you want to remove a line assignment from the Data Module and use it as a telephony line, use the procedure below:

Removing the line

1 Click the **Resources** key and click the **Media Bay Modules** key.

2 Click the key beside the Bus number assigned to the Data Module.

3 Click the **Data module** key and click the **Interfaces** key.

4 Click the key beside the Interface number from which you want to remove the line assignment.

5 Click the **Line assignment** heading.

6 Click on the line number you want to remove.

7 Click the **Delete** button.

8 On the confirmation dialog box, click the **Yes** button.

Configuring the line for telephony

1 Click the keys beside **Services** and **Telephony Services**.

2 Click the keys beside **Lines**, **Physical lines** and **All physical lines**.

3 Click the key of the line number you want to assign to telephony use.

4 Click the **Trunk/line data** heading.

5 Click the **Trunk type** drop list and then click on the correct type of trunk.

Configuring the DDI Mux to work with the DTE

After you have assigned the lines to the data module, you need to configure the DDI Mux so it can work with the DTE.

1 Click the keys beside **Resources** and **Media Bay Modules**.

2 Click the key of the Bus number for the Data Module portion of the DDI Mux.

3 Click the **Data Module** key and then click on **Configuration**.

4 Configure the setting to match the DTE you are connecting to the DDI Mux.

The following table describes the Data Module configuration settings.

Table 18 DDI Mux Configuration settings

Setting	Value	Description
Protocol	V.35	The DDI Mux supports a V.35 interface standard through its data interface port. You can select V.35.
B channel data rate	64 K 56 K	Select the transmission rate per channel (Fixed data lines) assigned to the module.
Transmit clock source	Auto DCE DTE	The DDI Mux requires a timing signal to clock data transmitted by the DTE. This signal can be supplied by the DTE or generated internally by the [Product Name (short)]. If the signal is generated by the DTE, the clock must be locked to the frequency of the DDI Mux clock. • **Auto**: The DDI Mux checks if the clock provided by the DTE is valid. If the clock is valid, the module uses DTE clocking. If the DTE clocking is not valid, the module uses its own internal clock (DCE). • **DCE**: The internal TxSync clock is used to clock data. • **DTE**: The TXClk clock provided by the DTE is used by the DDI Mux to clock data. **Note**: Use the DTE option only for diagnostic purposes. For all options, the DTE must synchronize to the module.

Table 18 DDI Mux Configuration settings (Continued)

Setting	Value	Description
Transmit clock inversion	Off On	When the internal DCE signal is used to clock in data, signal delays caused by cable length can cause clocking errors. To adjust for round trip delays between the DDI Mux and DTE, invert the internal clock used by the module to clock in data from the DTE. To enable clock inversion, select the **DTE** clock or **Auto** clock.
Data inversion	Off On	When Data Inversion is on, the DDI Mux inverts the data before routing it to the T1 connection and DTE. Inversion allows the module to use the properties of protocols such as HDLC/SDLC (a transmission standard for data) to meet the ones density requirement of the network. This feature must be available and activated at the far end.

Universal T1 WAN (UTWAN)

The UTWAN enables a Business Communications Manager system to use a Universal T1 connection to send and receive voice and data information. By sharing this connection you can make more efficient use of your digital network resources and reduce the amount of equipment needed to support your voice and data networks. The UTWAN is currently available only for North American installations.

Net Link Manager provides continuous WAN connection status monitoring. For information about Net Link Manager, see "Configuring Net Link Manager" on page 749.

UTWAN connection

The UTWAN connection supports frame relay or Point-to-Point protocol (PPP) at the link layer. The link protocol you use depends on the existing network or on the service you buy from your Internet service provider.

Frame Relay

In Frame Relay mode, the UTWAN interface allows up to 50 PVCs (permanent virtual circuits) to be configured. You can assign the same IP for multiple PVCs, or a unique IP for each PVC. To avoid IP routing confusion, it is important that each unique IP belongs to a unique subnet.

The available Data Link Control interface numbers are 0-1023. Of the 1024 PVCs, 16 are reserved. The maximum number of PVCs allowed is 1008.

The range of the Data Link Control Interface (DLCI) numbers is between 0 and 1023. However, within this range, only 16 through 991 are available for user connections. The other ports are reserved as follows:

- 0 and 1023 are reserved for the Local Management Interface (LMI) handshake
- 992 through 1007 are reserved for Frame Relay management at layer 2
- 1 through 15 and 1008 through 1022 are reserved for future use

Point-to-Point-Protocol (PPP)

Point-to-Point Protocol (PPP) is a full-duplex transmission protocol for communication between two computers using a serial interface. A typical PPP connection is a personal computer connected by telephone line to a server. For example, your Internet service provider (ISP) provides you with a PPP connection so that the ISP server can respond to your requests, pass them on to the Internet, and return your requested Internet responses to you.

Fragmentation

Frame Relay fragmentation and PPP fragmentation are link-layer fragmentation schemes.

Over a slow link, the major advantage of using link-layer fragmentation over IP layer fragmentation is that while it reduces the jitter effect for voice packets, it also reduces the end-to-end delay for data packets that is introduced by IP layer fragmentation.

RTP Header compression

The RTP Header Compression feature allows you to compress the 40 byte IP/UDP/RTP header to 2 or 4 bytes. This reduces the header-to-payload ratio of a data transmission. This is particularly true of data transmissions with smaller payloads, such as a IP telephony packets. By reducing the header-to-payload ratio, you can increase your bandwidth utilization. With slower links, this allows more data or simultaneous IP telephony conversations to be carried over the link at the same time.

Data compression

Business Communications Manager provides a WAN Data Compression feature.

On the UTWAN connection, Business Communications Manager supports the following data compression protocols:

- Frame Relay Forum standard FRF.9 data compression protocol with STAC compression algorithm
- PPP Compression Control Protocol (RFC 1962) with STAC compression algorithm

Configuring the Business Communications Manager to use the UTWAN

The UTWAN interface allows circuit-switched voice traffic and packet-switched data traffic (including IP Telephony) to use the same physical link. This requires you to assign some of the T1 lines for voice traffic and some of the lines for data traffic. After you have assigned the lines, you must configure UTWAN link layer parameters for data traffic.

- "Assigning lines for voice traffic" on page 161
- "Assigning lines for data traffic" on page 161
- "Configuring the UTWAN Network Interface parameters" on page 164

Note: Only one DTM can be used for UT1 connection.
Of the 24 available T1 lines, the maximum number of lines that can be assigned for data traffic is 16.

Assigning lines for voice traffic

A digital T1 line has up to 24 telephone lines available for use. When using the UTWAN feature, you can assign some of these lines to telephony traffic and some to data traffic. For the lines that you want to use for telephony traffic, configure the lines in the same manner as you configure other telephony lines. For information about how to configure digital lines, refer to "Provisioning lines (PRI, T1, DASS2)" on page 140.

Assigning lines for data traffic

The number of lines you assign for data traffic determines the bandwidth of your data networking connection. The following table shows the available bandwidth for data traffic on the UTWAN according to the number of lines assigned.

Table 19 Bandwidth available per channel

Number of lines	Bandwidth (bps)		Number of lines	Bandwidth (bps)
1	64000		9	576000
2	128000		10	640000
3	192000		11	704000
4	256000		12	768000
5	320000		13	832000
6	384000		14	896000
7	448000		15	960000
8	512000		16	1024000

Note: The maximum number of lines you can assign for data traffic is 16.
Both ends of the WAN link must be using the same number of lines for data traffic and start with the same time slot.

To assign a line for data traffic, you must change the line type to Fixed Data Channel and then assign the line to the data module.

Determining which lines are available to the UTWAN

The lines that are available to the UTWAN are determined by the DIP switch settings on the DTM you are using for the UTWAN connection. Refer to the table below for a list of lines assigned per DS30 bus.

Table 20 Line numbers for the UTWAN based on the DS30 bus of the DTM

DS30 bus	Type of module	Default Line numbers
02	Digital Trunk Module (DTM)	211-234
03	Digital Trunk Module (DTM)	181-204
04	Digital Trunk Module (DTM)	151-174
05	Digital Trunk Module (DTM)	121-144
06	Digital Trunk Module (DTM)	91-114
07	Digital Trunk Module (DTM)	61-84

Changing the line type

1. In the Unified Manager, click the **Services** key and click the **Telephony Services** key.
2. Click the **Lines** key and click the **Physical lines** key.
3. Click the **All physical lines** key.
4. Click the key of one of the line numbers you want to assign for data traffic.
5. Click the **Trunk/line data** heading.
6. Click the **Trunk type** drop list and click **Fixed data channel**.
7. Repeat steps 4 to 6 for each line you want to assign for data traffic.

Assigning lines to the Data Module

1. Click the **Resources** key and the **Media Bay Modules** key.
2. Click the key beside the Bus number assigned to the Data Module.
   In this release of Business Communications Manager, the Data Module is always Bus 08.
3. Click the **Data module** key and click the **Interfaces** key.
4. Click the key beside the Interface to which you want to add a line. For example, click the key beside **Interface 02**.

Note: You can add all of the lines to the single Interface, or you can the lines to multiple Interfaces.

5. Click the **Line assignment** heading below you Interface to which you are adding lines.

6 Click the **Add** button.
The Add Fixed line assignment dialog box appears.

7 In the **Line** box, enter the line number of one of the lines assigned to the Data Module.

8 Click the **Save** button.

9 If you are adding all of the lines to a single Interface, repeat steps 6 to 8 for each line you want to assign to the Data Module.
If you are adding the lines to multiple Interfaces, repeat steps 4 to 8 for each line you want to assign to the Data Module.

Removing a line assigned for data traffic

If you decide you want to stop using a line for data traffic and use it as a telephony line, use the procedures below:

Removing the line from the Data Module

1 Click the **Resources** key and click the **Media Bay Modules** key.

2 Click the key beside the Bus number assigned to the Data Module.

3 Click the **Data module** key and click the **Interfaces** key.

4 Click the key beside the Interface number from which you want to remove the line assignment.

5 Click the **Line assignment** key.

6 Click on the line number you want to remove.

7 Click the **Delete** button.

8 On the confirmation dialog box, click the **Yes** button.

Configuring the line for telephony traffic

1 Click the **Services** key and click the **Telephony Services** key.

2 Click the **Lines** key and click the **Physical lines** key.

3 Click the **All physical lines** key.

4 Click the key of the line number you want to assign to telephony use.

5 Click the **Trunk/line data** heading.

6 Click the **Trunk type** drop list and then click on the correct type of trunk.

7 Configure the line in the same manner as you configure other telephony lines. For information about how to configure digital lines, refer to "Provisioning lines (PRI, T1, DASS2)" on page 140.

Configuring the UTWAN Network Interface parameters

The first step to configuring the UTWAN Network Interface parameters is:

- "Configuring the UTWAN Summary parameters" on page 164

One of the UTWAN Summary parameters is the link protocol used on the T1 line. When you select the appropriate link protocol, the screen changes to show the parameters required for that link protocol.

The second step to configuring the UTWAN interface is to use one of the following procedures to configure the link protocol specific parameters.

- "Configuring the UTWAN to use a Frame Relay link" on page 166
- "Configuring the UTWAN to use a PPP link" on page 170

If the UTWAN interface has multiple IP addresses, the third step is:

- "Configuring additional IP addresses for the UTWAN" on page 176

Using multiple IP addresses is a common scenario when there are more than one frame relay PVC circuits. When you configure an IP address for each frame relay PVC, each IP address must be valid in the sense that the IP address must have been configured as the primary IP for the UTWAN, or as an additional IP for UTWAN.

Configuring the UTWAN Summary parameters

1. On the navigation tree, click the **Resources** key and click the **UTWAN** key.
2. Click the **UTWAN1** heading.
   The Summary screen appears.
3. Configure the Summary settings according to the information in the following table.

Table 21 UTWAN Summary parameters

Attribute	Description
IP Address	Enter the IP address of the UTWAN interface. The UTWAN IP address must be in the proper dotted format, for example 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask address of the UTWAN. The subnet mask must be in the proper dotted format, for example 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
Physical Address	Shows the physical address of the UTWAN interface.
Description	Provides a description of the UTWAN connection.
Version	Shows the version of the UTWAN interface.
MTU Size	Enter the value for MTU Size.

Table 21 UTWAN Summary parameters (Continued)

Attribute	Description
Status	Shows the current resource status of the UTWAN interface. The possible states are: **Up**: The UTWAN is operational. **Down**: The UTWAN is not operational.
Link Protocol	Lets you select a link protocol. The link protocol you choose depends on the existing network or the service you buy from your Internet service provider. The options for Link Protocol are: **FrameRelay_DCE**: Select this option if you are connecting two Business Communications Manager systems back to back and the other Business Communications Manager system is configured as FrameRelay_DTE. **FrameRelay_DTE**: Select this option if the other end of the WAN link is a Frame Relay router, a Frame Relay switch or a Frame Relay server provided by your Internet service provider. **PPP**: Select this option if the other end of the WAN link is configured to use PPP. The default is **PPP**. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**.

4 Press the **TAB** key to save your settings.

Note: Unified Manager refreshes the UTWAN screen according to the chosen protocol. Your choice of protocol depends on the existing network or the service you buy from your Internet service provider. PPP is the default link protocol. If you change the link protocol the following message appears: “Reminder! Previous setting requires rebooting the system to take effect. Please reboot the system...” Click **OK**.

Caution: Reboot the system.
You must remember to reboot your system for the changes you made to the link protocol to take effect. You can continue UTWAN configuration and reboot the system at a convenient time.

Configuring the UTWAN to use a Frame Relay link

Configuring the UTWAN to use a Frame Relay link consists of the following:

- "Configuring the UTWAN Summary parameters" on page 164
- "Configuring the Frame Relay parameters" on page 166
- "Configuring the PVC Configuration parameters" on page 167

Configuring the Frame Relay parameters

To set the UTWAN Frame Relay Parameters.

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **Frame Relay Parameters** tab.
The Frame Relay Parameters screen appears.

4 Configure the Frame Relay Parameters by referring to the following table.

Table 22 UTWAN frame relay parameters

Attribute	Description
LMI Type	Select the type of local management protocol used on this link. The link management type must be the same as the one used by the frame relay service provider. The available options are **Original LMI, ANSI T1.617 Annex D** or **ITU-T Q.933 Annex A**. The default setting is **ANSI T1.617 Annex D**. Note: The most commonly used setting for this parameter is **ANSI T1.617 Annex D**.
Polling Interval	Enter an interval, in seconds, between Status Enquiry messages. Possible values are between **1** and **100** seconds. The default setting is **6**.
Missing Status Enquiry	Enter the maximum number of consecutive failures permitted in the Status Enquiry before dropping the link. It is also the number of successful consecutive Status Enquiry messages that must be received before marking a link as operational. If you have a backup WAN connection and Net Link Manager configured, the backup connection is started and traffic is routed to the backup when this link is dropped. Also, the backup WAN connection is dropped and traffic is routed to this link when the link is operational. For information about Net Link Manager, refer to "Configuring Net Link Manager" on page 749. Possible values are between **1** and **100** messages. The default setting is **3**.
Expected Status Enquiry	Enter the number of events sampled for making decisions about the Missing Status Enquiry. This value must be set to a higher number than the value set in the **Missing Status Enquiry** box. Possible values are between **1** and **100** messages. The default setting is **6**.
LMI Polling Interval	Enter an interval, in seconds, between LMI status inquiry messages. The polling interval must be the same as the one used by the frame relay service provider's switch. Possible values are between **1** and **100** seconds. The default setting is **10**.

Table 22 UTWAN frame relay parameters (Continued)

Attribute	Description
Status Enquiry Msg Wait Interval	Enter the Status Enquiry Message Wait interval in seconds. Possible values are between **1** and **100** seconds. The default setting is **15**.
Fragmentation Status	Select **EtoE_Enabled** to enable Frame Relay end-to-end fragmentation on this link. Select **Disabled** to disabled Frame Relay Fragmentation on this link. The setting you choose for Fragmentation Status must be the same as the setting on the other end of the Frame Relay link. The default setting is **Disabled**. **Note**: If any PVC needs to do fragmentation, you must select **EtoE_Enabled** for this parameter and then select the End to End Frag option for that PVC.
Low Water Mark	This is one of the parameters that controls the link layer queuing behavior if link layer fragmentation is enabled for this PVC. The possible values are between 1 and 7. The default value is **6**. **Note**: Nortel Networks highly recommends that you do not change the Low Water Mark from the default value.
High Water Mark	This is one of the parameters that controls the link layer queuing behavior if the link layer fragmentation is enabled for this PVC. The possible values are between **2** and **8**. The default value is **7**. **Note**: Nortel Networks highly recommends that you not change the High Water Mark from the default value. **Note**: The high water mark must be larger than the low water mark.

5 Press the **Tab** key to save the settings.

Configuring the PVC Configuration parameters

You must configure the PVC Configuration parameters for each PVC.

Adding a PVC Configuration record

Follow these steps to add a PVC Configuration record:

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PVC Configuration** tab.
The PVC Configuration screen appears.

4 On the **Configuration** menu, click **Add PVC Configuration**.

5 Configure the WAN PVC Configuration parameters according to the information in the following table.

Table 23 WAN PVC Configuration parameters

Column	Description
Entry (CC#)	Define each PVC Configuration entry on the interface. A PVC Configuration entry must use the following format: CC#, where the prefix 'CC' is followed by a number. For example, 'CC2' is a valid PVC Configuration entry. Each entry must use a different number. You must use consecutive numbers when entering PVC Configuration entries. If you do not use consecutive numbers, the system adjusts them to be consecutive. If you add an existing entry, the existing entry is modified with new values. When you modify an entry, the name cannot be changed.
PVCName	Enter a name for this PVC Configuration entry.
DLCI	Enter the Data Link Connection Identifier (DLCI) number for this PVC.
Local IP	Enter the IP address for the PVC. You must enter the IP address in the dotted format, for example 255.255.255.255.
Subnet Mask	Enter the Subnet Mask for the PVC. You must enter the subnet mask in the dotted format, for example, 255.255.255.255.
CIR	Enter the committed information rate in Kbps. The CIR is the rate the carrier guarantees that the router transmits at over a predetermined time interval when congestion is not present. The possible values are **0** are **1024**. The default is 64. Contact your service provider for the correct setting. Business Communications Manager uses one-second intervals to measure this parameter.
Excess Burst BE	Combined with the committed burst rate, lets you set, in Kbps, the maximum number of bits the router transmits over a predetermined time interval if there is no congestion. The combined value of committed burst and excess burst must be less than or equal to the line speed. The possible values are **0** to **1024**. The default value is 64.
DC Retry Time	Enter the Data Compression Retry Time is seconds. The possible values are **1** to **15** seconds. The default value is 3 seconds.
DC Retry Count	Enter the Data Compression Retry Count. The possible values are **1** to **128** retries. The default value is 10 retries.
Compression	Select **RTP Header** to enable RTP Header compression on this PVC. Select **Data** to enable data compression on this PVC. Select **None** to disable compression.
Broadcast	Select **Enabled** to enable broadcast capability on this PVC. When broadcast is enabled, broadcast messages are sent out over this PVC. Select **Disabled** to disable broadcast capability on this PVC. The default setting is **Disabled**.

Table 23 WAN PVC Configuration parameters (Continued)

Column	Description
End to End Frag	Select **Enabled** to enable End-to-End Fragmentation on this PVC. Select **Disabled** to disable End-to-End Fragmentation on this PVC. The default setting is **Disabled**.
Frag Size	Enter the maximum frame size in bytes. Any packets that have a frame size larger than this value will be fragmented. The possible values are **200** to **800** bytes. The default value is 200 bytes.

6 Click the **Save** button.

Modifying the PVC Configuration settings

Follow these steps to modify a PVC Configuration setting:

1 On the navigation tree, click the **Resources** key and click the **UTWAN** Key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PVC Configuration** tab.
The PVC Configuration screen appears.

4 Click the entry you want to modify in the PVC Configuration table

5 On the **Configuration** menu, click **Modify PVC Configuration**.
The PVC Configuration dialog box appears.

6 Change the PVC Configuration parameters.

7 Click the **Save** button.

Deleting a PVC Configuration record

Follow these steps to delete a PVC Configuration record.

1 On the navigation tree, click the **Resources** key and click the **UTWAN** Key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PVC Configuration** tab.
The PVC Configuration screen appears.

4 Click the entry you want to delete in the PVC Configuration table.

5 On the **Configuration** menu, click **Delete PVC Configuration**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button.

Configuring the UTWAN to use a PPP link

Configuring the UTWAN to use a PPP link consists of the following:

Configuring the PPP Parameters

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PPP Parameters** tab.
The PPP Parameters screen appears.

4 Configure the PPP Parameters settings according to the information in the following table.

Table 24 PPP Parameters

Attribute	Description
Compression Status	Select **RTP Header** to enable RTP Header compression on this PPP link. Select **Data** to enable data compression on this PPP link. Select **None** to disable compression.
Fragmentation Status	Select **Enabled** to enable fragmentation on this link. Select **Disabled** to disabled fragmentation on this link. The setting you choose for Fragmentation Status must be the same as the setting on the other end of the PPP link. The default setting is **Disabled**.
Fragmentation Trigger	Select **FrameSize** if you want Business Communications Manager to use the size of the packet to decide if the packets need to be fragmented. Select **DelayTime** if you want Business Communications Manager to use delay time to decide if the packets need to be fragmented.
Frame Size	This parameter is only available if you selected **FrameSize** for the Fragmentation Trigger parameter. Enter the maximum frame size in bytes. Any packets that have a frame size larger than the size specified are fragmented. Possible values are **160** to **800** bytes. The default value is 256 bytes.
Delay Time	This parameter is only available if you selected **DelayTime** for the Fragmentation Trigger parameter. Enter the maximum delay time, in milliseconds, for the packets. If the delay time exceeds this value the packets are fragmented. Possible values are 10 to 40 milliseconds. The default value is 10.

Table 24 PPP Parameters (Continued)

Attribute	Description
Low Water Mark	This is one of the parameters that controls the link layer queuing behavior for PPP when link layer fragmentation is enabled. Possible values are **1** to **7**. The default value is 6. **Note**: Nortel Networks highly recommends that you do not change the Low Water Mark from the default value.
High Water Mark	This is one of the parameters that Controls the link layer queuing behavior for PPP when link layer fragmentation is enabled. Possible values are **2** to **8**. The default value is 7. **Note**: Nortel Networks highly recommends that you do not change the High Water Mark from the default value. **Note**: The High Water Mark must be a larger than the Low Water Mark.

5 Press the **TAB** key to save your settings.

Configuring the LCP Options

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **LCP Options** tab.
The LCP Options screen appears.

4 Configure the LCP Options according to the information in the following table.

Table 25 LCP Options

Attribute	Description
Receive packet size	Enter the maximum size of the received packets. Possible values are **64** to **1614** octets. The default value is **1500** octets.
Authentication Mode	Specify the Authentication mode used by this link. Select **CHAP** if you are using CHAP authentication on this link. Select PAP if you are using PAP authentication on this link. Select **None** if no authentication is required on this link. The default value is **None**.
MultilinkMRRU	Enter the maximum number of octets that can be in the information field of the reassembled packet. Possible values are **64** to **1614** octets. The default value is **1500** octets.

Table 25 LCP Options (Continued)

Attribute	Description
MultilinkSSN	Select if you want to receive fragments with short, 12-bit sequence numbers Select **Enabled** if you want to receive short sequence numbers. Select **Disabled** if you do not want to receive short sequence numbers. The default value is **Disabled**.
MultiLinkEDClass	Enter the Multilink Class for the Endpoint Discriminator. Possible values are **0** to **5**. The default value is 1.
MultiLinkEDValue	Enter the Multilink identifier address for the Endpoint Discriminator.
LCP Timeout Value	Enter the number of seconds waited before retransmitting Configure-Request and Terminate-Request packets. Possible values are **1** to **60** seconds. The default value is 3 seconds.
LCP Max Terminate Request	Enter the maximum number of Terminate-Request packets sent. Possible values are **1** to **5**. The default value is 2.
LCP Max Configure Request	Enter the maximum number of Configure-Request packets sent. Possible values are **1** to **15**. The default value is 10.
LCP Max Configure Nak	Enter the maximum number of Configure-NAK packets sent. Possible values are **1** to **10**. The default value is 5.
LQ Reporting Period	Enter the maximum time in 100th of seconds between the transmission of packets. Possible values are **100** to **60000**. The default value is 1000.
Retry Timer Timeout Value	Enter the number of seconds waited before retransmitting LCP Configure-Request packets. Possible value are **30** to **180**. The default value is 60.

5 Press the **TAB** key to save your settings.

Configuring the IPCP Options

1. On the navigation tree, click the **Resources** key and click the **UTWAN** key.
2. Click the **UTWAN1** heading.
   The Summary screen appears.
3. Click the **IPCP Options** tab.
   The IPCP Options screen appears.
4. Configure the IPCP Options according to the information in the following table.

Table 26 IPCP Options

Attribute	Description
IPCP Timeout Value	Enter the number of seconds waited before retransmitting Configure-Request and Terminate-Request packets. Possible values are **0** to **65000** seconds. The default value is 3 seconds.
IPComp Protocol	Enter the IPComp Protocol. Possible values are **0** to **65000**. The default value is 0.
IPCP Max Terminate Request	Enter the maximum number of Terminate-Request packets sent. Possible values are **0** to **65000**. The default value is 2.
IPCP Max Configure Request	Enter the maximum number of Configure-Request packets sent. Possible values are **0** to **65000**. The default value is 10.
IPCP Max Configure Nak	Enter the maximum number of Configure-NAK packets sent. Possible values are **0** to **65000**. The default value is 5.

5. Press the **TAB** key to save your settings.

Configuring the PPP User List

You can restrict access to the network using the PPP User List. Business Communications Manager uses the information on this list to verify and confirm the identity of the user. Only those users whose names appear on the PPP User List can access the network. The PPP User List configuration allows you to add, modify or delete an item on the list.

Adding an interface to the PPP User List

To add an item to the PPP Password List:

1. On the navigation tree, click the **Resources** key and click the **UTWAN** heading.
   The Resources screen appears.
2. Click the **UTWAN1** heading.
   The Summary screen appears.
3. Click the **PPP User List** tab.
   The PPP User List screen appears.
4. On the **Configuration** menu, click **Add PPP User&Password**.
   The Interface List dialog box appears.
5. Configure the PPP User List parameters according to the following table.

Table 27 PPP User parameters

Attribute	Description
Entry (PP#)	Enter the PPP User identifier. The Entry number uniquely identifies an user on the PPP User List. The value for this setting must follow certain conventions. You must type the prefix 'PP' followed by a unique number identifying the PPP User. For example, 'PP2' is a valid name. If you specify an existing Entry number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Entry number does not have any significance, other than uniquely identifying a PPP User.
Interface Name	Enter the name for the interface. This is the name that is used to identify this specific interface.
Host Name	Enter a name for the remote host. The host name can be up to 32 characters in length.
PPP User Name	Enter the user name associated with the computer you want Business Communications Manager to identify as a valid network user. The User Name can be up to 32 characters in length. You must overwrite the default user name User with the user name you want to add to the list.
PPP Password	Enter the password you want to assign to the user defined in the PPP User Name box. The password can contain a combination of lowercase and uppercase letters and numbers. The Password can be up to 32 characters in length.

Table 27 PPP User parameters (Continued)

Attribute	Description
PPP Remote User Name	Enter the user name associated with the computer you want Business Communications Manager to identify as a valid network user. The Remote User Name can be up to 32 characters in length. You must overwrite the default user name User with the user name you want to add to the list.
PPP Remote Password	Enter the password you want to assign to the user defined in the PPP User Name box. The password can contain a combination of lowercase and uppercase letters and numbers. The Remote Password can be up to 32 characters in length.

6 Click the **Save** button.

To modify an existing item on the PPP User List:

1 On the navigation tree, click the **Resources** key and click the **UTWAN** heading.
The Resources screen appears.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PPP User List** tab.
The PPP User List screen appears.

4 Click the PPP User you want to modify.

5 On the **Configuration** menu, click **Modify PPP User&Password**.
The PPP User List dialog box appears.

6 Change the PPP User parameters.

7 Click the **Save** button.

To delete an item from the PPP User List

1 On the navigation tree, click the **Resources** key and click the **WAN** heading.
The Resources screen appears.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **PPP User List** tab.
The PPP User List screen appears.

4 Click the PPP User you want to delete.

5 On the **Configuration** menu, click **Delete PPP User&Password**.
A confirmation dialog box appears.

6 Click the **Yes** button.

Configuring additional IP addresses for the UTWAN

You can assign multiple IP addresses to a single WAN interface that is configured to use frame relay. Using this functionality, you can configure the Business Communications Manager as the hub in a hub and spoke configuration. When Business Communications Manager is the hub or central site, Business Communications Manager can provide at least two IP address classes on the primary WAN interface. This allows the system to provide Direct Mode capability.

Examples of uses of multiple IP addresses

- You can use a single WAN physical link to connect to both an intranet and the internet using separate addressing schemes.
- A network service provider can create a separate IP address for management functions over the WAN interface.

In both of these examples, broadcast traffic destined for one IP address would not be transmitted on the links associated with the other IP address.

Restrictions when using multiple IP addresses

- Nortel Networks does not recommend using more than two IP address classes.
- Multiple IP addresses supports RIP routing.
- IPSec does not support the use of these multiple IP addresses for Branch Office Local Endpoint Addresses, Remote Endpoint Addresses or the Destination IP Address for IPSec VPN Clients

Adding an additional IP address

1. On the navigation tree, click the **Resources** key and click the **UTWAN** key.
2. Click the **UTWAN1** heading.
   The Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. On the **Configuration** menu, click **Add Additional IPAddress**.
   The Additional IP Address screen appears.
5. Configure the Additional IP Address parameters with the information in the following table.

Table 28 Additional WAN IP addresses

Attribute	Description
Range (AA#)	Enter the Additional IP Address identifier. The Range number uniquely identifies an Additional IP Address. The value for this setting must follow certain conventions. You must type the prefix 'AA' followed by a unique number identifying the Additional IP Address. For example, 'AA2' is a valid name. If you specify an existing Range number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Range number does not have any significance, other than uniquely identifying an Additional IP Address.
IP Address	Enter the Additional IP address of the WAN interface in the following format: 255.255.255.255.
Subnet Mask	Enter the subnet mask of the WAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your system administrator or your Internet service provider.

6 Click the **Save** button.

Modifying an additional IP address

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to modify.

5 On the **Configuration** menu, click **Modify Additional IPAddress**.
The Additional IP Address screen appears.

6 Change the Additional IP Address parameters.

7 Click the **Save** button.

Deleting an additional IP address

1 On the navigation tree, click the **Resources** key and click the **UTWAN** key.

2 Click the **UTWAN1** heading.
The Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to delete.

5 On the **Configuration** menu, click **Delete Additional IPAddress**.
A confirmation dialog box appears.

6 Click the **Yes** button.

Viewing the UTWAN performance

To access the UTWAN performance graphs and tables:

1. On the navigation tree, click the **Resources** key and click the **UTWAN** key.
2. Click the **UTWAN1** heading.
   The Summary screen appears.
3. On the **Performance** menu, click **UTWAN1 Graph**.
   The WAN Graph: Statistic Chart appears.
4. On the **Performance** menu, click **UTWAN1 Table**.
   The WAN Table: Statistic Table appears.

Viewing UTWAN resources

To view the UTWAN resource:

1. On the navigation tree, click the **Resources** key and click the **UTWAN** heading.
   The Resources screen appears.

Configuring a data module

DS30 bus 08 is reserved for configuring circuit switched B-channels as a WAN interface for the Business Communications Manager. This allows the Integrated QoS Routing feature to create one or more dial up ISDN connections via the PSTN network using PRI or BRI trunks. Business Communications Manager automatically configures the Module type as a Data Module and sets the Data module type to Baystack. Baystack is the only setting supported on Business Communications Manager.

This section includes information about:

- "Viewing the data module settings"
- "Programming the BayStack settings"

Viewing the data module settings

Use the following procedure to view the current settings for the data module.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** heading.
   The Bus 08 screen appears.

Programming the BayStack settings

When you select the BayStack data module, the following configuration settings appear:

- Line pool access
- Line assignment
- Interfaces

This section provides information about:

Fixed access

Fixed access is supported for the Norstar Data Interface (NDI) only. To assign one or more Fixed lines to the data module:

Adding line assignments

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Interfaces** key.
4. Click the key of the interface to which you want to assign lines.
5. Click the **Line assignment** heading.
6. Click the **Add** button.
   Or, right click the **Line assignment** heading and click **Add**.
   The Add Line assignment screen appears.
7. Enter the number of the Fixed line you need to assign to the interface.
8. Click the **Save** button.
9. Click the heading for the line you added.
10. Select **Unassigned** or **Assigned**.
11. Record each channel and line combination. Each channel used by the BayStack data module maps to a line.

Deleting line assignments

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Interfaces** key.
4. Click the key of the interface from which you want to delete lines.
5. Click the **Line assignment** key and click the heading for the line you want to delete.

6 Click the **Delete** button.
Or, right click the heading for the line assignment you want to delete and click **Delete**.
A confirmation dialog box appears.

7 Click the **Yes** button.

Switched access (PRI & BRI)

You can assign ISDN lines to the BayStack data module to provide:

- normal data network access for the data module
- dial-up backup and overflow bandwidth (additional channels or trunks) as needed

Line assignment

You can assign one or more lines to the BayStack data module for incoming data transmission.

Note: The data module will answer data calls only. It will not answer voice calls.

Adding line assignments

1 On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.

2 Click the **Bus 08** key and click the **Data Module** key.

3 Click the **Line assignment** heading.

4 Click the **Add** button.
Or, right click the **Line assignment** heading and click **Add**.
The Add Line assignment screen appears.

5 In **Line** box, enter the number of the trunk or a target line you need to assign to the BayStack data module.

6 Click the **Save** button.

7 Click the heading for the line you added.

8 In the **Dial-in number** box, enter the Dial-In Number for the line (up to 24 digits). The number must match the Dial-In Number entered for the line and channel in BayStack data module programming.

9 Assign additional lines to the BayStack data module as required.

Deleting line assignments

1 On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.

2 Click the **Bus 08** key and click the **Data Module** key.

3 Click the **Line assignment** key and click the heading for the line you want to delete.

4 Click the **Delete** button.
Or, right click the heading for the line assignment you want to delete and click **Delete**.
A confirmation dialog box appears.

5 Click the **Yes** button.

Line pool access

You can give the BayStack data module access to a line pool for outgoing data transmission.

Adding line pool access

1 On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.

2 Click the **Bus 08** key and click the **Data Module** key.

3 Click the **Line pool access** heading

4 Click the **Add** button.
Or, right click the **Line pool access** heading and click **Add**.
The Add Line pool access screen appears.

5 In **Pool** box, enter the letter of the line pool to provide access to the BayStack data module. You must program line pool access when you select the switched access settings for the BayStack data module. To use PRI line pools, program the BayStack data module to use a destination code.

6 Click the **Save** button.

Deleting line pool access

1 On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.

2 Click the **Bus 08** key and click the **Data Module** key.

3 Click the **Line pool access** key and click the heading for the line pool you want to delete.

4 Click the **Delete** button.
Or, right click the heading for the line pool you want to delete and click **Delete**.
A confirmation dialog box appears.

5 Click the **Yes** button.

Chapter 7
Telephony Services overview

The following sections provide a general overview of the Unified Manager **Telephony Services** headings. This group of settings is located under the **Services** heading on the Unified Manager main navigation tree. The records under this heading allow you to define how the lines and telephones in your system operate.

Caution: Programming affects system operation.
Only a qualified system administrator should perform startup, installation and maintenance programming. Many of the settings affect correct system operation.

This overview describes the following general process information:

- "Process map: Creating telephony services" on page 185
- "Telephony Services headings" on page 186
- "Planning your telephony services" on page 188

Planning: When you are ready to start planning your telephony system, the sections called "Telephony feature planning" on page 193 provides a quick reference guide to programming telephony features. Features are divided into sections based on task, and each feature provides links to the part of the document where detailed programming information resides.

Using Wizards: When you need to configure a number of telephones, the Edit DN Record Template and Add Users Templates wizards provide many of the programming details for telephone operations in easy-to-apply wizard applications. Refer to "Configuring DNs using the Wizards" on page 369.

Connecting: What lines and what type of devices are available to the system is determined by which media bay modules are active on your system. Refer to Chapter 5, "Configuring resources — media bay modules" on page 123, and to the installation charts from the Business Communications Manager *Installation and Maintenance Guide*.

Configuring: The headings under **Telephony Services** allow you to program and manage all the voice components associated with Business Communications Manager. You can set up lines and trunks, define settings for individual telephones, and customize your telephone network to suit your requirements.

IP telephony: IP telephones and voice over IP (VoIP) trunk configurations have additional screens not located under **Telephony Services**. These screens are located under **Services, IP Telephony**. Refer to the *IP Telephony Configuration Guide* for details about configuring IP telephones, NetVision wireless IP telephones, and voice over IP (VoIP) trunks.

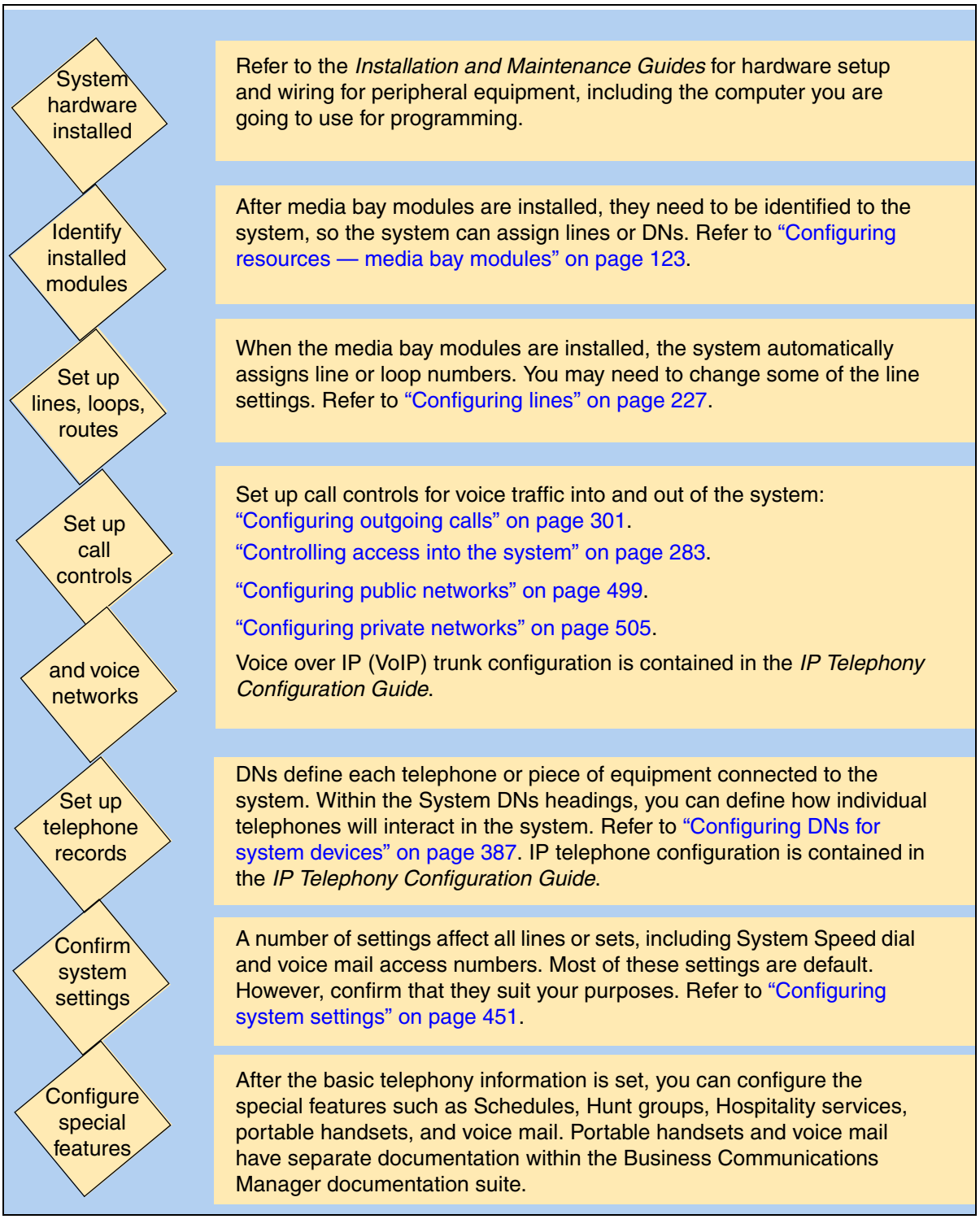
Doorphone The Business Series Terminal doorphone provides an intercom system at security doors. One or more internal telephones can receive notification from the doorphone. Refer to the BST doorphone documentation for configuration details for this piece of telephony hardware.

Voice mail	If you are using the voice mail application for this unit, you can set up mail boxes for system telephones as well as for telephones from other systems on the same private network. Voice mail configuration information is contained in the CallPilot suite of documents.
IVR	This application allows callers to receive assistance through an interactive interface. Configuration information is contained in the IVR document.
IP music	Music on hold can be configured either from an external source wired to the Business Communications Manager equipment, or by using computer-based music files (IP music). IP music configuration is explained in .....

Process map: Creating telephony services

The figure below lists the tasks involved in creating telephony services on your system.

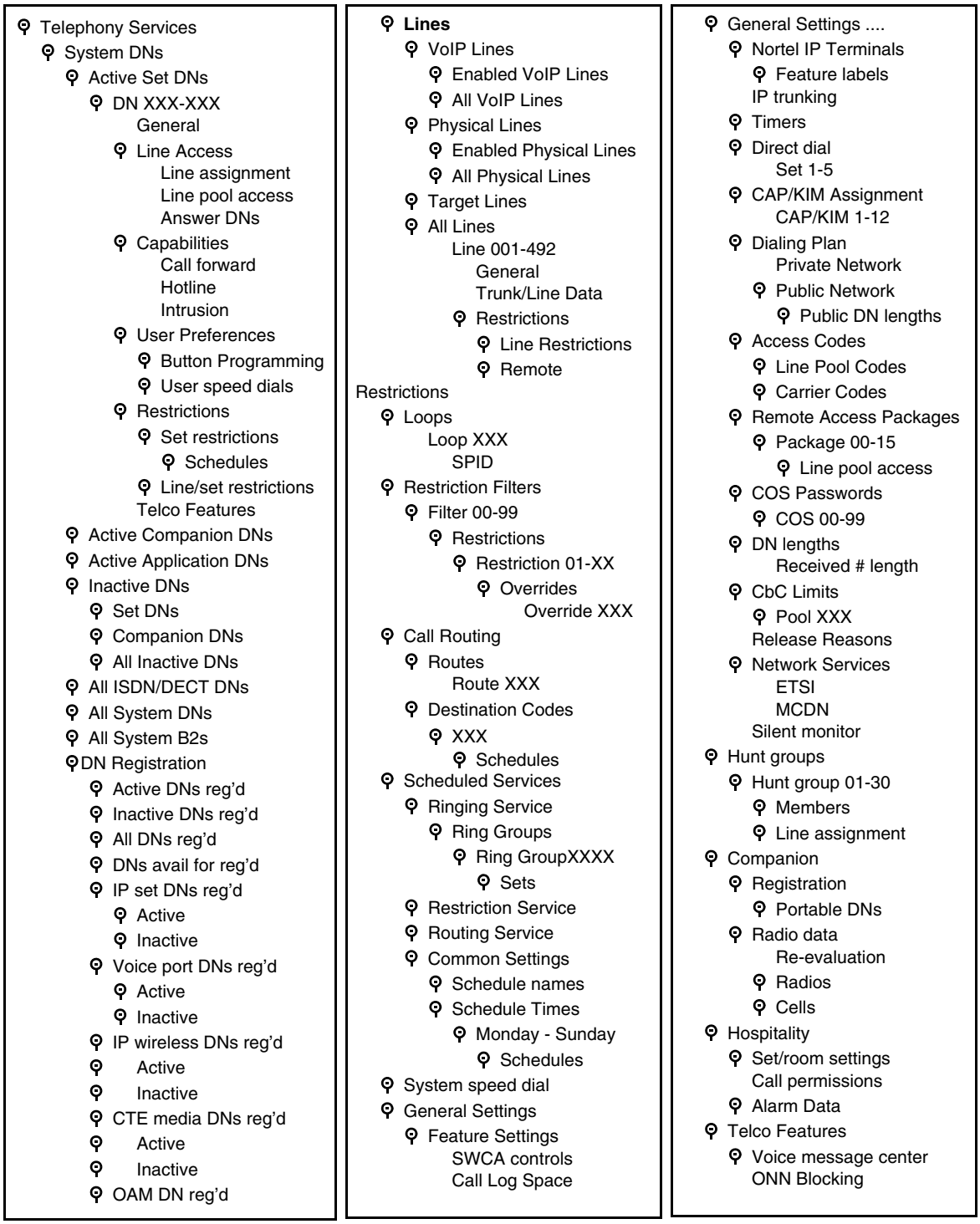
Figure 40 Tasks for installing the telephony components



Telephony Services headings

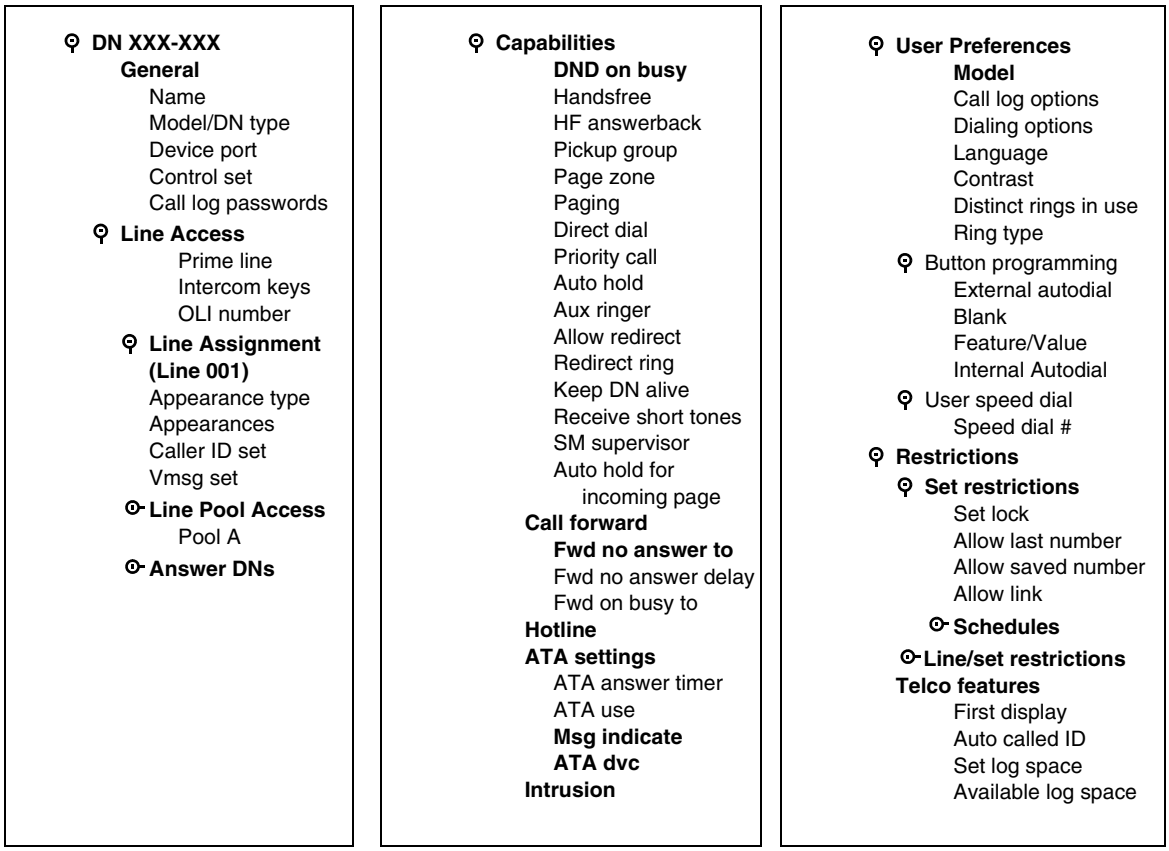
The following two figures show the **Telephony Services** headings in the Unified Manager.

Figure 41 Telephony Services menu options



Typical DN record headings

Figure 42 Headings found under typical DN heading



The following table summarizes the **Telephony Services** subheadings. The headings are arranged in the order in which they appear under the Telephony Services heading, not necessarily in the order you would use them to program your system.

Table 29 Telephony Services subheadings

System DNs	Allows you to assign settings to each telephone, including IP telephones. "Configuring DNs for system devices" on page 387
Lines	Allows you to assign settings to each trunk, including voice over IP (VoIP) trunks. Target lines are also defined under this heading. Target lines direct calls to specific sets or groups within the system. "Configuring lines" on page 227, "Assigning target lines" on page 287.
Loops	Allows you to configure settings for BRI loops. "Configuring BRI Loops" on page 265
Restriction filters	Allows you to apply restriction filters for external lines. "Defining restriction filters" on page 344,

Table 29 Telephony Services subheadings (Continued)

Call Routing	Allows you to define how calls are routed out of your system. "Configuring call routing" on page 320
Scheduled Services	Allows you to schedule services, such as night ringing, routing and restrictions. "Configuring schedules" on page 483
System Speed Dial	Allows you to create speed dial codes that can be accessed from any telephone in the system. "Configuring system speed dial numbers" on page 475
General Settings	Allows you to change system-wide settings. "Configuring system settings" on page 451
Hunt groups	Allows you to create and manage Hunt groups. "Configuring Hunt groups" on page 573
Companion	Allows you to assign settings for portable telephones.Companion configuration is described in the *Companion Configuration Guide*.
Hospitality	Allows you to assign Hospitality settings. "Configuring Hospitality Services" on page 589
Telco Features	Allows you to assign settings for external voice message services. "Setting system telco features" on page 478

Planning your telephony services

Nortel Networks strongly recommends that you use the planning tables from the *Installation and Maintenance Guide* or the Programming Records spreadsheets to understand what lines and set numbers (DNs) are available to you. Programming records, which are set up in Microsoft Excel*, provide a reference for your system programming. These forms are located on the documentation CD.

Coordinate this information with call planning to assess your system requirements ("Telephony feature planning" on page 193).

Chart this information to determine how to set up your lines and telephones. "Three basic system telephony configurations" on page 189 provides examples of three basic, single-office, configurations on which you can base your planning.

DN lengths and the Start DN are identified during initialization of the system, when you run the Quick Start Wizard. Ensure these settings are correct before you do any other programming. This is especially important if your system is part of a network, where your DN length and numbering plan must match that of the other systems in the network.

The Programming Records are divided into three sections:

- Start-up forms for system programming
- Data forms for the protocols you use to connect your Business Communications Manager to your business network
- Telephony forms, which you fill out for your system telephony configuration.

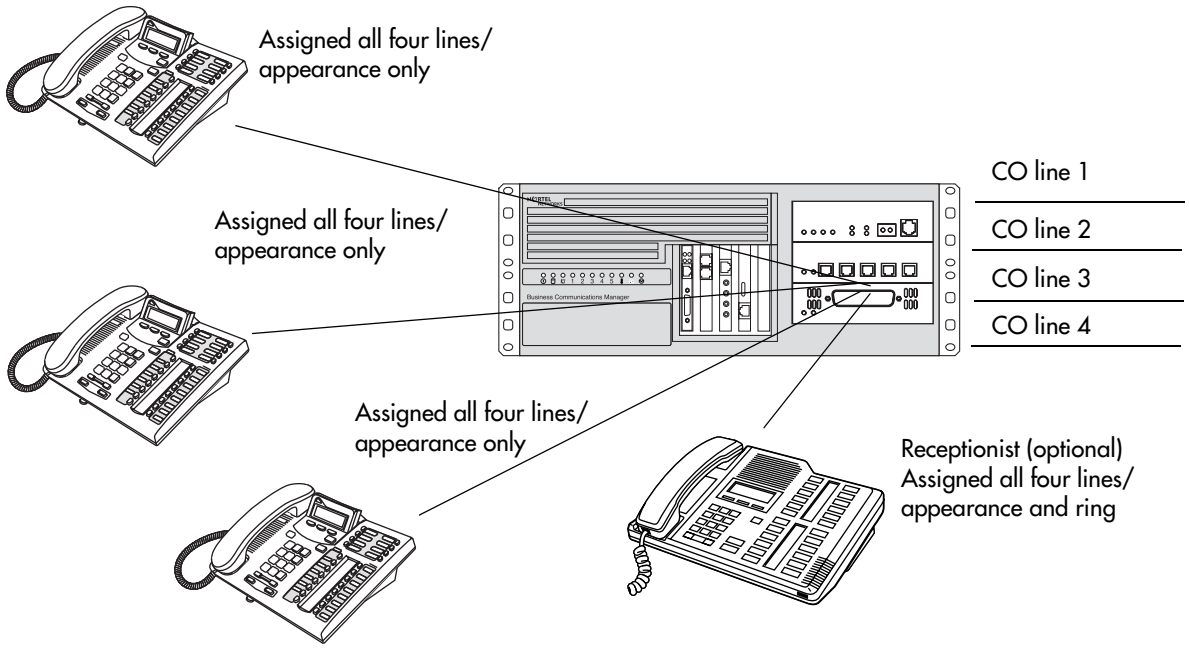
Three basic system telephony configurations

This section provides a broad overview of the telephony setup for three of the most common office telephone configurations.

Square system

This is a typical small-office setup, where all lines are available on any telephone. There may not be a designated attendant.

Figure 43 Square system



Incoming calls

1. Call comes in on a line.
2. Call rings and flashes at the Reception telephone (flashes, but no ring, on other telephones).
3. Receptionist answers and finds out who the call is for.
4. Receptionist calls or pages the person and tells them what line to pick up.
5. The person can pick up the call at any of the telephones.

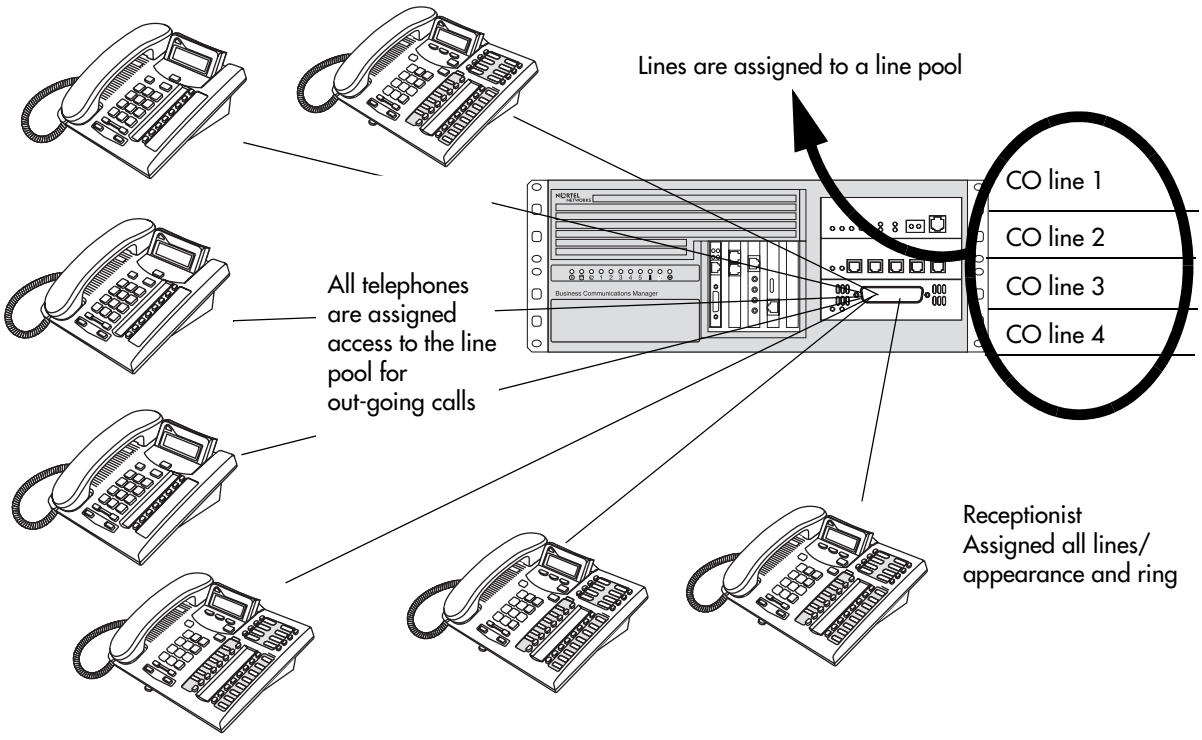
Outgoing calls

1. User selects a line button and dials the number.

PBX system

This setup is for a larger offices which have fewer CO lines than there are telephones. In this case the lines are pooled, and the line pool is assigned to all telephones. As well, there is a designated attendant with a telephone that has all lines individually assigned.

Figure 44 PBX system



Incoming calls

1. A call comes in on a line.
2. The receptionist answers the call and finds out who the call is for.
3. The receptionist transfers the call to a specific telephone (DN).
4. The person can pick up the call at that telephone only.

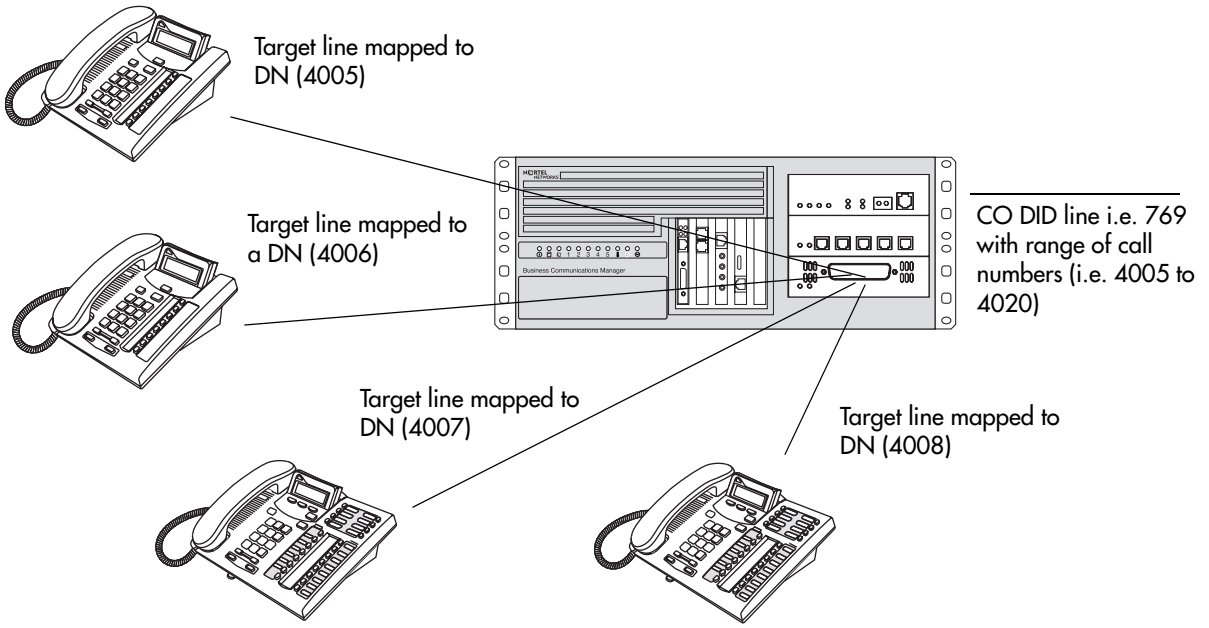
Outgoing calls

1. User selects the intercom button or dials a line pool access code, which selects a line in the line pool.
2. The user dials the outgoing CO number.

DID system

This setup allows you to assign a dedicated phone number to each telephone. The CO assigns a list of available numbers for each DID (Direct Inward Dial) line. You can change your DN range to match these numbers, or you can use target lines to match each number with a DN.

Figure 45 DID system



Incoming calls

1. DID trunks are assigned to be auto-answer.

   Note: PRI and BRI lines are automatically set to auto-answer.

2. All telephones are assigned target lines.
3. A caller dials a system code and a DN. In the example shown above, it might be 769-4006.
4. The call comes into the trunk, which answers and forwards the call on the target line assigned to that number.
5. The telephone assigned to that target line rings.

You can assign unanswered or busy telephones to Call Forward to a prime set, if you have a designated attendant, or to a voice mail system.

Telephony metrics

The system provides call metrics for Hunt groups ("Monitoring Hunt groups" on page 585), PRI Call-by-Call services limits ("Viewing CbC limit metrics" on page 343), and IP telephony fallback (*IP Telephony Configuration Guide*).

Chapter 8
Telephony feature planning

This section provides a quick reference to telephony programming basics, which you need to understand before you can decide what default*s* you want to change, and how you want to configure your telephones and routing.

- Understand how to plan system numbering strings and codes "Creating numbering plans" on page 194. It is important that you understand how calls get directed out of your system and accepted into the system. In a stand-alone system, only PSTN routing may be required ("Configuring public networks" on page 499). For systems on a private network, more complicated numbering plans and routing may be required ("Configuring private networks" on page 505).

- Understand how the system features work to provide call function. This section provides an overview of the various call features that are programmed through the Unified Manager. The features are divided into task categories, or categories of similar features. Each feature includes a link to the specific programming section.

  Refer to your *Telephony Features Handbook* for information about using these features and to view the display prompts and error prompts for the features.

  - "Name a telephone, a line or a Hunt group" on page 200
  - "Programming line access" on page 202
  - "Answering calls" on page 205
  - "Make a call" on page 209
  - "Handling calls" on page 212
  - "Communicating in the office" on page 216
  - "Using handsfree and mute" on page 218
  - "Track your incoming calls" on page 218
  - "Use alternate or scheduled services" on page 220
  - "Special telephones" on page 220
  - "Auxiliary devices" on page 221
  - "Call out to external systems using host system dialing" on page 222
  - "Call in from outside the system" on page 224
  - "Controlling telephone programming access" on page 224
  - "Special features" on page 225

Not all features require programming; for example, if they are a default function of the system.

Refer to Appendix B, "System Features," on page 861 for a comprehensive list of the features that are available on a fully-configured system.

Creating numbering plans

Access to and from and within your system is based on dialing strings and how the system adds or deletes from this sequence to route the call. A dialing string is the numbers that the caller physically enters on a telephone or programs onto a memory key. This can also include numbers the system adds to a dial string when a call goes through call routing. This process also includes how the receiving system reads the sequence. All of which means that coordination is required at both ends of the call to ensure that calls are routed correctly. This is especially important if calls need to be routed through your system, or through a remote system, to reach another node on the network. Refer to "Creating tandem private networks" on page 520.

The system performs some number programming checks on the initial digits of a dial string, such as for access codes. However, dial strings can contain more than one imbedded code, therefore, it is important that your dialing plan dials out the segments in the correct order. Refer to "Outgoing calls" on page 197.

Basic numbering: The first numbering that you set is your DN length (Start DN length) and Start DN and Public and Private Received # length. DN length and Start DN information is entered when the Quick Start Wizard runs at system setup. These numbers can be changed after the system has been set up, but only at the risk of compromising other numbering in the system. If your system is part of a network, these numbers must be coordinated with the other nodes in the network to ensure that the network dialing plans are consistent. Refer to "Incoming calls" on page 198.

For detailed information about the Quick Start Wizards, refer to the wizards help. For information about private networking, refer to Chapter 19, "Configuring private networks," on page 505.

Variable	Example settings
Start DN	2 (221)
DN length, Received # length	
Private length	3
Public length (max)	10 (North America)

Remote call-in: When you set up lines that do not offer DISA directly on the line, you can determine if remote access prompts with DISA or allows auto answering. This determines the Public/Private Auto DN and Public/Private DISA DN settings, which are set under **Services, Telephony Services, General settings, Access codes**. These numbers will have the same first number as you specified in the Start DN and be of the same length. Remote callers dial the system public or private access number, and then dial either the Private/Public Auto DN or Private/Public DISA DN, as determined by the line setup.

Variable	Example or default settings
Private Auto DN	2XX
Public Auto DN	2XX
Private DISA DN	2XX
Public DISA DN	2XX

Incoming calls: If your system is networked with other systems, you will also need to determine a private access code that tells your system when a call is to be dialed out over the private network instead of over the public network. This access code is also entered under **Services, Telephony Services, General settings, Access codes.** This code is included as part of any destination code or dialing sequence that is to be routed over the private network.

Variable	Example or default settings
Private Access Code	6

MCDN special call types: If your system is networked to other types of systems, such as Meridian 1, which sends calls through one or more Business Communications Manager systems to the public network, you need to specify specific call-type codes. These codes append to the incoming dial string, so that the call-type remains intact as it passes through the Business Communications Manager call processing:

Variable	Example or default settings	
Local Access Code	9	Coordinate these settings with Meridian routing for these calls types and the Private Access Code.
National Access Code	61	
Special Access Code	911	

Calls coming in over private networks or PRI/BRI lines can either terminate at one telephone, called the prime telephone, or target lines can be set up for each telephone or group of telephones to which the calls are directed. As with other incoming calls, these calls can have a public or private call type that matches to a public or private received number assigned to a target line.

Variable	Example or default settings
Private received number	<CDP: same as DN of telephone> <UDP: LOC code + DN>
Public received number	<North America: 10 digits XXX-XXX-XXXX, the trailing digits are the DN> <DPNSS: maximum number of digits in local dialing pattern>

Outgoing calls: Other network codes include the information about private and public dialing codes that you enter under **Services, Telephony Services, General settings, Dialing Plans**

Variable	Example or default settings
Private network ID	Number that identifies the system as part of the private network
Location code	UPD networks
Private DN length	DPNSS systems only
Public DN lengths (prefixes)	Public dialing table

Internal feature access: Meanwhile, you need to keep in mind that the leading digit of any of the above dialing codes cannot conflict with the other system access codes that you want to use:

Variable	Example or default settings
Park Prefix	1 (101-125)
Direct Dial Digit	0

Line pool and destination access codes: Once these basic numbers have been picked, you can decide what numbers to use for line pool access codes and/or destination codes. The system will not allow these codes to start with any of the numbers currently assigned. If you are working with an established system of dialing, you may want to ensure that the numbers that the users are familiar with dialing are reserved for these codes.

For instance, if the users are familiar with dialing 9XXXXXXX to access numbers outside of their own offices, you will want to reserve this number for the destination codes. If you are setting up a new system, you could opt to use the location codes of the other systems as destination codes, or you could define one number for local calls (but which are still outside the system) and one number for long haul calls. For example: The users may dial 6<DN number> for calls within a local system, but dial 8<area code><DN number> for calls in another city over the public network.

Variable	Example or default settings
Line pool codes (first character)	5
Destination codes (first character)	6<up to 11 more characters> 9<up to 11 more characters>

Analog telephones require a code to dial out of the system, since the intercom button only accesses the internal system. The external access code may be the same as a line pool code, in which case, the line pool code overrides this setting.

Variable	Example or default settings
External code	9

Outgoing calls

Outgoing calls require line pool access codes or destination code (with defined routes) to leave the system.

- Access codes provide direct, unscheduled access to an analog, digital (T1), of Voice over IP (VoIP) line pool. Refer to "Programming access codes" on page 310.

- Destination codes also provide access to line pools, but they also allow more flexibility in dialing, which allows for more complex routing options, such as scheduling, fallback routing (VoIP trunks), call definition, and multiple routing (least-cost routing). Routing also allows you to minimize the dialout for the user, especially to systems on the same private network. Refer to "Configuring call routing" on page 320.

Outgoing calls can be either public or private, which is defined by the route. The public or private designation determines which dialing plan is used to determine the validity of the call. Normally, public calls are routed over PSTN trunks and private calls are routed over a private network. However, MCDN trunks can also pass calls designated as public to allow remote nodes on the network to call out of the PSTN of a local node. This is called tandem dialing. Refer to "Outgoing private calls routing" on page 305, "Outgoing public calls routing" on page 307 and "Using the MCDN access codes (tandem calls)" on page 315.

- If the outgoing call is designated as private, the system checks the beginning of the string for a destination code that routes to a private network. It also checks that the dial string is the correct length. The destination code routing determines what the final dial out string will be, adding or removing digits, as required.

- If the outgoing call is designated as public, the system checks the beginning of the string for a destination code that routes to a PSTN or an MCDN trunk. If the call routes to a public route, the system checks the public dialing table to ensure that the dialout string has legitimate leading digits and is the correct length. If the call routes to an MCDN trunk, the call is passed as dialed, minus the private networking codes. The call will pass through the system until the system with the matching destination code receives it, at which point it will be sent through the local PSTN of that system.

Incoming calls

Incoming call handling also depends on the call type. The system also uses the Public and Private DN # length settings to determine call handling. Refer also to "Defining DN length" on page 284.

The system processes a call in the following way:

1. The system receives a call from the public or private network.
2. The system identifies the call type:

   Public calls:

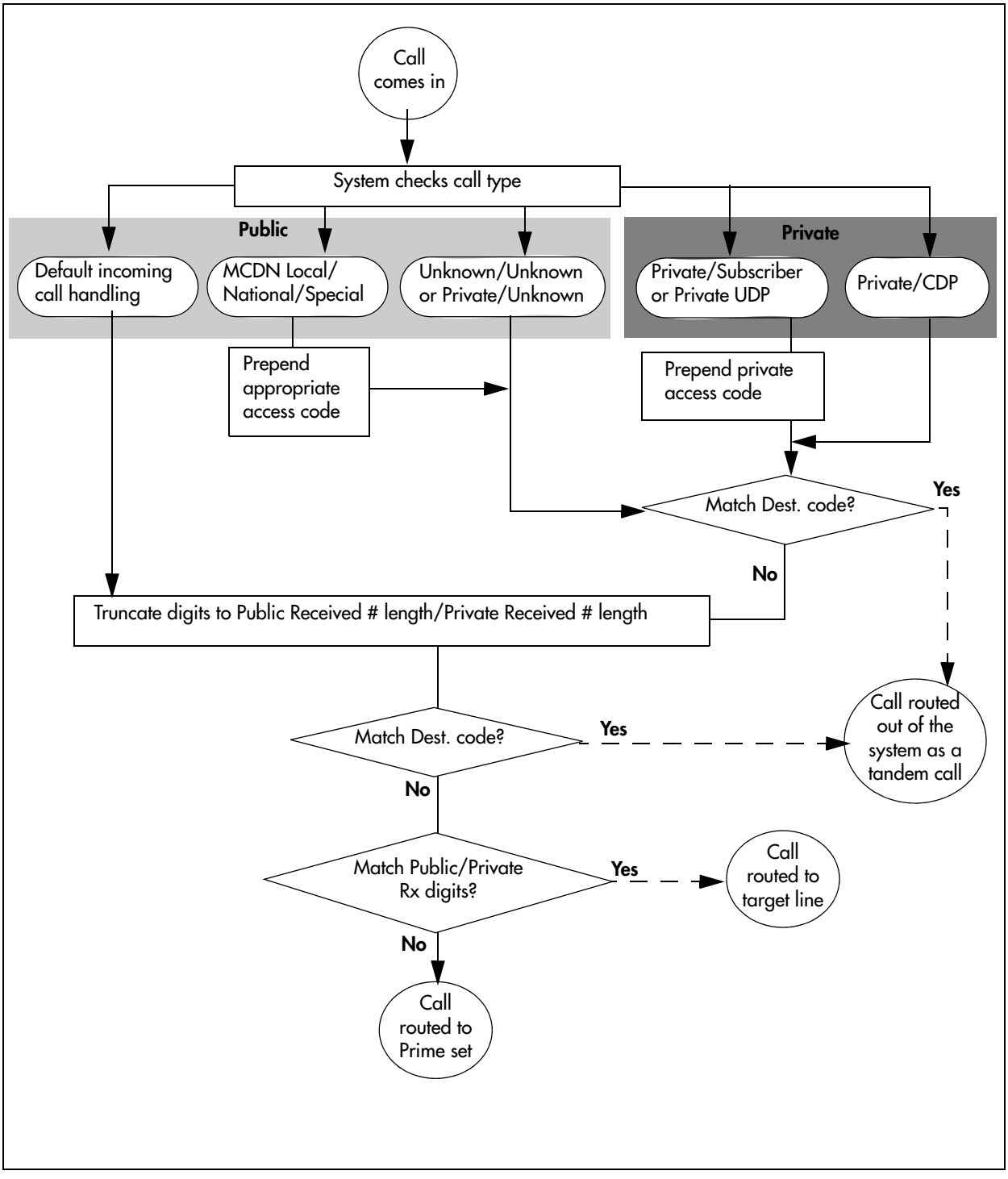
   - If the call is from the MCDN network and is a local, national, or special call type, the system prepends the appropriate access code.
   - If the call is from ETSI-QSIG, MCDN, NI, DMS100, DMS250) and tagged as Private/Subscriber, the system prepends the Private access code, if the dialing plan is UDP.
   - If the call is tagged as Unknown/Unknown or Private/Unknown (ETSI-QSIG, MCDN, N1, DMS100, DMS250 trunks), no access code is added.
   - For all other call types, the system truncates the trailing digits to the Public Received # Length. (Go to step 5)

   Private calls:

   - If the call is tagged as Private/Subscriber or Private/UDP, the system prepends the Private access code.
   - If the call is tagged as Private/CDP, no access code is added.
3. The system tries to match the first digit(s) of the dial string to a destination code. If the digit(s) matches, the dial string is routed out of the system.
4. If the system cannot match the first digit(s) to a destination code, it truncates the trailing digits to the Public Received # length or Private Received # length, as appropriate to the call type.
5. The system again tries to match the leading digit(s) to a destination code. If the digit(s) match, the dial string is routed out of the system.
6. If the system cannot match the first digit(s) to a destination code, the system tries to match the dial string to a target line (Public or Private Received Number). If the dial string does not match any target lines, the call is routed to the prime line.

Refer to the figure below for a graphic illustration of incoming call processing.

Figure 46 Incoming public and private call coding



Name a telephone, a line or a Hunt group

You can assign names to identify external lines, target lines, and your colleagues' telephones. During a call, the name (if programmed) appears on the telephone display instead of on the external line number or internal telephone number of the caller.

Names can contain both letters and numbers, but cannot be longer than seven characters. You cannot use the # and * symbols.

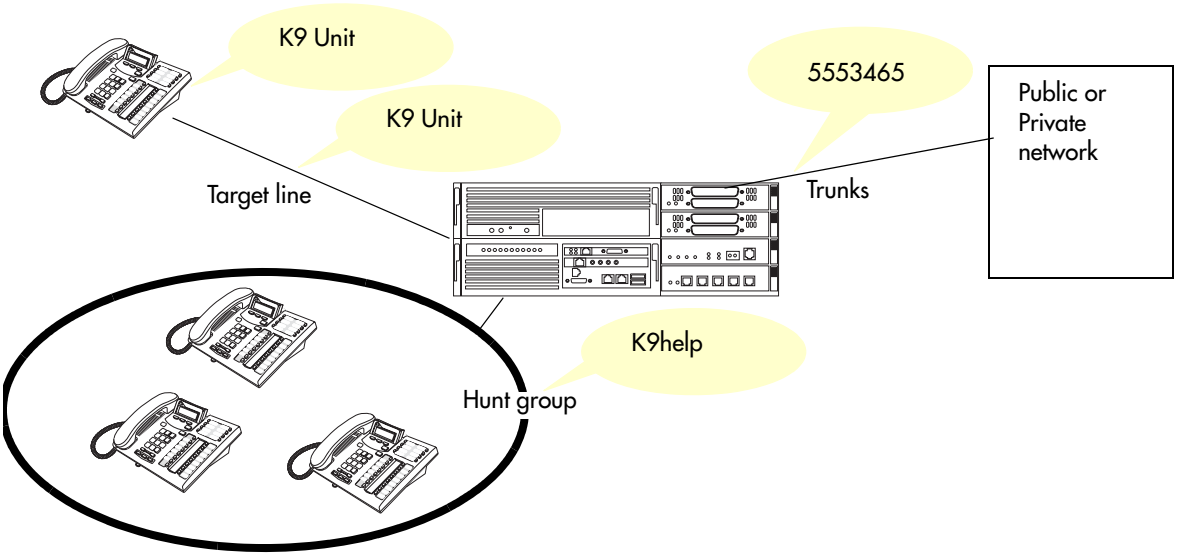
Note: You can give the same name to a telephone and a line in your system. Use initials, abbreviations, or even nicknames to give each telephone a unique name to avoid confusion.

Programming:

- Name a line/target line: "Using the General record" on page 235 (Services, Telephony Services, Lines)
- Name a telephone: "Identifying the telephone (General heading)" on page 391 (Services, Telephony Services, System DNs)
- Name a hunt group: "Identifying a Hunt group" on page 575 (Services, Telephony Services, Hunt Groups)
- Determine what displays first: "Configuring telco features" on page 445 (First display)

You can also determine if the calling line ID (CLID) is received by a telephone, or if the CLID information from a system telephone gets sent out over the network. Refer to "Incoming and outgoing call display" on page 201.

Naming components in the system



Incoming and outgoing call display

If you subscribe to Call Display services from your local telephone company, one line of information about an external caller appears on the display after you answer a call. If you answer before the Call Display information appears on your display, press **FEATURE 811** to view the line number or line name. When you transfer an external call to another telephone in your system, the same information appears on the recipient telephone display.

Depending on the services you subscribe to, incoming Call Display information can contain up to three parts:

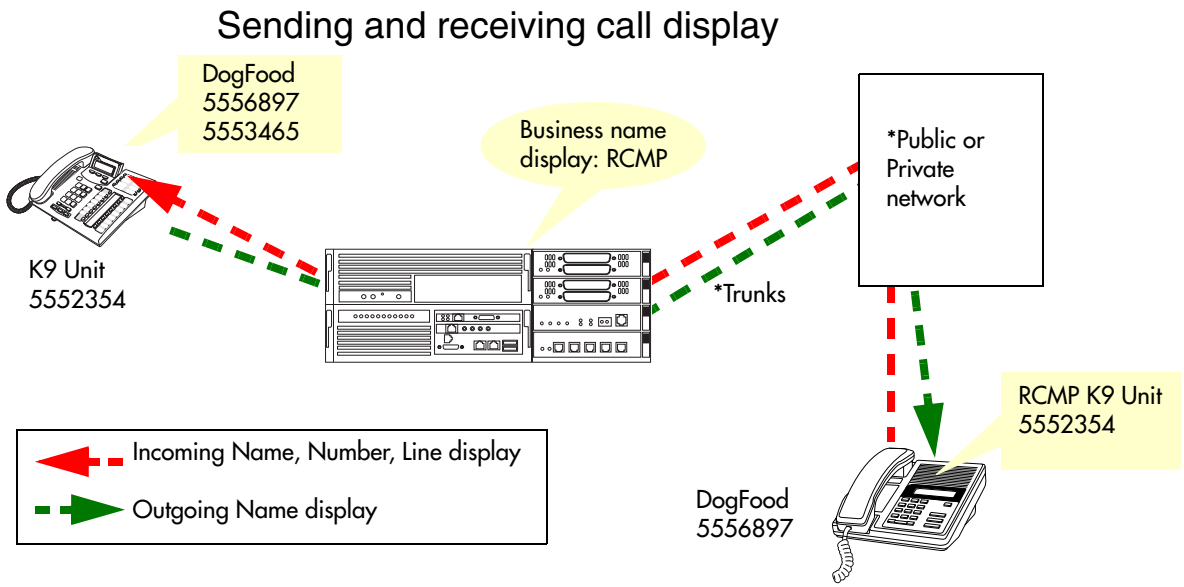
- the name of the caller
- the number of the caller
- the name of the line in your system that the call is on

Call display information can also be sent out when a system telephone calls out of the system. What displays at the called party's telephone, depends on what the private or public lines allow. Outgoing call display information can be allowed or blocked at the system level or single telephone level.

For each telephone, you can determine which information appears on the display first.

Programming:

- Lines: Determine which telephones display incoming CLID for an analog line or that provides CLID (ASM8+ module), or for a target line: "Determining line assignments" on page 397. (Caller ID set)
- Lines: Determine which PRI or BRI modules will allow outgoing CLID: "Configuring the trunk module to line type" on page 131. (Send name display)
- Loops: Determine which BRI modules will allow outgoing CLID (QSIG trunks, only): "Identifying BRI T-loops (ETSI, QSIG)" on page 271. (Send name display)
- VoIP trunks: Determine which VoIP trunks will allow outgoing CLID (Services, Telephony Services, General settings, IP trunking). (Send name display)
- Incoming call display, alpha tagging: Program a name to appear as call display when a call comes in on an analog line that supports number-only CLID, or on target lines. Refer to "Using alpha tagging for name display" on page 455.
- System: Determine whether name, line number, or system number appears first on the telephone display: "Configuring telco features" on page 445.
- Outgoing call display, telephones: Determine what number is displayed to a destination telephone when a call is made from a system telephone to a telephone on the private or public network: "Configuring line access" on page 393. (Public and Private OLI)
- Determine the system-wide name that displays for calls made to external numbers: "Programming Business name display" on page 455. **FEATURE** 819 blocks call display for an outgoing call.



Programming line access

There are a number of ways you can configure your lines. You can assign each line to each telephone, or a specific line to a specific telephone. You can also pool your lines so that a number of telephones have access to several lines.

This section contains the information split into these sections:

- "Making lines available" on page 202
- "Incoming calls" on page 204
- "Outgoing calls" on page 204

Refer to "Three basic system telephony configurations" on page 189 for examples of line settings for three common types of systems.

Making lines available

- You can determine whether a line will be assigned solely to one telephone, or if a group of users will have access to the line.
- Even when you use line pools, it is possible that a line pool will be unavailable for outgoing traffic. To alleviate this, you can determine overflow paths for any routes that you designate. Refer to "Using multiple routes and overflow routing" on page 336 for more information about overflow routing.
- Incoming lines can be assigned to telephones as individual lines or through target lines, depending on the type of trunk supplied from the central office (CO). Incoming lines do not need to have an appearance on the telephone. Target lines are for incoming calls only. Two-way single lines, such as analog lines, allow the user to make an outgoing call by

pressing the (idle) assigned line button or, if the line is part of a line pool, by entering a line pool access code or destination code to access the line pool. These lines can also be redirected on a per-trunk basis or from the telephone by using **FEATURE** 84.

- PRI lines are always configured into line pools. These lines require a destination code for outgoing calls. Incoming calls use target line assignments.
- Voice over IP (VoIP) trunks use the data network to provide line service in and out of the system. VoIP trunk configuration is described in the *IP Telephony Configuration Guide*. VoIP trunks use target lines for incoming calls, and require line pool codes or destination codes for outgoing calls.
- You can assign a line a maximum of 93 times.

Programming:

- Creating dialing plans: "Configuring the public and private dialing plans" on page 302
- Setting up the modules for the trunks: "Defining trunk module types and settings" on page 130
- Creating restriction filters: "Defining restriction filters" on page 344.
- Creating line pools and redirecting lines: "Assigning Trunk/line data" on page 236.
- Creating line pool codes: "Setting up line pool access codes" on page 317.
- Creating routes and destination codes: "Configuring call routing" on page 320.
- Creating scheduling for routes, ringing groups and restrictions: "Configuring schedules" on page 483.
- Assigning lines and line pools to telephones: "Assigning lines to telephones" on page 398, "Assigning line pool access" on page 402.

Incoming calls

For incoming calls, you can have a central reception point, or you can specify target line*s* to one or more telephones to receive directed calling.

You can arrange your telephones in Hunt group*s*, ringing groups, or call groups that use system-wide call appearance (SWCA) assignments to share calls.

You can also configure lines for use by system users who call in from outside the system. You can give them direct access to the system with an Auto DN, or you can configure the line so they hear a stuttered dial tone, at which point they need to enter a password (COS) to gain access (DISA DN). Refer to "Call in from outside the system" on page 224.

Programming:

- Assigning lines to telephones: "Determining line assignments" on page 397.
- Creating and assigning target lines (PRI and VoIP trunks): "Target lines and DASS2 fields" on page 247 (configuring target line*s*) and "Received #" on page 259 (received #, if busy); "Assigning target lines" on page 287; "Configuring line access" on page 393 (appearances).
- Creating direct-dial telephones: "Creating Direct Dial sets" on page 313.
- Configuring Hunt groups: "Adding a Hunt group member" on page 579.

- Configuring and scheduling ringing groups: "Defining ring groups" on page 490.
- Creating a group using SWCA keys: "Configuring system-wide call appearance groups" on page 462.
- Setting up users and remote access packages to support calling in from outside the system into the system: "Configuring for remote access" on page 291
- Refer to the Call Center documentation for information about setting up call centers.

Outgoing calls

For outgoing calls, you can assign one or more intercom keys to directly link to a line pool or prime line, or allow line pool access codes, destination code, or internal system numbers to direct the call. Telephones without intercom keys on the telephone, still have intercom keys assigned, but to access calls, they must pick up the handset to connect. In this case, the intercom key is

Calls within the system: All telephones are virtually linked within the system. To call another telephone inside the system, you can lift the handset and dial the local DN. In this case, the prime line has to be set to intercom or none.

Calls going outside the system:

- If you assign the prime line to a line pool, all the lines in that line pool must be assigned to the telephone. When you pick up the handset, the telephone automatically grabs the first available line from the assigned line pool. In this configuration, you must ensure that the outgoing number is allowed by the line pool.
- If you assign the prime line to an intercom button, when you press the intercom button you get system dial tone. Then, you enter a line pool access code or a destination code to direct the outgoing call to the appropriate line pool, where it exits the system on any available line in that pool.

Programming:

- Creating restriction filters: "Defining restriction filters" on page 344.
- Creating line pools and redirecting lines: "Assigning Trunk/line data" on page 236.
- Creating line pool codes: "Setting up line pool access codes" on page 317.
- Creating routes and destination codes: "Configuring call routing" on page 320.
- Assigning prime line*s*, intercom keys, and outgoing number display to each telephone: "Assigning line access" on page 394.
- Assigning lines and line pools to telephones: "Determining line assignments" on page 397, "Assigning line pool access" on page 402.
- Creating scheduling for routes, ringing groups and restrictions: "Configuring schedules" on page 483.

Answering calls

Incoming calls do not have to both appear and ring at a telephone. They can be programmed to only show an appearance on a line or intercom button. They can also be programmed to only ring. How a call alerts at a telephone is determined when you assign lines to each telephone. "Assigning lines to telephones" on page 398.

This section contains information about:

Distinctive ring patterns

There are four Distinctive ring patterns (DRP) that can be assigned to lines, telephones, or Hunt group*s* to differentiate incoming calls on telephones where Ring has been allowed:

DRP 4	Highest priority
DRP 3	2nd highest priority

DRP 2	3rd highest priority
DRP 1 (or None) (default)	Lowest priority

Call Ringing: When more than one call rings at a telephone, highest priority DRP rings first.

Hunt groups: If the Hunt Group DRP is higher than the DRP of line of the incoming call and the telephone DRP, all telephones in the group will ring with the ring pattern assigned to the Hunt Group.

Note: External calls have a higher priority than internal calls. You cannot press **FEATURE *6** to change the ring type on a telephone when the Distinctive Line Ring feature is in service. When the call is finished, your telephone reverts to the ring you set.

Programming:

- Lines: "Assigning Trunk/line data" on page 236 (Services, Telephony Services, Lines)
- Telephones: "Defining user preferences" on page 415 (Services, Telephony Services, System DNs,)
- Hunt groups: "Identifying a Hunt group" on page 575 (Services, Telephone Services, Hunt groups)

Centralized and group answering

- **Prime telephone:** The prime telephone is usually the monitored telephone in a reception area or at the desk of the designated attendant. Calls not answered at their normal destinations transfer to the prime telephone. Business Communications Manager allows for a prime telephone for each line, if needed.

  Programming:

  - Lines: "Assigning Trunk/line data" on page 236
  - Telephones: "Assigning line access" on page 394

- **Central answering position (CAP station):** A CAP can consist of a BST T7316E plus one to four eKIMs (key indicator modules) or one to nine OKIMS, or a M7324(N) plus one or two CAP(N)s (Central Answer Position modules). When the CAP is assigned under **CAP/KIM assignment** in the Unified Manager it becomes an enhanced CAP (eCAP). The T7316E modules become known as eKIMs.

  An eCAP can monitor system telephone status, answer external calls on line buttons, and send up to 30 messages to other system telephones. Additionally, the eKIMs can monitor Hunt group appearances and support multiple appearances of a target line. You can configure a maximum of 12 telephones as eCAPs on each Business Communications Manager. One eCAP station can be designated as the prime telephone and direct-dial telephone for the system lines

and telephones.
Telephones with KIMs or CAP modules that are not configured in system programming allow only memory button programming on the modules. In this case, the KIM is known as an OKIM (ordinary KIM).

Programming:

- "Identifying the telephone (General heading)" on page 391
- "Configuring CAP/KIM assignment" on page 436
- "Programming CAP/KIM buttons" on page 438

- **Hunt groups:** This feature allows you to create groups of telephones that are assigned to a single DN. This provides the capacity for call groups that are dedicated to specific products or projects, and provides the flexibility of determining how the calls will be presented to the group.

Programming: "Configuring Hunt groups" on page 573

- **Ringing groups:** If you set up call scheduling on the system, you can define groups of telephones into ring groups, which allows you to specify schedules where Trunk Answer can be used within the ring group to answer incoming calls, even on telephones which do not have that line specifically assigned. You can also define a second direct dial set for a ringing group.

Programming: "Configuring ringing service" on page 490

- **Other options:** There are optional applications which allow you to set up service centers and customized mailboxes. These are described in the CallPilot documentation suite.

Pick up features

There are a number of features you can use to pick up calls, including calls that do not come directly to your line buttons:

- **Call Queuing:** This feature code (**FEATURE 801**) allows you to answer the next incoming call. The feature selects the call with the highest priority, if there are a number of calls arriving at the same time. Call Queuing answers incoming external calls before callback, camped, and transferred calls. There is no programming for this feature.
- **Directed Pickup:** This feature allows a user to answer any telephone that is ringing in the system.

Programming: "Programming Feature settings" on page 457

- **Group Pickup:** Your system can support nine pickup groups. If a telephone has been assigned as a member of a pickup group, the user can pick up a call that is ringing at any telephone in the pickup group (**FEATURE 75**).

  Programming:
  - "Configuring the Capabilities features" on page 406
  - "Configuring ringing service" on page 490

- **Trunk Answer:** By pressing **FEATURE 800** the user can answer a ringing call in any area in the system from any telephone in the system. The line being answered does not have to appear or ring at the telephone being used to answer the call. This feature is only active when a ringing service schedule is running.

  Programming:
  - "Configuring ringing service" on page 490
  - "Turn services on and off" on page 484

- **Answer DNs:** Telephone DNs can be assigned to indicator buttons on other telephones to provide backup answering. The indicator buttons on your telephone that are assigned to answer DNs are called answer keys. You can assign a maximum of eight answer DNs to a telephone. You cannot assign Answer DNs to analog telephones or Model 7000 or 7100 telephones.

  On the answer telephone, an indicator beside the answer key lights when a call comes in from the original telephone. When the call is answered, the indicator disappears on the non-answering telephone, freeing that line for another call. You can also determine which calls alert at Answer DNs (Answer key access levels).

  For systems running BCM 3.6 and newer software, the Answer DN can be used as an autodial button to the assigned telephone.

  On systems running BCM 3.5 and newer software, if call logging is set, then calls received through Answer DN are logged at the receiving telephone that picks up the call.

  Programming:
  - Answer DNs: "Assigning Answer DNs" on page 403
  - Answer Keys access levels: "Programming Feature settings" on page 457

- Listen to a call as a group: This feature (**FEATURE 802**) allows more than one person to listen to a telephone, without the caller hearing everyone in the group (the handset is offhook).

Make a call

You can set up your system in several ways that will determine how users can make calls.

This section includes:

Some of the ways you can set up the system and the telephones to make calls includes:

- You can assign every line to every telephone, in which case, the user presses a line button or intercom button to dial out a call.

  Programming: "Assigning line access" on page 394

- You can assign lines to pools (Line pool A to O and PRI pool A to F) and assign the pools to all telephones. To make a call over line pools, users use the line pool feature code (**FEATURE 64**) and then enter a line pool access code.

  Programming:
  - "Assigning Trunk/line data" on page 236
  - "Setting up line pool access codes" on page 317

- You can assign line pools to routes and assign the routes with destination codes. To make calls with destination codes, the user enters the destination code, and then dials out the required digits to contact the destination telephone. The digits the users dial will depend on what the destination code is, and what dial-out digits have been specified within the route record. Note: All PRI line pools must be accessed through routes, using destination codes.

  Programming: "Configuring call routing" on page 320

- If a prime line is specified for the telephone, the telephone will automatically dialout on this line if an intercom button is pushed, or the handset is picked up.

  Programming: "Assigning line access" on page 394

- **Auto dial:** You can program an internal or remote dialout string onto a memory key. When the user presses the key, the system automatically dials the digits stored on the button.

  Programming: "Configuring buttons from the DN record" on page 420

Emergency 911 Dialing

Emergency 911 dialing is the capability to access a public emergency response system. State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Ask your local telecommunications service provider about compliance with applicable laws and regulations.

Emergency 911 dialing may not apply to International systems.

IP telephones: If you allow this service on IP telephones that are installed or used off-site, you must ensure that the 911 telephone number is not mapped to the system address in the emergency response system.

Select how you dial your calls

The system digital telephones provide three methods for dialing calls:

- **Standard dial:** allows you to make a call by selecting a line and dialing the number. If you have a prime line, it is selected automatically when you lift the handset or press the handsfree button.
- **Automatic dial:** allows you to dial a number without selecting a line. Your prime line is selected when you start dialing a number. Your Prime line must be free to make a call.
- **Pre-dial:** allows you to enter a telephone number, check it, then change it before making the call. The call does not dial until you select a line or line pool, or pick up the handset. You can pre-dial both external and internal numbers. You must, however, select the correct type of line (external or internal) for the type of number you have entered.

Programming: “Defining user preferences” on page 415

Receive a busy signal on an internal call

When the internal number you dialed is busy, there are three possibilities:

- **Priority Call:** You can use this code to override a busy signal or Do Not Disturb.

  Programming: “Defining device capabilities” on page 405. (**FEATURE** 69)

- **Ring Again:** You can use this code to tell you when a telephone you want to call is no longer busy or when a line pool becomes available. (**FEATURE** 2)

  Programming: There is no system programming to allow/disallow this feature.

- **Message:** Use this code to leave a message on the display of the telephone you are trying to call. (**FEATURE** 1)

  Programming: There is no system programming to allow/disallow this feature.

Create a conference call

You can establish calls to two people at the same time, and allow each caller to hear the other two callers. You must have at least two intercom button*s* assigned to your telephone to initiate a conference call (**FEATURE** 3).

The person who establishes the conference call, has several options available to provide control within a conference call.

- remove callers temporarily (put on Hold), or permanently
- split the conference into two separate calls
- leave the conference, and allow the other two callers to remain connected

Programming: "Assigning intercom (I/C) buttons (keys)" on page 396

The *Telephony Features Handbook* describes the feature codes and the dial pad actions that are required for controlling conferences.

Time-saving features

There are a number of features that allow you to save time when dialing, including:

- **Autodial:** You can program memory buttons for one-touch dialing of internal or external telephone numbers. When you program an external autodial, you must specify a path out of the system.

  Programming: "Programming telephone buttons" on page 419

- **Last Number Redial:** This feature (**FEATURE 5**) allows the user to redial the last external number that was dialed from that telephone. This feature records a maximum of 24 digits.

  Programming: "Programming restrictions for DNs" on page 441 (allow or disallow feature)

- **Speed dialing:** Business Communications Manager provides two types of speed dialing:
  - System Speed Dial programming allows you to assign two or three-digit speed dial codes to the external numbers called most often. You can set the system to have 01 to 70 codes or 001 to 255 codes. To activate a speed dial, enter **FEATURE** 0 and the speed dial code. The names you enter for speed dials are also used as CLI display for calls that come in on lines that offer number-only CLID on telephones that are configured to receive CLID for those lines. (Services, Telephony Services, System speed dial)
  - User Speed Dial programming (**FEATURE** *4) allows users to program their own speed dial numbers. (Services, Telephony Services, System DNs, Active Set DNs, DN XXXX, User Preferences, User speed dials)

  Speed dial numbers are subject to the same restriction filters as normally-dialed numbers. However, your system administrator can program system speed dial numbers to bypass dialing restrictions.

Programming:

- System speed dials: “Configuring system speed dial numbers” on page 475.
- Alpha tagging: “Using alpha tagging for name display” on page 455.
- User speed dials: “Configuring user speed dialing” on page 432.

- **Saved Number Redial:** This feature allows you to save the number of the current external call, provided that you dialed the call, so that you can call it again later. Each telephone can save one number at a time. You can also copy a number from an autodial using this feature.

Programming: “Defining telephone dialing restrictions” on page 442

Handling calls

Once you answer a call, there are a number of ways of passing the call to someone else to deal with or holding the call until it can be dealt with.

This section includes:

Holding calls

- **Use Hold**: You can put a call on hold by pressing **HOLD**. If you have system-wide call appearance (SWCA) keys defined, this might also park the call on a SWCA key and allow others who have the same SWCA keys defined to pick up the call. Refer to the SWCA section for more details.

- **Hold automatically (Auto Hold):** If a line or the telephone are programmed with full auto hold, you can answer a second call without dropping the first call and without pressing **HOLD**. Model 7100 and 7000 telephones, and NetVision, DECT and Companion wireless handsets, which do not have line keys, also use the **HOLD** key to toggle between active calls. **FEATURE** 73 activates this feature. **FEATURE** #73 cancels the feature.

Programming: “Defining device capabilities” on page 405

- **Hold a call exclusively:** You can put a call on Exclusive Hold so that you can retrieve it only at your telephone (**FEATURE 79** or **FEATURE HOLD**).

Parking or transferring calls

- **Transfer calls (call forward)**: Allows you to direct a call to another telephone internally or externally. To transfer a call to an external destination, you need to know the line pool or destination code to route the call. (**FEATURE** 70). You can also set up a telephone to automatically send calls to another telephone or to a voice mail box if the telephone is not answered or if it rings busy.

  Programming: "Forwarding calls" on page 214

- **Camp-on:** Use this feature to (**FEATURE 82**) transfer an external call to another telephone when all the lines assigned to that telephone are busy. A message appears on their display and they hear the camp-on tone if all lines remain busy, or the call gets transferred to a free line when one becomes available. If your system is part of a private network that uses the Meridian call attendant as part of a centralized voice mail system, the attendant can use camp-on to camp a call on any telephone in any system on the network.

- **Call Park** (**FEATURE** 74): Use one of 25 possible codes to park a call on the system. These codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101. You must also set a delay period for when the call returns to the telephone from which it was parked. You can also determine the order used to assign the codes (Park mode).

  Programming:
  - "Understanding access codes" on page 309
  - "Setting system timers" on page 472
  - "Programming Feature settings" on page 457

- **Callback:** When you direct a call you have answered to another telephone, the system monitors the call to make sure it is answered. If no one answers the call within a set length of time, the system returns it to you.

  Programming: "Setting system timers" on page 472

Sharing calls by parking on SWCA buttons

System-wide call appearance (SWCA) keys (**FEATURE *521** to **FEATURE *536**) allow you to control call park and retrieval features on any type of line, across the local system. These features expand the Business Communication Manager call park and call retrieve features by providing visual indications of the status of any call parked on a SWCA button that has indicators. The calls can also be controlled by directly entering the SWCA feature codes.

You can use SWCA programming to define logical groups of telephones. Each group can be assigned a set of the SWCA codes, which allows them to pass calls within the group. Each telephone in the group also displays the current status of the call, so users can determine which calls are being dealt with.

Programming: "Configuring system-wide call appearance groups" on page 462

Forwarding calls

- **External call forward:** This feature allows you to transfer a call to an external number. To allow external destination programming ensure that Allow Redirect to Y (enabled). The other programming is the same as for the following call forward features.

Programming:
- "Configuring the Capabilities features" on page 406 (Allow redirect)

- **Call Forward no answer:** redirects calls to another telephone in your system or to the voice mail system when there is no answer at your telephone. Line Redirection takes priority over Call Forward no answer.

Programming:
- "Assigning Call Forward" on page 409
- "Configuring centralized voice mail" on page 559

- **Forward no answer delay:** Determines the number of times that an incoming call rings at your telephone before the system forwards the call. To estimate the delay time in seconds, multiply the number of rings by six.

Programming: "Assigning Call Forward" on page 409

- **Call Forward on busy:** redirects calls to another telephone on your system or to a voice mail system when you are busy on a call, or when you have Do Not Disturb activated at your telephone. Telephones that have this active can still receive priority calls. If you are busy on a target line call, another call to that target line redirects to the prime telephone for that line or to the designated voice mail system. Line Redirection takes priority over this feature. Call Forward programming does not affect calls redirected by Line Redirection.

Programming:
- "Assigning Call Forward" on page 409
- "Configuring centralized voice mail" on page 559

- **Call Forward and voice mail:** If you want a voice mail system to pick up unanswered calls:
  - use the internal number of your voice mail as the destination when you program Forward no Answer and Forward on busy
  - if your voice messaging system or service automatically retrieves calls, make the ring delay greater than the delay used by your voice mail system

— if the voice mail system is on a remote system, ensure that the correct routing codes are added to the voice mail forwarding dial string.

— if calls are being forwarded to telephones or voice mail outside the system, ensure that Allow redirect is set for the telephones.

Programming:

- "Configuring centralized voice mail" on page 559
- "Configuring the Capabilities features" on page 406 (Allow redirect)

- **Line redirection:** This feature (**FEATURE** 84) allows you redirect all calls coming in on a specific line to a telephone outside the office. You can decide to redirect all, or just some, of your external lines. You also specify whether the user will hear a ring each time a call is redirected. In programming, you can allow/disallow this feature for each telephone. The telephone must have this setting enabled to allow call forward outside the system, such as for external voice mail.

  You can also set up line redirection on a system level. This can be cancelled for the line(s) from a telephone with line redirection allowed.

Programming:

- Allow redirect: "Configuring the Capabilities features" on page 406
- System-level redirect: "Assigning Trunk/line data" on page 236

Prevent calls from ringing at your telephone

To maintain your privacy, you can use one of these features to block calls or ensure a private line:

- **Do Not Disturb:** Use this feature (**FEATURE** 85) to forward your calls to the prime telephone when there is no other telephone on which the line appears. If there is another telephone that shares the same line, the call can be answered by that person. The Delayed Ring Transfer feature transfers all calls not answered, to the prime telephone after a defined time.

  Do Not Disturb also prevents voice calls from alerting at your telephone. Voice calls appear as normal intercom calls. Use **FEATURE** #85 to cancel DND.

- **DND on Busy:** When you are busy on a call and a second call comes in, your telephone alerts you to the second call with a light ring. If you find this second call and ring is disruptive, you can prevent a second call by assigning Do Not Disturb (DND) on Busy to your extension.

  If you use DND, the line indicator for an external incoming call flashes, but your telephone does not ring. Internal and private network callers hear a busy tone instead of ringing when you are on the telephone. External callers are transferred to the prime set used in your system or to your voice mail. Forward on Busy takes priority over DND on Busy.

If an external call uses a target line, the call is processed according to the programming of the target line. If the target line is busy, the caller hears a busy tone or routes the call to the prime set for the target line or to the voice mail system, even if there is DND on Busy programming.

Programming: "Configuring the Capabilities features" on page 406 (DND on busy)

- **Turn Privacy on or off:** When you have lines assigned to more than one telephone, anyone with the line appearance can take a call, or join a call in progress. To provide exclusive access for a user, you can program privacy on a line, in which case, only one person at a time can use the line. If privacy is enabled, it can be turned off by the user (**FEATURE 83**).

  Privacy control cannot be used for internal or conference calls.

  When another telephone joins a call on a non-private line, the participants on the call hear a tone, and a message appears on the display.

  Programming:
  - "Assigning Trunk/line data" on page 236
  - "Turn Privacy on or off for a call" on page 258

- **Intrusion controls:** If your system is part of a private network that uses the Meridian call attendant on a centralized voice mail system, the attendant can use the break-in feature to interrupt a call, regardless of any other settings on your line. The exception is if you have a higher intrusion priority than the attendant. If this is the situation, the attendant would be forced to camp the call at your telephone or redirect the call elsewhere in the system.

  Programming:
  - "Setting intrusion controls" on page 414
  - "Break-in" on page 568

Communicating in the office

Your system allows you to communicate in ways other than making a phone call.

- **Page** (**FEATURE 60** to **FEATURE 63**): The page feature can be allowed/disallowed for individual telephones. You can also assign each telephone to specific page zones. Zone paging allows a user to alert a select group of users without disturbing other users. However, external pages will be broadcast wherever the external speakers are mounted.

  You can also determine whether a tone sounds before the page begins and what the maximum length of the page will be.

  — Creating page zones: A zone (1-6) is any group of telephones grouped together for paging, regardless of their location. The maximum number of telephones in a page zone is 50.

  — Using Page with external equipment: When you make a page that uses external paging equipment (external page or combined page), the Long Tones feature automatically activates for the external paging system only. This allows you to control optional equipment with the Long Tones feature.

Programming:

- "Configuring the Capabilities features" on page 406
- "Programming Feature settings" on page 457
- "Setting system timers" on page 472

- **Messages:** This feature allows you to leave a message on the display of another telephone in your system or to analog telephones connected to an Analog Station Module (ASM/ASM8+). The Messages feature indicates if you have any messages waiting.
The Messages feature uses a message waiting list to keep a record of your internal messages and your (external) voice mail messages.

  Note: To keep a record of external voice mail messages, you must have access to Business Communications Manager Voice Messaging service with visual message waiting indication and a Business Communications Manager digital telephone.

  Programming: There is no system programming for this feature, other than the voice messaging requirements which are discussed in the voice messaging documentation. However, the message waiting indicator (MWI) feature on some telephones, may require system programming.

  Programming:

  - "Determining analog settings" on page 412
  - "Message Waiting Indication" on page 565 (MCDN programming)
  - "Configuring MWI on DPNSS 1 networks" on page 569 (DPNSS 1 features)

  User codes for messaging:

  — Send message **FEATURE** 1 (Cancel using **FEATURE** #1)
  — Reply message **FEATURE 65**
  — Cancel Message Waiting (**FEATURE #65**)
  — Log into mail box to leave message (**FEATURE 980**)
  — Log into mail box to play message (**FEATURE 981**)

- **Voice Call:** Use this feature (**FEATURE 66**) to make an announcement to a specific person through their telephone. This feature includes the ability to sound a tone or mute the tone before the call is heard. You can set up your telephone to deny voice calls (**FEATURE 88)**.

  Note: Voice calls made to portable handsets, such as Companion, the BST T7406 cordless handset, and NetVision telephones, will occur as a ringing call.

  Programming: If you want to a use to be able to respond to a voice call without picking up the handset, enable HF answerback ("Configuring the Capabilities features" on page 406).

Using handsfree and mute

If the telephone you program has a speaker, you can configure a button that allows the user to speak to the caller without lifting the handset, or to use a headset instead of the handset. If this feature is assigned, the system automatically assigns:

- the bottom, right button on the telephone to be the handsfree/mute button on all M-series telephones and on the T7208 Business Series Terminals (BST).
- handsfree-only to the bottom right button for IP telephones and T7316 telephones, which have a separate mute button located under the dial pad.
- handsfree and mute to the buttons located under the dial pad for T7316E telephones.
- T7406 handsets must have handsfree active or the telephone will not work. NetVision handsets, model 7000 and 7100 telephones and i2001 IP telephones do not use this feature.
- **Handsfree speaker volume:** The handsfree speaker volume returns to the telephone volume default setting after a call is released.

Programming: "Configuring the Capabilities features" on page 406.
Note: Ensure that the **Handsfree** field is set to **Auto** for T7316E telephones.

Track your incoming calls

You can track your calls using these features:

- **Call log:** If your system has the appropriate equipment and you subscribe to the call information feature supplied by your service provider, you can record information about calls received on an external line. The line does not need to be assigned to the telephone that receives the call for it to be logged (BCM version 3.5 and newer software, passive logging). Nor does an assigned line need to be a ringing line to log a call. ISDN service packages that come with calling line identification (CLID) can supply the same feature.

Note: Portable telephones: Your portable telephone may not support this feature, or it may only support some of the functions of the feature.

Call Log creates a record of incoming external calls. For each call, the log can contain:

— sequence number in the Call Log
— name and number of the caller
— indication if the call was long distance
— indication if the call was answered and by whom
— time and date of the call
— number of repeated calls from the same source
— name of the line on which the call came

Call Log can help you to

— keep track of discarded calls or calls not answered
— track patterns for your callers (for example volume of calls and geographic area of calls)
— record caller information quickly and accurately
— build a personal telephone directory from log items

This feature allows users to:

— manually log a call (**FEATURE 813**)
— delete old log items (**FEATURE 815**)
— view the log (**FEATURE 812**) or about a current call (**FEATURE 811**)
— view charges for a call (**FEATURE 818**)
— view details about a specific item
— make a call using a call log entry

Information such as long distance indicator and the caller name and number may not show in the log. The appearance depends on the Call Display services provided by your local telephone company and the local telephone company of the caller.

Programming:

- "Identifying the telephone (General heading)" on page 391 (call log password)
- "Defining user preferences" on page 415 (call log options)
- "Call log notes" on page 417

Auto dumping: Ensure that you have autodumping (**FEATURE** 815) is enabled on any telephones that have call logging active, otherwise, the logs fill up and subsequent calls do not get logged.

- **Malicious Caller ID (MCID):** This feature records caller information at the central office for the last external call on the active ETSI ISDN line. This feature must be available from your service provider before you activate it in your system.

  If this service is active on the line, you must press **FEATURE 897** within 30 seconds after a caller hangs up, and before you hang up.

  Programming: "ETSI Euro network services" on page 545

Use alternate or scheduled services

There are three types of services for Business Communications Manager to handle calls in a different way on different days, and at different times of the day. These services for scheduling call restrictions, ringing groups, and routing services are controlled through the control telephone. A password is required to access the Restriction and Routing service schedules from the control telephone.

You can also determine time tables and specific names for each schedule.

Programming:

- Set up system schedule information:

  Programming:
  - "Defining common schedule settings" on page 485
  - "Defining service schedules" on page 489
  - "Turn services on and off" on page 484

- Set up ring groups and ringing schedules

  Programming: "Configuring ringing service" on page 490

- Set up routing schedules:

  Programming: "Configuring routing service" on page 495

- Set up restriction schedules:

  Programming: "Configuring restriction service" on page 493

Special telephones

- **Hotline telephone:** You can define a telephone that automatically dials an emergency or direct number when the handset is picked up.

  Programming: "Assigning a Hotline" on page 411

- **Control telephone:** This telephone allows you to control other telephones in the system by turning service schedules off and on.

  Programming: "Identifying the telephone (General heading)" on page 391

- **Prime telephone:** This telephone, which is defined for each line, receives unanswered calls when call forward when the line cannot deposit the call at the intended telephone.

  Programming: "Assigning Trunk/line data" on page 236

- **Direct dial telephone:** This is the telephone that system users can dial with one digit (direct dial access code). An example of this would be a receptionist telephone. This telephone is also usually the control telephone for system scheduling. You can create up to five direct dial telephones, however, they all respond to the same direct dial access code.

  Programming:
  - "Programming access codes" on page 310
  - "Creating Direct Dial sets" on page 313
  - "Configuring the Capabilities features" on page 406
  - "Defining ringing service schedules" on page 491 (extra dial telephone)

Auxiliary devices

A music source or an auxiliary ringer can be connected to the system hardware. In programming, you need to define how these features will be accessed and used.

- **Background music:** If there is an external music source connected to your system or if you have the IP music feature set up to use internet-based music distributors or download music clips onto your system, you can listen to music through the speaker on the telephone (**FEATURE 86**), or you can allow the music to be heard by callers who have been put on hold.

  Programming:
  - "Programming Feature settings" on page 457 (Background music and On hold)
  - "Configuring the music source" on page 601 (IP music)

- **Auxiliary ringer:** This optional device can be connected through a RJXX connection to your system. The auxiliary ringer is best suited to factory type locations that require loud ringing bells or horns.

  Programming:
  - "Assigning Trunk/line data" on page 236 to turn the feature on/off for a line
  - "Configuring the Capabilities features" on page 406 to turn the feature on for specific telephones
  - "Assigning ringing groups to lines" on page 492, for the ring group settings

- **Companion handset:** This portable handset communications with the Business Communications Manage through radio base stations connected to digital trunk modules (DTM) installed in the system. Note: Telephony region restrictions.

  Programming: Refer to the *Companion Installation and Configuration Guide*. The handsets also come with a user guide that describes the handset features.

- **DECT handset:** This portable handset communications through radio base stations connected to a DECT media bay module installed in the system. The module also provides access for configuration of the firmware that controls the handset function. Note: Telephony region restrictions.

  Programming: Refer to the DECT deployment documentation and the *DECT Installation and Configuration Guide* on your documentation CD. Deployment documentation is also available. The handsets also come with a user guide that describes the handset features.

- **Symbol NetVision handsets:** These portable handsets connect to the internet through an IP access point which is connected to the LAN or WAN to which the Business Communications Manager is also connected. They can call out using physical or VoIP trunks. Target lines direct incoming calls to the handsets.

  Programming: Refer to the *IP Telephony Configuration Guide*. Handsets also come with user guides that describe the handset features.

- **BST T7406 cordless handset:** This handset communicates with the BCM through a station module that supports three handsets. The station module connects to a digital trunk installed on the system. The handset emulates the T7324, although it only has six memory buttons.

  Programming: Same as for T7310/T7316 telephone. This telephone has six display keys.

- **BST Doorphone:** This is a device that installs at security entrances. This device uses a DN record in the system DNs range. The DN record for a doorphone will display M7324. However, there are specific required settings for the doorphone. Also, the doorphone does not use the user preferences or the Telco features settings. Installation and configuration information is contained in the *BST Doorphone Installation and Configuration Guide*.

Call out to external systems using host system dialing

When you make external calls, or forward calls to external systems, such as private branch exchanges (PBX system), you may need to insert one or more Host System dialing signals to connect the call. These features are also known as end-to-end signaling. Signaling features either send a special signal to the host system or allow you to program delays required by host systems in external autodial or speed dial sequences.

- **Link:** If you connect the system to a private branch exchange (PBX), you can use a Link signal to access special features. On some telephones, Link is called FLASH. You can include the Link signal as part of a longer stored sequence on an external autodial button or in a speed dial code. The Link symbol uses two of the 24 spaces in a dialing sequence. (**FEATURE** 71)

  Programming:

  - “Assigning Trunk/line data” on page 236 (Link at CO)
  - “Defining telephone dialing restrictions” on page 442 (Allow link)
  - “Setting system timers” on page 472

- **Pause:** This feature enters a 1.5-second delay in a dialing sequence on an external line. The use of this feature is often required for signaling remote devices, such as answering machines, or when reaching through to PBX features or host systems. You can program more than one pause in an external autodial or speed dial sequence. (**FEATURE** 78)

  The Pause symbol uses one of the 24 spaces in a dialing sequence.
  For pulse dialing, pressing * inserts a 1.5-second pause into the dialing sequence.

  Programming: There is no system programming for this feature.

- **Long Tones:** This feature (**FEATURE 808**), when invoked while a call is active, allows you to control the length of a tone to signal devices such as fax or answering machines, which require tones longer than the standard 120 milliseconds. You can use Long tones on any call except a conference call. You can use internal lines of the system to activate a device connected to an ATA2 or an ASM in another area of your office, or external lines to access devices outside the system.

  Programming: There is no system programming for this feature.

- **Run/Stop:** This feature (**FEATURE** *9) inserts a break point into a sequence of dialed numbers or characters used for automatic dialing. This can be necessary when you are connecting to a PBX or similar host system. For example: you can call a company with an automated attendant that instructs you to dial the internal number you need. You can program the company number, a Run/Stop, then the internal number on one external autodial button.

  The Run/Stop symbol uses one of the 24 spaces in an autodial or speed dial sequence.

  You can include up to three Run/Stop commands in a dialing string. The system ignores a fourth Run/Stop, and any digits or commands that follow three Run/Stop commands in a programmed dialing sequence.

  To use:

  a Press the autodial button one time to dial the company number.

  b When you hear the automated attendant, press the autodial button again to dial the internal number.

  Programming: There is no system programming for this feature.

- **Wait for Dial Tone:** This feature (**FEATURE** 804) causes a sequence of numbers to pause until dial tone is present on the line before continuing to dial. You can use this feature if you must dial a remote system and then wait for dial tone from that system before dialing the remainder of your number. The Wait for Dial Tone symbol uses two of the 24 spaces in an autodial or speed dial sequence.

  Programming: There is no system programming for this feature.

- **Pulse or tone dialing:** If your external lines use pulse dialing, you can switch temporarily to tone dialing. Tone dialing allows you to communicate with devices such as answering machines or automatic switchboards, to access the features that PBX systems can provide, or to access another system remotely.

  Press # while on an active line. After you hang up, your telephone returns to pulse dialing.

Call in from outside the system

Callers can access the system over the public telephone network when away from the office, or you can call from another system, over a private network.

- You can determine which lines will be available for remote access, and define further restrictions.
- You can control which lines and what features are available to these callers by specifying class of service (COS) passwords and identifying restrictions for each password.

Programming:

- "Using the General record" on page 235 (use remote package)
- "Creating Direct Inward System Access (DISA)" on page 291
- "Remote access line settings" on page 292
- "Defining remote access packages" on page 294
- "Using COS passwords" on page 296

Security Note: It is important to maintain the security of your system by limiting access to authorized users and limiting those users to the features they need.

Controlling telephone programming access

You can control the amount of access users have to the programming features on their telephones using the Set lock feature.

Programming: "Defining telephone dialing restrictions" on page 442

Special features

This section describes features on the system which serve a specific purpose that is optional to the general function of the system.

- **Hospitality services:** This feature allows small to medium service facilities to provide customer telephone service, as well as administration services through a telephone interface. Programming: Besides the general line and telephone programming required for individual group members, Chapter 24, ”Configuring Hospitality Services” on page 589 explains the feature in detail.

- **Hunt groups:** This feature allows you to group your call center operators so you can target specific types of calls to specific groups. As well, you can define how calls enter the group, so you can control the work load based on your requirements for your operators.
Programming: Besides the general line and telephone programming required for individual group members, Chapter 23, ”Configuring Hunt groups” on page 573 provides details about setting up hunt groups and hunt group features.

- **Silent Monitor:** This feature allows specified two-line display telephones to be used to monitor Hunt group and Call Center operators. You can specify whether the system sound a tone before breaking into a call, or whether the break-in will be silent. Display prompts on the supervisor telephone allows the supervisor to unmute or move from user to user.

  Programming:
  - “Defining device capabilities” on page 405 (SM supervisor)
  - “Monitoring Hunt groups” on page 585 (General settings, Silent monitor)

- **Call Center:** The Business Communications Manager provides a suite of applications that support call center activities through the CallPilot application. This information is explained in detail in separate documentation, including: *Call Center Set Up and Operation Guide*, *Call Center Agent Guide*, *Call Center Supervisor Guide*, and the *Call Center Reporting Set Up and Operation Guide*

- **CallPilot:** The Business Communications Manager provides an on-board voice mail system, however, external voice mail systems can also be used, including a centralized system off a Meridian 1 if the Business Communications Manager is networked to the Meridian through PRI SL-1lines or VoIP trunks with the MCDN protocol active. This information is explained in detail in separate documentation, including: *CallPilot Manager Set Up and Operation Guide*, *CallPilot Reference Guide*, *CallPilot Quick Reference Guide*, *CallPilot Programming Record*, *CallPilot Message Networking Set Up and Operation Guide*, *CallPilot Message Networking User Guide*, *CallPilot Unified Messaging Installation and Maintenance Guide*, *CallPilot Desktop (Unified) Messaging Quick Reference Guide, CallPilot Fax Set Up and Operation Guide*, *CallPilot Fax User Guide*.

- **Call activity:** The Call Detail Recording part of the Business Communications Manager allows you to monitor call activity for specific calls or telephones. Configuration information is detailed in *Call Detail Recording System Administrator Guide*.

- **IVR:** The Interactive Voice Response feature allows your customers greater interaction with your call centers. Configuration information is located in Interactive Voice Response Installation and Configuration Guide (IVR)

Information matrices

Each section in this book provides a matrix containing the field information from that section. You can use this information to create a spreadsheet record of your system configuration or for a quick overview of the information that you require for each type of programming.

Programming Record forms set up in Microsoft Excel* are available on your documentation CD.

- "Line matrix" on page 263
- "Loop matrix" on page 281
- "Dialing Plans matrix" on page 307
- "CbC matrix" on page 342
- "Routing matrix" on page 338
- "Restriction filters matrix" on page 350
- "Direct dial matrix" on page 314
- "Target lines matrix" on page 290
- "Remote access matrix" on page 300
- "Digital telephones DN record matrices" on page 447
- "System features matrix" on page 471
- "Timers matrix" on page 473
- "System speed dial matrix" on page 477
- "Telco features matrix" on page 480
- "Services matrix" on page 496
- "Hunt group matrix" on page 584
- "Hospitality matrix" on page 595

Chapter 9
Configuring lines

This section describes the information accessed under the **Services, Telephony Services**, **Lines** headings.

Task:
• Configure the lines connected to the system, or call channels configured as Voice over IP (VoIP) trunks or target lines.

This section contains:

The screens accessed through these headings define the line numbers that correspond to the DIP switch settings that were configured on the trunk media bay modules installed on your system. Check your Programming Record to see which modules are installed, and what settings were chosen. The screens also are used to assign Voice over IP (VoIP) trunks and target line*s*, however, the process for defining these lines is described in other sections since they are not related directly to external hardware.

Note: External lines are also referred to as trunks. External lines include the lines between the public network (PSTN) and between the nodes in a private network. Non-physical connections, such as voice over IP (VoIP) and target lines, are also referred to as trunks and lines, respectively, even though they do not describe actual wired connections.
All physical trunks connect to the Business Communications Manager through a media bay module of some sort. All non-physical trunks and lines use a LAN or WAN connection (VoIP trunks) or internal call processing (target lines).
However, the connection, all lines are configured under the Lines or loops headings.

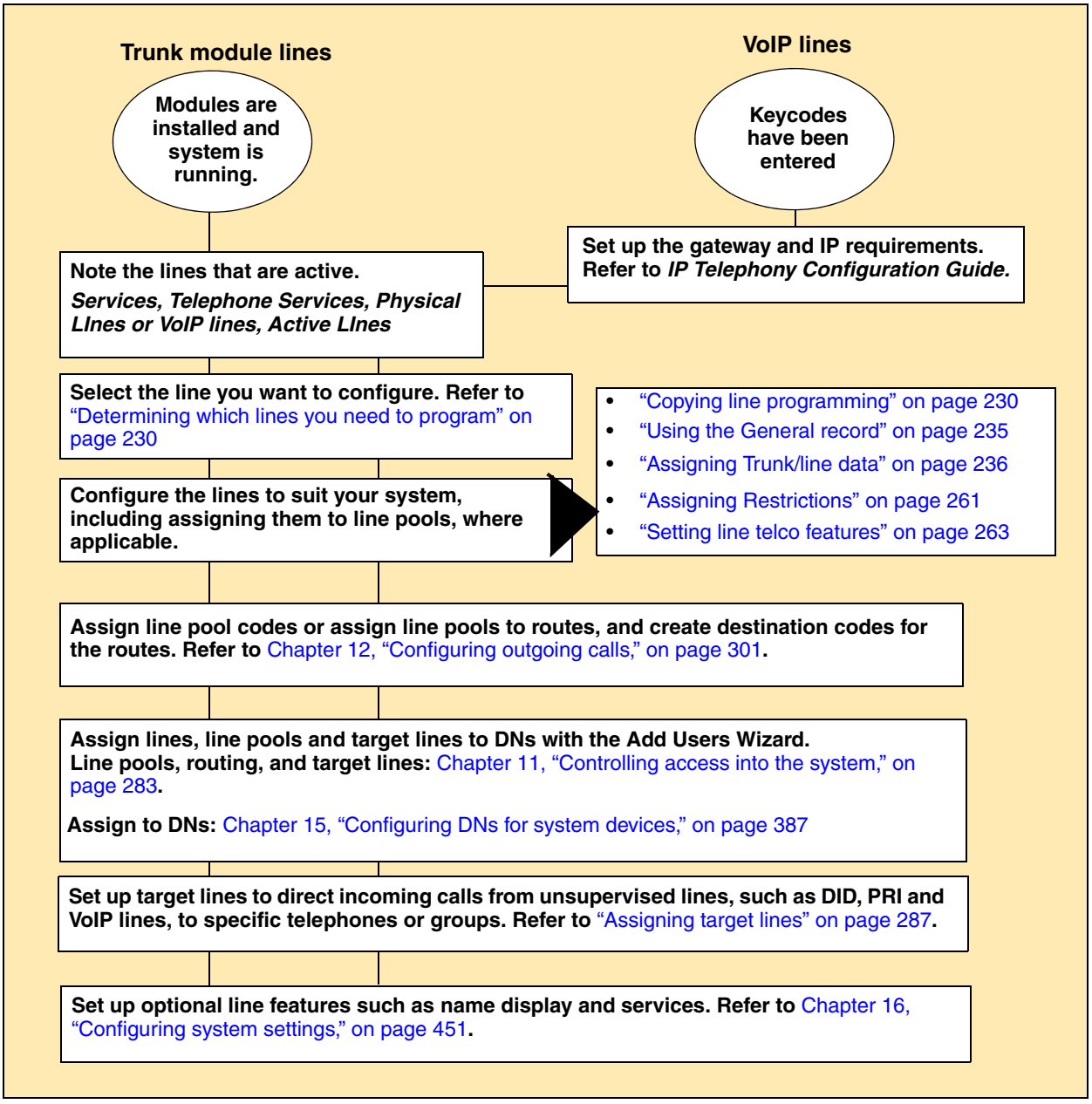
Other configuration options or equirements:

- **BRI loops** require configuration and provisioning before the BRI lines can be configured. Refer to Chapter 10, "Configuring BRI Loops," on page 265.
- The Business Communications Manager also offers facilities for **splitting trunks** to deliver both data and telephony services. Refer to the chapter titled "Data and split-line configuration" on page 151 for a description of how the Business Communications Manager uses data modules and WAN programming in this context.

Understanding the process of line configuration

Refer to the process map below, which leads you through the order for configuring the lines for your system.

Figure 47 Process map: Configuring the lines for your system



Understanding how the system identifies lines

On a new system, lines and loops are numbered and assigned defaults based on the type of media bay modules that have been connected to the system. The exception is the voice over IP (VoIP) trunks, which require a keycode to activate.

The Unified Manager displays all active physical lines under:
Lines, Physical Lines, Enabled Lines.

These screens allow you to easily view which lines have been enabled through a media bay module. (Refer to "Configuring resources — media bay modules" on page 123 for information about configuring media bay module records.)

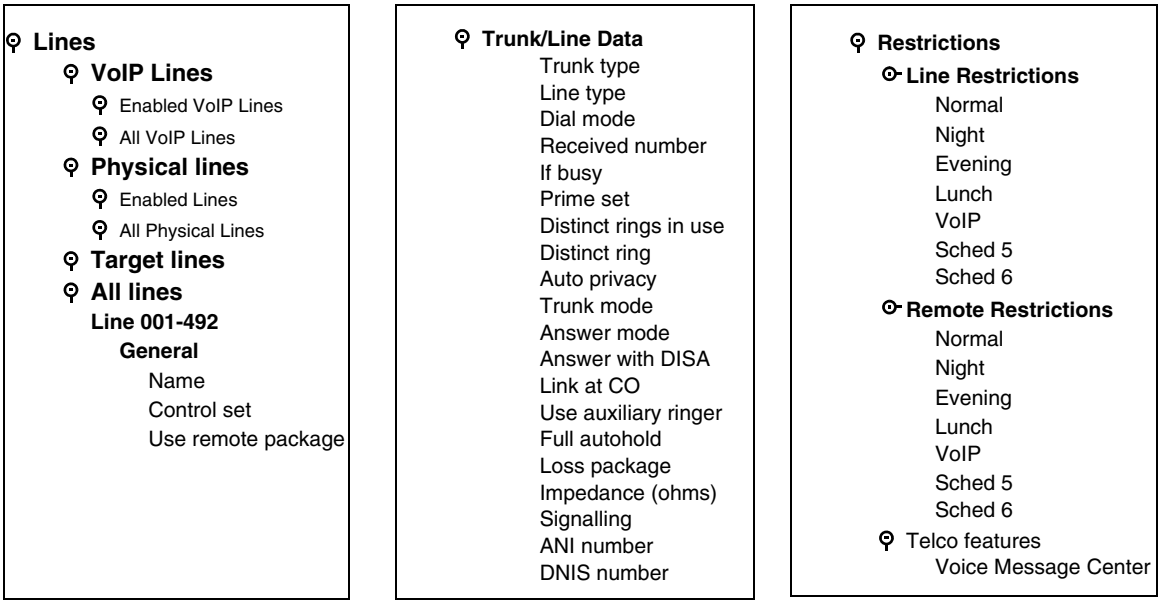
From this heading, you can access each line record and assign attributes, as you require.

This section describes:

- "Copying line programming" on page 230
- "Determining which lines you need to program" on page 230

The following figure shows a detailed view of the Lines navigation tree headings.

Figure 48 Lines menus and fields



Copying line programming

The **Copy** command allows you to duplicate programming for a line and apply it to another line.

You cannot copy programming between lines on different types of media bay modules. The Received number of a target line is a unique number and cannot be copied.

When you copy data from a physical trunk to a target line (or the other way around), only the data in common is copied. For example, copying a target line to a T1 E&M trunk copies only the Line data settings because there are no Trunk data settings for a target line.

Follow these steps to copy a line setting to a single line.

1. Click on the keys beside **Services, Telephony Services, Lines, Physical Lines, Enabled Lines**.
2. Click the line number from which you want to copy settings.
3. Choose the subheading for the information that you want to copy: **Trunk/Line data**, **Restrictions**, or **Telco features**.
4. From the **Edit** menu, click **Copy**.
5. In the **Copy to** box, type the line number where you want to copy the settings.
6. Click the **OK** button.

Determining which lines you need to program

Under **Lines**, note that line types are divided into three headings. The fourth heading contains all line numbers.

VoIP lines (require keycode)

Voice over IP (VoIP) lines are signaling channel*s* that simulate how CO lines work. However, VoIP lines transmit data to the IP network over a LAN or WAN rather than over physical lines. Once the VoIP trunks are set up, you can assign them to line pools, and program their behavior in the same way you would PRI lines.

VoIP lines use line numbers 001 to 060. These line records appear under **Services, Telephony Services, Lines, VoIP Lines**. To access VoIP lines, you need to enter software keycode*s*. Each keycode supports a specific number of lines. If you are using both SIP and H.323 trunks, the H.323 trunks start numbering up from 001, and the SIP trunks start numbering down from 060. No entries appear in the **Enabled VoIP lines** field until you complete the **IP Trunks Settings** field, which displays when you click on **IP Trunks** under **Services**, **IP Telephony**.

VoIP trunks should be configured to use a single line pool, per trunk type. Do not mix other trunk types on the same line pool. The VoIP line pools are assigned to routes, which, in turn, are configured with destination codes that route calls to the designated remote gateways of other

Business Communications Manager systems or Meridian 1-IPT systems. **Note:** SIP trunks can only be used between Business Communications Managers.

You can also create a fallback for the trunk. This is a situation where the system reroutes the call to a PSTN line pool if the primary route is not available or the call quality is not suitable. If you do not configure your network for fallback and the call quality is below threshold, the IP call fails.

Refer to the *IP Telephony Configuration Guide* for information about configuring VoIP trunks.

Target lines

Target lines are internal communications paths that directly connect auto-answer trunks to system telephones. These lines are in-coming only.

Target lines allow you to make more efficient use of DID line resources.You can map a range of target lines for each DID line. The incoming call is routed according to the mapped dialed digits, rather than a one-to-one line assignment. Refer to "DID system" on page 191 for an example of a system using DID trunks and target lines. Systems configured using the DID template, automatically assign target lines to all assigned DNs.

You also require target lines when you use PRI or VoIP trunks.

Target lines use line numbers 241 to 492. These lines are found under **Services, Telephony Services, Lines, Target Lines**. Record this information in your system Programming Records so you have a clear view of where each line is assigned.Refer to "Assigning target lines" on page 287 for instructions about setting up target lines.

Other features:

- Each target line also can be assigned to more than one telephone.
- A telephone can have multiple appearances of a target line.

Physical lines

Physical lines are the central office (CO) trunks assigned to the trunk media bay modules. Which lines are enabled is determined by the DIP switch settings on the installed trunk modules.

You can change the line types to suit your system. For instance, BRI and DTM modules can be designated to a number of line types, depending on the type of line service provided through the central office (CO). However, the line numbers are associated for specific tasks or to specific DS30 bus numbers.

Refer to the table below for a list of lines assigned per bus (DS30 bus and offset), based on the module type configured with that address. You can use this chart to note which lines should be active for the modules you installed. You can also note which line pool you put the lines in, and note the line pool access codes or routes and destination codes to which you assigned the line pools (or use your programming records).

Follow these steps to use the table.

1. For each bus number, circle the module you set to that number.
2. Beside the module name, circle the group of line numbers appropriate for the offset you set on the modules.
3. In the Line pool column, indicate a line pool name if you want to associate lines into a pool. This enables assigned telephones to grab any free line from the pool.
4. On the far right column, list the access codes and routes associated with the lines.

Table 30 DS30 number and offset line-loop default list

DS30 bus	Type of module	Line/Loop numbers (default) Offset 0	1	2	3	Line pool A-O/PRI	Access codes and routes
		Default Start DN: 221					
02	Trunk modules						
	DTM (T1)	211-234					
	DTM (NA-PRI)	211-233					
	DTM (E1 PRI)	211-240					
	DDI MUX DTM	211-234*					
	BRI	211-218	219-226	227-234			
	CTM4, GATM4 and **4X16**	211-214	219-222	227-230	235-238		
	CTM8, GATM8 (upper/ lower)	211-214 219-222	219-222 227-230	227-230 235-238	N/A		
	ISDN loops						
	BRI ST/U2/U4	201-204	205-208	209-212			
*Note which lines are for data and which are for telephony.							
03	Trunk module						
	DTM (T1)	181-204					
	DTM (NA-PRI)	181-203					
	DTM (E1 PRI)	181-210					
	DDI MUX DTM	181-204*					
	BRI	181-188	189-196	197-204			
	CTM4, GATM4 and **4X16**	181-184	189-192	197-200	205-208		
	CTM8, GATM8 (upper/ lower)	181-184 189-192	189-192 197-200	197-200 205-208	N/A		
	ISDN loops						
	BRI ST/U2/U4	301-304	305-308	309-312			
*Note which lines are for data, and which are for telephony.							

Table 30 DS30 number and offset line-loop default list (Continued)

DS30 bus	Type of module	Line/Loop numbers (default) Offset 0	1	2	3	Line pool A-O/PRI	Access codes and routes
04	Trunk module						
	DTM (T1)	151-174					
	DTM (NA-PRI)	151-173					
	DTM (E1 PRI	151-180					
	DDI MUX DTM	151-174*					
	BRI	181-188	189-196	197-204			
	CTM4, GATM4 and **4X16**	151-154	159-162	167-170	175-178		
	CTM8, GATM8 (upper/ lower)	151-154 159-162	159-162 167-170	167-170 175-178	N/A		
	ISDN loops						
	BRI ST/U2/U4	401-404	405-408	409-412			
*Note which lines are for data and which are for telephony.							
05	Trunk module						
	DTM (T1)	121-144					
	DTM (NA-PRI	121-143					
	DTM (E1 PRI)	121-150					
	DDI MUX DTM	121-144*					
	BRI	151-158	159-166	167-174			
	CTM4, GATM4 and **4X16**	121-124	129-132	137-140	145-148		
	CTM8, GATM8 (upper/ lower)	121-124 129-132	129-132 137-140	137-140 145-148	N/A		
	ISDN loops						
	BRI ST/U2/U4	501-504	505-508	509-512			
*Note which lines are for data, and which are for telephony.							
06	Trunk module						
	DTM (T1)	91-114					
	DTM (NA-PRI)	91-113					
	DTM (E1 PRI)	91-120					
	DDI MUX DTM	91-114*					
	BRI	91-98	99-106	107-114			
	CTM4, GATM4 and **4X16**	91-94	99-102	107-110	115-188		
	CTM8, GATM8 (upper/ lower)	91-94 99-102	99-102 107-110	107-110 115-188	N/A		
	ISDN loops						
	BRI ST/U2/U4	601-604					
*Note which lines are for data and which are for telephony.							

Table 30 DS30 number and offset line-loop default list (Continued)

DS30 bus	Type of module	Line/Loop numbers (default) Offset 0	1	2	3	Line pool A-O/PRI	Access codes and routes
07	Trunk module						
	DTM (T1)	61-84					
	DTM (NA-PRI)	61-83					
	DTM (E1 PRI)	61-90					
	DDI MUX DTM	121-144*					
	BRI	61-68	69-79	77-84			
	CTM4, GATM4 and **4X16**	61-64	69-72	77-80	85-88		
	CTM8, GATM8 (upper/ lower)	61-64 69-72	69-72 77-80	77-80 85-88	N/A		
	ISDN loops						
	I**BRI** ST/U2/U4	701-704	705-708	709-712			
*Note which lines are for data, and which are for telephony.							

All lines

This heading contains all possible lines available to the system.

Using the General record

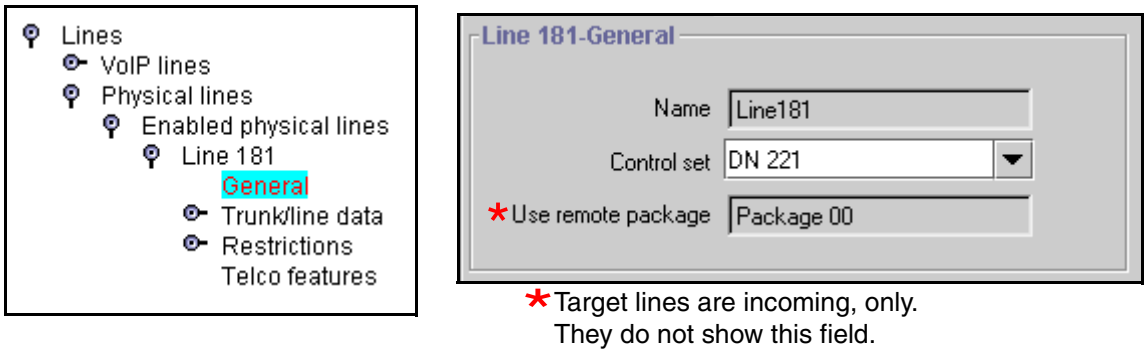
The **Lines XXX General** record allows you to assign a name, a control telephone, and a remote package for a line.

1 Choose the type of line with which you want to work.

2 Under that heading, choose the line number record you want configure.

3 Click **General**.

Figure 49 Using the Lines General screen



4 Change the headings to fit your requirements.
The following table shows the possible settings for the General record.

Table 31 General record values

Attribute	Value	Description
Name	<maximum of seven alphanumeric characters>	Identify the line in a way that is meaningful to your system, such as by the type of line and line pool or the DN it is attached to in the case of target lines.
Control set	DN <control telephone DN> Default: 221 (default Start DN)	Enter a telephone DN for a telephone that you want to use to turn service off or on for other telephones using this line. The control telephone must have the line assigned, or must be assigned to the line pool the line is in. Refer to "Assigning line pool access" on page 402
	Tips: External lines and telephones must be programmed to use one of the Scheduled Services: Ringing, Restriction, and Routing Services. For maximum flexibility, Nortel Networks recommends that you create two different control telephones, one for the lines and one for the telephones. You can turn on a service manually or automatically for all external lines from an assigned control telephone. However, you cannot combine schedules. A service can only be active as normal service or one of the six schedules at any one time. Several schedules can be active at one time, but they must use different services.	
Use remote package	<two-digit remote package number>	Package 00: Prohibits remote access to: • line pools • external page This package cannot be changed. Package 01-15 are programmable. Refer to "Defining remote access packages" on page 294

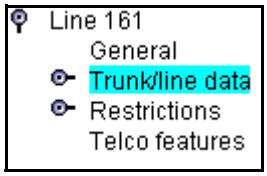
Table 31 General record values (Continued)

Attribute	Value	Description
	Tips: You can program a line pool access code under **Telephony Services, General Settings, Access Codes**. Refer to "Setting up line pool access codes" on page 317.	

Assigning Trunk/line data

The **Trunk/line data** heading allows you to program settings for lines that affect how the Business Communications Manager communicates with other switches. These settings also allow you to determine how lines, including target lines, are used in Business Communications Manager.

1 Under the line number you are configuring, click the **Trunk/line data** heading.



2 The **Trunk type** field is read-only unless the trunk type is **T1**.

Note: You can change the trunk type setting only for lines connected to a T1 line. All other lines are automatically configured, based on the type of media bay module present.

Trunk types:

- VoIP
- DTM: TI types (Loop, E&M, DID, Ground, or fixed data channel), PRI, DASS2, DPNSS. The DDI MUX module contains a DTM.
- CTM (North America): Loop
- BRI: BRI S/T, BRI U2, U4
- Target lines

BRI note: BRI U2 and BRI U4 are only available through a FEM module connected to a Norstar trunk module with a BRI U2 or BRI U4 card.

3 Configure the line settings.
The fields that appear will depend on the type of line. Refer to the charts below for descriptions of applicable fields:

- "Loop start analog/digital fields" on page 237
- "Ground start fields" on page 240
- "DID fields" on page 242
- "E&M fields" on page 244
- "Target lines and DASS2 fields" on page 247
- "PRI fields" on page 249

- "BRI fields" on page 250
- "DPNSS fields" on page 252
- "VoIP fields" on page 253
- "Lines field cross-reference chart" on page 255

Loop start analog/digital fields

Table 32 Loop start analog and digital fields

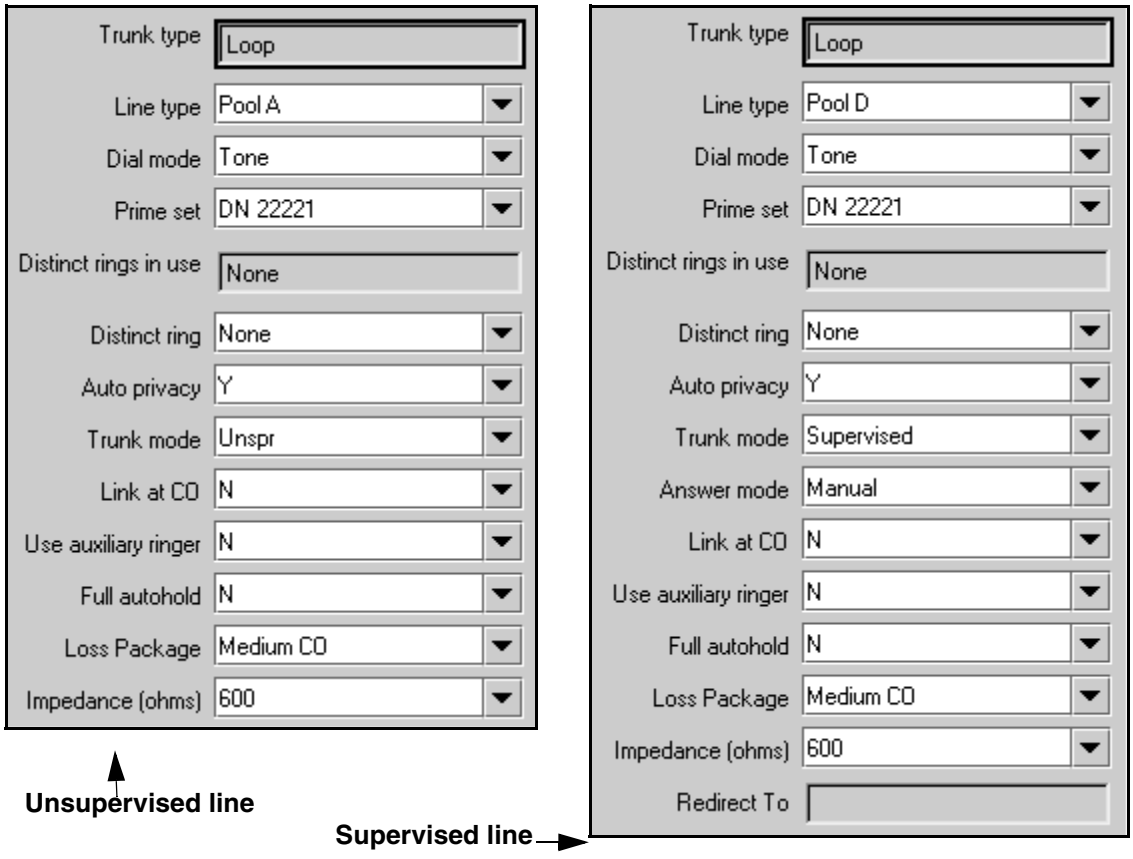
Attribute	Value	Description
		
Line type	Public Private to: Pool A to O	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O: assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to "Line pool tips" on page 259.
Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk.

Table 32 Loop start analog and digital fields (Continued)

Attribute	Value	Description
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone. Doorphone note: Ensure that this DN does not belong to a doorphone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to “Turn Privacy on or off for a call” on page 258 (**FEATURE** 83).
Trunk mode	Unspr Supervised * Earth calling *Loop guarded *Loop unguarded ^Reversal on Idle (ROI)	Define whether disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. You must set this to Supervised if a loop trunk has its Answer mode set to Auto or if you enable Answer with DISA. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Supervised option to work. * These listing only appears for UK analog lines. Note that Earth calling is only supported by a FEM connected to a Norstar analog trunk module. The GATM does not support Earth calling, even though the setting appears for the lines on the module. ^This listing appears only for the Australia profile.
		Tips: The duration of an open switch interval (OSI) before Business Communications Manager disconnects a call is programmed by the Disconnect timer setting. Refer to “Configuring the trunk module to line type” on page 131.

Table 32 Loop start analog and digital fields (Continued)

Attribute	Value	Description
Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
		Note: You require Disconnect supervision on the line if loop start trunks are to operate in auto-answer mode (Trunk mode).
Answer with DISA	Y or N	If Y, when a remote user calls into the system on an unsupervised line, the system prompts a caller for a six-digit class of service (COS) password. If N, when a remote user calls into the system on an unsupervised line, the call is connected as dialed.
Link at CO	Y or N	Some exchanges respond to a Link signal (**FEATURE 71**) by providing an alternative line for making outgoing calls. Enabling Link at CO causes the system to apply the restrictions on outgoing calls to the digits dialed after the Link signal. As well, the call on the alternative line is subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the Business Communications Manager restrictions in cases where the host exchange does not provide an alternative line. You also need to ensure that telephones using the line have the feature allowed. Refer to "Defining telephone dialing restrictions" on page 442.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. The default setting should be changed only if Full autohold is required for a specific application.
Loss Packages	Short CO Medium CO Long CO Short PBX Long PBX	Select the appropriate loss/gain and impedance settings for each line. For more information refer to "Using loss packages" on page 260.
Impedance	600 ohm 900 ohm	The GATM can be set to a specific impedance level. This is determined by local line requirements.

Table 32 Loop start analog and digital fields (Continued)

Attribute	Value	Description
Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
⚠	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

Ground start fields

Table 33 Ground start fields

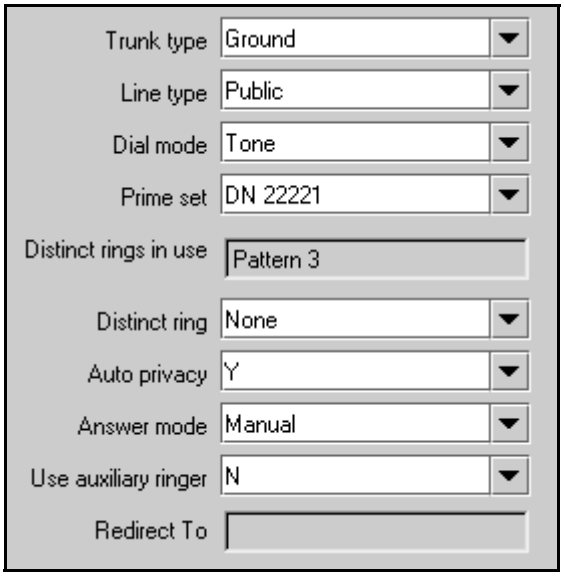
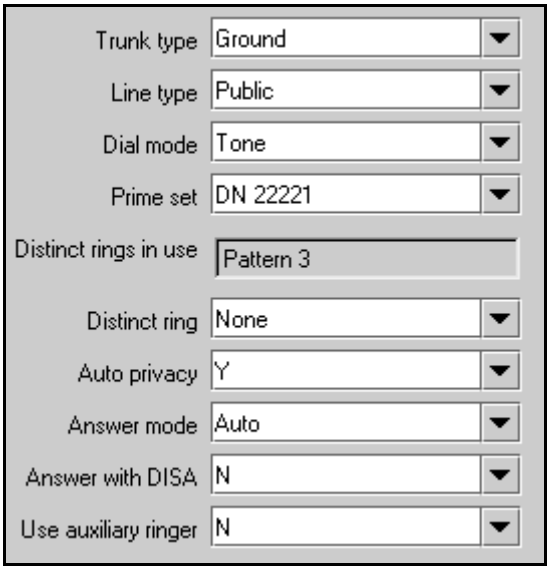
Attribute	Value	Description
Manual answer line  **Auto answer line** 		
Line type	Public Private to: Pool A to O,	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O: assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to "Line pool tips" on page 259.
Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk.

Table 33 Ground start fields (Continued)

Attribute	Value	Description
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to "Turn Privacy on or off for a call" on page 258. (**FEATURE** 83)
Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
Answer with DISA	Y or N	If Y, when a remote user calls into the system on an unsupervised line, the system prompts a caller for a six-digit class of service (COS) password. If N, when a remote user calls into the system on an unsupervised line, the call is connected as dialed.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490

Table 33 Ground start fields (Continued)

Attribute	Value	Description
Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
⚠	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

DID fields

Table 34 DID line fields

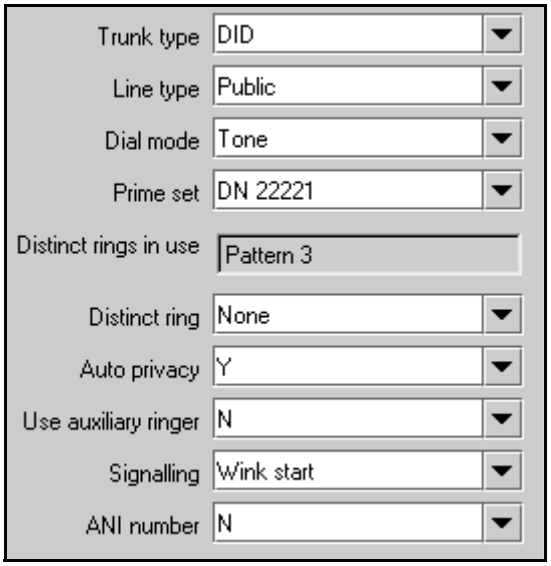
Attribute	Value	Description
		

Table 34 DID line fields (Continued)

Attribute	Value	Description
Line type	Public Private to: Pool A to O	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O: assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to "Line pool tips" on page 259.
Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk. Tone does not appear if Signaling is set to Immediate (T1 DID &T1 E&M trunk types only).
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to "Turn Privacy on or off for a call" on page 258. (**FEATURE** 83)
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Signaling	WinkStart Immediate DelayDial	Select the signal type for the line. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to a DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch.

Table 34 DID line fields (Continued)

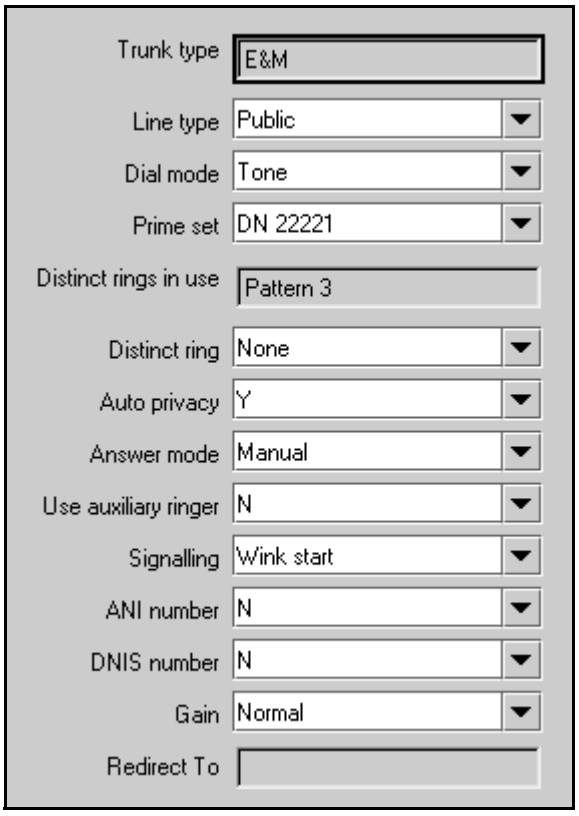
Attribute	Value	Description
ANI Number	Y or N	Define whether the telephone number of the caller will be collected for this line. For T1 E&M and T1 DID trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required.
Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
⚠	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

E&M fields

Table 35 E&M line fields

Attribute	Value	Description

E&M trunk



T1 E&M

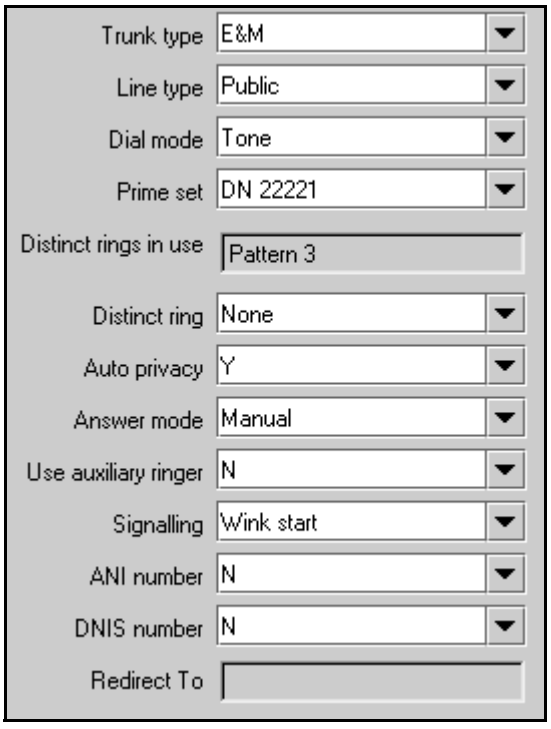


Table 35 E&M line fields (Continued)

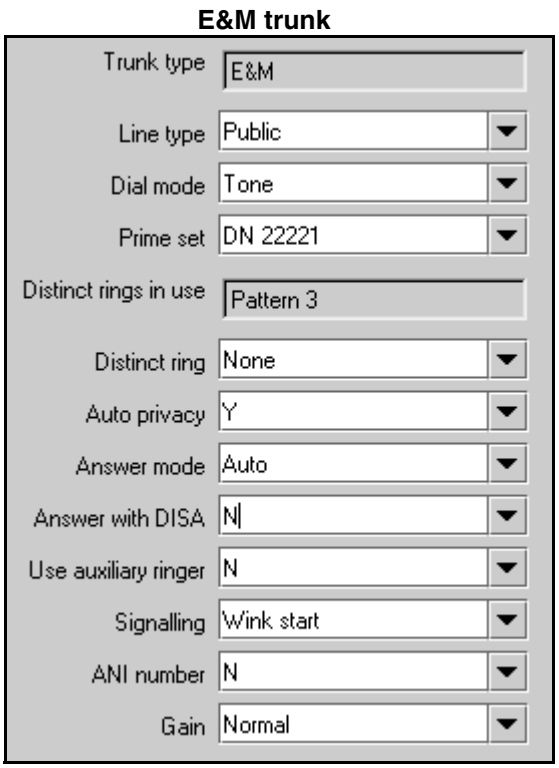
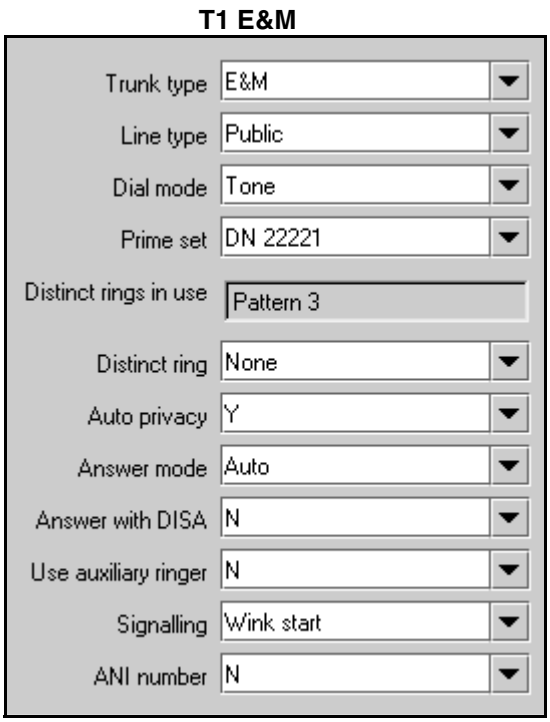
Attribute	Value	Description
		
Line type	Public Private to: Pool A to O	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O: assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to "Line pool tips" on page 259.
Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk. Tone does not appear if Signaling is set to Immediate (T1 DID &T1 E&M trunk types only).
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.

Table 35 E&M line fields (Continued)

Attribute	Value	Description
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to "Turn Privacy on or off for a call" on page 258. (**FEATURE** 83)
Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
Answer with DISA	Y or N	Define whether the system prompts a caller for a six-digit class of service (COS) password (Y). This setting appears for T1 loop start and T1 E&M lines that have auto-answer mode. Set this option to No for T1 E&M lines on a private network that have auto-answer mode.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Signaling	WinkStart Immediate DelayDial	Select the signal type for the line. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to a DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch.
ANI Number	Y or N	Define whether the telephone number of the caller will be collected for this line. For T1 E&M and T1 DID trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required.

Table 35 E&M line fields (Continued)

Attribute	Value	Description
DNIS Number	Y or N	Defines whether the digits dialed by an external caller on this line will be collected.For T1 E&M trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart and Answer mode is set to Manual. These digits are required for some third-party software applications.
*Gain	Normal High	Set the level of gain for the channel. *E&M trunks only. T1 E&M trunks do not have this field.
Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

Target lines and DASS2 fields

Table 36 Target lines and DASS2 line fields

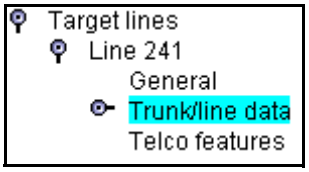
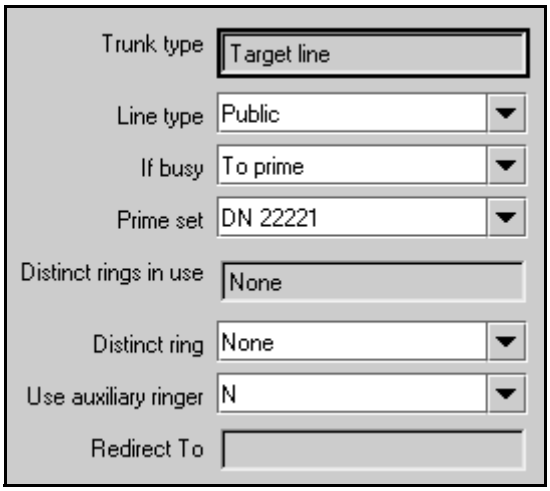
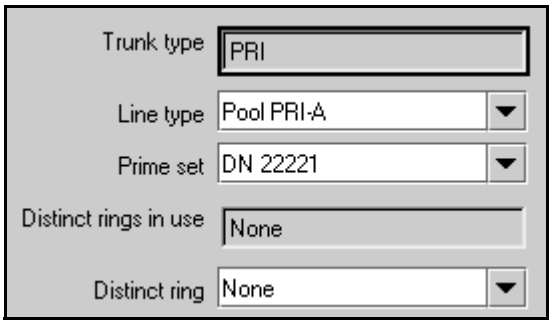
Attribute	Value	Description
 		
Line type	Public Private to:	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone.
If busy	To Prime Busy Tone	Define whether a caller receives a busy tone or the call forwards to the prime telephone when the target line is busy. Busy tone only works for PRI trunks.
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.

Table 36 Target lines and DASS2 line fields (Continued)

Attribute	Value	Description
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Received # (Private Number/ Public Number)	<digits associated with a specific target line>	Specify the digits to make a specific target line ring. • A received number cannot be the same as, or be the start digits, of a line pool access code, a destination code, the DISA DN or the Auto DN. • If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used. For further information, refer to "Received #" on page 259.
Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	
Assign target lines		Refer to "Assigning target lines" on page 287.

PRI fields

Table 37 PRI line fields

Attribute	Value	Description
		
Line type	PRI A to PRI-F	Define how the line is used in relation to other lines in the system. • PRI A to PRI F: you must use routes and destination codes to direct PRI lines.
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**WARNING:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

BRI fields

Table 38 BRI line fields

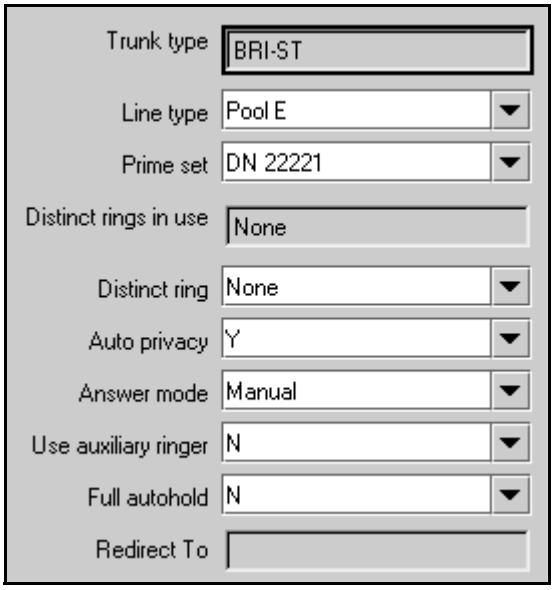
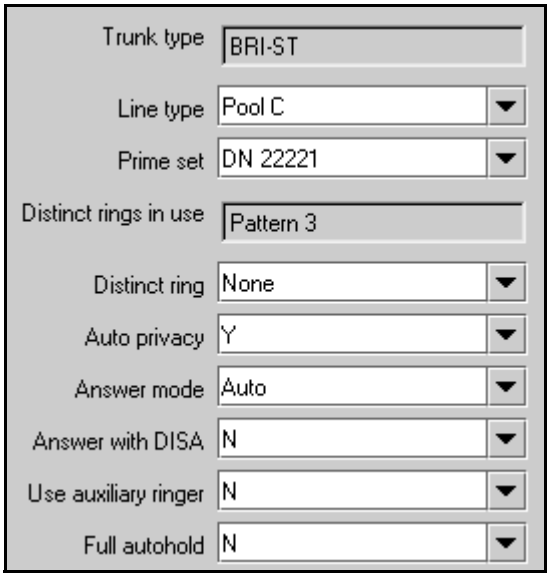
Attribute	Value	Description
Manual answer line 	**Auto answer line** 	
Line type	Public Private to: PRI A to PRI-F	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • PRI A to PRI F: assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to “Line pool tips” on page 259.
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None

Table 38 BRI line fields (Continued)

Attribute	Value	Description
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to "Turn Privacy on or off for a call" on page 258. (**FEATURE** 83)
Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
Answer with DISA	Y or N	Define whether the system prompts a caller for a six-digit class of service (COS) password. This setting appears for T1 loop start and T1 E&M lines that have auto-answer mode. Set this option to No for T1 E&M lines on a private network that have auto-answer mode.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. The default setting should be changed only if Full autohold is required for a specific application.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

DPNSS fields

Table 39 DPNSS line fields

Attribute	Value	Description
Line type	Public Private to: PRI A to PRI-F	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • PRI A to PRI F: assigns the line to one of the line pools. PRI line pools must be used in conjunction with routes and destination codes.
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None. Refer to “Defining user preferences” on page 415 for information about assigning a distinctive ring pattern to a telephone. You can also assign a distinctive ring pattern to a Hunt group. Refer to “Identifying a Hunt group” on page 575.
Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.

Table 39 DPNSS line fields

Attribute	Value	Description
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring ringing service" on page 490
Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. The default setting should be changed only if Full autohold is required for a specific application.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

VoIP fields

Table 40 VoIP line data fields

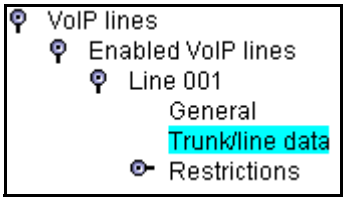
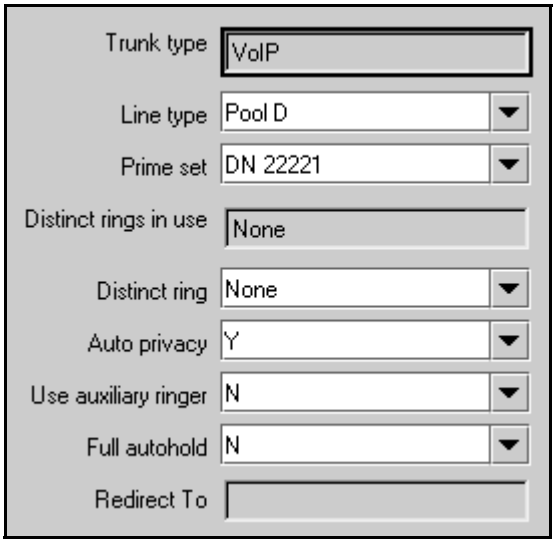
Attribute	Value	Description
 		
Line type	Public Private to: Pool A to O	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O/PRI A to PRI F: assigns the line to one of the 15 line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to "Line pool tips" on page 259.

Table 40 VoIP line data fields (Continued)

Attribute	Value	Description
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**Warning:** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None.
Auto privacy	Y or N	This setting has no effect on VoIP lines.
Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
		Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to “Configuring ringing service” on page 490
Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. The default setting should be changed only if Full autohold is required for a specific application.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.	

Lines field cross-reference chart

The following table provides a quick cross reference that shows common line fields, noted by trunk type.

Table 41 Combined line settings table

Trunk types	Attribute	Value	Description
All	Line type	Public Private to: Pool A to O, PRI A to PRI-F	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O (digital lines and VoIP trunks/PRI-A to PRI-F (PRI and BRI lines): assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. PRI line pools must be used in conjunction with routes and destination codes. target line*s* cannot be put into line pools. For more information and tips, refer to "Line pool tips" on page 259.
Loop start analog Loop start digital Ground start digital DID E&M	Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk. Tone does not appear if Signaling is set to Immediate (T1 DID &T1 E&M trunk types only).
Target lines DASS2	Received # (Private Number/ Public Number)	<digits associated with a specific target line>	Specify the digits to make a specific target line ring. • A received number cannot be the same as, or be the start digits, of a line pool access code, a destination code, the DISA DN or the Auto DN. • If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used. For further information, refer to "Received #" on page 259.
Target lines DASS2	If busy	To Prime Busy Tone	Define whether a caller receives a busy tone or the call forwards to the prime telephone when the target line is busy. Busy tone only works for PRI trunks.
All	Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
All	Distinct rings in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.

Table 41 Combined line settings table (Continued)

Trunk types	Attribute	Value	Description
All	Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
		**WARNING** If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None. Refer to "Defining user preferences" on page 415 for information about assigning a distinctive ring pattern to a telephone. You can also assign a distinctive ring pattern to a Hunt group. Refer to "Identifying a Hunt group" on page 575.	
Loop start analog Loop start digital Ground start digital DID E&M BRI VoIP	Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call. Refer to "Turn Privacy on or off for a call" on page 258 (**FEATURE** 83). Note: This setting has no effect on VoIP lines.
Loop start analog Loop start digital	Trunk mode	Unspr Supervised *Earth calling *Loop guarded *Loop unguarded	Define whether disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. You must set this to Supervised if a loop trunk has its Answer mode set to Auto or if you enable Answer with DISA. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Supervised option to work. * These listing only appear for UK analog lines. Note that Earth calling is only supported by a FEM connected to a Norstar analog trunk module. The GATM does not support Earth calling, even though the setting appears for the lines on the module.
			Tips: The duration of an open switch interval (OSI) before Business Communications Manager disconnects a call is programmed by the Disconnect timer setting. Refer to "Configuring the trunk module to line type" on page 131.

Table 41 Combined line settings table (Continued)

Trunk types	Attribute	Value	Description
Loop start analog Loop start digital Ground start digital E&M BRI DPNSS	Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password. The COS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
			Note: You require Disconnect supervision on the line if loop start trunks are to operate in auto-answer mode.
Loop start analog Loop start digital Ground start digital E&M BRI	Answer with DISA	Y or N	Define whether the system prompts a caller for a six-digit class of service (COS) password. This setting appears for T1 loop start and T1 E&M lines that have auto-answer mode. Set this option to No for T1 E&M lines on a private network that have auto-answer mode. To program DISA on a PRI trunk you need to specify a DISA DN, see "Creating Direct Inward System Access (DISA)" on page 291 and "Programming access codes" on page 310.
Loop start analog	Link at CO	Y or N	Some exchanges respond to a Link signal (**FEATURE 71**) by providing an alternative line for making outgoing calls. Enabling Link at CO causes the system to apply the restrictions on outgoing calls to the digits dialed after the Link signal. As well, the call on the alternative line is subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the Business Communications Manager restrictions in cases where the host exchange does not provide an alternative line.
Loop start analog Loop start digital Ground start digital DID E&M BRI Target lines VoIP DASS2 DPNSS	Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
			Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Configuring routing service" on page 495.
Loop start analog Loop start digital BRI VoIP DPNSS	Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. Full autohold is always in place for T1 E&M trunks because it has no meaning for incoming-only T1 DID trunks. The default setting should be changed only if Full autohold is required for a specific application.

Table 41 Combined line settings table (Continued)

Trunk types	Attribute	Value	Description
Loop start analog	Loss Packages	Short CO Medium CO Long CO Short PBX Long PBX	Select the appropriate loss/gain and impedance settings for each line. For more information refer to "Using loss packages" on page 260.
DID E&M	Signaling	WinkStart Immediate DelayDial	Select the signal type for the line. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to a DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch.
DID E&M	ANI Number	Y or N	Define whether the telephone number of the caller will be collected for this line. For T1 E&M and T1 DID trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required.
E&M	DNIS Number	Y or N	Defines whether the digits dialed by an external caller on this line will be collected.For T1 E&M trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart and Answer mode is set to Manual. These digits are required for some third-party software applications.
E&M	*Gain	Normal High	Set the level of gain for the channel. *E&M trunks only. T1 E&M trunks do not have this field.
Loop Start (GATM only)	Impedance	600 ohm 900 ohm	The GATM can be set to a specific impedance level.
Loop start analog Loop start digital Ground start digital DID E&M Target lines DASS2	Redirect to	<dial string>	Enter a dial string (including routing code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update.
	**WARNING:** Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.		

Turn Privacy on or off for a call

You can configure lines in your system to have automatic privacy. With a line not programmed with privacy, anyone with the line assigned to their telephone can join your call by pressing the line button. With a line programmed with privacy, one person at a time can use the line.

Use **Feature** 83 to turn the privacy feature off and on.

Privacy control cannot be used for internal or conference calls.

When another telephone joins a call, the participants on the call hear a tone, and a message appears on the telephone display. It is not possible to join a call without everyone hearing this tone.

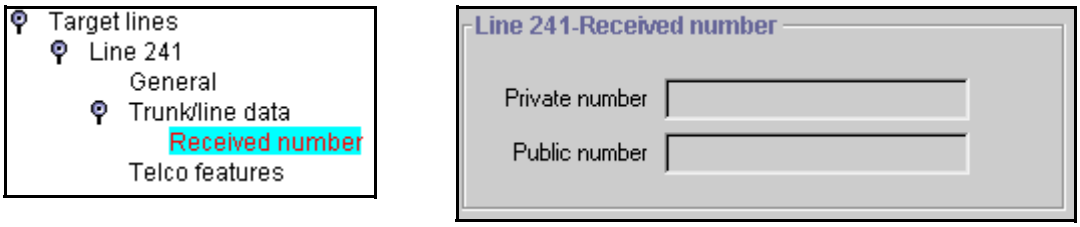
Note: The Auto privacy setting does not apply to target lines, PRI lines or VoIP trunking lines.

Received

Target lines provide an additional record under **Trunk/Line Data**, and that is the **Received number**. You can specify received numbers for both private (VoIP and MCDN) and public network connections. This allows the system to identify the source of the call on a per-call basis.

1 Click on **Received Number**.
The Line XXX Received Number screen appears.

Figure 50 Target line Private and Public received numbers



2 Public number: The Network DN supplied by your service provider.

Private number: The DN number of the telephone or Hunt group.

3 Go to the DN record for that telephone and ensure that the target line number is specified in the Line Assignment section.

Caution: Changing the received # length:
If you change the received number length for your system, the **Public number** entry for the target lines will clear if the new received # length is less than the number entered in this field.
If the new received # length has more digits than the number entered in this field, you need to change the entry manually, if changes are required. Refer to "Changing the received # length" on page 286.

Line pool tips

Read these tips before you assign your line pools.

- Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location.
- Avoid putting unsupervised loop start lines in a line pool. These lines can become unusable, especially when a remote user uses the line pool to make an external call.
- Assign line pool access to telephones in **Line access** programming.
- Assign system-wide line pool access codes in **General settings** (not applicable to PRI pools).

- A telephone can be administered to search automatically for an idle line from several lines that appear on the telephone. Assign a line pool as the prime line (in **Line access**) and all the lines in the line pool must appear on that telephone. When the user lifts the receiver or presses Handsfree, any one of the lines, if idle, can be selected by Automatic Outgoing Line selection.
- Changes in the settings for trunk type on a system that is in use, can result in dropped calls.
- When assigning lines to line pools, consider your network configuration. You can create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have tie lines to system C, assign the tie lines to pool D on each of the systems. You cannot assign target lines to a line pool, as they are incoming-only.

Using loss packages

The **Loss package** settings allow you to select the appropriate loss/gain and impedance settings for each line. The setting is based on the terminating switch type and the distance between Business Communications Manager and the terminating switch.

When measuring the distance from Business Communications Manager to CO and from Business Communications Manager to PBX system*s*, use 600 ohms as the termination resistance setting.

Table 42 Loss package settings

Loss Package	Receive Loss	Transmit Loss	Impedance	Distance to switch/cable loss/terminating switch
Short CO	0 dB	3 dB	Short	Short/<2 dB/Business Communications Manager to CO
Medium CO	0 dB	0 dB	TIA/EIA 464	Medium/>2 dB and <6 dB/Business Communications Manager to CO
Long CO	-3 dB	0 dB	TIA/EIA 464	Long/>6 dB/Business Communications Manager to CO
Short PBX	0 dB	0 dB	Short	Short/<2 dB/Business Communications Manager to PBX
Long PBX	-3 dB	0 dB	TIA/EIA 464	Long/>2 dB/Business Communications Manager to PBX

A loss of 4 dB corresponds to a cable length of approximately 2700 m (9000 ft).

Assigning Restrictions

Restrictions prevent you from making certain kinds of calls from specific lines on the telephone. You can also restrict some features. This section describes how to apply restriction filters to lines.

You can assign a different restriction filter for normal service and for each of six schedules.

Refer to "Defining service schedules" on page 489 for more information about setting up schedules. For PRI, line restriction changes apply to all 23 lines.

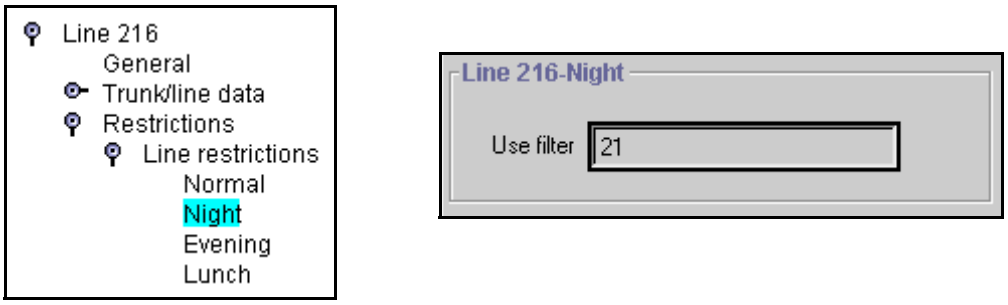
Note: The template has a set of default restrictions in Restriction 02, only. You must create your own restriction files if you want to use other settings. For details about creating restriction files, refer to "Defining restriction filters" on page 344.

Setting line restrictions

The Line Restrictions heading allows you to specify the filter applied to this line to restrict the dial-out numbers. Follow these steps to create line restrictions:

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**, **Restrictions**,
2. Click on the key beside **Line restrictions**.
3. Click the schedule heading that you want to configure.
   For example, **Night**.
   The Line restriction window for that schedule appears.

Figure 51 Entering a line restriction filter



4. In the **Use filter** box, type in the number of the restriction filter you want to assign as the line restriction for this schedule.

   The default restriction filters are listed in the following table.

Table 43 Default restriction filters

Schedule	Restriction filter
Normal	03
Schedule 1 (Night)	21
Schedule 2 (Evening)	22
Schedule 3 (Lunch)	23

Schedule	Restriction filter
Schedule 4	00
Schedule 5	00
Schedule 6	00

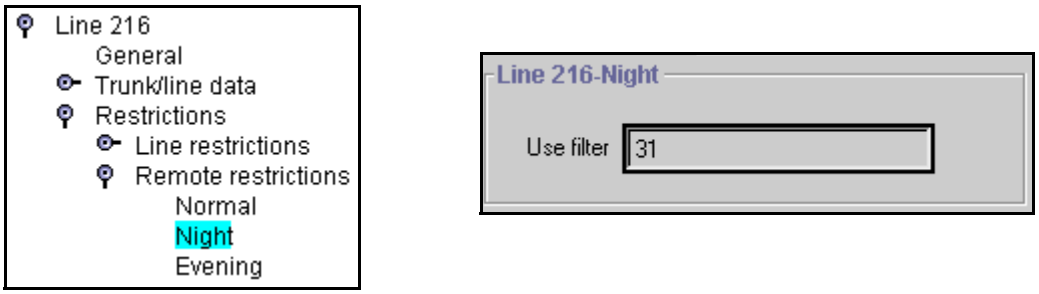
Note: When a remote user places an external call on a line, any filters used with the line still apply. However, if DND is active on the line, no set or set/line restrictions apply.

Setting remote restrictions

Specify the restriction filter for the line that remote callers use to call in to Business Communications Manager.

1. From the **Lines** headings, choose the line you want to set restrictions for.
2. Click on the key beside **Remote restrictions**.
3. Click the schedule heading that you want to configure. For example, **Night**. The Remote restriction window for that schedule appears.

Figure 52 Enter remote restriction filters for a line



4. In the **Use filter** box, type in the number of the restriction filter you want to assign as the remote restriction for this schedule.
5. Select the remote restrictions for each schedule. The default restrictions are shown in the following table.

Table 44 Default remote restrictions

Schedule	Restriction filter
Normal	04
Schedule 1 (Night)	31
Schedule 2 (Evening)	32
Schedule 3 (Lunch)	33

Schedule	Restriction filter
Schedule 4	00
Schedule 5	00
Schedule 6	00

Note: The remote restriction restricts the numbers a user can dial on an incoming auto-answer line. If a remote user then selects a line to place an external call, any filter used with the line still applies.

Setting line telco features

If you subscribe to a voice message service outside your office, you can access it through your Business Communications Manager system. You can specify what voice message center you use for each external line that receives message waiting indication.

1 Click on the keys beside **Services**, **Telephony Services**, **Lines**.

2 Click on the Line record.

3 Click the **Telco features** heading.
The Telco features window for the line appears.

Figure 53 Choosing a remote voice message center

4 Select the Voice message center for the line, **Center 1** - **Center 5** or **None**.

Note: To program the external numbers for each Center, refer to "Configuring centralized voice mail" on page 559. If you have an MCDN private network set up, where the voice message center is on a voice message device attached to the Meridian, this feature would have to be set in all systems to point to that system, except for the telephones directly attached to the Meridian system.

Line matrix

To help you with your line planning, transfer the following information to a spreadsheet and fill out the values for each line you provision.

Table 45 Line attributes

General			
Name			
Control set			
Use remote package			
Trunk/line Data			
Trunk Type			
Line Type		Answer with DISA	
Dial mode		Link at CO	
Received #		Use auxiliary ringer	
If busy		Full autohold	

Table 45 Line attributes (Continued)

Prime set			Loss package	
Auto privacy			Signaling	
Trunk mode			ANI Number	
Answer mode			DNIS Number	
Received #			Distinctive Ring	
Line restrictions			**Remote restrictions**	
Normal	03		Normal	04
Schedule 1 (Night)	21		Schedule 1 (Night)	31
Schedule 2 (Evening)	22		Schedule 2 (Evening)	32
Schedule 3 (Lunch)	23		Schedule 3 (Lunch)	33
Schedule 4	00		Schedule 4	00
Schedule 5	00		Schedule 5	00
Schedule 6	00		Schedule 6	00
Telco features: Voice message center		Center 1 to 5 or None		

Chapter 10
Configuring BRI Loops

The following sections describe the information accessed under the **Services, Telephony Services**, **Loops** headings. The **Loops** headings allow you to program BRI S, T, U2, and U4 ISDN loop settings.

Task:
Configure the BRI loops connected to the system through BRI modules. **Note:** DECT programming is contained in separate documentation.

This section includes information about:

The Loops screens define the loop numbers and loop attributes that correspond to the DIP switch settings that were configured on the BRI trunk media bay modules installed on your system. Check your Programming Record to see which modules are installed, and what settings were chosen.

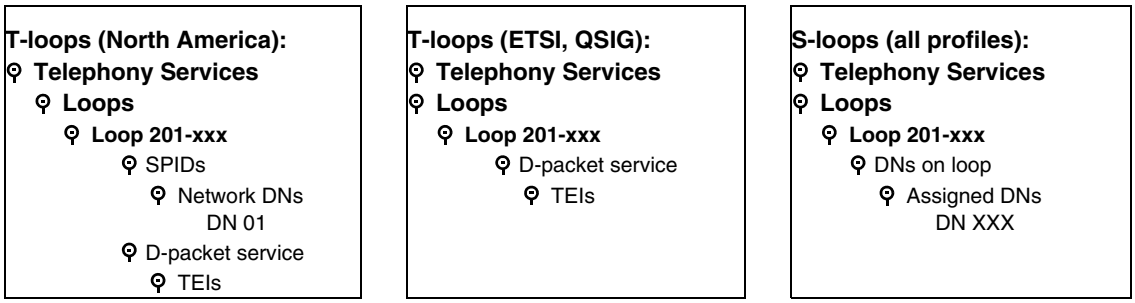
Available BRI trunk loop attributes are determined by the country profile that is assigned to your system. All profiles allow BRI programming, however, there is a difference between T1-based profiles and for E1-based profiles. Refer to "Core software and regions" on page 846 for a list of countries and profiles.

Once loops are provisioned, the system assigns two line numbers per loop. These lines are then programmed as you would any other lines. Refer to "BRI fields" on page 250 for a description of the headings that appear for lines defined for BRI loops. Lines programming is explained under Chapter 9, "Configuring lines," on page 227.

Note: DECT modules contain BRI lines, however, these lines are configured as part of the DECT programming. Refer to the *DECT Installation and Configuration Guide* for details.

The following figure shows a detailed view of the Loops headings.

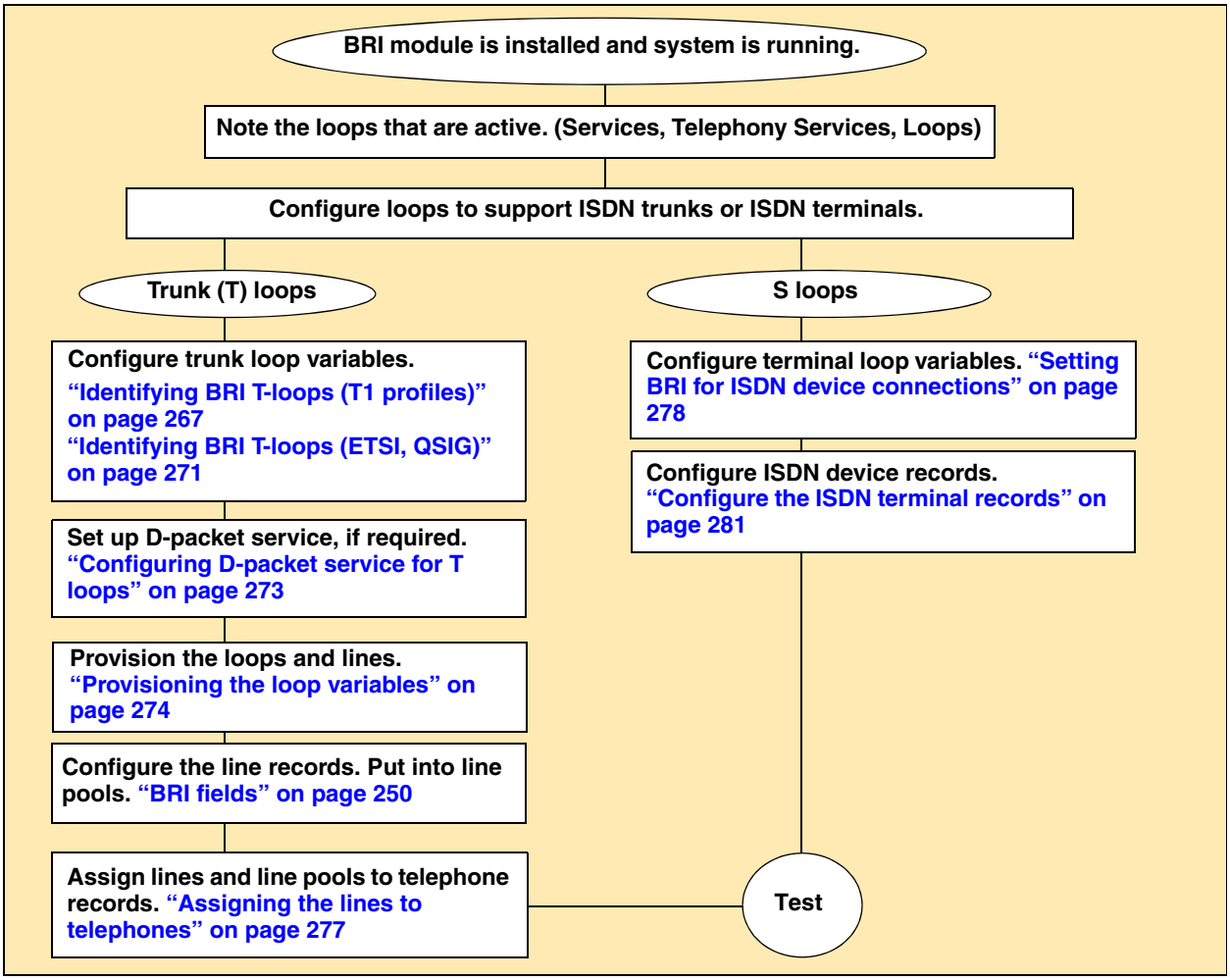
Figure 54 Loops headings



BRI configuration process map

The following process map shows the steps for configuring loops for T-1 based BRI modules.

Figure 55 Process map: Configuring the loops for your BRI module



You can program a loop to support either trunking services to the ISDN network, or terminal services to one or more ISDN devices. The following sections describe the programming for each type of loop. For complete module installation instructions and safety precautions, see the *Installation and Maintenance Guide*.

Using an NT-1 for BRI U2/BRI U4

The Business Communications Manager supports the BRI S/T protocol. If your ISDN service provider provides U-type ISDN service or the BRI devices are U-type devices, you need to obtain a network terminal (NT-1) device. This device is installed between the ISDN network feed and the Business Communications Manager for trunking loops. It is installed between the Business Communications Manager and the ISDN device or the ISDN bus connecting several ISDN devices on a BRI terminal loop.

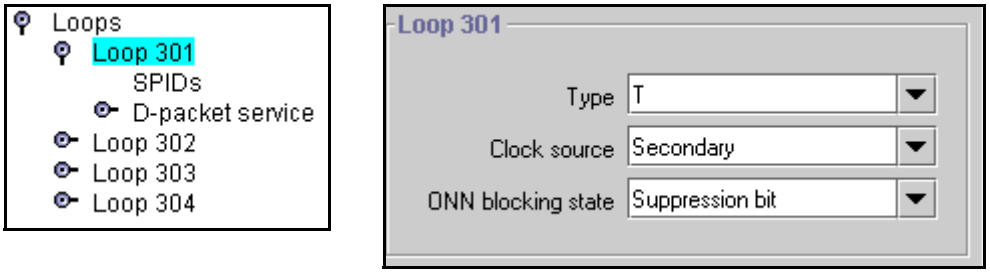
Identifying BRI T-loops (T1 profiles)

T1-based BRI loops have three parameters that identify loop characteristics.

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

2 Click on the loop number you want to configure as an ISDN trunk connection.

Figure 56 T-loop screen (T1 profiles)



3 Configure the loop settings according to the following table:

Table 46 Loop settings

Attribute	Value	Description
Type	T	
Clock Source	Primary Secondary Master	Default: Master This setting determines whether the system uses this module as the clock source for the network.

Table 46 Loop settings (Continued)

Attribute	Value	Description
ONN blocking state	Suppression bit, Service code	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press **FEATURE** 819 to block the outgoing name and number on a per call basis. **Suppression bit:** the system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call. **Service code:** VSC digits are dialed out before the called number to activate ONN at the central office. These codes are supplied by your service provider for the lines. Refer to "Configuring ONN blocking service codes" on page 480. PRI lines have only one code, so do not require specific configuration. **Programming note**: Ensure that all telephones that have this feature available are assigned valid OLI numbers. Refer to "Assigning line access" on page 394.

Adding SPIDs

System running with T1 country profiles (North American) support additional BRI services offered by ISDN service providers and defined by network service profile identifiers (SPIDs). The SPID allows you to enter a network connection that provides a path for voice or data services.

1 Collect the information supplied by your service provider: SPIDs, Network DNs, TEIs.

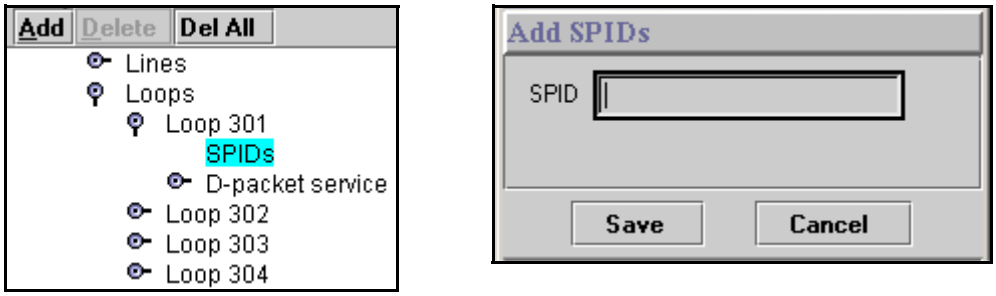
For ISDN BRI service, your service provider supplies Service Profile Identifiers, network DNs. You need to assign a SPID to a loop before you can assign Network DNs to that loop.

2 Click on the keys beside **Services**, **Telephony Services**, **Loops, Loop XXX**, where Loop XXX is the loop where you want to assign SPIDs.

3 Click the **SPIDs** heading.

4 Click the **Add** button.
The SPID dialog box appears.

Figure 57 Adding a SPID



5 Type in the SPID number.

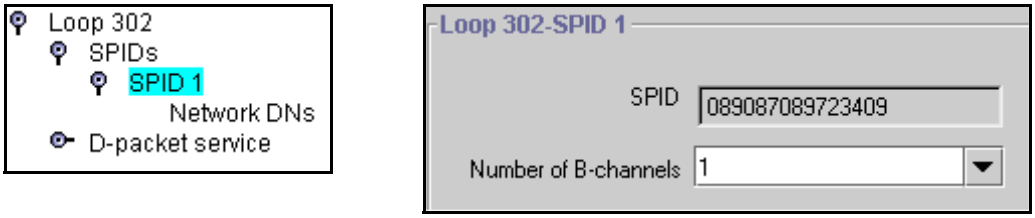
6 Click **Save**.
SPID 1 appears as a sub-heading.

Identifying the SPID B-channels

1 Click on the keys beside **Services**, **Telephony Services**, **Loops, Loop XXX**, **SPIDs**.

2 Click the **SPID #** heading for the SPID record for which you want to assign B-channels.

Figure 58 Assign number of B-channels per SPID



3 Select **1** or **2** in the **Number of B-channels** box.

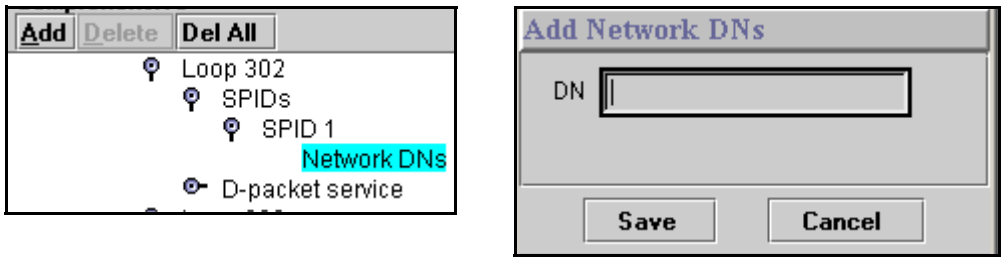
4 Click outside the window to save the setting.

Adding SPID network DNs

1 Under the **SPID #** heading, click the **Network DNs** heading.

2 Click the **Add** button above the navigation tree.

Figure 59 Add Network DN to SPID X



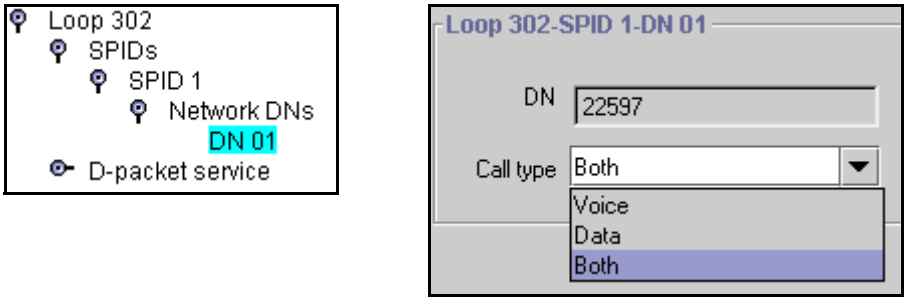
3 Type the ISDN DN number in the **DN** box for the device you want to use.

4 Click the **Save** button. **DN 01** appears as a sub-heading.

5 Click the first DN #.

6 In the **Call type** field, select **Voice**, **Data** or **Both**.

Figure 60 Specifying a Network DN call type



7 Repeat for all the DNs assigned to the Network DN.

Identifying BRI T-loops (ETSI, QSIG)

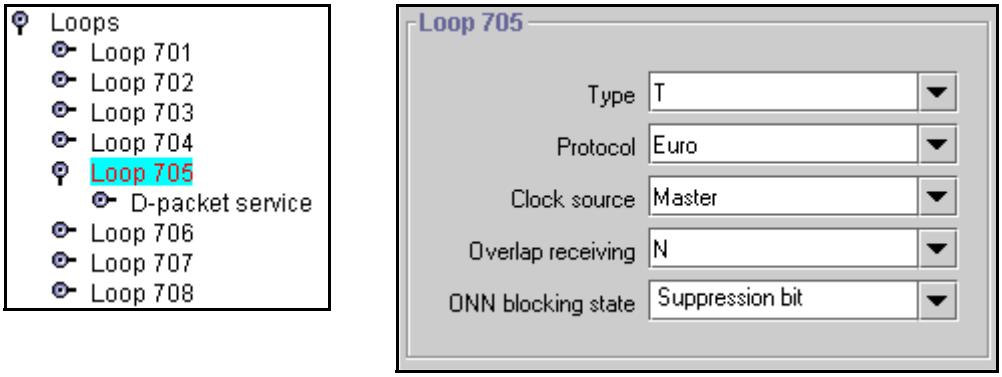
BRI loops for ETSI and ETSI-QSIG provide some flexibility in defining the T-loop characteristics. Refer to "Core software and regions" on page 846 for a detailed list of countries that use these profiles.

1 Collect the information supplied by your service provider.

2 In the Unified Manager, click on the keys beside **Services**, **Telephony Services**, **Loops**.

3 Click on the loop number you want to configure as an ISDN trunk connection.

Figure 61 T-loop screen (UK profile)



4 Configure the loop settings according to the following table:

Table 47 Loop settings

Attribute	Value	Description
Type	T	
Protocol	Euro, QSIG	Select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes. Euro - ETSI ISDN standard QSIG - also an ETSI standard. Only appears if the ETSI QSIG keycode is loaded.
Clock Source	Primary Secondary Master	Default: Master This setting determines whether the system uses this module as the clock source for the network. **Note:** Most service providers will be the Master, so this field will be set to Primary or Secondary.
Overlap receiving	Y or N	Supports target lines in markets which use Overlap receiving signaling on the BRI trunks. Overlap receiving must be configured for each BRI loop.

Table 47 Loop settings (Continued)

Attribute	Value	Description
Local number length	0-10	Set the local number length for loops to interfaces that receive overlap rather than enbloc digits. This number is the total length of the called party number received. This number is used to calculate the number of leading digits that need to be removed by the system.
		**Note:** This parameter appears only when Overlap receiving is set to Y. Example: Public received number = 4502303 Target line received numbers = 303 Local number length = 7 Public received number length = 3 Thus the first four digits are deleted by the system.
ONN blocking state	Suppression bit, Service code	Set the Outgoing Name and Number (ONN) Blocking. When the user presses **FEATURE** 819, on a per-call basis, the system flags the call to the Central Office (CO) so that the name and number is not sent to the person being called. Set this field to **Suppression bit** to use the Calling Line Information Restriction (CLIR) service. For ETSI ISDN lines that do not use the ETSI CLIR service, the Central Office (CO) may use a Service code to provide blocking service. In that case, this field must be set to **Service code**. The service provider code must then be programmed into the ONN blocking section. Refer to "Configuring ONN blocking service codes" on page 480. **Programming note**: Ensure that all telephones that have this feature available are assigned valid OLI numbers. Refer to "Assigning line access" on page 394.
Send Name Display (Type: QSIG trunks only)	Y, N	If you want the OLI of the calling telephone to display on the called telephone, with this type of trunk, set this field to Y. If this field is set to N, no outgoing call display is sent. Refer also to "Setting BRI for ISDN device connections" on page 278.

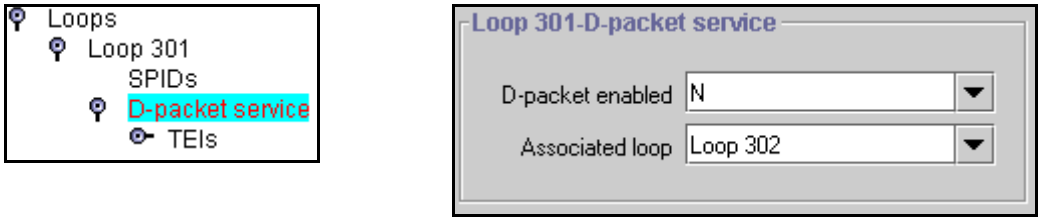
Configuring D-packet service for T loops

This configuration occurs for all profiles.

A T-loop can be used in combination with an S-loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. To deliver D-packet service, a network connection (T-loop) is programmed to work with a terminal connection (S-loop). The loops must be on the same physical module. This service is disabled by default.

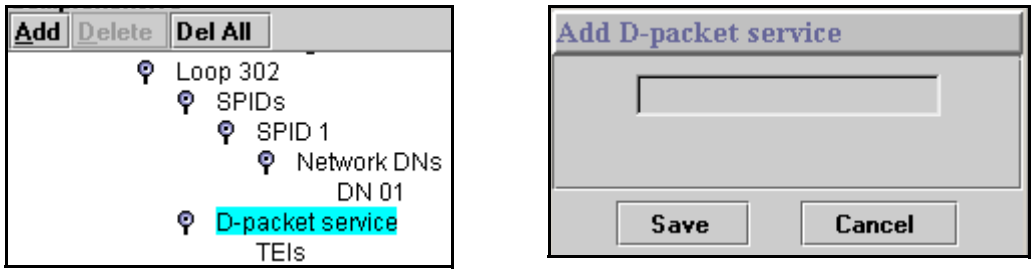
1. Under the T-loop you want to configure, click on **D-packet service**.
2. Beside **D-packet enabled**, choose **N** (disabled) or **Y** (enabled).
3. If you enable D-packet service, beside **Associated loop**, enter the S-loop you want to associate.

Figure 62 Enable/disable D-packet service, and associate a loop



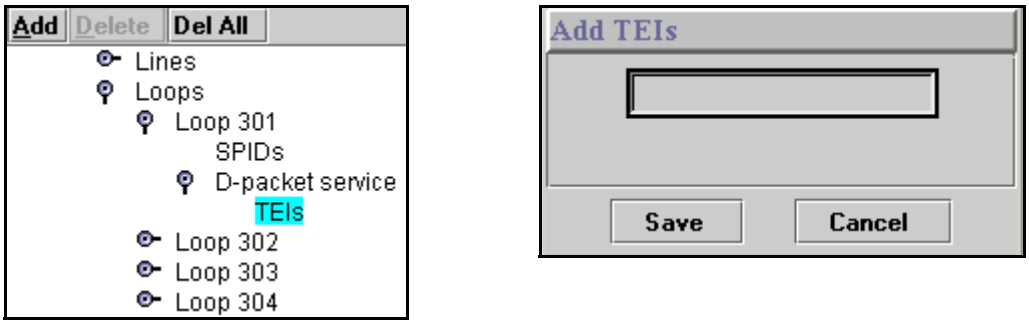
4. At the top of the navigation tree, click on the **Add** button.
5. In the **Add D-packet dialog**, enter a service number.

Figure 63 Add a D-packet service



6. Click on **TEI**.
7. At the top of the navigation tree, click on the **Add** button.
8. In the **Add TEI** dialog, enter the TEI number supplied by your service provider.

Figure 64 Add a TEI to the D-packet service



Provisioning the loop variables

When you assign a BRI loop as a trunk loop, you need to return to the media bay module settings and provision the loop, and the lines assigned to the loop. Once the loop is provisioned, it displays the two line numbers that are assigned to the loop, these also need to be provisioned.

Once the lines are provisioned, you can configure them in the same way as you would other lines. Refer to "Programming BRI lines" on page 276.

Provisioning the Loop

1 Click the keys beside **Resources**, **Media Bay Modules**, **Bus 0X**, **Modules on bus**, **Module X**, **Provision loops**

where Bus 0X is the bus to which the BRI module is configured; Module X is the offset (1, 2, or 3) to which the BRI module was set.

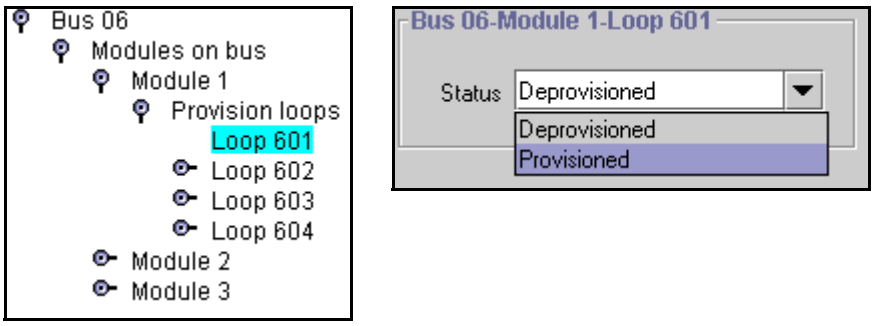
2 Click on **Loop XXX**.

Loop XXX is the BRI loop that you specified as a trunk loop (T)

3 Beside the **Status** field, select **Provisioned** from the drop down list.

4 Click outside the Bus 0X-Module X-Loop XXX window to invoke the change of status.

Figure 65 Provisioning BRI loops



5 Click the key beside Loop XXX twice to close and then reopen the heading.

Provisioning the lines

Once you provision the loop, two numbers are assigned to the loop. These also need to be separately provisioned.

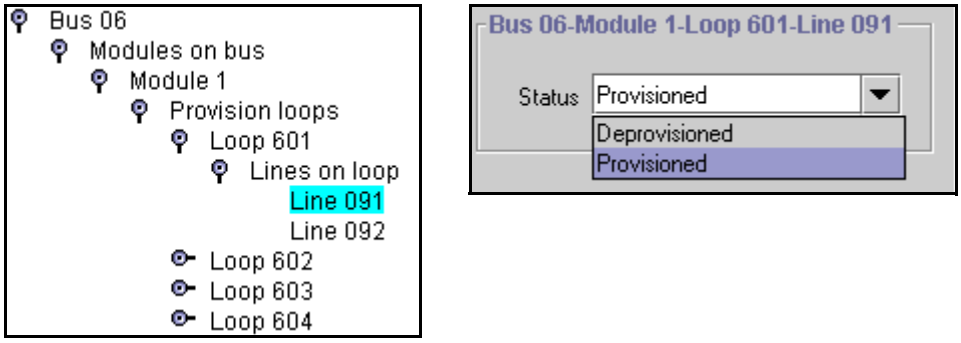
1 Click the keys beside **Resources**, **Media Bay Modules**, **Bus 0X**, **Modules on bus**, **Module X**, **Provision loops, Loop XXX, Lines on Loop.**

where Bus 0X is the bus to which the BRI module is configured; Module X is the offset (1, 2, or 3) to which the BRI module was set, and Loop XXX is the BRI loop that you specified as a trunk loop (T).

2 Click on **Line XXX**.

3 Beside the **Status** field, select **Provisioned** from the drop down list.

Figure 66 Provisioning BRI loop lines



4 Click outside the Bus 0X-Module X-Loop XXX window to invoke the change of status.

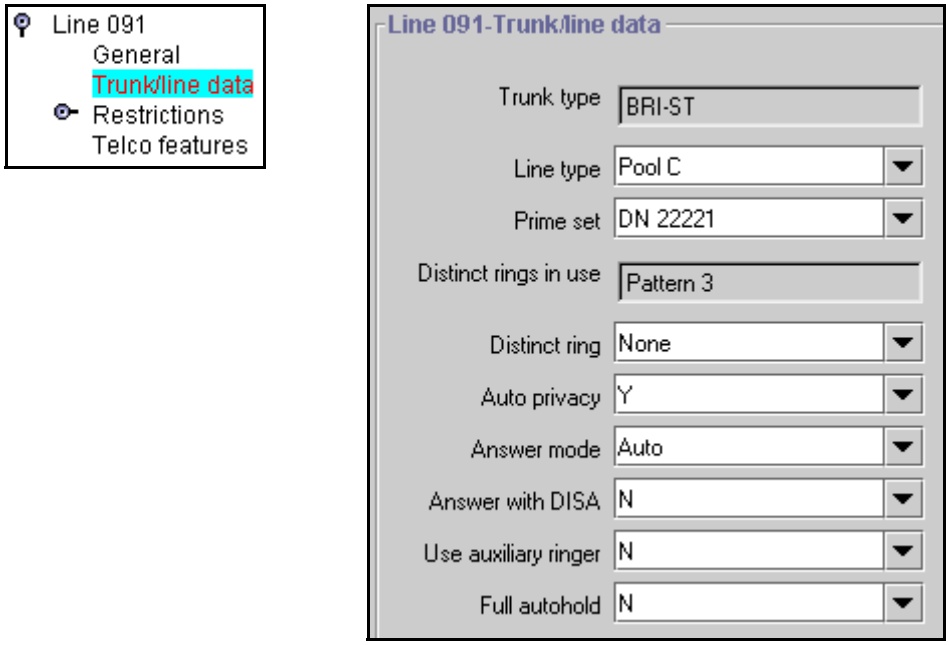
5 Repeat for second line, if there is one.

6 Make a note of the line numbers.

Programming BRI lines

Once the loops and lines are provisioned ("Provisioning the Loop" on page 274 and "Provisioning the lines" on page 275), you program the lines in the same manner as you do for non-BRI lines, under the Services, Telephony Services, Lines heading. Refer to "BRI fields" on page 250.

Figure 67 Configuring an auto-answer BRI line



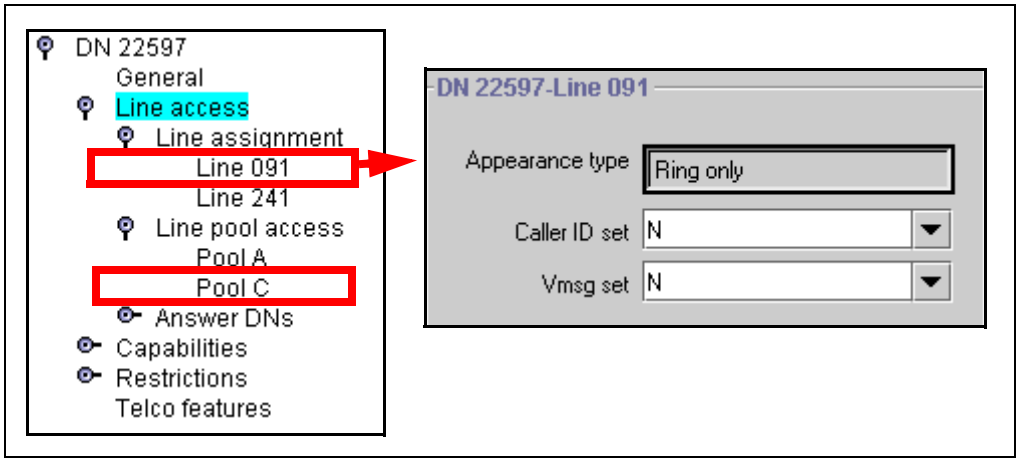
Programming note: BRI lines can be configured as manual answer or auto-answer lines. If the lines are configured as auto-answer lines, you need to set up target lines with the received # set to the network number supplied by the ISDN service provider, then assign the target line to the ISDN devices and other system telephones that will receive calls over this line. Refer to "Assigning target lines" on page 287.

BRI lines can also be assigned restrictions ("Assigning Restrictions" on page 261) and the Telco features ("Setting line telco features" on page 263).

Assigning the lines to telephones

Once the line records are programmed, assign the BRI lines or target lines and BRI line pools to the DN records for the telephones that will use the line(s) to receive/send calls. Refer to "Determining line assignments" on page 397 and "Assigning line pool access" on page 402.

Figure 68 Assigning the BRI line to a DN record.



Setting BRI for ISDN device connections

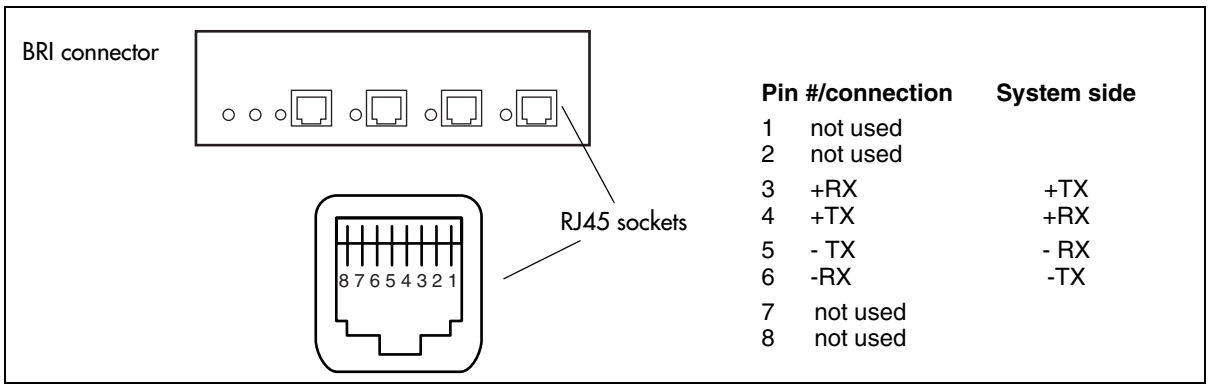
BRI S-loops support devices that use an ISDN interface. You can assign a single device to a loop, or multiple devices connected through an NT-1 interface ("Using an NT-1 for BRI U2/BRI U4" on page 267).

- You can assign a maximum of eight devices to a loop.
- Any device can only be configured to one loop.
- S-loops do not supply any voltage for ISDN devices requiring power, such as video cameras. Voltage for these devices must be supplied by an external source on the S-loop.

Wiring internal connections

The following diagram shows how to wire the BRI to connect to such S-Loop devices as video phones, terminal adapters, and Grp 3 Fax machines.

Figure 69 BRI RJ45 wiring array

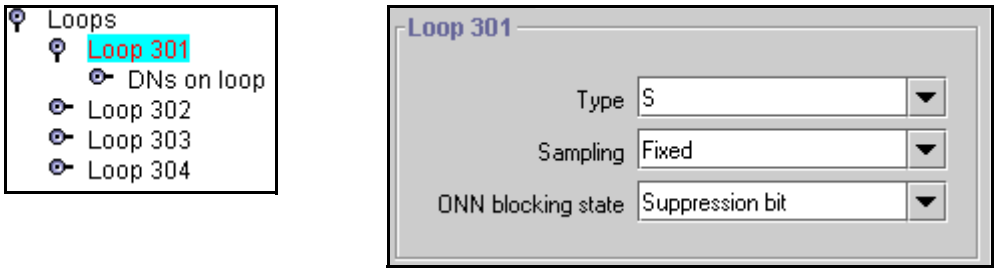


Configuring S-loops

1 Click on the keys beside **Services**, **Telephony Services**, **Loops**.

2 Click on the loop number you want to configure.

Figure 70 S-loop screen (North American profile)



3 Configure the loop settings according to the following table:

Table 48 Loop settings

Attribute	Value	Description
Which fields appear depends on the loop type.		
Type	S	
Sampling	Adaptive, Fixed	Select a sampling rate for the S-loop. Fixed: two or more S-interface devices use the loop, and the length of the loop is less than 200 m (650 ft.). Adaptive: two or more S-interface devices use the loop, and the length of the loop is greater than 200 m (650 ft.). If one device is using the loop, the length of the loop can be a maximum of 1000 m (3230 ft)
ONN blocking state	Suppression bit, Service code	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press **FEATURE** 819 to block the outgoing name and number on a per call basis. The system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call.

S loops allow you to assign ISDN DN record numbers for the terminal equipment on the loop. As well, one of the terminal records must be designated as the Loop DN, to act as the termination point for incoming data calls that do not get answered by the target device.

Assigning DNs to the S- loop

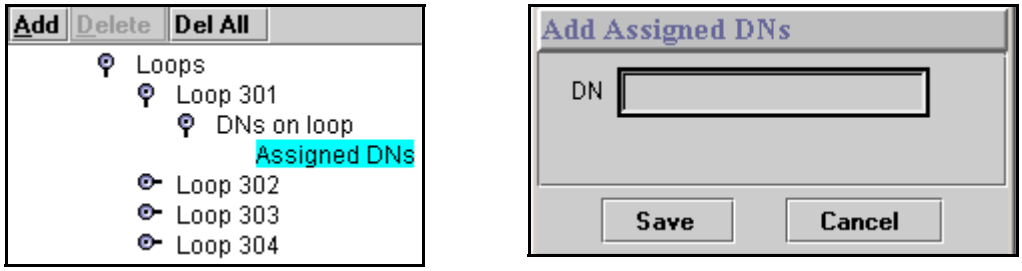
You can have a maximum of 58 ISDN DNs on your system. However, there are only 28 default DNs provided. The default ISDN DN range is 597 to 694. To add to the defaults, you need to use DNs from the Companion range: 565 to 597 (change DN type to **ISDN and DECT**)

Companion: If you have either a Companion wireless system, which uses the **Companion** DNs, or a DECT portable system, which uses the ISDN and DECT DNs, ensure you do not overwrite any DNs assigned to the handsets for these systems.

To assign device DNs to the loop DN (maximum of eight devices per loop):

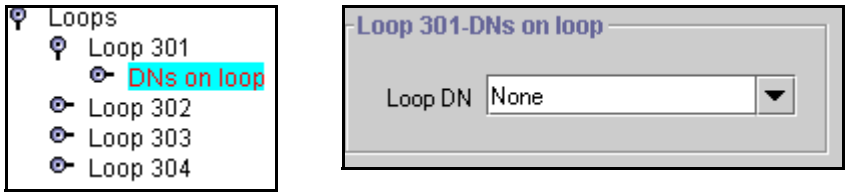
1. Choose **Services**, **Telephony Services**, **Loops.**
2. Click the key beside the loop number (for example, Loop 201) where you want to assign DNs, and beside the DNs on loop heading.
3. Click the **Loop DN** heading.
4. At the top of the navigation tree, click on the **Add** button.
5. In the **Add DNs** dialog, enter an ISDN DN.

Figure 71 Adding a DN to the Loop DN group



6. Click **Save** to add the DN.
7. Repeat steps 4 to 6 for all the DNs you want to add to the loop.
8. Click the **DNs on loop** heading.
9. In the **Loop DN** field, enter an ISDN DN that you assigned to the Assigned DNs group in the previous procedure. This telephone acts in a similar way that a Prime telephone works. Incoming calls that are not answered go to this device. Also, if the other devices on the loop do not have specified DNs, calls coming into the Loop DN ring at all these devices.
   - If you leave **None** in the field, unanswered calls will be dropped.
   - If the field is left blank, none of the Assigned DNs will be able to make or receive data calls.

Figure 72 Adding a Loop DN



10 Click outside the right frame to save the entry.

Configure the ISDN terminal records

You configure the ISDN terminal records in the same way that you do any other DN record. These records are found under the **Services**, **System DNs**, **All ISDN/DECT DNs** heading. For information about each heading within the DN record, refer to "Configuring DNs using the Wizards" on page 369 and "Configuring DNs for system devices" on page 387.

Loop matrix

To help you with your loop planning, transfer the following information to a spreadsheet and fill out the values for each BRI loop.

Table 49 Loop attributes

Type		SPIDS	
Protocol		Network DNs	
Overlap receiving		Call type	
Local number length		D-packet service	
ONN blocking state		TEIs	
Sampling (S loop only)		DNs on loop	
Note: The loop type dictates which fields appear.		Assigned DNs	

Chapter 11
Controlling access into the system

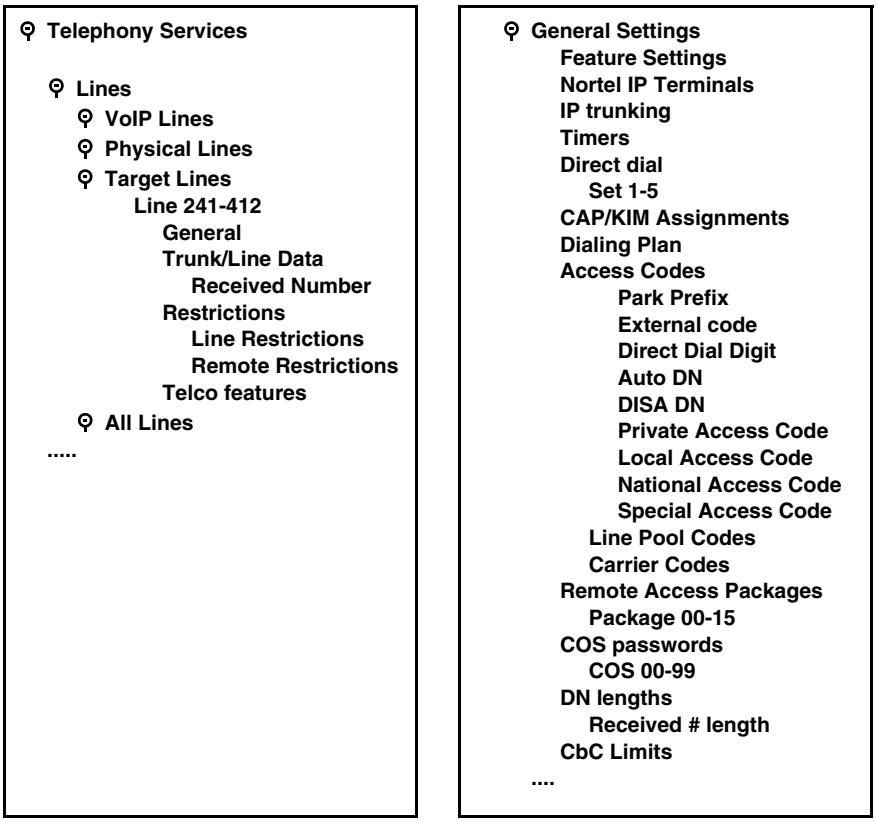
This section describes the telephony configurations that are used to control system access within the system and to control remote access into the system to access system features.

Task:

- Ensure that the DN length and Received # length are correct. "Defining DN length" on page 284 (Changing the DN length, Using the Received # length)
- Assign target lines for all telephones, if required. "Assigning target lines" on page 287
- Set up the system parameters for system users to call into the from a remote location. Note that Remote Access Packages are required for private network trunks, as well. Creating Direct Inward System Access (DISA), Defining remote access packages, Using COS passwords

The following figure highlights the Unified Manager navigation tree headings that will be discussed in this chapter.

Figure 73 Process map: Access headings



Defining DN length

The DN lengths setting allows you to change the number of digits for the Received number length and the DN length, which are used by the system to determine if an incoming call is valid for the system.

Each increase in length repeats the first digit in front of any existing DN. For example, if DN 234 was increased to a length of 4, the new DN would be 2234.

This section contains this information:

Warning: Do not change DN length immediately after a system startup.
You must wait for at least two minutes after a system startup before you change the DN length. It is preferable that you change this setting at system startup using the Quick Start Wizard. Refer to "What you need to know before you use the wizard" on page 93.

If you change the DN length after startup:

- Data devices using B2 channels drop calls when you change the DN length during system operation.
- The change takes up to two minutes, depending on the size of the system. System response can briefly slow down during this time.

Warning: Increasing the DN length affects other areas of the system:

If the DN length change creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Optional applications affected by DN length changes:

Voice mail, and **Call Center** applications are reset if you change the DN length after these services are installed.

If you are using IVR, you will need to correct the scripting.

If you have a **DECT** system, you will need to rerun the DECT Wizard to ensure that the DECT module firmware recognizes the change in DN numbers.

Changing the DN length

Warning: If your system is running with a PBX telephony template, the Public and Private received # length are hardcoded to 3 (digits) at startup. Increasing the DN length after system startup does not change these digits, so you will need to manually change the Public and Private receive # length. Refer to "Changing the received # length" on page 286.

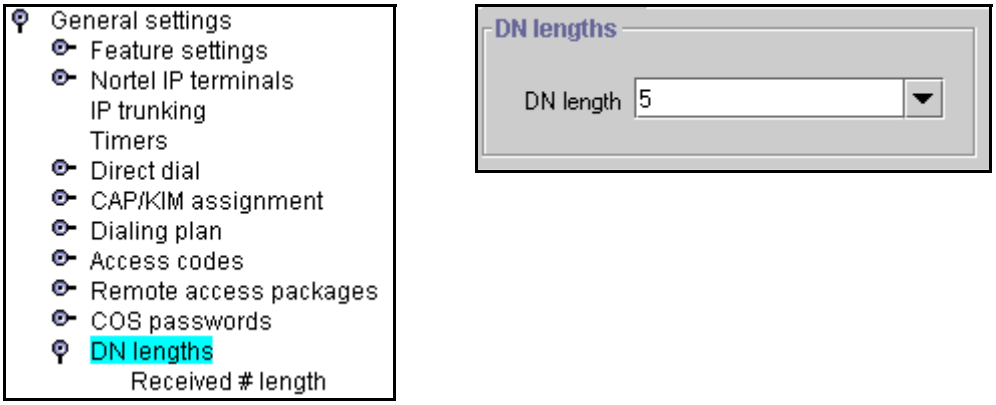
Private OLIs are automatically assigned to the DN records if the DN length and the Private received # length are the same. If this changes, the Private OLIs are cleared, or are not assigned (PBX template). Refer to "Assigning line access" on page 394.

Network note: If your system is part of a private network, ensure that you confirm the numbering plan for the network before changing this length. If you change the length, ensure that you check all DN-related settings after the change.

To change the DN length after startup, follow these steps:

1. Click the keys beside **Services, Telephony Services, General settings**
2. Click on **DN lengths**.
   The DN lengths window appears in the right frame.

Figure 74 DN length screen



3. In the DN length field, enter a new length (3, 4, 5, 6, 7) or use the drop down list to select a new setting. The default DN length is 3.
4. Press <**TAB**> to save the new DN length.
   The prompt appears: *If Business Communications Manager Voice Messaging is installed all messages and mailboxes will be deleted.*
5. Click **OK** to save the new DN length.

   Click **Cancel** to restore the original value.

Using the Received # length

If you change the DN length of your system, you may need to change the Received # length, which is what the system uses, in conjunction with the dialing table coding, private and public networking, and the access codes to determine a route for an incoming call over an auto-answer trunk.

On systems running the DID telephony template, the Private and Public Received # length is set to the same length as the DN length for the system. On systems running the PBX telephony template, the Private and Public Received # length default to 3, unless the DN length is changed during the Startup procedure.

These digits identify target lines ("Assigning target lines" on page 287), Auto DN*s*, and DISA DN*s* ("Programming access codes" on page 310).

TIPS: The target line number (for example, line 241) and the Received number for the target line (for example, Received number: 123 maps to line 241) must be different numbers. ("Target lines and DASS2 fields" on page 247).

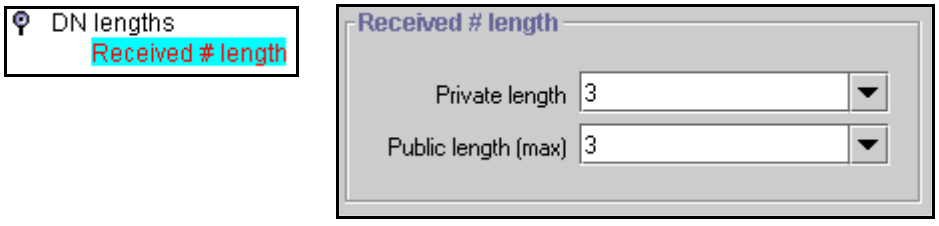
However, the received number can be shorter if network or central office constraints require this. This number cannot be greater than the system DN length on a networked system using a coordinated dialing plan (CDP) or a universal dialing plan (UDP). On a standalone system it is possible that the received number length would be greater than the DN length.

Warning: Decreasing the received number length clears all programmed received digits.

Changing the received # length

1. Click the keys beside Services, Telephony Services, General settings, and DN lengths.
2. Click on **Received # length**.
3. On the navigation tree, click on **Received # length**.
   The Received # length screen appears in the right frame.

Figure 75 Received # length, (PBX template default)



4 The following table provides the possible values for each field.

Table 50 Private and Public received numbers

Attribute	Value	Description
Private length	1, 2, 3, 4, 5, 6, 7	The number of digits that the system uses to determine if a call tagged as Private fits the system private DN numbering. Default: DID, same as DN length; PBX: 3
Public length (max)	2, 3, 4, 5, 6, 7	The maximum number of digits (2, 3, 4, 5, 6, 7) that the system uses to determine if a call tagged as public fits the system public DN numbering. Default: DID, same as DN length; PBX: 3

5 Check all equipment assigned to DNs.

6 Check target line received numbers and OLI entries.

- If you change the received number length for your system, the **Public number** entry for the target lines will clear if the new received # length is less than the number entered in this field. Refer to "Configuring the target line received number" on page 289.
- If the new received # length has more digits than the number entered in the target lines Public Number field, the entry remains, but does not update to the new DN length.
- A private OLI is automatically assigned to the DNs if the DN length and the Received # length are the same. If either changes so that they are not the same, the private OLI field is cleared or not assigned (PBX template). Refer to "Assigning line access" on page 394.

7 Reapply whatever voice mail applications you had installed. If you have a DECT system, rerun the DECT wizard to update the DECT module firmware.

Assigning target lines

Target lines are internal direct links the Business Communications Manager uses to allow external callers to dial specific system telephones, or a group of system telephones. You assign the target line to one or more telephone DNs ("Assigning a target line to a telephone"), and then configure the target line to function as you require ("Configuring the target line received number" on page 289). You can also assign multiple appearances of a target line to one telephone. This allows more than one call to simultaneously use the target line. Target lines are required by lines that support multiple numbers over one trunk (DID trunks, T-1 DID trunks, PRI trunks, and voice over IP (VoIP trunks).

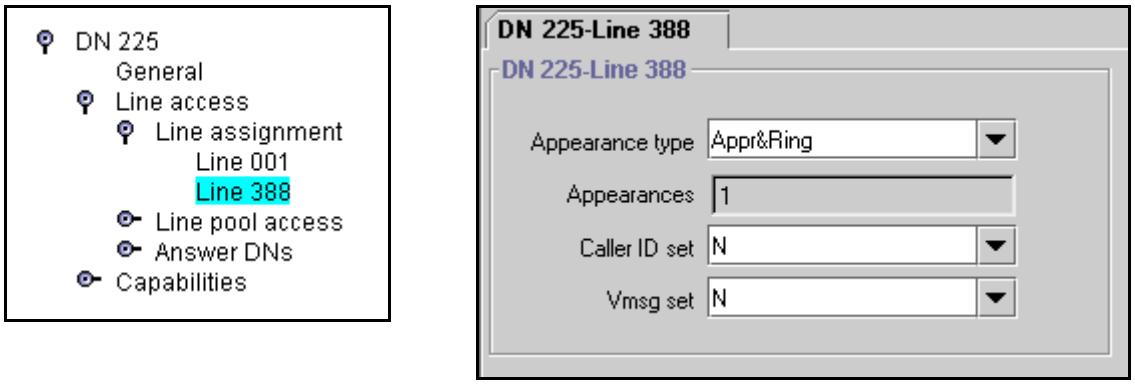
Note: You can also assign target lines to telephone DNs using the Add Users Wizard. Refer to "Creating telephone records with the Add Users Wizard" on page 375. The wizard can **Auto Assign** target lines to all the selected DNs. As well, the prime set DNs are also automatically updated to be the DN to which the target line is assigned.

If a target line in a sequence specified on the Wizard is already assigned to an existing DN, the system will also assign the line to one of the DNs on the list. If this is not what you want, you need to go into Unified Manager and change the target line number for one of the DNs.

Assigning a target line to a telephone

1. Ensure you have auto-answer lines such as analog DID, T1 lines set to auto answer, PRI, or VoIP trunking lines.
2. Click the keys beside **Services, Telephony Services, System DNs, Active Set DNs**.
3. Choose the DN of the set where you want the line to be directed.
4. Choose **Line assignment** and click the **Add** button.
5. Enter the number of the target line you want to assign to the set (241-492).
6. Click on the line number. The DN/Line screen appears in the right frame.

Figure 76 Assigning a target line to a set



7. Ensure the **Appearance type** is set to **Appr&Ring**.

   The following table shows the possible settings for the line record.

Table 51 General record values

Attribute	Value	Description
Appearance type	**Appr&Ring** RingOnly Appr	Always choose Appr&Ring for target lines. Choose RingOnly if the telephone does not have any line buttons to support target line appearances.
Appearances	<digit>	This is how many line appearances will appear on the telephone
Caller ID set	Y or **N**	Specify whether the telephone can display caller ID information.
Vmsg set	Y or **N**	Select whether an indicator shows on the telephone for voice message waiting to an external voice message system. The line must appear on receiving telephone. Note: the Message Waiting Indicator (MWI) is currently supported exclusively by Meridian Mail and CallPilot. **MCDN note:** If your system is part of an MCDN network connected to a Meridian 1 system, and you are using the voice mail system off the Meridian 1, you need to set this field to Y.
		Note: Contact your voice message service provider to find out if your voice message service works with Business Communications Manager, or if you have any problems with your service.

8 Repeat steps 3 to 7 for all the DNs you want to assign with target lines.

Configuring the target line received number

Configure the numbers that the system uses to identify the destination for the target line.

1 Click the keys beside **Services, Telephony Services, Lines, Target Lines**.

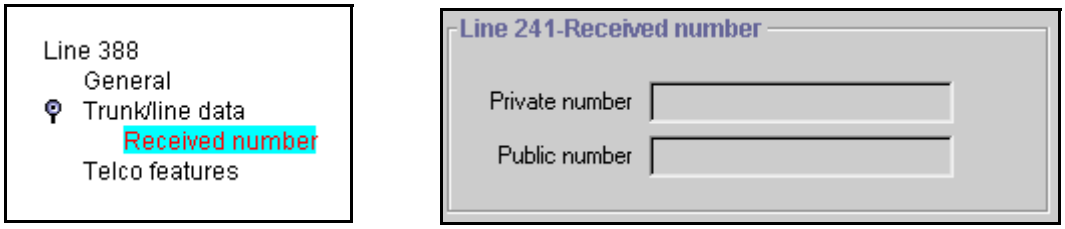
2 Click the **Line XXX** you want to set.

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

Note: For Trunk/line data programming, refer to "Target lines and DASS2 fields" on page 247.

4 Click on **Received number**. Refer to "Notes about the Public and Private Received Numbers" on page 290 for details.

Figure 77 Defining a Received number



5 Press <**Tab**> to save the changes.

6 Program the **General**, and **Telco** features as you would for any other line. Refer to "Target lines and DASS2 fields" on page 247.

7 Repeat steps 2 to 6 for all the target lines you want to configure.

Caution: Changing the received # length:
If you change the received number length for your system, the **Public number** entry for the target lines will clear if the new received # length is less than the number entered in this field.
If the new received # length has more digits than the number entered in this field, you need to change the entry manually, if changes are required. Refer to "Changing the received # length" on page 286.

Notes about the Public and Private Received Numbers

If the received number is different than the regular DN number, enter the number in the **Private number** and/or **Public number** field. For instance, in North America, you can enter the 10-digit public number in the Public number field. If you leave these fields blank, the system will use the DN of the telephone assigned with this line.

Upgrade note: If you upgraded your system from a version of Business Communications Manager previous to BCM 3.6, the Private number field of assigned target lines will autofill with the same value that is in the Public number field (usually the assigned DN). However, if the DN length of the system was different from the Received number length, this field will be blank after the upgrade. Systems running with a DPNSS keycode will also need to reenter the information in this field after an upgrade to BCM 3.6 or newer software.

Programming note: The following trunks use one or both of these settings to route calls:

- DPNSS lines use the Private received number to route calls in the system.
- BRI ETSI-QSIG, PRI ETSI-QSIG, MCDN, DMS100, DMS250 and VoIP trunks route calls on a per-call basis to either the public or private received digits. **Note:** VoIP trunking MCDN calls do not support Auto DN/DISA DN functionality.
- BRI (ETSI-Euro, NI), PRI (ETSI-Euro, NI, 4ESS), T1 (LoopStart, E&M, DID, GroundStart), Analog LEC (LoopStart, E&M, DID), and DASS2 trunks route calls using the Public received number.

Other settings to note:

- “Programming access codes” on page 310 (Public/Private DISA DNs and Auto DNs)
- “Assigning line access” on page 394 (Public/Private OLI)

Target lines matrix

To help you with your target line planning, transfer the following information to a spreadsheet and fill out the values for each target line you create.

Table 52 Target line record

Target line no. (3 digits)	
Telephone number (DN)	
Control set	
Line type	Public Private to:_____
Rec’d #	None DN
Prime Set	221 None

Entered in target DN record with appr and ring?	
Is DN length tied to Public Length (MAX)?	
Use Aux. ringer	Y N
If busy	PrimeSet BusyTone
Distinct Ring	None 2 3 4
Voice Message Center	

Configuring for remote access

If you want callers from a different node on the network or from the public network to be able to access system features or the system network lines, you need to set up remote access packages and COS password*s* to control outside access.

Programming note: If your system is hosting a centralized voice mail system, all calls from non-host systems to the voice mail on your system are considered remote calls and you need to set up the lines and remote access packages to accommodate this. If your system is using centralized voice mail on another system, users on your system need to be advised of the appropriate voice mail access codes.

This section provides information about:

- "Creating Direct Inward System Access (DISA)" on page 291
- "Defining remote access packages" on page 294
- "Using COS passwords" on page 296
- "External access tones" on page 299

Creating Direct Inward System Access (DISA)

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a COS password that determines what they are allowed to do in the system.

- Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default.
- T1 DID trunks: You cannot configure T1 DID trunks to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.
- You cannot program a DISA DN or Auto DN to VoIP trunks, because they act as auto-answer lines for private networks. However, you still need to assign remote access package*s* to the VoIP trunks, to ensure that remote access restrictions are properly applied to incoming calls trying to access the system or the system network.

This section also includes information about:

- "Remote access line settings"
- "Remote access on loop start trunks" on page 292
- "Remote access on T1 DID trunks" on page 292
- "Remote access on PRI" on page 293
- "Remote access on DPNSS lines" on page 293
- "Remote access on a private network" on page 293

Remote access line settings

The remote access feature allows callers elsewhere on the private or the public network to access your Business Communications Manager by dialing directly and not going through the attendant. After the remote user is in the system, they can use some of the system resources. You must enable remote access in programming before callers can use it.

Business Communications Manager supports remote system access on a number of trunk types which may require the remote caller to enter a password for DISA.

The system resources, such as dialing capabilities, line pool access and feature access, that a remote user may access depends on the COS password assigned to them. See "Using COS passwords" on page 296.

Note: Callers remotely accessing the Business Communications Manager press * followed by the feature code to use the system features. Even if you are calling from another Business Communications Manager system, press * instead of the Feature key.

Remote access on loop start trunks

Loop start trunks provide remote access to Business Communications Manager from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk **must** have disconnect supervision if it is to operate in the auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer without no DISA, the system answers with system dial tone and no COS password is required. In this case, the restriction filters assigned to the line control system capabilities available to the caller.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a COS password that determines which system capabilities are available to the caller.

Remote access on T1 DID trunks

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- The digits received are delivered by the central office.
- DISA cannot be administered to a T1 DID trunk. You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN. If you program the dialed digits to the DISA DN, only the incoming calls that match the programmed DN will receive a DISA dial tone. Incoming calls with other digits will route to a target line.

Remote access on PRI

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- A remote caller is on the public network dialing standard local or long-distance telephone numbers.
- The digits received are delivered by the central office.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote access on DPNSS lines

A remote caller can access a Business Communications Manager system dial tone, select a line pool that contains exchange lines or DPNSS lines, then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are:

- Calls coming from another switch to the Business Communications Manager system are routed in two ways, depending on the Answer mode that you program. If the **Answer mode** is set to **Manual**, and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If **Answer mode** is set to **Auto**, Business Communications Manager automatically answers the incoming call. Because most other DPNSS features are extension-specific, Nortel Networks recommends that all DPNSS lines are configured as auto-answer lines.
- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.
- The line redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Remote access on a private network

Systems connected to the private network deliver the last dialed digits to the destination Business Communications Manager system for interpretation. The destination Business Communications Manager system matches the digits to a target line or interprets the digits as a remote feature request. Business Communications Manager then routes the call to the specified target line or activates the remote feature.

- By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA. If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a COS password.
- The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in "Understanding access codes" on page 309.

- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN on the other system.
- Answer with DISA cannot be administer to voice over IP (VoIP), since they do not connect systems outside the private network. However, a user calling in remotely on another system on the network can use the trunk to access the system or a user calling in on a PSTN line can use the trunk to access the private network. To provide control for this type of access, ensure that you specify remote access packages for the trunk.

Defining remote access packages

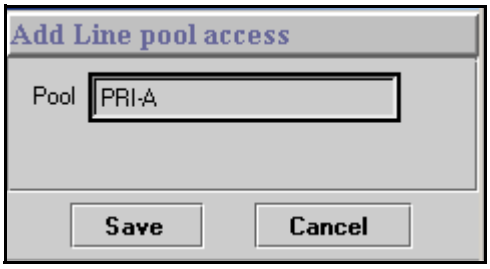
The Remote access packages setting allows you to control the remote use of line pools.

Create a remote access package by defining the system line pools remote users can access. You then assign the package to individual lines, (refer to "Defining line pool access for remote packages"), and to a particular Class of Service password (see "Using COS passwords" on page 296).

Defining line pool access for remote packages

Perform the following procedure for each package you defined in the previous section:

1. Click on the key beside **Line pool access**.
2. Click the **Add** button.
   The Add Pool Access dialog box appears.



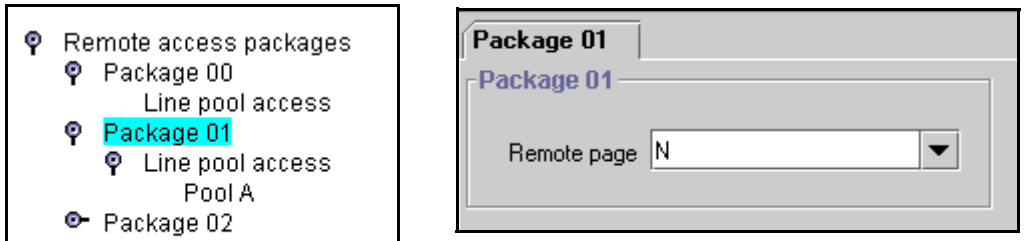
3. In the Pool field, enter a line pool.
4. Click **Save**.
5. Repeat steps 1 to 4 for all packages you require line pool access codes for.

Defining remote Page for remote packages

To define Remote access packages, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General settings**, and **Remote access packages**.
2. Click a Package number (**00** to **15**).
   The Package window appears. Refer to Figure 78.
3. Type in **Y** or **N** to enable/disable remote paging for each pool in the Remote access package.
4. Repeat steps 3 and 4 until you have defined all the package values you require.

Figure 78 Setting remote page for a remote access package



Using COS passwords

COS passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a COS password at a telephone, the restriction filters associated with the COS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a COS password on an incoming auto-answer line, the restriction filters and remote package associated with their COS password apply instead of the normal restriction filters and remote package.

This section includes information about:

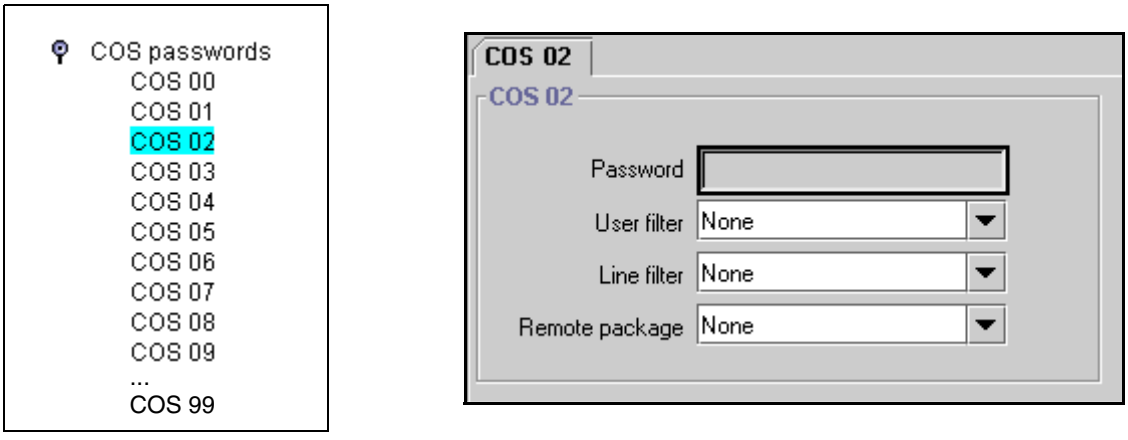
Creating COS parameters

Follow these steps to create COS groups and passwords:

1 Click the keys beside **Services**, **Telephony Services**, **General Settings**, and **COS Passwords**.

2 Click on a COS group (**COS 00-99**).
The **COS** window appears in the right frame.

Figure 79 Assigning COS password and remote access parameters



3 Use the information in the following table to determine which values to set for each password.

Table 53 COS password values

Attribute	Values	Description
Password	<six digits>	Enter a combination of numbers that the user needs to dial to get into the system. Refer to "Notes about COS passwords" on page 297.
User filter	None Filter <plus a two-digit user filter>	Assign a restriction filter to a Class of Service password. The user filter associated with the Class of Service password replaces any normally-applicable set restriction, line/set restriction, and remote restriction. The default setting (**None**), means that any normally- applicable filters (set restriction, line/set restriction, or remote restriction) still apply.
Line filter	None Filter <plus a two-digit line filter>	Assign a specific line restriction to a Class of Service password. The line filter associated with the Class of Service password replaces any normally applicable line restriction. The default setting (**None**), means that any normally applicable line filter still applies.
Remote package	None Package <plus a two-digit remote package>	Refer to "Defining remote access packages" on page 294 for more information.

Notes about COS passwords

The COS password can define the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The class of service (COS) that applies to an incoming remote access call is determined by:

- the filters that you apply to the incoming trunk
- the COS password that the caller used to gain access to Business Communications Manager.
- in cases where DISA is not automatically applied to incoming calls, the remote caller can change the class of service by dialing the DISA DN and entering a COS password.

Remote users can access system lines, line pools, the Page feature, and remote administration (if enabled through Software Keys). The exact facilities available to you through remote access vary depending on how your installer set up your system.

Note: If the loop start line used for remote access is not supervised, auto-answer does not function and the caller hears ringing instead of a stuttered tone or the system dial tone.

Security note:

COS password security and capacity

- Determine the COS passwords for a system randomly and change them on a regular basis.
- Users should memorize their COS passwords and keep them private. Typically, each user has a separate password. However, several users can share a password or one user can have several passwords.
- Delete individual COS passwords or change group passwords when employees leave the company.
- A system can have a maximum of 100 six-digit COS passwords (00 to 99). You can copy the restriction filters and remote package from one COS password to another. COS passwords must be unique.

To maintain the security of your system, the following practices are recommended:

- Warn a person to whom you give the remote access number to keep the number confidential.
- Change COS passwords often.
- Warn a person to whom you give a COS password, to memorize the password and not to write it down.
- Delete the COS password of a person who leaves your company.

Security note: Remote users can make long distance calls.
Remember that a remote user can make long distance calls that are charged to your company. They can also access line pools and make page announcements in your office.

COS examples

Example: Using the COS feature to access a restricted line

A sales representative out of the office needs to make long distance calls to the European office. Your system has a leased line to Europe with reduced transatlantic charges. You provide the sales representative with a Class of Service password that gives access to the transatlantic line. The sales representative can telephone into the system (DISA DN) from a hotel, enter the Class of Service password, and then use a destination code to access the leased transatlantic line to make calls.

To bypass the restriction filters on a line or telephone:

1. Press **FEATURE 68**.
2. Enter the six-digit COS password that allows the required type of call.
3. Enter the number to be dialed.

Example: Remote access over the public network

Follow this procedure to access the system over a public network.

1 Dial the system remote access number.

2 When you hear a stuttered dial tone, enter your COS password.

3 Wait for the system dial tone.

To use the system at a distance, you must use a telephone with tone dialing to call the system. Remote access is possible only on lines that your installer programs to auto-answer calls.

To use features on a remote system, press * followed by the feature code. When you are calling from within Business Communications Manager, press * instead of **FEATURE**.

In some conditions, you can experience lower volume levels when using the system from a distance.

External access tones

You can hear some of the following tones when accessing Business Communications Manager from a distance. The following table shows the different types of tone and what they mean.

Table 54 External access tones

Tone	What it means
System dial tone	You can use the system without entering a COS password.
Stuttered dial tone	Enter your COS password.
Busy tone	You have dialed a busy line pool access code. You hear system dial tone again after 5 seconds.
Fast busy tone	You have done one of the following: • Entered an incorrect COS password. Your call disconnects after five seconds. • Taken too long while entering a COS password. Your call disconnects after five seconds. • Tried to use a line pool or feature not permitted by your Class of Service. You hear system dial tone again after five seconds. • Dialed a number in the system which does not exist. Your call disconnects after five seconds.
	IP trunk lines do not produce tones when accessed from a remote location.

Remote access matrix

To help you organize your external access, transfer the following information to a spreadsheet and fill out the external access information you want to use.

Table 55 Remote access matrix

Pswd # (00-99)	Assigned to (owner of password)	Password	User filter (None, Filter#)	Line filter (None, Filter#)	**Remote pkg** (None, Filter#)
Remote access packages		Package #	Line pool access A: **9** B: to O:_____ PRI-__		

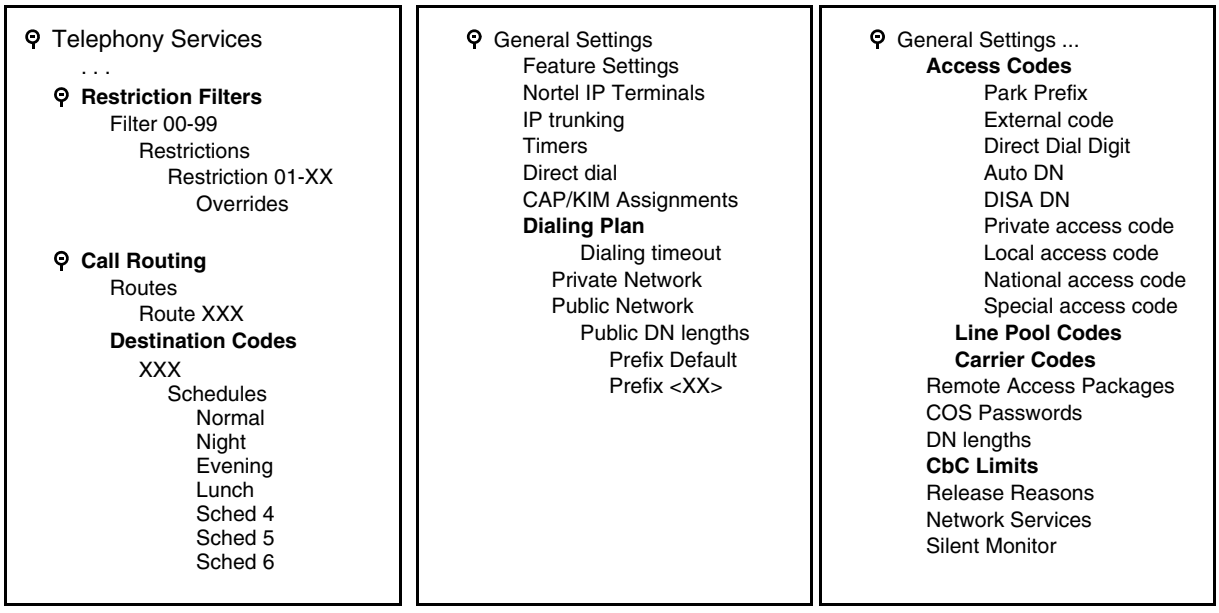
Chapter 12
Configuring outgoing calls

This section describes how you can configure the lines and loops to allow system users to dial out of the system over a public or private network.

Task:
• Understand what dialing plan is being used for the public and private networks ("Configuring the public and private dialing plans" on page 302)
• Set up call controls, when required, such as CbC limits ("Configuring Call by Call services" on page 339)
• Set up access codes, routes, and destination codes ("Programming access codes" on page 310, "Understanding access codes" on page 309, "Configuring call routing" on page 320)
• Set up restriction filters, as required ("Defining restriction filters" on page 344)

The following figure shows the position of the headings in the Unified Manager for the information covered in this chapter.

Figure 80 Unified manager telephony services headings



Refer also to "Information matrices" on page 226.

Configuring the public and private dialing plans

The dial plan you choose determines the type of numbering required to access a public and private network by defining the DN lengths for the codes that access the networks. You can define only one private network per system.

This section provides information about:

Setting Dialing timeout

Dialing timeout specifies how long the Business Communications Manager waits between user-dialed digits. This value allows Business Communications Manager to determine when the user stops dialing.

The user can also use the # key to indicate that they are finished dialing. This is not usually required except for international calls where the number of dialed digits varies.

A timeout value that is too small forces the caller to enter the digits very quickly. A timeout value that is too large causes the system to wait for extra time after the last digit is entered before the call is actually made.

To view or set the dialing time out, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General Settings**.
2. Click on **Dialing plan**. The Dialing plan window appears in the right frame.
3. In the **Dialing timeout** box select a timeout value (in seconds): **3, 4, 5, 6, 8, 10, 15**.

For more information about non-PRI routing tables and destination codes, refer to "Configuring routing service" on page 495.

For more information about how dialing rules are used in networking situations, refer to Chapter 18, "Configuring public networks," on page 499 and Chapter 19, "Configuring private networks," on page 505.

Using private network dialing

If your Business Communications Manager is part of a private network, you have a choice of dialing plans. However, all Business Communications Managers on a network must use the same type of dialing plan and have the same Private DN lengths to ensure proper call direction. Plan out these settings before you start programming for the network.

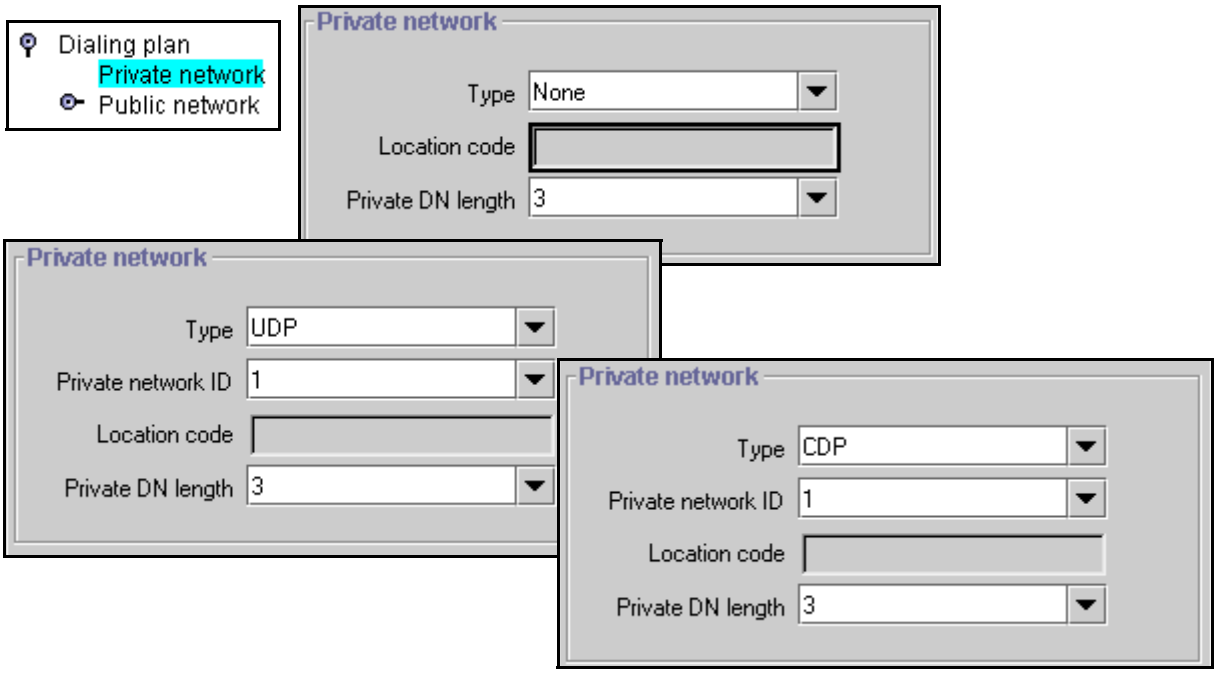
- UDP plans use a routing code and a location code plus the set DN (i.e. 6-403-XXXX) to determine where a call gets routed. You specify a Private DN length to allow all required digits to be dialed. Each node on the network has a unique location code.
- CDP plans use a unique steering code that gets dialed as part of the set DN (i.e. 2XXXX for one node, 3XXXX for another node, and so on) to determine where the call gets routed. Since each node on the network has a unique code, no other routing is required.
- The Meridian system administrator generates the Private Network IDs. These IDs are unique to each node on a network. Both UDP and CDP must include this code in programming.

Setting up the dialing plan

To set up a private network dialing plan, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General Settings**, and **Dialing plan**.
2. Click on **Private network**.

Figure 81 Configuring private network types



3. Use the following table to determine which values to set so callers can access a private network.

Table 56 Private network values

Attribute	Values	Description
Type	None, CDP, UDP	You can specify if your Private network uses a coordinated dialing plan (CDP) or a universal dialing plan (UDP). If you choose None, the private networking supplementary services are not available.
Location code	<unique three-digit number>	This code identifies this particular system for calls within the network for a UDP dialing plan. This number must be unique. Note: The system uses the Private Access Code length, plus the Location code length, plus the DN length to determine the DN length required to determine that a call is a private network call.
*Private DN lengths (DPNSS only)	3-14	The Private DN lengths parameter specifies the length of a dial string that the system uses to determine that the call is a private network call, when the route uses DN Type: Private.
Private Network ID (CDP/UDP networks)	1-127	This is the unique number that identifies the system to the Meridian PRI-MCDN network. Both end points must match on a PRI-MCDN network. On a VoIP trunking-MCDN network, this ID must be the same on all nodes. This number is supplied by the private network administrator. Refer also to "Configuring special IP trunking interoperability" on page 541.
* CDP and UDP private DN lengths are determined this way: CDP: the system uses the telephone DN length UDP: the system combines the private access code length + location code length + telephone DN length. When a call comes in, the system recognizes the leading digits as a private call and removes (truncates) them, leaving the telephone DN, which is recognized as the private DN length.		

Outgoing private calls routing

When you set up routing for private calls, the route is set to Private. Refer to "Configuring call routing" on page 320.

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the table below.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network screen)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS100/DMS250/ETSI-QSIG trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network screen)
UDP	Private/Subscriber	private access code + home location code (LOC) + private received digits
CDP	Private/Subscriber	private received digit

Setting up public network dialing

The Public network settings allows you to enter DN lengths for the networks the callers are allowed to dial, including special numbers such as 411 and 911.

The public DN lengths table is used for all PRI calls except for those routes that use service type Private or service type Tie with DN Type specified as Private. This table allows the Business Communications Manager to determine the length of a DN, based on the initial digits dialed.

A set of default Public DN lengths is included with the default template. In most cases it is not necessary to change the default values.

About the Public DN lengths table

In the public DN lengths table:

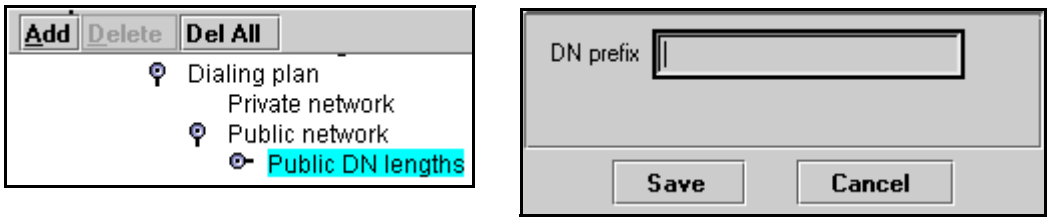
- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 - 25).
- Several entries are predefined in the North America profile. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries.
- The table always contains one default entry. You cannot remove this entry. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Adding or modifying dialing plan Public DN lengths

To add or modify Public DN lengths, follow these steps:

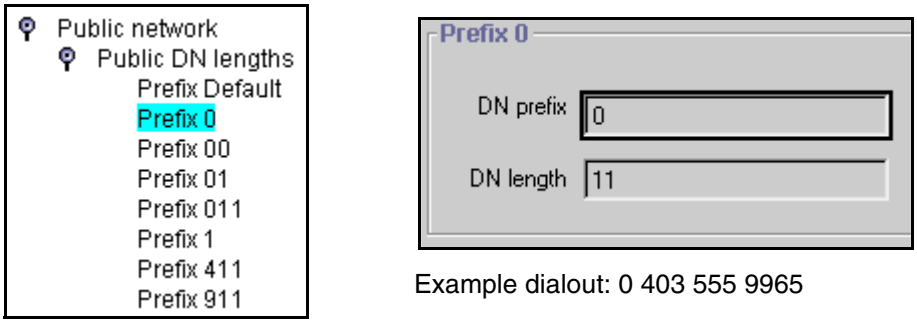
1. Click the keys beside **Services, Telephony Services, General Settings**, **Dialing Plan** and **Public network**.
2. Click on **Public DN lengths**.
3. At the top of the column, click **Add**.
   The Add Public DN Lengths dialog box appears.

Figure 82 Adding a Public DN length prefix



4. In the **DN prefix** field, enter the prefix for the public network.
5. Click **Save** to save the setting.
6. Repeat steps 4 and 5 until you have added all the public DNs you need.
7. Click on **Cancel** to exit the dialog box.
8. On the menu, click the first **Prefix** number you added.
   The Prefix window appears in the right frame.

Figure 83 Defining the prefix DN length



Example dialout: 0 403 555 9965

9. Enter the **DN length** for that prefix.
   This defines the number of digits the system will scan to find the prefix.
10. Press <TAB> to save.
11. Repeat for all DN length records you added or that you need to change.

Outgoing public calls routing

Outgoing public calls from within the system typically have the routes set to Public. Refer to "Configuring call routing" on page 320. The NPI/TON gets sent as Unknown/Unknown. The public called number length is based on the Public DN lengths table in the Public networks dialing plan.

MCDN trunks also allow public call types when tandeming calls from another system on the private network. Some of these systems use specific call types that the Business Communications Manager needs to recognize to pass on correctly. Also refer to "Using the MCDN access codes (tandem calls)" on page 315.

Type of call	NPI/TON	BCM prepend access code	BCM monitor display
Local	E164/Local	Local access code (9)	E.164/Subscriber
National	E164/National	National access code (X1)	E.164/National
Special calls (international, 911, etc.)	Private/Special	Special access code (9)	

Dialing Plans matrix

To help you understand how you are using networking on your system, transfer the following information to a spreadsheet and fill out the information you chose.

Table 57 Dialing plan matrix

Private network	Type	Private Network ID	Location code	Private DN length
	None	N/A	N/A	N/A
	UDP			N/A
	CDP			N/A

Public network	Pub DN length	DN prefix	DN length	

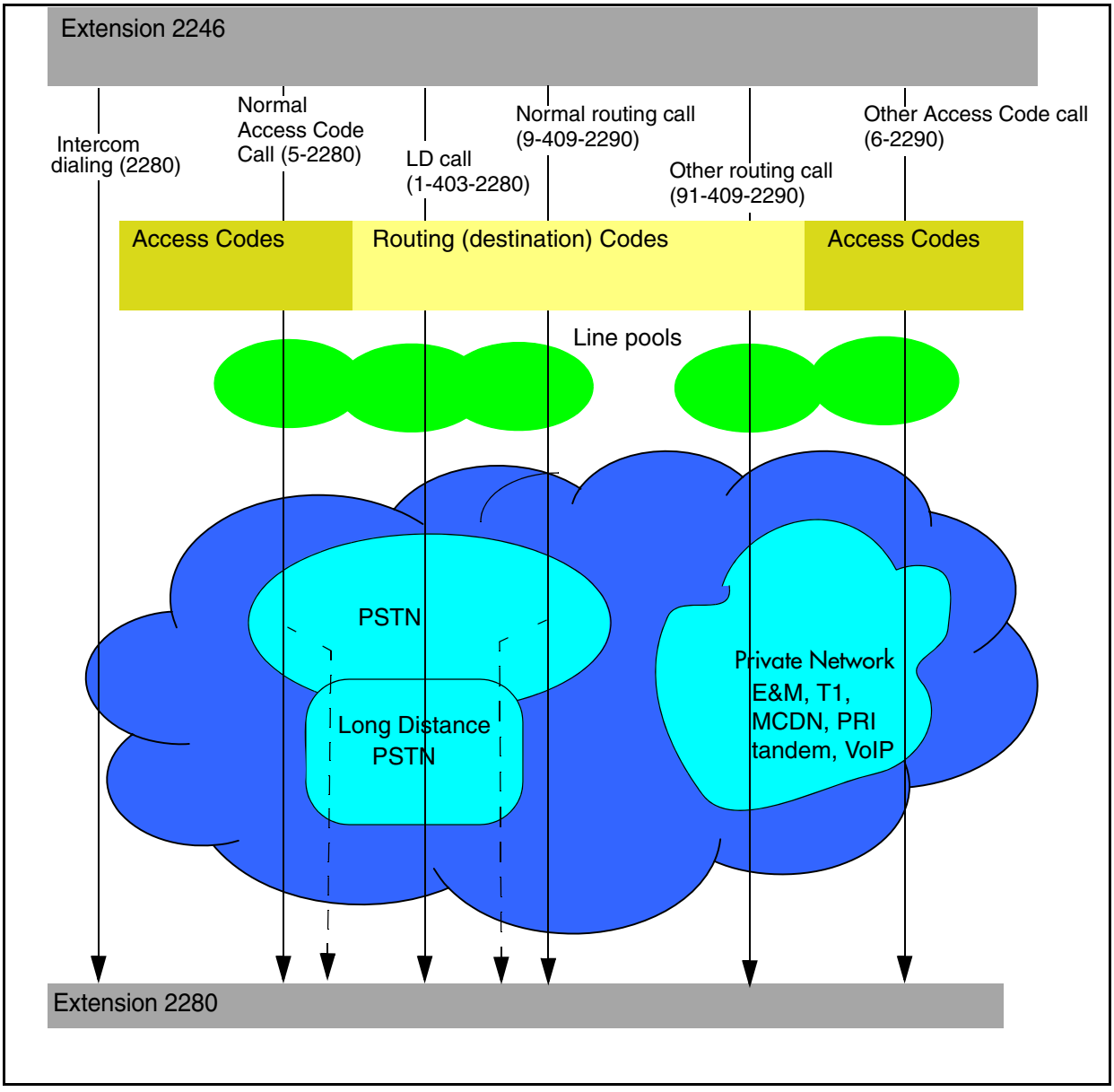
Determining line access dialing

The next two sections, "Understanding access codes" on page 309 and "Configuring call routing" on page 320 describe what you do with the lines and loops you previously set up into line pools.

By using access codes or call routing, which uses destination codes, you can determine which lines (routes) outgoing calls use. When you create a route, you can also specify restrictions that apply to how or when the line will be used.

The following figure provides an overview of how access codes and routing is used within the system to direct calls from a telephone in one system to a telephone in another system.

Figure 84 Line management diagram



Understanding access codes

The system uses access codes to direct calls to the correct lines and destinations. If the codes conflict, some of the features on the system do not work. Refer to "Creating numbering plans" on page 194 for a general overview about using access codes within the system dialing plan.

Task:

Set up access codes for internal features:

- park prefix
- direct dial digit

Set up access codes that affect users dialing in from remote locations:

- Private Auto DN
- Public Auto DN
- Private DISA DN
- Public DISA DN

Set up access codes that affect calls coming in over the private network:

- Private access code
- Local access code
- National access code
- Special access code

Set up access codes that affect calls leaving the system:

- External code (ATA and analog devices)
- Line pool access codes
- Destination codes
- Carrier codes

The table of default settings shown in the following table can help you plan your access codes so there are no conflicts.

Table 58 Default codes table

Digit	Use	System screen
0	direct dial digit	Access codes
1	park prefix	Access codes
2XX	first digit of DNs/DN lengths	Set through Quick Start Wizard
9	line pool A access code (Takes precedence over the External line access code if there is a conflict.)	Access codes

Programming access codes

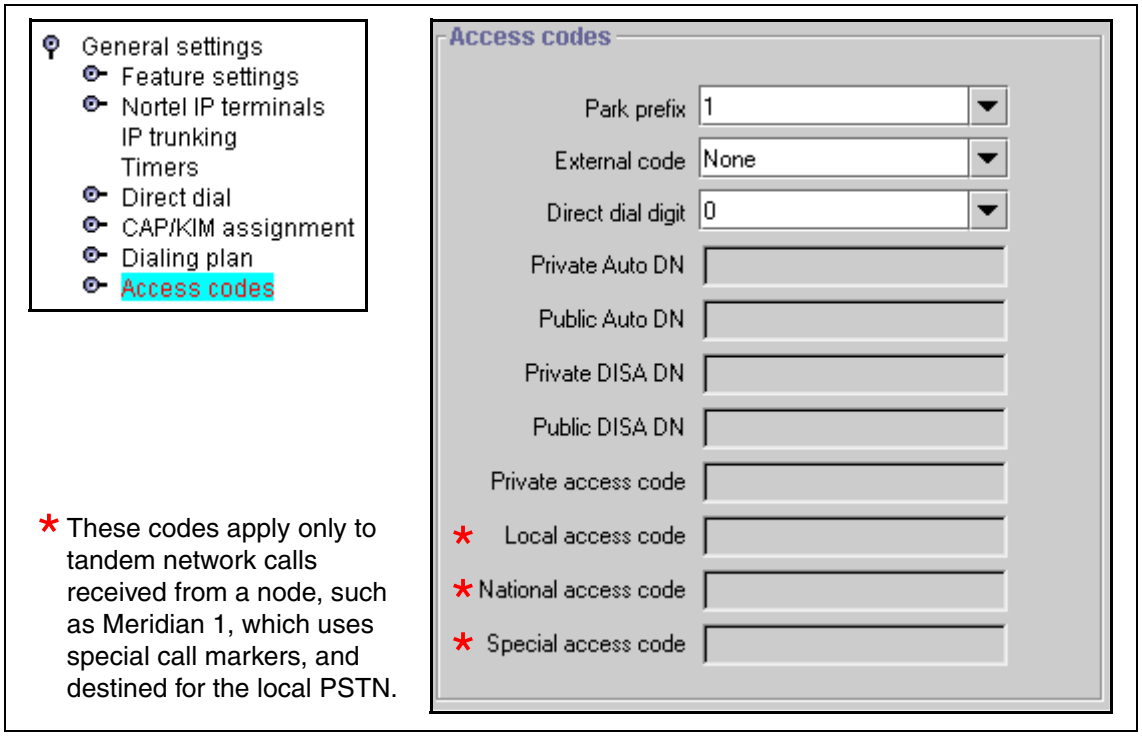
Your system requirements will determine which access codes you need to set up.

Follow these steps to set up codes found on the Access codes screen:

1 Click on the keys beside **Services**, **Telephony Services**, **General Settings**

2 Click on **Access codes**.
The Access codes window appears.

Figure 85 Defining access codes



3 Use the following table to determine which values to set for access codes for your system.

Note: Read "Tips about access codes" on page 314 before you choose a value to ensure the value does not conflict with related variables.

Table 59 Access codes values

Attribute	Values	Description
Internal features		
* Park prefix	None <one-digit number>	The Park prefix is the first digit of the call park retrieval code that a user enters to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked. Refer to "Call Park codes" on page 312 before choosing a number. **SWCA note:** If this field is set to **None**, you cannot program the system-wide call appearance (SWCA) feature.

Table 59 Access codes values (Continued)

* Direct dial digit	None <one-digit number>	The Direct dial digit setting allows you to specify a single system-wide digit to call a direct dial telephone.
Remote dial-in (Also refer to "Configuring for remote access" on page 291)		
* Private Auto DN	<DN digits to be received from a private auto-answer trunk>	Private network calls answered without DISA require no password to access the Business Communications Manager. The type of service that applies to the call depends on the restrictions assigned to the trunk.
* Public Auto DN	<DN digits to be received from the auto-answer trunk>	Public network calls answered without DISA require no password to access the Business Communications Manager. The type of service that applies to the call depends on the restrictions assigned to the trunk.
* Private DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For private network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (COS) that applies to the call is determined by this COS password. After a remote user accesses the Business Communications Manager, they can change the existing COS password using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate COS passwords with different dialing out privileges for individuals.
* Public DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For public network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (COS) that applies to the call is determined by this COS password. After a remote user accesses the Business Communications Manager, they can change the existing COS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate COS passwords with different dialing out privileges for individuals.
Incoming and tandem calls (Refer also to "Defining routes" on page 322)		
Private access code	<systemcode> **MCDN:** coordinate with National access code	This code identifies this system to the private network. It comes in as the first digit in a dial string defined as private and is read based on the private DN length. Example: if the dialed number is 7880, and the private DN length is 4, the system scans the four digits from the right, recognizing the 7 as the private access code for this system.
	Private networking also provides access to tandem calling and toll bypass functionality to users calling into the system. For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to the Ottawa office and then out to the PSTN from the Ottawa office. This bypasses any long distance toll charges. BCM to BCM to PSTN: Calls are routed as private over the private network, and then flagged as public to go out to the end node PSTN. Meridian to BCM to PSTN: Special call codes from the Meridian (Local, National and Special access codes) need to be recognized by the BCM and correctly passed to the local PSTN.	

Table 59 Access codes values (Continued)

* Local access code	*<code to access local PSTN>*	MCDN connections only. This number is prepended to an incoming M1 local dial string and designates the call as a Local call type (typically 9). Refer to "Using the MCDN access codes (tandem calls)" on page 315. Refer also to "Creating numbering plans" on page 194.
* National access code	<private access code + 1>	MCDN connections only. This number is prepended to an incoming call marked as a long distance call, and designates the call as a National type call (private access code + 1). Refer to "Using the MCDN access codes (tandem calls)" on page 315.
* Special access code	*<code to access local PSTN>*	MCDN connections only. This number is prepended to an incoming international (011....) or special-case dial string (911, 411) and designates the call as a special type call (9011 ...., 9911, 9411). Refer to "Using the MCDN access codes (tandem calls)" on page 315.
Outgoing calls		
* External code	None <one-digit number>	The External code setting allows you to assign the external line access code for T7100/T700 telephones and analog telephones attached to ATA 2s to access external lines. When the caller picks up the handset, the system tone sounds. The caller then enters this number to access an external line. **Note:** This number is overridden by line pool or destination codes starting with the same digit(s). Refer to "Tips about access codes" on page 314 before choosing a number.

Call Park codes

When you park a call (**FEATURE 74**), the system assigns one of 25 codes for the retrieval of the call. You can then press the Page display key to announce the code that appears on the display.

These three-digit codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101.

	XXXXX Numbering cannot conflict with these features							
Access numbering	**Park prefix**	**External code**	**Direct dial digit**	**Private access code**	**Public/ Private Auto DN**	**Public/ Private DISA DN**	**Line pool code/ destination code**	**Telephone DN**
Park prefix		**XXXX**	**XXXX**	**XXXX**	**#XXXX**	**#XXXX**	**#XXXX**	**#XXXX**
# Cannot conflict with first digit.								

Note: Other programmable settings may affect what numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes.
If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

The system assigns Call Park codes to calls in sequence, from the lowest to the highest, until all the codes are used. A round-robin method means the use of different of codes ensures a call reaches the right person, especially when more than one incoming call is parked.

The highest call number (the Call Park prefix followed by 25) is used by model 7000 and 7100 telephones, analog telephones, or devices connected to the system using an ATA2. Analog telephones or devices cannot use the other Call Park codes.

Calls are retrieved by pressing the intercom button and dialing the retrieval code. On model 7000 and 7100 telephones, pick up the receiver, and then dial **<*parkcode*>25**.

You also need to program the delay timer that determines when external parked calls that are not answered return to the originating telephone. Refer to "Setting system timers" on page 472.

You can disable Call Park by setting the Park Code to None.

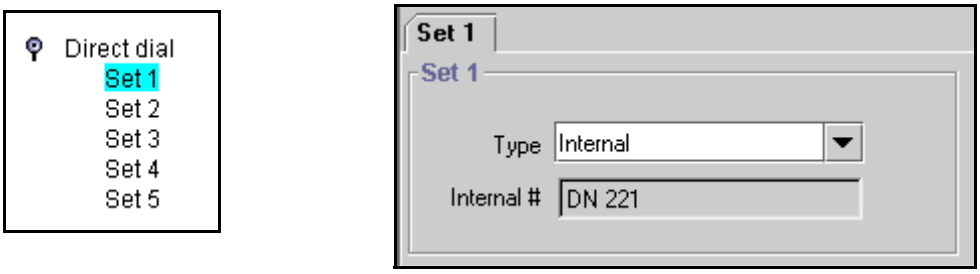
Creating Direct Dial sets

The Direct dial setting allows you to dial a single system-wide digit to call a specific telephone, called a direct dial telephone. The most common example of a direct dial set is a telephone for an operator, a receptionist or an attendant. You can program a maximum of five direct dial sets on the system, however, you can only specify one direct dial number for the system ("Programming access codes" on page 310).

1 Click the keys beside **Services**, **Telephony Services**, **General Settings**, and **Direct dial**.

2 Click the Set you want to program (**Set 1**-**Set 5**).
The Set # window appears.

Figure 86 Direct dial menu and screen



3 Use the following table to determine the settings you want to define direct dial sets.

Table 60 Direct dial values

Attribute	Values	Description
Type	Internal External None	This is the type of number for the direct-dial set.

Table 60 Direct dial values (Continued)

Internal/External#	DN <external dial string>	The DN number of the telephone to be designated as the direct dial set. (Internal sets). The actual phone number of the direct dial set (External sets).
Facility	Line Pool (A-O) Use prime line Use routing table	The facility to be used to route the call to a direct dial set that you define with an external number. **Note:** If you choose **Use prime line**, ensure that prime line is not assigned to the intercom button*s* for your telephones. When prime line is assigned as an intercom button, it chooses the first available line pool assigned to the telephone to make a call. If this line pool does not have the correct lines for routing the call, the direct dial call will fail. Refer to "Assigning line access" on page 394.

Security note: The Business Communications Manager cannot verify that the number you assign as an external direct dial set is valid. Check the number before assigning it as a direct dial set by calling the direct dial you have assigned.

Direct dial matrix

To help you with your direct dial planning, transfer the following information to a spreadsheet and fill out the values for each target line you create.)

Table 61 Direct dial sets

Direct Dial Set			
Set 1 Set 2 Set 3 Set 4 Set 5	None	Internal #	External # Use Prime line Use line Pool code_____ Use routing table

Tips about access codes

Here are some helpful pointers to assist you in planning the access codes for your system.

Table 62 Access/dialing codes: avoiding numbering conflicts

	XXXXX Numbering cannot conflict with these features							
Access numbering	**Park prefix**	**External code**	**Direct dial digit**	**Private access code**	**Public/ Private Auto DN**	**Public/ Private DISA DN**	**Line pool code/ des. code**	**Telephone DN**
Park prefix		XXXX	XXXX	XXXX	#XXXX	#XXXX	#XXXX	#XXXX
External code	XXXX		XXXX	XXXX	#XXXX	#XXXX	*XXXX	#XXXX
Direct dial digit	#XXXX	XXXX		XXXX	#XXXX	#XXXX	#XXXX	#XXXX
Private Access code	#XXXX	XXXX	XXXX					
Pub//Priv/ Auto DN		#XXXX	#XXXX			XXXX	XXXX	
Pub//Pri/ DISA DN		#XXXX	#XXXX		XXXX		XXXX	
Line pool/dest. code	#XXXX	*	XXXX		XXXX	XXXX		XXXX

Table 62 Access/dialing codes: avoiding numbering conflicts

Access numbering	**XXXXX** Numbering cannot conflict with these features							
	Park prefix	**External code**	**Direct dial digit**	**Private access code**	**Public/ Private Auto DN**	**Public/ Private DISA DN**	**Line pool code/ des. code**	**Telephone DN**
Telephone DN	**#XXXX**	**#XXXX**	**#XXXX**				**XXXX**	
* If the line pool code and the External code start with the same digit, the line pool code programming supersedes the external code. # Cannot conflict with first digit.								

- **External line access code**:

  If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.

- **Direct dial telephone:** Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

  If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.

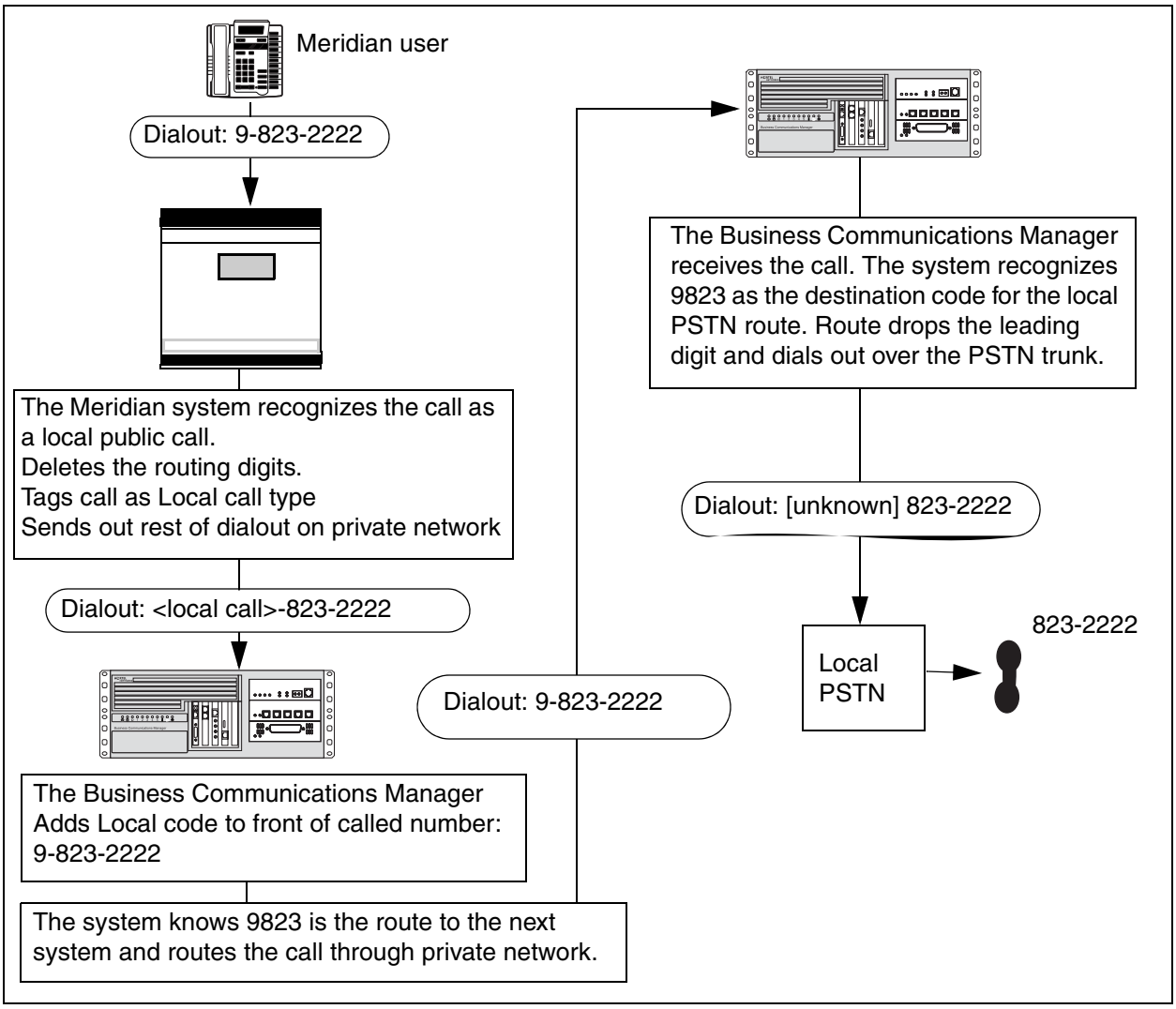
- **Public/Private Auto DN:** The length of the Auto DNs are the same as the Public or Private Received Number Lengths specified under **General Settings, DN lengths**. The public/private Auto DN is cleared if the corresponding Received Number Length is changed.
- **Public/Private DISA DN:** The length of the DISA DNs are the same as the Public or Private Received number length specified under **General Settings, DN lengths**. The public/private DISA DN is cleared if the corresponding Received number length is changed.

Using the MCDN access codes (tandem calls)

Three special codes exist specifically for programming over PRI and VoIP trunks that are using the MCDN protocol, and which connect to a call server systems that use specific call codes for special call types, such as the Meridian 1 (M1). The purpose of the codes is to allow easier programming of the call server systems when calls are tandemed through a Business Communications Manager to the local PSTN.

Calls tandeming to the public network through the private network need to retain their dialing protocol throughout the private network. This means that a call from an M1 node tagged as a local call gets received by the BCM node and is recognized as a call intended for the public network, but also as a call that needs to maintain the local call tag until it gets to the BCM node that is directly connected to the PSTN. This is accomplished by ensuring that the destination code, which starts with this access code, passes the call on using the route designated with the correct call type. Refer to "Defining routes" on page 322. The following figure charts this process.

Figure 87 Local call tandemed through Business Communications Manager nodes



This is how the codes relate:

Meridian 1 access codes	Business Communications Manager access codes	Sample code
Network/long distance code	Private access code	6
	National access code	61
Local code	Local access code	9
	Special access code	9

Calls coming in from the public network need to be translated to their private network destination before routing/tandeming through the private network. In this case, the route used is defined with the call type of Private.

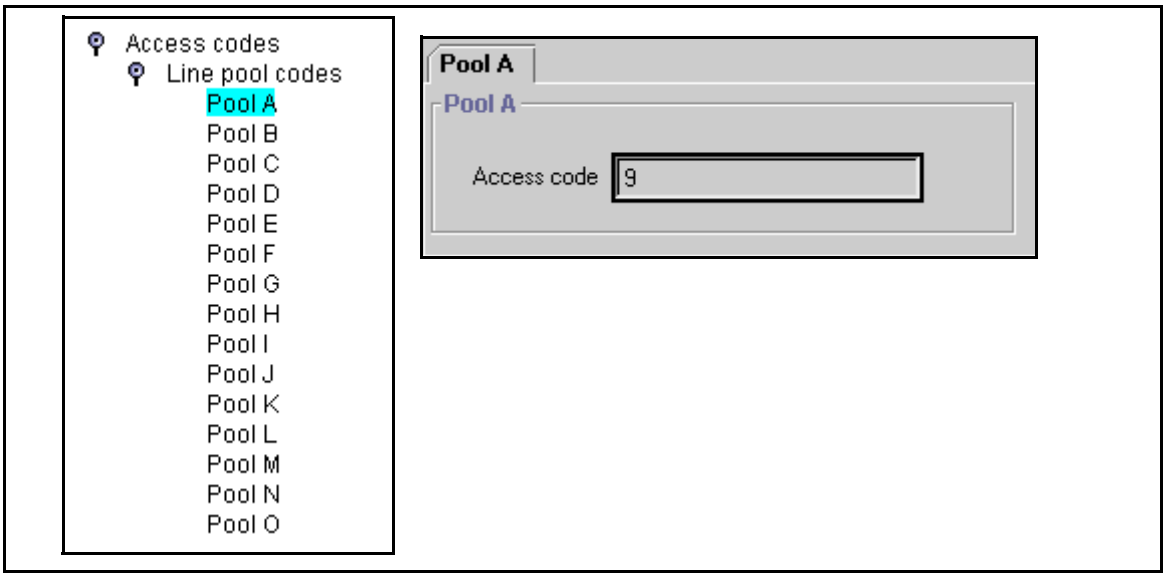
Setting up line pool access codes

Line pool access codes allow you to assign an access code for each of the line pools (A to O). These codes specify the line pool for making an outgoing external call.

Follow these steps to set line pool access codes:

1. Click on the keys beside **Services**, **Telephony Services**, **General Settings**, **Access codes**.
2. Click the key beside **Line pool codes**.
   Pool A-Pool O appears on the navigation tree.
3. Click the Pool you want to program.
   The Pool window appears.

Figure 88 Defining line pool access codes



4. Type the Access code (up to four digits).
   The default Access code is **9** for **Line Pool A**.
   There is no default Access code for Line Pools B to O.

   Note: You cannot assign PRI line pools with a line pool access code. You must define PRI line pools under routing, and create destination codes for the routes.

   Note: A line pool access code cannot conflict with:

Access numbering	**XXXXX** Numbering cannot conflict with these features						
	Park prefix	**External code**	**Direct dial digit**	**Private access code**	**Public/Private Auto DN**	**Public/Private DISA DN**	**Telephone DN**
Line pool/ destination code	**#XXXX**	*	**XXXX**		**XXXX**	**XXXX**	**XXXX**

* If the line pool code and the External code start with the same digit, the line pool code programming supersedes the external code.

Cannot conflict with first digit.

VoIP lines and access codes: Although VoIP trunking lines are not physical lines, you can create a line pool and line pool access codes to access this service. However, if you want to provide fallback to a CO line, you must use routes and destination codes both for the VoIP lines and for the physical line pool.

The VoIP keycode must be enabled before you can access any VoIP lines. The VoIP keycode on a remote target Business Communications Manager must also be enabled for that system to receive VoIP-based calls from your system.

For detailed information about VoIP lines, refer to the *IP Telephony Configuration Guide.*

Using Carrier codes

A multi-digit Carrier access code contains an Equal Access Identifier Code (CAC) followed by a Carrier Identification Code (CIC). The CIC identifies the carrier that handles the call. The Carrier Access Code table stores the CAC digit pattern that you define for your region.

In most cases it is not necessary to change the default values.

About Carrier access codes

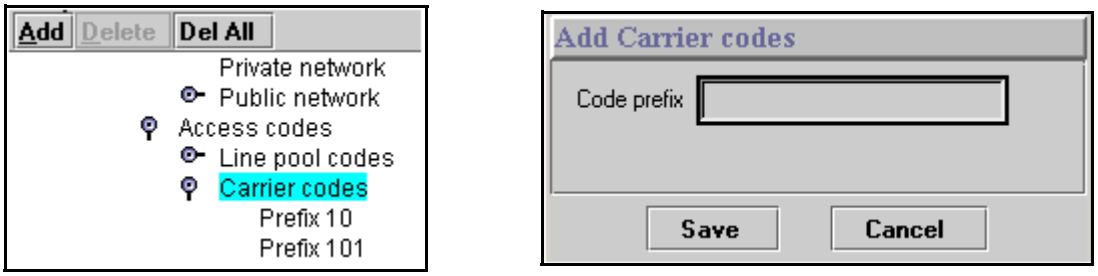
Here are some general points about carrier access codes:

- You can define up to five carrier codes.
- Two entries will be pre-defined in North America, but you can remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 to 9).
- Each entry is identified by the prefix digits themselves.

Identifying Carrier access codes

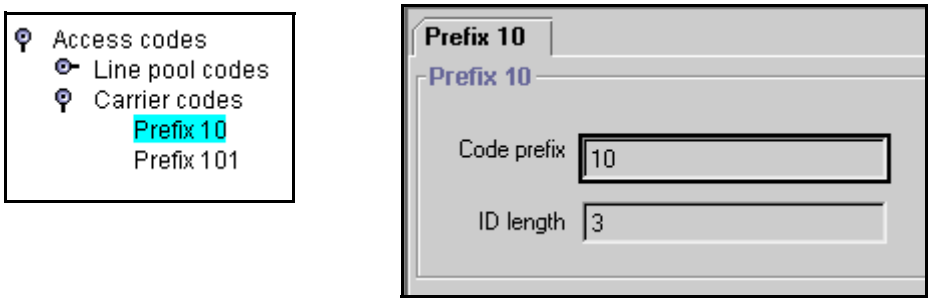
1. Click the keys beside **General settings** and **Access codes.**
2. Click **Carrier codes**.
3. To add a new prefix, click the **Add** button located above the navigation tree.

Figure 89 Adding Carrier code prefix records



4 Click on the Prefix number you created.

Figure 90 Configuring a carrier code prefix ID length



5 Use the following table for information about the two fields on this screen.

Table 63 Carrier access code values

Attribute	Values	Description
Code prefix	<one to six digits> (Read-only)	This value defines the prefix that will be used to access the carrier code.
ID length	1, 2, 3, 4, 5, 6, 7, 8, or 9	This value defines the carrier ID length.

Access code matrix

To help you with your Access code planning, transfer the following information to a spreadsheet and fill out the access codes you want to use.

Table 64 Access code values

Line pool codes	**A: 9** B: _____ C:_____ D:_____ E:_____ F:_____ G:_____ H:_____ I: _____ J: _____ K:_____ L:_____ M:_____ N:_____ O:_____
Park prefix	0 **1** 2 3 4 5 6 7 8 9 None
Extrnl code	0 **1** 2 3 4 5 6 7 8 9 None
Direct-dial digit	0 **1** 2 3 4 5 6 7 8 9 None
Private Auto DN	None Received #_____
Public Auto DN	None Received #_____
Private DISA DN	None Received #_____
Public DISA DN	None Received #_____
Private Access Code	0 **1** 2 3 4 5 6 7 8 9 None
Local Access Code	0 **1** 2 3 4 5 6 7 8 9 None
National Access Code	0 **1** 2 3 4 5 6 7 8 9 None
Special Access Code	0 **1** 2 3 4 5 6 7 8 9 None

Table 64 Access code values (Continued)

Carrier Codes (five codes)	
Code prefix	ID length: 0 **1** 2 3 4 5 6 7 8 9 None

Configuring call routing

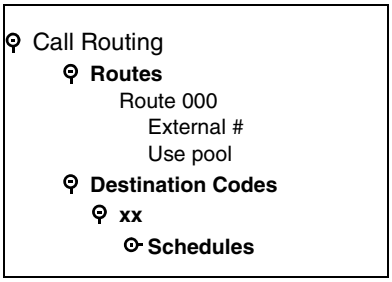
Call routing allows you to define how calls are routed by your Business Communications Manager system.

Task:

- Set up routes to external numbers using a specific line pool:
  - "Defining routes" on page 322
  - "Programming the PRI routing table" on page 325
- Enter destination codes to key access to a route: "Using destination codes" on page 326
- Assign schedules for special routing requirements:
  - "Setting up a destination for local calling" on page 332
  - "Adding Carrier access codes to destination codes" on page 334
  - "Programming for least-cost routing" on page 335
  - "Using multiple routes and overflow routing" on page 336

The following figure shows a detailed view of the Call Routing programming map.

Figure 91 Call Routing headings



Call routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

When you select an internal line and dial, the system checks the numbers you enter against the routing tables. If the number you dial starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of manual tasks, including:

- entering a line pool code
- dialing an access code for a long distance carrier
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system cannot tell what lines are cheaper to use.

For Call by Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (for example, Foreign Exchange, Tie Trunk, or OUTWATS). The user dials a number using the intercom button without entering any special information. For more information see "Provisioning for Call by Call limits with PRI" on page 340.

Using routing to create a coordinated dialing plan is explained in "Configuring the public and private dialing plans" on page 302.

Warning: Plan your routing service before you do any programming. Routing affects every call placed in the system and must be carefully planned to avoid conflicts and gaps in the programming. Use tables to design routes and destination codes, then check for potential problems before you start programming. It also saves you time when all the settings are written out in front of you.

Routing configuration

The settings for a call routing include:

- a three-digit route number (000-999)
- external # digits (up to 24 digits)
- a line pool
- destination codes (max. of 500 available, up to 12 digits)
- DN type and/or Service Type
- public and private DN lengths
- a schedule (optional)

TIPS: To dial a telephone number that does not match a programmed destination codes, you must choose a line and dial the number. For long distance dialing, you can program the area codes in the North American numbering plan as destination codes.

Defining routes

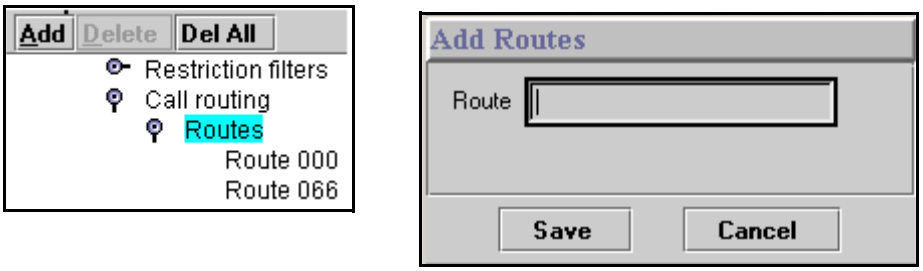
Use the Routes command to configure route records that are assigned to telephones.

1 Click on the keys beside **Services**, **Telephony Services**, **Call Routing**.

2 Click **Routes**.

3 Click the **Add** button.
The Add Routes dialog box appears.

Figure 92 Add a route



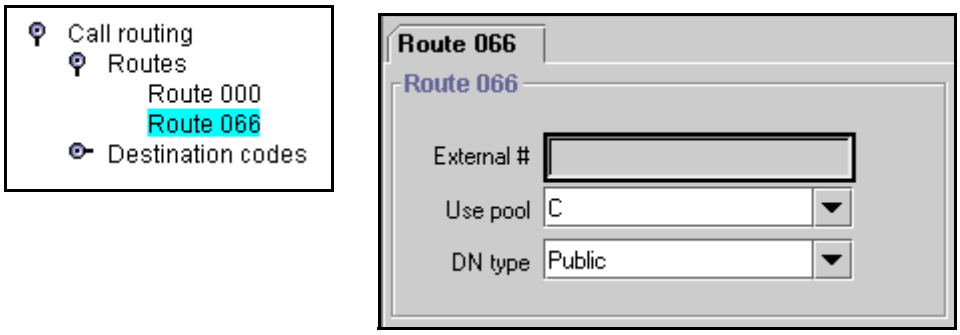
4 Enter a three-digit route number (001-999).

Note: Route 000 is a default route and cannot be changed or deleted.

5 Click **Save**.

6 Click the **Route** number in the navigation tree. The Route window appears.

Figure 93 Define route parameters



7 Use the information in the following table to configure the route settings.

Table 65 Route settings

Attribute	Value	Description
External #	<a maximum of 24 digits>	Enter the external or dial-out number for the route you want the assigned telephone to use. If all the required numbers are defined in the destination code/dial string, this box can be left empty. Optional entries: F78: 1.5 second pause (counts as one digit in the dialing string) F804: wait for dial tone (counts as two digits in the dialing string) F71: Link F808: Long tones F*89: Programmed release F*9: Run/Stop Leave this entry blank if the route is directed to a VoIP line pool.
Use pool	Pool A to Pool O or PRI-A to PRI-F	Select a line pool for the route. The PRI pools only display if you configure an DTM for PRI.
DN type or Service type	Public Private Local (Subscriber) National Special (International) Tie Foreign exchange (FX) Outwats Switched Digital (SDS)	This setting tells the system what type of line protocol the route uses to process the dial string. The heading changes between DN type and Service type, depending on the PRI line protocol. Refer to "Programming the PRI routing table" on page 325.  **MCDN private networks:** Local, National and Special are special designators used to route calls from Meridian 1 systems, through Business Communications Manager systems, out to the public network. The codes for these settings are defined in the Access codes table. Refer to "Using the MCDN access codes (tandem calls)" on page 315. When the Business Communications Manager receives outgoing calls from the Meridian 1, it recognizes the call type and appends the appropriate access code to the Meridian dial string. This code then matches to a route that uses the same DN type, passing the call along, either to another node (the route would have the same DN type) or to the public network (the route would have a Public DN type), depending on the routing information. **Outgoing call display:** If you have the trunks set up to send called number information ("Defining trunk module types and settings" on page 130 and "Identifying BRI T-loops (ETSI, QSIG)" on page 271), and the DN type is set to anything, except Private, the system sends the Public OLI number you specified under line programming. If the DN type is set to Private, the system sends the Private OLI number. Refer to "Configuring line access" on page 393.

Refer also to "Call by Call service routing" on page 324 and "Programming the PRI routing table" on page 325.

Call by Call service routing

The following table provides an example of a Routing Table containing Call by Call programming (available in the North America market profile). Refer also to "Configuring Call by Call services" on page 339.

Table 66 Call by Call routing table example

Route # (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		PRI-A	Public	
004		PRI-A	FX	xxxxx
005		PRI-A	Tie	xxxxx
006		PRI-B	OUTWATS	xxx
007		PRI-B	Private	
008		PRI-B	Switched Digital	

Note: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private.

Note: This type of routing only applies to those PRI trunks set with a protocol of NI, DMS100, DMS250 or 4ESS. Refer to "Configuring the trunk module to line type" on page 131.

The service identifier (SID) depends on the selected service type (for example, with NI-2 protocol).

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
Tie	Facility Number 1-5 digits
OUTWATS[a]	Optional Band Number 1-3 digits
Private	None
Switched Digital	None

a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.

When you select or change a PRI protocol, the Service Type and Service ID fields automatically clear for each entry in the routing table for that PRI.

Programming the PRI routing table

The dialing plan must be thoroughly planned out in advance before programming the information into the Business Communications Manager system.

To program the routing table:

1. Click on the keys beside **Services**, **Telephony Services**, **Call Routing**, **Routes**.
2. Click on the route number record you want to use.
3. Beside **External #:**, type a dialout number (up to 24 digits).
   If you are creating a route for a VoIP trunk, leave this field blank.
4. Under **Use pool,** select a PRI line pool.

   The PRI pool(s) that are displayed depend on how you allocate PRI lines into pools in the **Trunk/Line Data** section of line programming. It is possible to have only pool PRI-A, or only pool PRI-B, or only pool PRI-C, etc., even if there are three DTMs configured as PRI in the system.
5. **Choose a service type or DN type, refer to the table below:**
   - **Service type:** displays for PRI lines with protocol set to NI, DMS100, DMS250, 4ESS. **Service ID:None** appears where the service requires an ID.
   - **DN type:** displays for PRI lines with protocol set to SL-1 (MCDN, ETSI Euro).

The following table lists the service/DN type choices available for PRI lines:

Table 67 PRI Service type/DN type values

PRI Protocol	Type	Values
MCDN	DN	Public, Private, Local, National, Special
ETSI Euro	DN	None, Overlap
ETSI QSIG	N/A	
NI	Service	Public, Tie, Foreign Exchange (FX), Outwats
DMS100	Service	Public, Private, Tie, Foreign Exchange (FX), Outwats
DMS250	Service	Public, Private, Tie, Foreign Exchange (FX), Outwats
4ESS	Service	Tie, Outwats, Switched Digital (SDS)

Enbloc dialing

Enbloc dialing allows the system to determine where a call should be routed on a PRI line. By not dialing out until all digits are entered, the system looks at the entire code and can tell whether the call should be routed through public lines, to another system on a network through private lines, or to the local system.

Public and Private DN lengths and destination codes are used by the system to determine routing. Any prefixes that need to be added on the dialed number, can be included in these settings.

Using destination codes

Destination codes allow you to control how the system interprets and routes dial strings from internal sources. Destination codes are similar to line pool codes except that by using routes (which attach dial strings and DN type designators to line pools) and schedules you can control what digits the user has to dial and how the system routes the call out of the system, including what numbers from the dial string get added or deleted to the route dialout.

The numbers used for destination codes must not conflict with the following:

Table 68 Destination codes: avoiding numbering conflicts

	XXXX Numbering cannot conflict with these features									
	First digit must not conflict with:							**Entire code must not conflict with:**		
	Park prefix	**External code**	**Direct dial digit**	**Auto DN**	**DISA DN**	**Private access code**	**Line pool codes**	**Telephone DN**	**Other destination codes**	**Public target line recv'd digits**
Destination code	**XXXX**	***XXXX**	**XXXX**	**XXX**	**XXX**		**XXXX**	**XXXX**	**XXXX**	**XXXX**

You can enter destination codes to a maximum of 12 digits.

This section includes the following information:

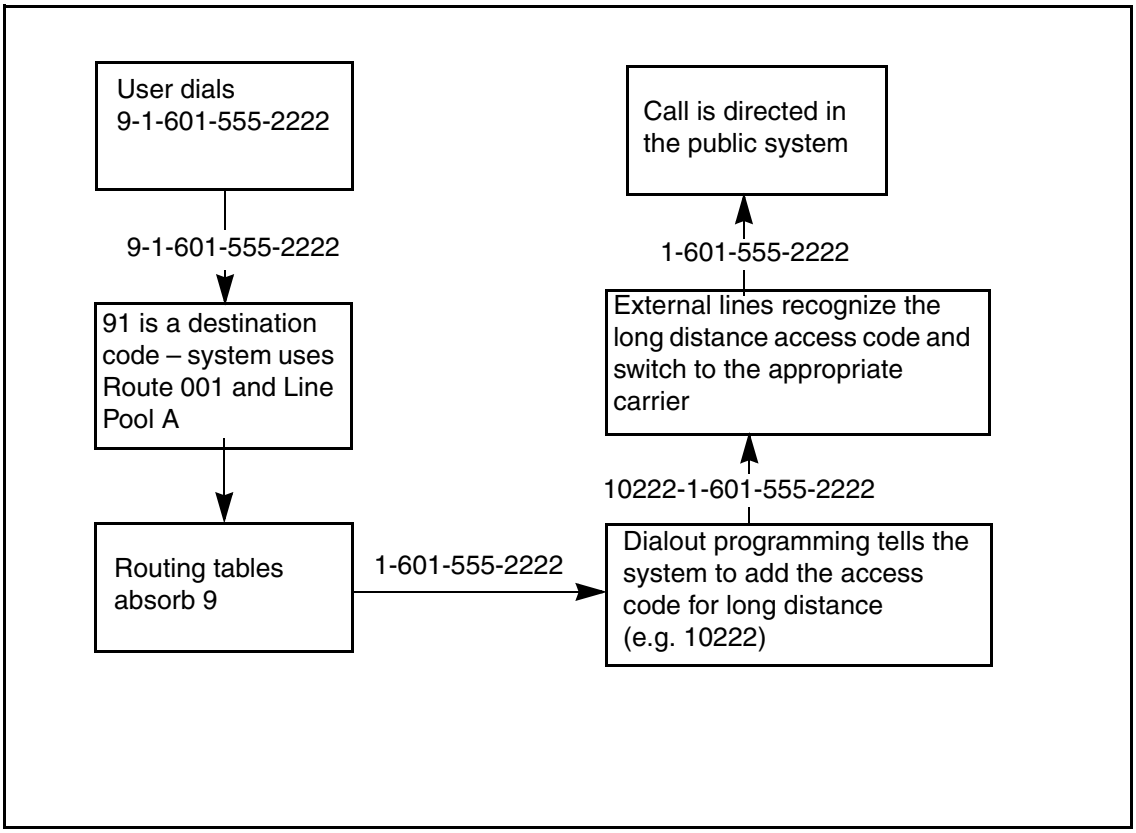
Why use destination codes?

Routes determine path (line or pool) and any required access numbers.

Destination codes determine which route to take (i.e. an end node uses one destination code for all other nodes in the system). If you choose to use the destination codes Normal schedule, the call will always go out over the same route. If you choose to use the other destination codes schedules, you can set up a more responsive plan, whereby calls can go out over more than one route, based on scheduled times.

Destination codes provide you with the opportunity to create a dialing plan that allows users to connect to other systems in a relatively seamless or consistent manner, regardless of the lines or routes that are being used to get there. For example, connecting through VoIP lines requires significantly different ways of dialing than dialing over T1 lines. However, you can configure destination codes, such that the user dials the same number of digits regardless of the trunks over which the calls are routed.

Figure 94 Using destination codes to access another system



Deciding on a code

When deciding on which digit(s) to use to start your destination code(s), you need to take into consideration:

- that the digit or digits you want to start your destination codes with do not match any of the access codes, including the line pool codes that already exist in your system.
  You may find that you need to delete line pool codes and create a route and destination code instead. This could occur if you want to set up fallback to a public line, for instance. If the public line is accessed by a line pool code, you would have to change access to a route so you could create a fallback schedule with the destination code used for the primary line (or lines, if you have more than one outgoing line pool that requires fallback).
- how much of the common part of a dial string you want your users to have to dial, and how much you can put in the dial string.
- if you want specific dial strings to use specific routes, map these out first.

  For instance, if you want users to dial between Business Communications Managers over VoIP lines, you would create destination codes specific to those systems which use the VoIP line pool, using the digits with which the users are familiar. You can then create a unique destination code for the call you want to route over the land line.

  Example: If users are used to dialing 9-1-555-555-<DN number> to reach another system (whose DN codes start with 6), you create a destination code of 915555556A, using the VoIP line pools (users dial the destination code plus the DN of the telephone they want to reach on the other system). The letter A at the end of the code represents any number from 0 to 9 which is not used by any other destination code.

  If you need to use land lines for a specific connection on the other system, you can create a destination code specific to that destination number and attach it to the route set up with the landline line pool (i.e. 915555556333, 6333 being the DN of the device on the other system. When the user dials that specific number, the call will always go over the land line). Note that by entering this code, users dialing with the code in the previous paragraph could never dial any DN that started with 63XX.
- If you want to use VoIP lines as your main lines, but you want to program one or more land lines as fallback lines, you need to configure the routing and routing schedules so that the user dials the same number, regardless of which routes get used. You use the external # dialout string and absorb digits fields under the schedules in Destination code programming for this purpose.
- If a company wants to use VoIP lines between sites for interoffice calls, but not necessarily for all the voice traffic, they can configure specific destination codes for the VoIP routes. In this case, the destination code contains the same digits as a user would dial for a landline, thus, making the shift transparent to the user and, at the same time, ensuring that the most economical route is being used. Depending on how many exceptions there are, you can use the wild card at the end of the string to save yourself from the necessity of entering a number of destination codes with the same leading digits. Refer to “Grouping destination codes using a wild card” on page 329.
- If you are setting up a new system where users do not have previously-established dialing patterns, you can use simpler destination codes. For example: You can establish 9 as the destination code for dialing outside the system, 5 for dialing any calls within networks on the

local exchange, and 7 for dialing any calls within the network to destinations outside the local exchange.

Therefore:

System A calling to the public network would dial 9XXXXXXX or 91XXXXXXX if the call is long distance.

System A calling to System B, which is in the same city, would dial 5XXXX

System A calling to System C, which is in another exchange area, would dial 7XXXXXXX

Note: If the network is using CDP for the dialing plan, the destination codes could be the leading digit of the DN code, since that needs to be unique for each system. However, this would depend on which digits have already been taken by other coding in the system.

Grouping destination codes using a wild card

If you have a number of destinations that have the same route and digit absorb length, you can group these codes under one destination code to maximize your destination code table. In this case, the start digits will be the same, but the last character will be the wild card, and indicates any digit between 0 and 9. However, if there is a conflict with other digits already programmed or used by other destination codes, an error message appears.

For instance, you might use the same route (555) to a number of remote sites. Each site is accessed with the same external # (dial out string), except for the last digit, which is unique to each site. The exception to this is a site with a totally different access number and line pool requirement (route 565). This example is shown in the following table.

Table 69 Establishing routes and dialout requirements

Route	Dial Out (external #)	Line Pool
555	0162 237 625<unique number from 0 to 9>	Line Pool C
565	0173 133 2211	Line Pool A

If you do not use wild cards, you would need to create a separate Destination code for each unique dialout, as shown in the following table.

Table 70 Destination codes not using a wild card

Destination codes	Route	Absorb Length	Dial Out
0621	555	3	0162 237 6251
0622	555	3	0162 237 6252
0623	555	3	0162 237 6253
0624	555	3	0162 237 6254
0625	555	3	0162 237 6255
0626	555	3	0162 237 6256
0627	565	All	0173 133 2211
0628	555	3	0162 237 6258

Table 70 Destination codes not using a wild card (Continued)

Destination codes	Route	Absorb Length	Dial Out
0629	555	3	0162 237 6259

If you use the wild card character *A (*ANY), you can reduce the number of destination codes you require to two, as shown in the following table.

Table 71 Destination codes using the ANY character

Destination codes	Route	AbsorbLength	Dial Out
062A	555	3	0162 237 625X where X is the last digit of the destination code dialed out, from 1 to 9, but not 7
0627	565	All	0173 133 2211

Tips
The digit absorption setting (absorbed length) applies to a maximum of two schedules. To minimize the effort involved in preparing destination codes, set the digit absorption to 0. With set to 0, the actual digits dialed by a caller are preserved in the dial out sequence. The need to program a dial out sequence as part of the route depends on the required dialout.

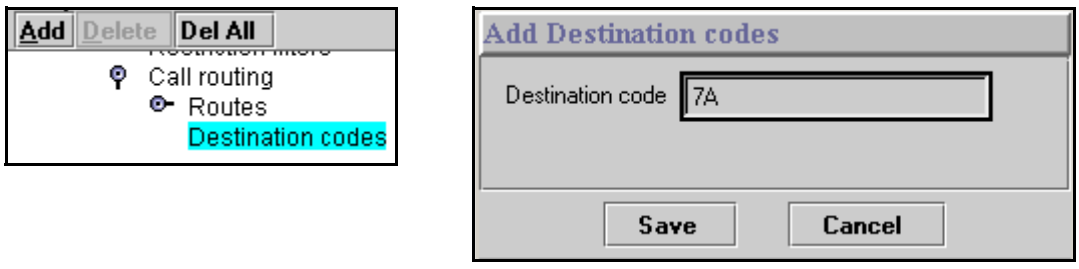
Configuring destination codes with wild cards

Create the routes with dialout strings containing the common digits, then follow these steps to create a destination code with a wild card character.

Create the destination code

1. Click on the keys beside **Services**, **Telephony Services**, **Call Routing**.
2. Click on **Destination codes**.
3. Click on the **Add** button**.**
   The Destination code dialog box appears.
4. Enter a destination code, typing the letter A for the last digit of the code.

Figure 95 Adding a destination code with a wild card

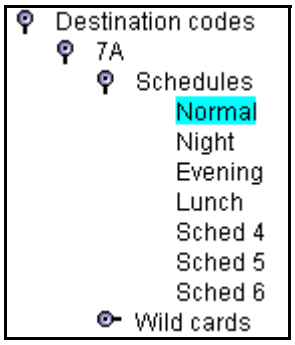


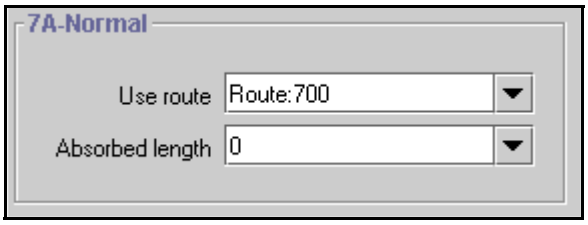
5. Click the **Save** button to save the destination code.

Set up the destination code schedules

1. Click on the key beside **Schedules**.
2. Click on the schedule name you want to program. For example: Normal.
3. Choose the **Use route** you want the destination code to refer to during operation of the schedule.
4. In **Absorb Length**, choose a number to define which part of the destination code will be ignored by the system when it dials out.

   Programming note: All schedules except Normal allow you to specify up to three routes, to allow for fallback.
5. Click outside the window to save the changes.





Enable/disable wild card digits

1. Click on the key beside **Wild cards**.

   The valid numbers for the wild card for this code are displayed.
2. Click on the number you want to change.
3. In the **Wild card state** field, choose **Assigned** (can be used with this destination code) or **Available** (can be used as part of another destination code).
4. Repeat steps 2 and 3 for all the numbers you want to change.

Setting up a destination for local calling

An office can have different suppliers for local and long distance telephone service. By programming a destination code, any call that begins with 9, which is the most common dial out digit, automatically uses lines dedicated to local service.

Note: 9 is the default setting for the line pool code for Pool A. If you want to use 9 as a destination code, you must change the Pool A code. Refer to "Assigning line pool access" on page 402.

Follow these steps to build a route to allow local calls.

1. Create a route that uses the line pool you assigned for the PSTN trunks. ("Defining routes" on page 322).
2. Create a destination code record and enter a destination code, such as 9, which is a common local call code. ("Configuring destination codes with wild cards" on page 330)

   For local calls only, there are no dial out numbers (compare with "Setting up a route through a dedicated trunk" on page 333).

   The destination code can use a different route, depending on what schedule is assigned. In the current example, the route you define is used when someone dials 9 during Normal mode, when the other Schedules are turned off.
3. Set up the Normal schedule with the route number you defined in step 1.

Figure 96 Routing Service programming example

Routing Service (Services: Routing Service)		
Route # (000-999)	**Dial out (if required) (max. 24 digits or characters)**	**Use Pool**
001	none	A B C D E F G H I J K L M N O
002	none	A B C D E F G H I J K L M N O

The following figure shows an example of a Destination codes programming record filled out

Figure 97 Destination codes for call routing

Destination codes (Services; Routing service; Destination codes)								
Service Schedule (max. 7 char)	**Normal Rte**		**Route schedule**					
DestCode (max. 7 digits)	**Use route (000-999**	**Absorb Length**	**1st route (000-999**	**Absorb Length**	**2nd route (000-999**	**Absorb Length**	**3rd route (000-999**	**Absorb Length**
9	003	All						
1	002	0						

An office can have leased lines or private network trunks that provide cheaper to long distance calls by routing through the dedicated lines to remote systems, then using the local PSTN from that system to make the call. The routing should take place automatically when the number of the outgoing call begins with 1.

Setting up a route through a dedicated trunk

If your long distance is supplied by an alternate service or if you want to use different trunks at different times of the day, you can configure a route to use a specific trunk.

1. Create a route that uses the line pool containing the discounted lines for long distance calling. ("Defining routes" on page 322).
2. Create a destination code record and enter a valid destination code (maximum of 12 digits). ("Configuring destination codes with wild cards" on page 330)

   You must use a valid destination code, such as 91 (9, indicating PSTN; 1, indicating a long distance). See "Using destination codes" on page 326. View existing destination codes before entering a new code. The destination code can use a different route depending on the Schedule.
3. Under the **Normal** schedule for the destination code, enter the route you specified in step 1.

Notes about the Absorbed length:

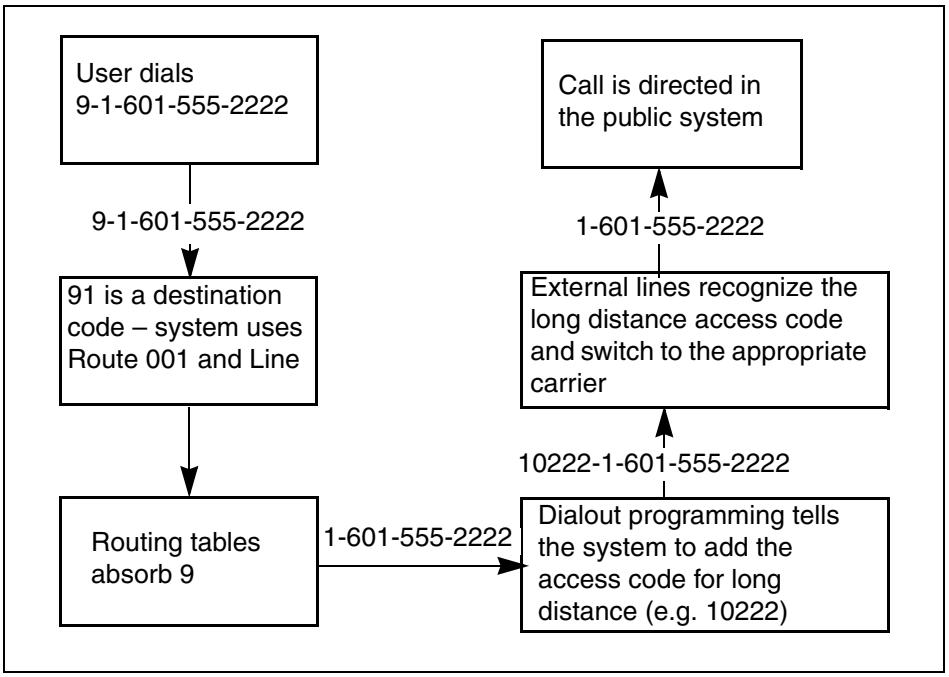
The digit absorption setting (**Absorbed Length**) applies to a maximum of two schedules.

Setting **Absorbed Length** to 0 minimizes the effort involved in preparing destination codes. When the Absorbed Length is at 0, the actual digits dialed by a caller are preserved in the dialout sequence. It is not necessary to program a dial out sequence as part of the route.
If rates change depending on the time of the day or week, a different route can be used for the same destination code when a particular schedule is in use. See "Programming for least-cost routing" on page 335.

Adding Carrier access codes to destination codes

In many cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number, which is sometimes referred to as an equal access code (CAC). Route programming can include the access number so the users do not have to dial it every time they make a long distance call. The following figure shows an example of how the system interprets what the user dials into a valid outgoing call.

Figure 98 Carrier code call numbering sequence



Follow these steps to program a long distance carrier access code into a destination code.

1. Create a route that uses a line pool containing local lines only.
2. Program the route to use a line pool containing the lines used to access the long distance carriers.
3. Type the dialout digits, which are the same as the access digits. For example, if the access code is 10222, the dialout digits are 10222.
4. Create a destination code 91: 9 (for outside access) and 1 (for long distance). You must use a valid destination code. Refer to "Using destination codes" on page 326.
5. Set **Absorbed Length** to 1.
   The digit 9 is only used internally and should be dropped. The 1 is needed to direct the call to the public carrier network.

TIPS: The destination codes 9 and 91 used in the examples cannot be used together. If you need the destination code 91 to direct long distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. Refer to "Grouping destination codes using a wild card" on page 329 for information on programming destination codes.

Programming for least-cost routing

It can be less expensive to use another long distance carrier at a different time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode are also used for long distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, you must build another route.

Follow these steps to build a route for a secondary carrier:

1. Beside **Route:** enter an available route number.
2. Choose **No number** for the dialout.
3. Choose the line pool that contains the local service carrier lines.
4. Now you need to create a destination code and assign the route to the Night schedule. In this case, the change in route uses the start and stop times for Night Schedule.
5. Add 91 as a **Destination code.**
6. Make sure **Absorbed length** is set at 1.
7. Under **Night schedule:** enter the route you defined in step 1.

Calls that begin with the digits 91 travel out without using the access code when the Night schedule becomes active or when you turn it on at a control telephone.

Using multiple routes and overflow routing

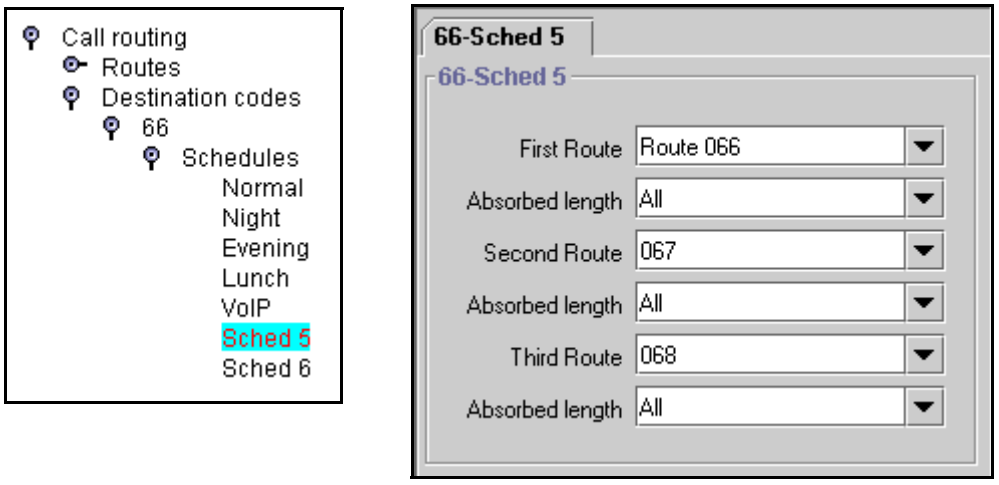
If all the lines used by a route specified by a destination code are busy when a call is made, you can program other routes that the system automatically flows the calls to, or you can allow the call to overflow directly to the Normal route schedule (usually the most expensive route). However, this only takes effect if an active schedule is applied to the line. Overflow routing is not available in Normal mode.

You must create overflow routes for each destination code for which you want to allow overflow routing.

To set up the multiple routing overflow feature, follow these steps:

1 You assign the preferred routes in a Destination code schedule (**Services, Telephony Services, Call Routing, Destination code**).

Figure 99 Multiple routing with destination schedules



a Pick a schedule when you want these routes to be in effect.

b In the **First Route** field enter the route number for the preferred route for the call.

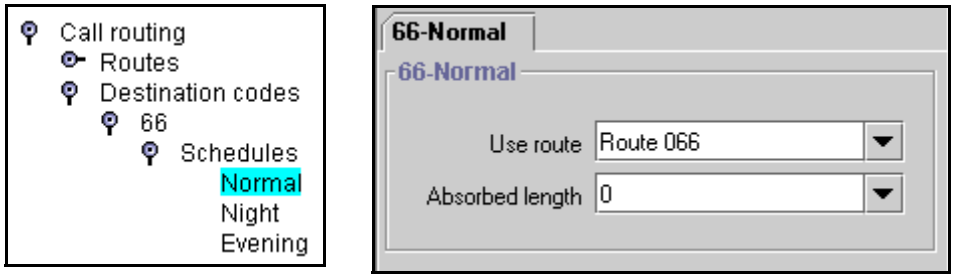
c Choose the absorb length for the first route that is appropriate for the dialout numbers you entered for the route.

d Repeat steps b and c for **Second Route** and **Third Route** fields.

e Define the start/stop time as 0100 under the equivalent Routing Services schedule. This setting means that the schedule is active 24 hours a day. Refer to "Configuring routing service" on page 495.

2 Assign an overflow route, usually the most expensive route, to the same Destination Code, but for the Normal schedule.

Figure 100 Configuring the Normal schedule for overflow



3 Under **Scheduled Services, Routing Service, <preferred route schedule>**, choose **auto** for **Service Setting,** and **Y** for **Overflow**.

4 Use a control telephone to activate the feature on the telephones on which you want preferred routing to be active.

Note: You must also ensure that the route correctly absorbs or passes dialed digits so that the number dialed for each line is the same from the user perspective.

When a user dials, and the telephone cannot capture the preferred line (First Route), the system tries each successive defined route (Second Route, then Third Route). If none of these routes have available lines, the call reverts to the Normal mode. When the call switches from the preferred routing mode (First Route, Second Route, Third Route), to Normal mode, the telephone display flashes an “expensive route” warning.

Note: Overflow routing directs calls using alternate line pools. A call can be affected by different line filters when it is handled by overflow routing.

VoIP trunking uses a similar process for setting up fallback from the VoIP trunk to a PSTN line. Refer to the *IP Telephony Configuration Guide* for details.

Using dialing restrictions with routing

You can further customize routing service by adding dialing filters to lines in line pools. Filters restrict the use of the line to specific area codes.

To set up restriction filters, refer to "Defining restriction filters" on page 344.

TIPS: host system signaling codes can be part of the dial out.
You can also use routing as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dialout. Set the digit absorption to 1.

Routing matrix

To help you with your route planning, transfer the following information to a spreadsheet and fill out the values for each route you create.

Table 72 Routing

Call Routing: Routes			
Route #	External #	Use Pool	DN type Public Private
Destination code: *You can specify three alternate routes for these services.	Normal *Night *Evening *Lunch *Sched 4-6	Use route None Route: Route 001	Absorb length All 1 2 3 4 etc. _____

Configuring Call by Call services

Call by Call service selection (CbC) allows you to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network.

This section includes information about:

Supporting protocols

The following protocols support Call by Call limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250 (MCI, Sprint, Generic)
- AT&T 4ESS custom

Call by Call services

Business Communications Manager supports the Call by Call Services listed in the following table.

Table 73 Call by Call Services available on the system

Service	Description
Public	Public calls connect Business Communications Manager and a Central Office (CO). Business Communications Manager supports both incoming and outgoing calls over the public network. Dialed digits conform to the standard North American dialing plan (E.164 standard).
Foreign Exchange (FX)	Foreign exchange service connects a Business Communications Manager site to a remote central office (CO). This provides the equivalent of local service at the remote location.
Tie	Tie lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as another Business Communications Manager.
OUTWATS	Outward Wide Area Telecommunications: This outgoing call service allows a Business Communications Manager user to call telephones in a specific geographical area referred to as a zone or band. Typically, a flat monthly fee is charged for this service.
INWATS	Inward Wide Area Telecommunications: This long distance service allows a Business Communications Manager user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.

Table 73 Call by Call Services available on the system (Continued)

Service	Description
International INWATS	An international long distance service that allows a Business Communications Manager user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
Switched Digital	This service provides premises-to-premises voice and data transport with call management and monitoring features.
Nine Hundred	This service is commonly referred to as fixed-charge dialing.
Private	Private incoming and outgoing calls connect Business Communications Manager to a virtual private network. Dialed digits can conform to the standard North American dialing plan (E.164 standard) or the dialed digits can use a private dialing plan.

Switches supporting Call by Call limits

The following table lists the service types and cross-references them with four common switches.

Table 74 Switches and service types chart

	Switches			
Service types[1]	**NI-2**6	**DMS-100 (custom)**	**DMS-250 (MCI, Sprint, Generic)**	**AT&T 4ESS**
FX	FX	FX[2]	N/A	N/A
Tie[3]	Tie	Tie	Tie	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private[5]	VNET (virtual network)	N/A
Switched Digital	N/A	N/A	N/A	ACCUNET[4]
Nine Hundred	N/A	N/A	Nine Hundred	MultiQuest
Public	Public	Public	Public	N/A

1. N/A indicates that the protocol does not support the service.
2. DMS-250 Sprint and UCS support incoming FX only (i.e. Network-to-Business Communications Manager). DMS-250 MCI does not support FX.
3. NI-2 allows two Tie operating modes: senderized and cut-through. Business Communications Manager supports only senderized mode.
4. Rates greater than 64 kbps are not supported.
5. Bell Canada VNET.
6. Not all service types may be supported by a switch type. For information, contact your service provider.

Provisioning for Call by Call limits with PRI

To program the system for Call by Call Limits with a PRI interface, you must:

- provision a DTM as PRI, if one is not already configured as part of the system
- select a protocol, on page 99
- program incoming call routing, on page 152
- program routes that use the PRI pools, see "Configuring call routing" on page 320.

Other required programming in the Unified Manager

Programming Call by Call on PRI requires these settings:

- under **Line Access**, assign the line pool
- under **Services**, in routing services, assign a pool for routing, and assign the service type and service id, if required
- under **General settings**, specify the minimum and maximum values for the pools

Setting CbC limits

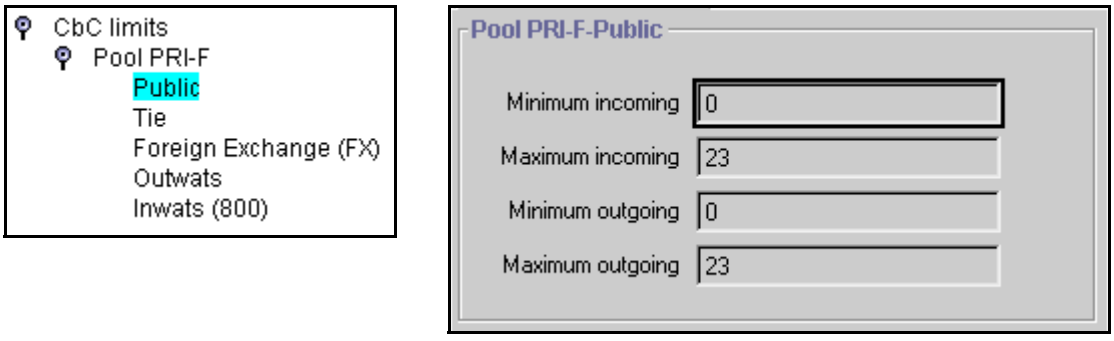
PRI pool limits for Call by Call services allows you to configure limits for service types without interacting with the CO. This feature sets the minimum and maximum number of incoming and outgoing calls per service type for the PRI pool.

The number of active calls are tracked. Whenever a call is setting up, a check determines if the call is allowed. Calls are not allowed if they exceed the maximum value for that service type or if they use lines needed to maintain the minimum value of other service types.

Follow these steps to program CbC Limits

1. Click on the keys beside **Services**, **Telephony Services**, **General settings**, and **CbC limits**
2. Click on the key beside a pool type (PRI-A to PRI-F).
3. Select a service.
   For example, Public. The services that display depend on the PRI protocol.

Figure 101 Setting CbC limits parameters



4 The following table lists the possible values to enter into the pool fields.

Table 75 DN length values

Attribute	Values	Description
Minimum incoming	Default: 2	**Note**: The total of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the PRI pool. The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the PRI pool.
Maximum incoming	Default: 23	
Minimum outgoing	Default: 4	
Maximum outgoing	Default: 23	

PRI line pools

All lines in a PRI interface are in the same PRI line pool. This pool cannot contain any non-PRI lines. There is one PRI pool available for each PRI interface. Depending on the order that the modules are configured as PRI, Pool PRI-A represents lines 061 to 083, Pool PRI-B represents lines 085 to 107, and Pool PRI-C represents lines 109 to 131, etc. to Pool PRI-F. If all PRIs are connected to the same service provider and use the same protocol, lines 061 to 083, 085 to 107, and 109 to 1311 etc. can be put in the same pool, PRI-A, PRI-B, PRI-C up to PRI-F.

CbC matrix

To help you organize your PRI call by call limits lines, transfer the following information to a spreadsheet and fill out the information.

Table 76 CbC matrix

PRI pool	Type	Incoming lines	Outgoing lines
PRI-A PRI-B	Public, Tie, Foreign Exchange OUTWATS, INWATS International INWATS, Private Switched Digital, Nine hundred	Minimum incoming: _____ Maximum incoming: _____	Minimum outgoing: _____ Maximum outgoing: _____

Viewing CbC limit metrics

You can view statistical information about call-by-call limit settings for PRI when the protocol is set to call-by-call routing.

1 Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, **CbC limit metrics**.
The display shows the pools that supports CbC routing.

2 Choose a PRI pool.
The display shows the services in the pool. The Call-by-Call services that display are determined by the PRI protocol of the line.

3 Select a service. For example, **Public**.
The display shows the settings for the selected service.

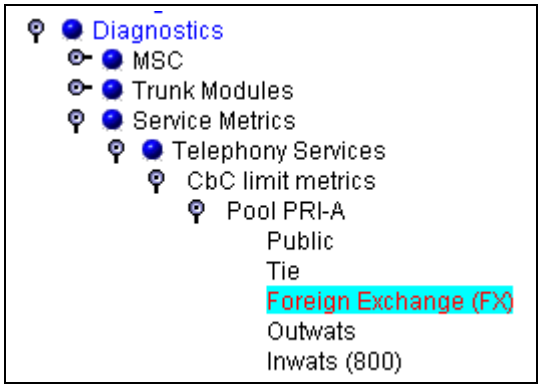
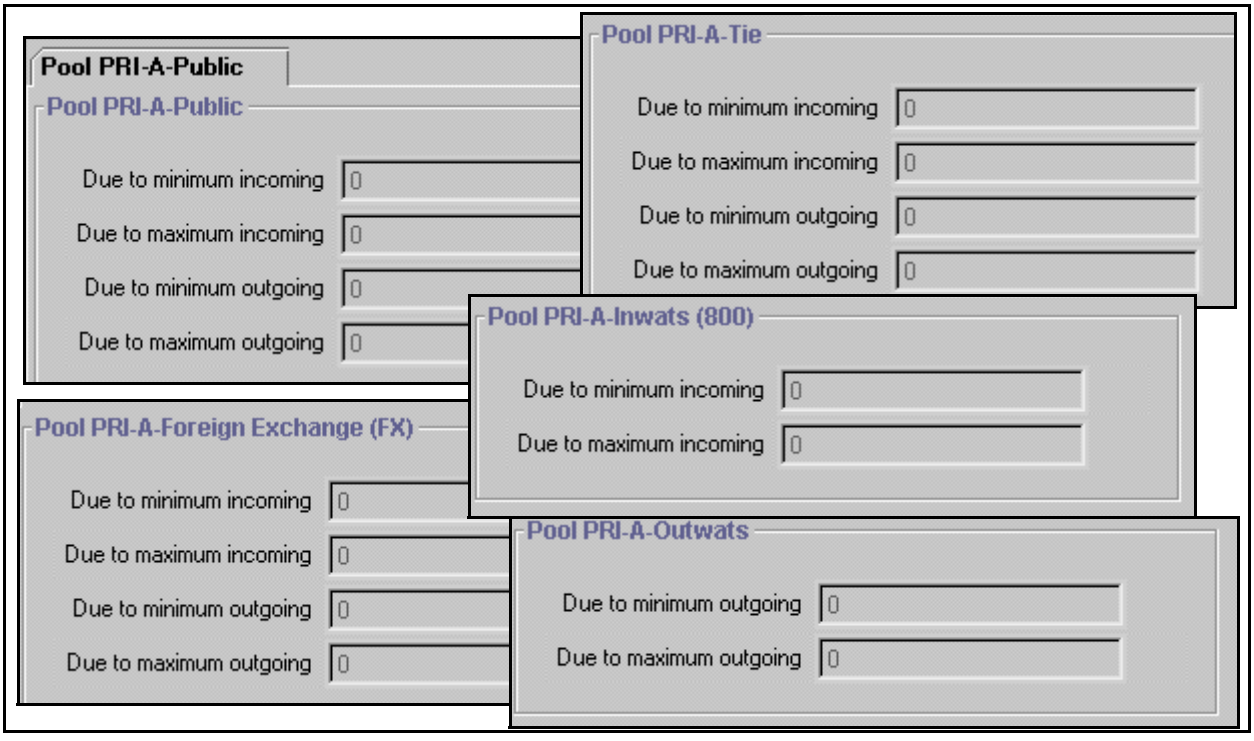


Figure 102 Metrics for all CbC options



4 To clear the settings for a selected service, click **Clear metrics** on the **Configuration** menu.

Defining restriction filters

Restriction filters allow you to restrict the numbers that can be dialed on any external line within Business Communications Manager. Up to 100 restriction filters can be created for the system.

To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

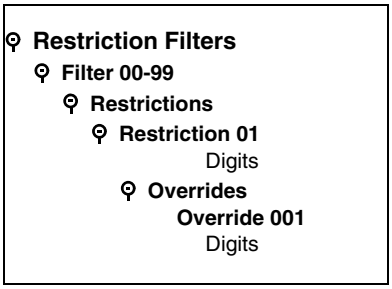
Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

This section includes the following information:

- "Adding a restriction filter" on page 345
- "Notes about restriction filters" on page 345
- "Adding overrides to restrictions" on page 348
- "Restriction filter examples" on page 349

The following figure shows the Restriction Filters headings.

Figure 103 Restriction Filters headings

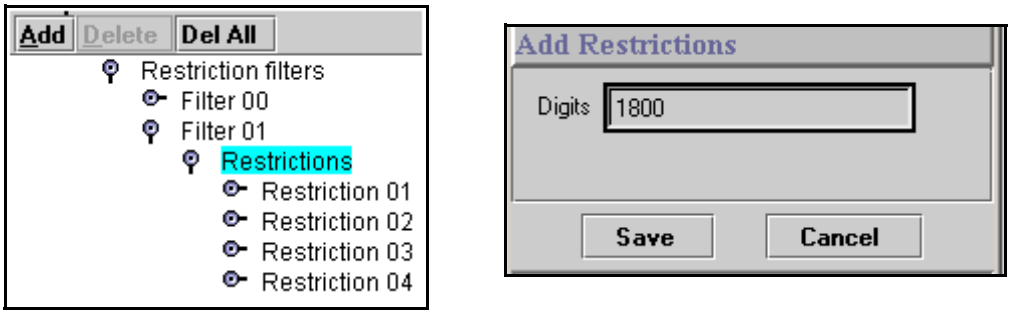


Adding a restriction filter

Follow these steps to add new restriction filters:

1. Click on the keys beside **Services**, **Telephony Services.**
2. Click on **Restrictions**.
3. Click the Add button located above the navigation tree.
   The Add Restrictions dialog appears.

Figure 104 Adding restriction filters



4. Enter the digits you want to restrict.
5. Click **Save**.
   The new restriction is added to the button of the restrictions list for that filter.
6. If you want to add numbers that will override the restrictions, refer to "Adding overrides to restrictions".

Removing restrictions

To remove restrictions that no longer apply, click on the Restriction # you want to remove, then click the **Delete** button at the top of the column.

Exercise caution when removing overrides.
If you remove a restriction, the overrides associated with the restriction are also removed. This action also changes the identifying numbers of the subsequent restrictions that you have defined. For example, if you remove Restriction 01, Restrictions 02 to 08 are renumbered as 01 to 07.

Notes about restriction filters

A restriction filter is a group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. The restriction filters setting allows you to assign restrictions in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), therefore, users have an opportunity to bypass restrictions. To prevent this from happening, you can create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There are also variations of each sequence that you want users to be able to dial, these are called overrides. Overrides are defined within each restriction package for each filter.

Once you create the filters, you can assign the restrictions to a telephone (**System DNs**), to a line (**Lines**), to a particular line on a telephone (**System DNs**), and to remote callers (**Lines, Remote access**).

Note: Filter 00 cannot be changed. Filter 01 has a set of defaults. Filters 02 to 99 can be set to suit your special requirements. See "Default filters (North America)" on page 347.

- Each programmable filter can have up to 48 restrictions.
- There is no limit on the number of overrides that can be allocated to a restriction. However, there is a maximum total of 400 restrictions and overrides allocated to the 100 programmable filters.
- The maximum length of a restriction is 15 digits.
- The maximum length of an override is 16 digits.
- Entering the letter *A* in a dialing sequence indicates a wild card, and represents any digit from 0 to 9.
- You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).
- When restricting the dialing of a central office feature code, do not forget to create separate restrictions for the codes used for DTMF and pulse lines (for example, *67 and 1167).
- Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.
- You can copy restrictions and overrides from one filter to another. You can use a restriction or override in any number of filters. Each time you use a restriction or override, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.
- Removing a restriction from a filter has no effect on the contents of other filters, even if the restriction was copied to them.
- You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Default filters (North America)

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with 10 restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911, which is the number for emergency assistance in North America, is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Table 77 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
01	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are loaded only when the system is cold started.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Table 78 Default filters for program headings

Filter	Heading	Sub-heading
02	System DNs	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Default filters (other)

Three profiles have global overrides which do not appear in Unified Manager restriction programming and cannot be changed.

Australia: 000, 13144A

Brazil: 194A

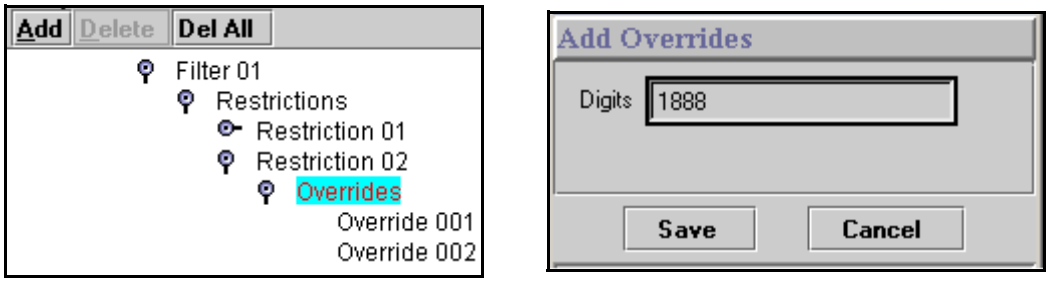
UK: 999, 112

Adding overrides to restrictions

1 Click on the keys beside **Services**, **Telephony Services**, **Restrictions**.

2 Click on the restriction number where you want to add an override.
The Add Overrides dialog appears.

Figure 105 Adding overrides to restrictions



3 In the Digits field, enter the number that you want to be able to override the restriction filter.

Note: Enter the letter **A** as a wild card character that represents any digit from 0 to 9 in a sequence of numbers when denying numbers or creating overrides.

4 Repeat steps 2 and 3 for all the overrides you want to add

5 Click **Save**.
The new override is added to the bottom of the Overrides list.

To view an Override to a restriction: click on the **Override XXX** headings.

To delete an override: Select the override you want to delete, and then click on the **Delete** button at the top of the column. If you want to delete all overrides for that restriction, click the **Delete All** button.

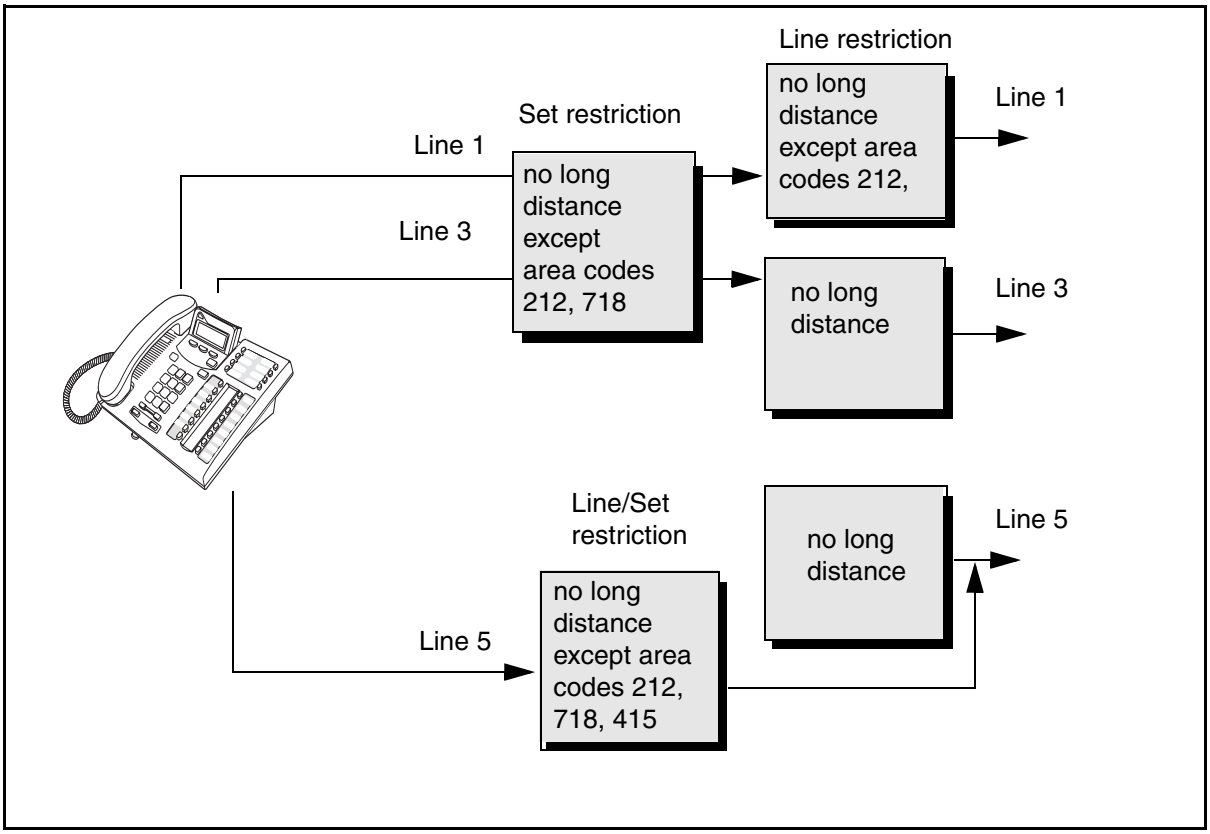
Restriction filter examples

Line and set restrictions are shown in the following figures.

In the first figure, below, a caller using line 001 could only dial long-distance numbers to area codes 212 and 718. A caller using line 003 could not dial any long-distance numbers. A caller using line 005 could dial long-distance numbers to area codes 212, 718, and 415.

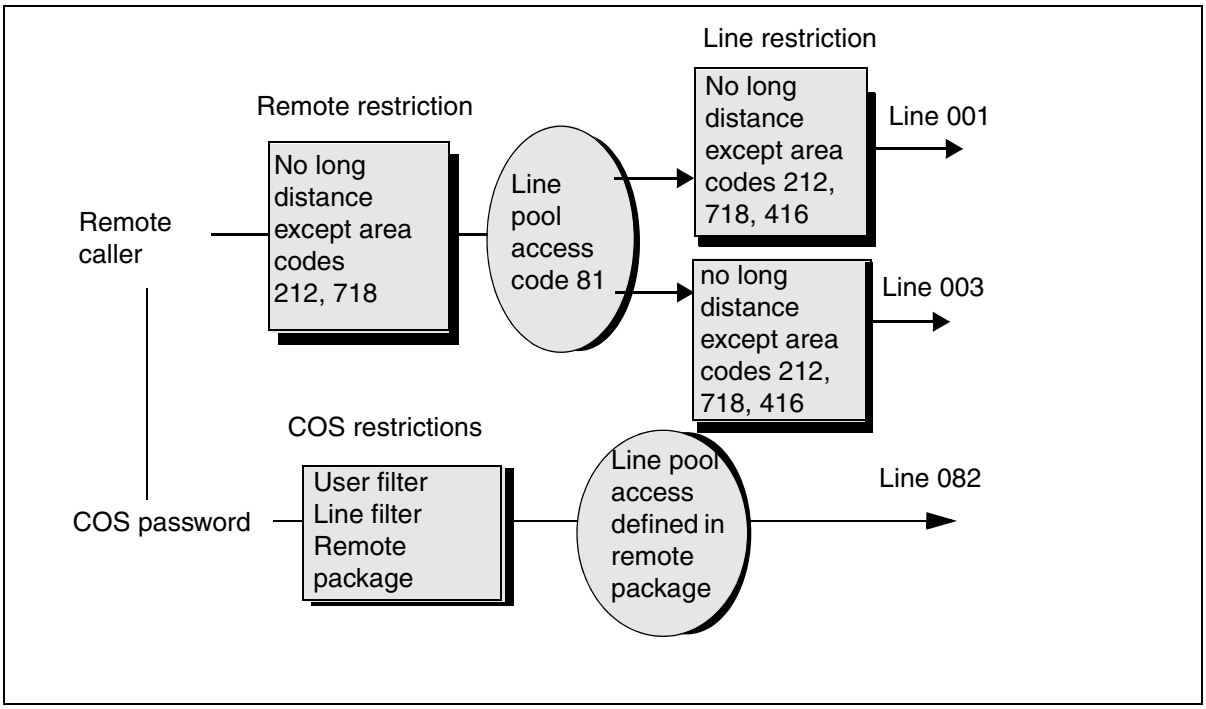
TIPS: To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).

Figure 106 Line restriction example



In the following figure, dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a COS password.

Figure 107 Remote line restriction example



Restriction filters matrix

Transfer the following information to a spreadsheet and fill out the restriction filter information you want for your system.

Table 79 Restriction filters matrix

Filter #	Restriction #	Overrides			

Enhanced 911 (E911) configuration

Government rules vary about support for Enhanced 911 (E911) dialing service by Customer Premises Equipment. Legislation may require that the Customer Premises Equipment give a more precise location of the source of a 911 call than the billing address of the central office line.

Consult your service provider about the laws and regulations.

Task:

Set up emergency access number to comply with local regulations.

Use the following configuration rules when installing the Business Communications Manager system to assure compliance with local regulations:

- When equipped with PRI trunks, Business Communications Manager can deliver the Calling Line ID of a telephone dialing 911 through the Public Switched Telephone Network, if the proper programming has been implemented and PRI trunk service has been installed by the service provider. If you are using ISDN PRI, implement OLI programming and Business Name programming to add the Set ID to the CLASS information.
- By default, Restriction Filter 02 is assigned to all sets on startup. There are no restrictions applied in Restriction Filters 02-99. Restriction Filter 01 has restrictions, but 911 is an exception for this filter. For information on how to change the Restrictions, refer to "Defining restriction filters" on page 344.
- When using other trunk interfaces, you can assign separate line pools to groups of telephones in different areas (for example, in different buildings, floors or sections).
- Be careful when using the Set Relocation feature. You may have to reprogram the line pool access to send the right location on 911 calls.
- Configure the 911 destination code to dial out over a Normal Schedule in all applicable Service Modes, as this is the default route should any other programmed routing attempts fail. When using PRI interfaces, make sure all sets can use the PRI line pool that the Normal Schedule route uses.

911 and IP telephones

DO NOT program IP telephones with a 911 code mapped to a line pool for the Business Communications Manager, unless it is co-located with the system.

Chapter 13
Configuring DN records, an overview

This section provides an overview about the process for programming the records of the telephones and equipment attached to the station modules on the Business Communications Manager. Refer also to the process map on the next page ("Understanding the configuration process" on page 354).

For a detailed description about what DNs are, and what the different categories of DNs in the navigation menu mean, refer to Defining the System DN headings on page 358. System DNs also contains a **DN registration** heading, which lists the DNs which are, or which can be, registered to the system ("DN Registration headings" on page 363).

Task overview: To set up each telephone or device attached to your system:

- Determine which DNs will be assigned to the telephones and devices. ("DN mapping for digital telephones" on page 355)
- Use the Wizards to configure telephones ("Configuring DNs using the Wizards" on page 369)

  OR
  Configure each telephone record individually ("Configuring DNs for system devices" on page 387).
- Determine the call display and log options. ("Configuring telco features" on page 445)
- If you have optional voice mail active on your set, you will also see the active phone number for each telephone. ("Voice Mail settings" on page 446).
- If your attendants have M7324 telephones with CAP modules or BST T7316E telephones with KIM modules that are assigned as CAP stations, you need to assign these systems under "Setting up CAP stations" on page 434.

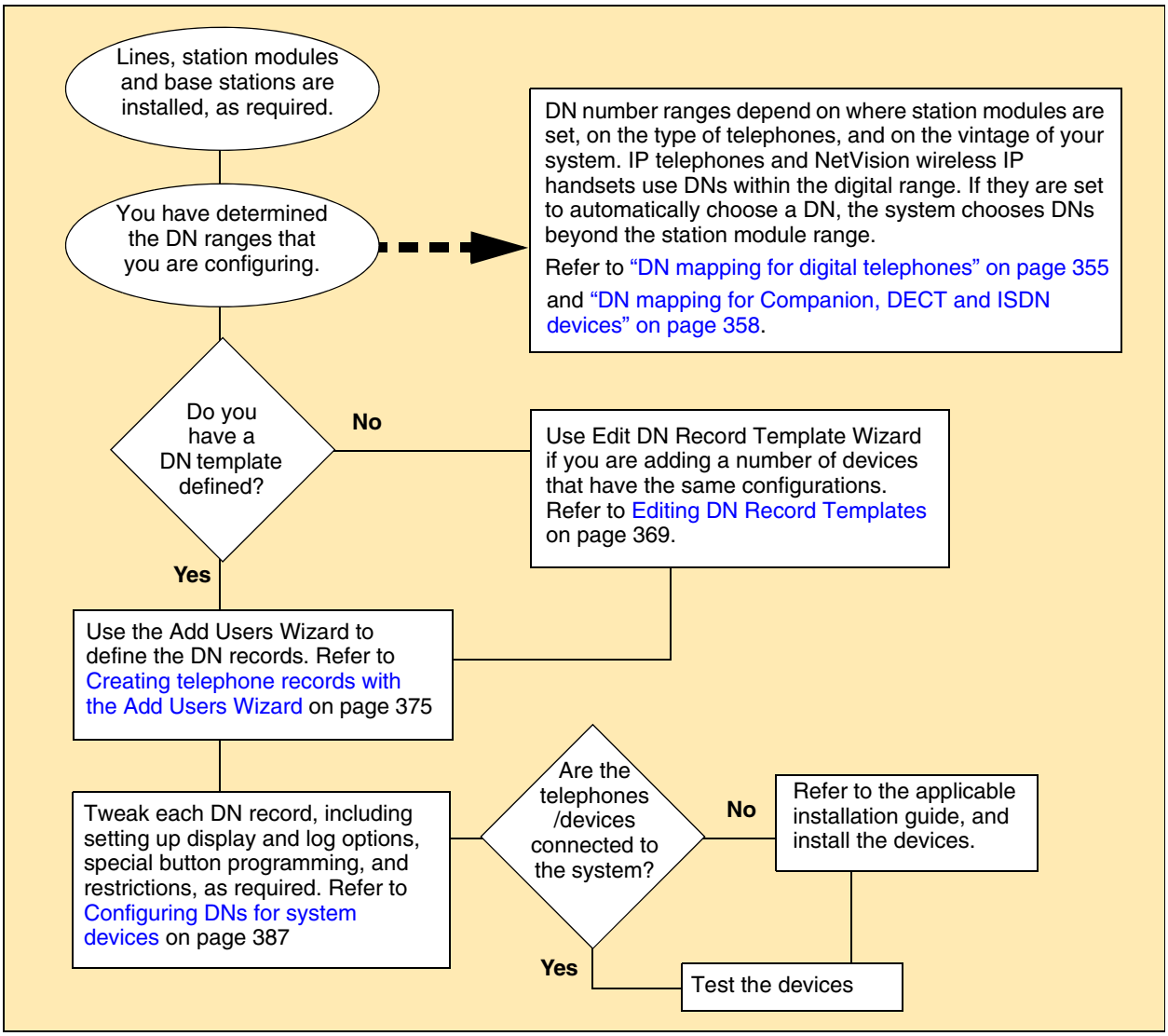
The new BTS Doorphone, which uses the M7324 model name, has separate installation and configuration guides.

IP telephones require the programming described in this section, but they also have specific IP configuration parameters, which are described in the *IP Telephony Configuration Guide*.

Understanding the configuration process

The following process map provides an over-all view of how to set up telephone configurations.

Figure 108 Process map: Configuring DNs for system devices



Note: References in this document to *terminal*, *set,* and *telephone* all refer to telephones that are compatible with the Business Communications Manager system.

DN mapping for digital telephones

Use the following tables to determine which DNs can be assigned to your telephones if your system administrator did not provide you with a list of available DNs or did not fill out the Programming Record forms. You will need to determine which media bay modules are installed, and to which DS30 bus number they are configured. Your system administrator can determine this for you, or refer to Chapter 5, "Configuring resources — media bay modules," on page 123.

As a rule, your station modules will be installed starting from DS30 02 and working down.

- Use the first table, below, if you had an existing 2.5 system that was upgraded with the 3.0 or later software.
- Use the second table, below, if you are installing telephones on a brand new 3.0 or later system.

  Note: The tables below are based on a three-digit DN numbering system. The first digit on your system may be different, or you may have more than three digits, however, the sequencing will be the same, unless some DNs have previously been renumbered.

Double Density and DNs

In BCM 3.0 and later software, the system can support double density modules. This means that twice as many DNs can be assigned per DS30 bus when double density modules are installed on the channel.

Upgraded systems: The DN number for upgraded systems goes from the Start DN (default is 221) up to 316 from Bus 02 to 07, respectively. The second level of DNs, then start at Bus 02 (317) and flow consecutively to Bus 07 (472). Refer to the DN chart in "DN chart for upgraded 2.5 systems" on page 356.

New 3.0 or later systems: If you are installing a new 3.0 or later system, the DN numbers flow consecutively. For example, Bus 02 has DN 221 to 253, and so on. Refer to the DN chart in "DN chart for new 3.0 or newer systems" on page 357.

PDD and FDD: If the system is configured to be in Partial Double Density (PDD) (the default setting for version 3.0 and later systems), Bus 06 and 07 only have 16 available DNs. The exception to this is the DN count for the Companion sets, which can use both B-channel*s*, and, therefore, can support 64 handsets when Bus 06 and 07 are fully loaded using a DSM32 set to single density. Refer to "DN mapping for Companion, DECT and ISDN devices" on page 358. You system can bet set to Full Double Density (FDD), in which case Bus 06 and 07 have 32 available DNs, but neither can support Companion.

DN chart for upgraded 2.5 systems

BCM 2.5 systems upgraded to 3.0 or newer software

Module location DS30 bus #[4]	Module offset	Module type (SD = single density; FDD = full double density; PDD = Partial double density)					Customized DNs[1]
		DSM16 or DSM 16+PDD	DSM16+ FDD	DSM 32 or DSM32+ PDD (First 16 DNs for each DS30)	DSM 32+ FDD (offset 0)	ASM8[2]	
02	0 1 2 3	221-236[1]	221-236 or 377-392	221- 252	221-236 and 377-392	221-228 229-236 377-384 385-392	
03	0 1 2 3	237-252	237-252 or 393-408	237- 268	237-252 and 393-408	237-244 245-252 393-400 401-408	
04	0 1 2 3	253-268	253-268 or 409-424	253- 284	253-268 and 409-424	253-260 261-268 409-416 417-424	
05	0 1 2 3	269-284	269-284 or 425-440	269- 300	269-284 and 425-440	269-276 277-284 425-431 432-440	
06	0 1 2 3	285-300	285-300 or 441-456	285- 316	285-300 and 441-456	285-292 293-300 441-448 449-456 (PDD offset 1 and 2, only. 441-456 appear under B2s heading)	
07[3]	0 1 2 3	301-316	301-316 or 457-472		301-316 and 457-472	301-308 309-316 457-464 465-472 (PDD offset 1 and 2, only. 457-472 appear under B2s heading)	

[1] DNs are based on the default, three-digit DN. If your system has another numbering system, make a note of your DN ranges in the Custom DN column.

[2] ASM 8 modules do not have special double density settings. However, on a PDD system, on DS30 06 and 07, only offset 0 and 1 are available.

[3] If you system is set to a 3/5 DS30 split, these DNs are not available to digital telephones.

[5] Each Bus has 32 ports, numbers <bus#>XX (for example: 0201 is the first port on Bus #2). Ports are assigned sequentially to each DN number. However, if you change the DN number of an assigned telephone, the port number remains the same.

DN chart for new 3.0 or newer systems

If your system is a brand new BCM 3.0 or newer system, the DN numbering is consecutive from DS30 02 to 07.

New BCM 3.0 or newer systems

Module location DS30 bus #[4]	Offset	Module type (SD = single density; FDD = full double density; PDD = Partial double density)					Customized DNs[1]
		DSM16 or DSM 16+ PDD	DSM16+ FDD	DSM 32 or DSM32+ PDD (First 16 DNs for each DS30) (offset 0)	DSM 32+ FDD	ASM8[2]	
02	0 1 2 3	221-236[1]	221-236 or 237-252	221-236 and 253-268	221-252	221-228 229-236 237-244 245-252	
03	0 1 2 3	253-268	253-268 or 269-284	253-268 and 285-300	253-284	253-260 261-268 269-275 276-284	
04	0 1 2 3	285-300	285-300 or 301-316	285-300 and 317-332	285-316	285-292 293-300 301-308 309-316	
05	0 1 2 3	317-332	317-332 or 333-348	317-332 and 349-364	317-348	317-324 325-332 333-340 341-348	
06	0 1 2 3	349-364	349-364 or 365-380	349-364 and 381-396	349-380	349-356 357-364 365-372 373-380 (PDD offset 1 and 2, only. 365-380 appear under B2s heading)	
07[3]	0 1 2 3	381-396	381-396 or 397-412		381-412	381-388 389-396 397-404 405-412 (PDD offset 1 and 2, only. 397-412 appear under B2s heading)	

[1] DNs are based on the default, three-digit DN. If your system has another numbering system, make a note of your DN ranges in the Custom DN column.
[2] ASM 8 modules do not have special double density settings. However, on a PDD system, on DS30 06 and 07, only offset 0 and 1 are available.
[3] If you system is set to a 3/5 DS30 split, these DNs are not available to digital telephones.
[4] Each Bus has 32 ports, numbers 0<bus#>XX (for example: 0201 is the first port on Bus #2). Ports are assigned sequentially to each DN number. However, if you change the DN number, the port number remains the same.

DN mapping for Companion, DECT and ISDN devices

Companion, DECT, and ISDN equipment have pre-set DNs that are automatically assigned on a default system.

Table 80 DN mapping for DECT, Companion and ISDN

System version	Equipment	Default DN range	Media Bay Module	DS30
All	Companion	565-596	DTM	6 and/or 7 (only on PDD systems)
updated from 2.0	DECT	501-532	DECT	6 or 7
updated from 2.5	DECT	597-624	DECT	6 or 7
all	ISDN	597-624	DTM or BRI	any

Defining the System DN headings

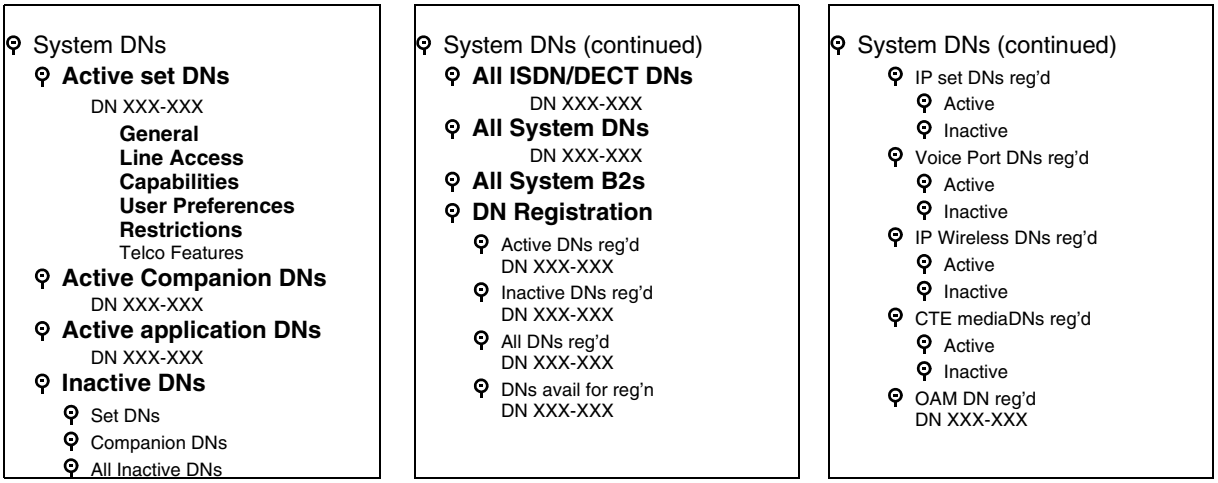
This section provides general information about what DN records and how the Unified Manager categorizes active and inactive DN records.

This section includes information about:

- "The two sides of a DN record" on page 359
- "The System DN headings" on page 361
- "DN Registration headings" on page 363
- "Moving between the Inactive and Active lists" on page 365
- "Deregistering IP and wireless IP devices" on page 366
- "Feature DNs" on page 366
- "Renumbering DNs" on page 366

The System DN heading provides access to the DN records of telephones that are active on the system, records of all the DNs that are available, and a comprehensive list of all DN possibilities. Use the list that is most convenient for what you want to do.

Figure 109 System DNs main headings



The two sides of a DN record

There are two sides to DNs that affect system telephones and equipment.

1 On the system side, each telephone on the network is assigned a DN number, which identifies it to the system. DNs for digital telephones, the M-series telephones and the Business Series Terminal (BST) telephones map to each wire pair on a station media bay module. ISDN, DECT, and Companion devices also require media bay modules to operate. However, they have a specific set of DNs that are not mapped directly to the hardware. Refer to table entry: *Active Companion DNs* on page 361 and table entry: *All ISDN/DECT DNs* on page 362.

IP telephones do not use media bay modules because their connections occur over the internet and directly through the Media Services Card (MSC) within the Business Communications Manager hardware. However, the system uses DN records from the digital range to identify these terminals because their functionality closely mirrors the digital telephones.

As well, certain applications running on the Business Communications Manager are assigned DNs, so that the system can access the application functionality. These would include direct inward access (DISA) DNs, and DNs for CallPilot access. Refer to table entry: *Active application DNs* on page 361.

When you initialize your system with the Quick Start Wizard, you will be asked to specify a DN length and a Start DN.

Warning: Changing DN settings after system startup:

Changes to the **Start DN**, **DN length** or **Received # length** can affect other applications. Make changes to these settings only at system installation, before you do any other programming.

You can also renumber a group of DNs after you initialize your system. For example, if your service provider has given you a specific list of DID numbers, you might choose to ensure the DNs mirror those numbers, to make it easier to administer the telephones. The **DN Renumber Wizard** allows you to accomplish this quickly. Refer to "Using a wizard to renumber telephone DNs" on page 367. If you do this after you have programmed telephones to the DNs, the programming attached to the original DN is transferred to the new DN and the new DN record displays the new port number.

The exception to this is the DECT DNs. If you change DNs in the range you specified for your DECT handsets, you must rerun the **DECT Configuration Wizard** to reset the DNs on the DECT module.

To view your system settings: Click on **Diagnostics, MSC**, then select **Configuration** and click on **System Startup**. This screen displays the telephony template that is active for your system and the start DN that is assigned to the system.

2 The second part of a DN is the content of the DN record. Each DN heading provides a number of parameters that get assigned to the telephone that accesses that DN. Some of these parameters can be copied to other telephones, while others, such as the name of the telephone, and button programming, is unique to each DN record or to each type of telephone.

DN content can be updated at any time, such as if you upgrade the model of telephone. For details about setting up or changing a DN record, refer to the sections "Defining the System DN headings" on page 358 and "Configuring DNs for system devices" on page 387.

The System DN headings

These are the types of headings found under **System DNs**:

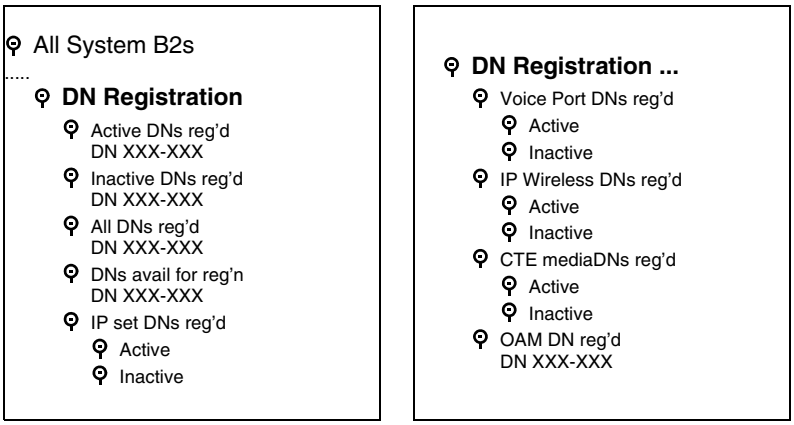
Active set DNs	This list displays only the DNs for digital (M-series and BST T-series telephones), IP telephones, BST T7406 and NetVision telephones that are actually connected to the system and are activated. Use this list when you want to change a configuration, or to remove a telephone. Nortel IP telephone and Symbol NetVision configuration records are located under **Services, IP Telephony**. Although you do not have to assign DNs to configure IP telephony DN records, they will not appear under this listing unless the telephone has been registered to the system. Refer to the *IP Telephony Configuration Guide* for details about configuring IP telephone telephones.
Active Companion DNs	This list displays only the DNs for Companion sets that are registered on the system. Use this list when you want to change a configuration, or remove a telephone. **Note:** This item only appears on the navigation tree for systems set to regions that support the Companion Wireless system. Refer to "Mobility services by region" on page 848.
Active application DNs	This list segregates the list of DNs that are used for running applications, such as Voice Mail, Interactive Voice Response (IVR), and Call Center. These DNs are assigned within the applications that they apply to. You do not need to do anything to any of these DNs, other than to note they are not available for application to your telephones. **Note:** Call DNs (CDN) and IP telephones get their DNs from a common pool. If you set your IP telephony to auto assign DNs, check the DN listings for new telephones to ensure that the DNs are not assigned to CDNs. **Warning:** Changing the settings on these DNs could cause malfunctions in the applications to which they apply.
Inactive DNs	The DNs listed in this section do not yet have telephones assigned to them. This list contains all possible DNs in the digital and Companion ranges. However, you can only assign a digital, BST T7406 or Companion telephone to a DN that is connected to an installed station module. IP telephones and NetVision telephones can use any available DN in the digital range. If IP telephones are set to auto-assign DNs, the system will select DNs that are not likely to be required by installed station modules. **Warning:** Changing the settings on these DNs could cause malfunctions in the applications to which they apply.

Set DNs	This list displays the digital (M-series and BST T-series telephones), BST T7406 cordless, IP telephone, and NetVision DNs that are not assigned or are not active. Use this list to set up new telephones before they are installed in the field. **Note:** If IP telephones are set to auto-assign DNs, the system will select DNs that are not likely to be required by installed station modules. You cannot pre-configure the records since you cannot know which DNs the system will assign to which IP telephone. Once the IP telephone is configured, the DN record moves to the active list, and you can access it from this list to perform the required configurations.
Companion DNs	This list displays the Companion DNs that do not have registered handsets. Use this list to define new handset records.
All Inactive DNs	This list displays all digital, IP, and Companion DNs that are not assigned or are not active. **Note:** Companion DNs can also be used for DECT system that require more than the default number of ISDN and DECT DNs. In this case, when you define the Companion DN as ISDN/DECT, the record disappears off this list and appears on the All ISDN/DECT DNs list.
All ISDN/DECT DNs	This list displays all the DNs that default to ISDN or DECT applications, plus any DNs from the Companion range that have been changed to ISDN/DECT. **Note:** ISDN/DECT DNs can also be used for Companion handsets that require more than the default number of Companion DNs. In this case, when you define the ISDN/DECT DN as Companion, the record disappears off this list and appears on the Active Companion DNs list.
All System DNs	This list displays all possible DNs, regardless of whether a station module is configured to activate them or not. This list begins with the Start DN that was defined when the system was initialized.
All System B2s	This list displays DNs only if your system is set to PDD (partial double density). If the system is set to FDD, these are the second-level (B2) DNs that assign to DS30 bus 06 and 07. This is a read-only list and includes B2 DNs assigned to devices such as Companion handsets. B2 DNs are also used in some call center applications.

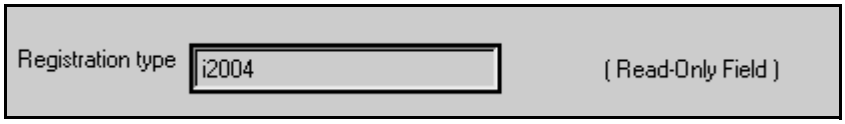
DN Registration headings

The DN records found under this heading indicate whether a device is registered to the system, and, if it is, whether it is active.

Figure 110 Registration DNs, main headings



All registered devices display a **Registration type** field when the DN is selected. This field indicates the type of device.



These are the types that display under the various headings:

Device type	Registration type
i2004	i2004
i2002	i2002
i2050	i2050
i2001	i2001
IP wireless (NetVision)	IP wireless
Voice Port	Voice Port
Unified Manager	Remote admin
Call Center	not used
Voice CTE	CTE media

The devices listed under this heading are registered with the system, but are not necessarily active. This would explain why an application DN, for example, for voice mail, shows up under both the **Application DNs** and the **DN Registration**/**Active DNs reg'd** headings. If the service were to stop, however, the heading under **Application DNs** would disappear and under **DN Registration**, the heading would appear under **Inactive DNs reg'd**.

Following is a brief description of the type of devices found under each heading.

Active DNs reg'd	This is a list of registered DNs that are currently in contact with the Business Communications Manager.
Inactive DNs reg'd	This is a list of DNs that are registered but which are inactive. For example, in the case of a NetVision handset, this might mean that the user has the handset turned off.
All DNs reg'd	This list has all the DNs that are currently registered with the system.
DNs avail for reg'n	This list identifies the DNs that are not yet registered to a device but which could be assigned to a device. Keep in mind, this list may include digital DNs that do not yet have a telephone attached. Check your system DN record to ensure that you do not assign DNs that you might want to assign to a wired telephone.
IP set DNs reg'd	This list has both an active and inactive list. The active list indicates the IP telephones (i-series) that are registered and active on the system. The inactive list indicates the IP telephones that are registered but which are not yet active on the system.
Voice Port DNs reg'd	This list has both an active and inactive list. The active list indicates the voice ports that are registered and active on the system. The inactive list indicates the voice ports that are registered but which are not yet active on the system. Refer to your voice mail documentation for information about setting up voice port DNs.
IP wireless DNS reg'd	This list has both an active and inactive list. The active list indicates the NetVision telephones that are registered and active on the system. The inactive list indicates the NetVision telephones that have registered with the system but which are not active.
CTE media DNs reg'd	If you have any applications that use LAN CTE, the DNs are listed here. This list has both an active and inactive list. The active list indicates the devices using CTE that are registered and active on the system. The inactive list indicates the devices using CTE that are registered with the system but which are not active. Refer to the CTE documentation for information about assigning these DNs.
OAM DN reg'd	This is the DN that is used for remote administration. Refer to the remote administration guides for details about assigning this DN.

Moving between the Inactive and Active lists

DNs move between active and inactive lists based on a number of factors which are described in the two sections below.

From Active list to the Inactive list

A DN record heading will move from the Active list to the Inactive list in the following circumstances:

- A digital or analog hard-wired telephone (M-series or T-series telephones) remains unplugged from a port for more than two minutes.
- An IP telephone is disconnected from the system for more than 30 seconds and the **Keep DN alive** setting for that telephone is set to **No**. If **Keep DN alive** is set to **Yes** for the telephone, that DN remains active until the field is set to No, or the system administrator removes the DN.
- An active IP telephone or wireless IP telephone (NetVision) DN is deregistered through the Unified Manager.
- A Companion handset is deregistered, or a DECT handset is unsubscribed.
- An application such as voice-mail, IVR, or the Unified Manager no longer requires DN(s) and stops communicating on them.
- In the case of a registered DN, if the device or service is turned off.

From Inactive list to Active list

A DN will move from the Inactive list to the Active list in the following circumstances:

- A digital telephone (M-series or T-series) is plugged into the port assigned to the DN.
- An IP telephone (2001, 2002, 2004, 2050) registers to the system and gets assigned a requested or automatically-selected DN. IP telephones also assign to one of the IP keycoded positions, which is indicated in the Device port field.
- An IP cordless telephone (NetVision) registers to the system and gets assigned a pre-programmed DN. The handsets also assign to one of the IP keycoded positions, which is indicated in the Device port field.
- An application such as voice-mail, IVR, or the Unified Manager allocates and starts using DN(s)
- A Companion or a DECT handset is registered to the system.
- In the case of a registered device, if the device or service is started or turned on.

Deregistering IP and wireless IP devices

If you select the DN for an IP telephone or a wireless IP handset (NetVision), which is listed under **Active DNs reg'd**, **Inactive DNs reg'd**, **All DNs reg'd**, **IP set DNs reg'd**, or **IP wireless DN's reg'd** you can deregister that device using the **Deregister** heading under **Configuration** on the top menu. In this case the record will return to the **DNs available for reg'n** list.

- If you run **Deregister** on an active device, you will be prompted to confirm that you understand that the device will be terminated. If you click **OK**, the device is deregistered immediately.
- If you run **Deregister** on an inactive device, there will be no prompts, and the action will occur immediately.

Refer to the *IP Telephony Configuration Guide* for detailed instructions about installing IP telephones.

Feature DNs

The system also uses DNs to define remote access features and Hunt group*s*. These DNs do not show up on the System DNs list.

- **System Access DNs:** For remote access to direct-dial lines, the system requires an Auto DN or a DISA DN. These two settings are found under the Access codes heading. Refer to the remote access information in "Understanding access codes" on page 309.
- **Hunt Group DNs:** Hunt Groups are identified by a unique DN for each defined Hunt group. Refer to Chapter 23, "Configuring Hunt groups," on page 573 for more information.

Renumbering DNs

Your system auto assigns DNs based on the hardware for digital telephones, or, in the case of IP telephones, you choose to auto assign DNs when the telephones register to the system. If you need to change the DN numbers for any reason, there are two ways to do this.

- "Using a wizard to renumber telephone DNs"
- "Change telephone DNs using the Unified Manager"

When you change a DN, the DN record retains the same port number, since the telephone is not being physically moved. The original DN then assigns to the port vacated by the DN that you assign as the *new* DN. If you filled out the DN/Port record in the Programming Records, remember to change the entries.

Using a wizard to renumber telephone DNs

If you need to renumber any DNs, you can use the DN Renumber Wizard, which allows you to renumber a range of DNs.

Follow these steps to use the DN Renumber Wizard to renumber DNs on your system:

1. From the first page of the Unified Manager, click the Wizards button.
2. Enter your system user ID and password, then click **Login**.
3. Click the **DN Renumber** button.
4. On the first screen, enter the range of DNs to change, and the DN with which to start re-numbering.
5. The **Summary** page displays the information you entered. Review and revise, if necessary.
6. Click the **Apply** button.

Warning: DECT DNs

Do not change DECT DNs after the DECT Configuration wizard has run. Doing so will make the DECT handsets inoperable until you reconfigure the DECT module with the DECT Wizard and resubscribe the handsets.

Change telephone DNs using the Unified Manager

The **General Settings** heading also provides access to a screen where you can change the DN setting.

1. Click on the keys beside **Services**, **Telephony Services**.
2. Click on **General settings**.
3. On the top menu, click on **Configuration** and choose **Change DN**.
   The Change DN screen appears.
4. Click beside **Old DN** and enter the DN or group of DNs you want to change.
5. Click beside **New DN** and enter the DN or group of DNs you want to change to.
6. Click **OK** to start the change process.

Warning: DECT DNs

Do not change DECT DNs after the DECT Configuration wizard has run. Doing so will make the DECT handsets inoperable until you reconfigure the DECT module with the DECT Wizard and resubscribe the handsets.

Chapter 14
Configuring DNs using the Wizards

Wizards are used to make telephone configuration faster and more convenient, especially for sites where most of the telephones have the same programming. Each record still may require some adjustments for individual users, but most of the tedious programming can be done using the Wizards.

The wizards used for the task of configuring telephones are accessed through the Wizards button on the first page of the Unified Manager. Refer to "Accessing the Wizards" on page 92.

This section describes these wizards and functions:

- "Editing DN Record Templates" on page 369
- "Creating telephone records with the Add Users Wizard" on page 375
- "Using remote templates" on page 384
- "Changing button programming in the wizard" on page 382
- "Saving wizard pages on your computer" on page 385

Even when you use a wizard, there may be unique settings that need to be added to DN records. For details about each DN heading, refer to the information under "Configuring DNs for system devices" on page 387.

For a general discussion about programming DNs, the DN headings under Telephony Services, System DNs, and how to work with the DN records, refer to the information under "Configuring DN records, an overview" on page 353

Editing DN Record Templates

The Edit DN Record Template Wizard allows you to edit templates to define the user settings that can be used repeatedly to add terminals with the same characteristics. These templates are stored in a file for use with the Add Users Wizard.

This template assumes you have already set up your lines and line pools, performed any DN renumbering that may be required, configured your CallPilot Messaging, and added any required CallPilot Mailbox keycodes that may be applicable. Check your Programming Records for these settings. If this is not the case, refer to "Configuring lines" on page 227 for lines information and "DN mapping for digital telephones" on page 355 for information about which DN records are available for your system. Refer to "Renumbering DNs" on page 366 for details about how to renumber a group of DNS. Refer to the CallPilot documentation for any CallPilot configuration that you require.

Refer to "What you need to know to fill out a template" on page 371 for a description of the information required by this Wizard. You can print out this list and insert the data you want to enter. If you filled out the telephony programming forms in the Programming Records, use the information in those forms to configure the templates. After you fill out the information, follow these steps to run the wizard:

1. From the first page of the Unified Manager, click the Wizards button.
2. When prompted, enter your system user ID and password.
3. Click the **Login** button.
4. Click the **Edit DN Record Template** button.

5. Enter the information on these pages. Use the form in What you need to know to fill out a template on page 371 to ensure you have all the information.
   - Page 1: Choose the template you want to edit
   - Page 2: Enter the Name of template and the type of telephone
   - Page 3: Indicate CallPilot Mailbox information
   - Page 4: Define Line access
   - Page 5: Determine Capabilities
   - Page 6: Determine Call Forward and Hotline settings
   - Page 7: Set up User Preferences and determine button configurations
6. The last page, Page 8, provides a summary of the information you entered.
   If you need to make changes, use the **Back** button to return to the pages where the information was entered and make the corrections, then use the **Next** button to return to the Summary page.
7. Click the **Apply** button.
8. To use a template, refer to "Creating telephone records with the Add Users Wizard" on page 375.

What you need to know to fill out a template

Before you fill out a template, look at the following list and determine what entries you want to include in the template. Photocopy the list and fill it out for each template you want to create. Detailed explanations of the fields can be found elsewhere in this chapter.

Remember that some telephones do not allow some of these features or may have specific configuration requirements. Refer to the relevant sections under "Configuring DNs for system devices" on page 387.

Table 81 Edit DN Record Template information

Screen 1, Edit Template	
• Do you want to edit an existing template?	(Template <number> - <name>)
Screen 2, Template Name	
• Find a name that provides a descriptive clue as to what the template contains.	(Template Name)
• Do you want this template to be used for a specific model of telephone? Use the Multiple listing (default) if the template is meant to apply to more than one type of telephone.	(Set model)
Screen 3, CallPilot Voice Messaging*	
*These settings are only for those systems actually running the CallPilot application. Connection to remote voice mail systems is set under **Telco Features** and **Target lines**. Refer also to "Configuring centralized voice mail" on page 559.	
• Do you want to add a new voicemail mailbox for the set?	No, Yes
If yes . . .	
• Do you want this telephone in the Auto Attendant directory?	(In directory?): No, Yes
• How do you want the telephone to dial out to voicemail? If Pool, you will be prompted to choose a Line pool. If Line, you will be prompted to choose a line.	Pool, Line, Route, None
Screen 4, Line Assignment Refer to "Configuring line access" on page 393.	
• Do you want the Prime line for your telephones to be the intercom button?	(Prime line) None, Pool (A to O), I/C (intercom), Line: <line number>
• How many intercom buttons do you want to assign to the telephone.	(Intercom Keys) 0 to 8
• Which line pools do you want this telephone to have access to for outgoing calls?	(Pool) (enter line pool name) Add
• Which lines do you want this telephone to have access to?	(Line) (enter line number) Add

Table 81 Edit DN Record Template information (Continued)

Screen 5, Capabilities Refer to "Defining device capabilities" on page 405.	
• Do you want a second call to ring if the telephone is busy?	(DND on busy): No/Yes
• How do you want the handsfree feature to be activated?	(Handsfree) None/Auto/Standard
• Do you want to be able to answer a voice call without lifting the receiver or pressing the handsfree button on the telephone?	(HF Answerback) No/Yes
• Do you want to include this telephone into a pickup group?	(Pickup group) None or Group: 1-9
• Which Page zone do you want this telephone to be in?	(Page zone) None or Zone: 1-6
• Do you want to allow the user of this telephone to access the Paging feature?	(Paging) No/Yes
• Which telephone, if any, do you want the telephone to dial when the direct dial number is entered on this telephone?	(Direct dial) None or Set: 1, 2, 3, 4, 5
• Do you want the user to be able to use the Priority call feature?	(Priority Call) No/Yes
• Do you want an active call to automatically be put on hold when another call comes in and is picked up?	(Auto hold) No/Yes
• Do you want lines to this telephone to use an auxiliary ringer?	(Aux ringer) No/Yes
• Do you want to allow the line to be redirected?	(Allow redirect) No/Yes
• Do want redirected lines to ring at this telephone?	(Redirect ring) No/Yes
• Are you programming an analog telephone or a telephone attached through an ATA2 device?	(Receive short tones) No/Yes
Screen 6, Call Forward Refer to "Assigning Call Forward" on page 409.	
• If the call is not answered, where do you want to forward it to? (i.e. voicemail DN)	(Forward no answer to)
• How long do you want forward to delay on a call that is not answered? Note: This field appears after you enter a Forward no answer to DN.	(Forward no answer delay) 2, 3, 4, 6, 10
• If the telephone is busy, where do you want to forward the call? (i.e. voicemail DN)	(Forward on busy to)
• CallPilot Messaging DN (F985)	<DN number> (read-only)

Table 81 Edit DN Record Template information (Continued)

• Do you want the telephone to have access to a Hotline number? Refer to "Assigning a Hotline" on page 411.	(Type) None, Internal/External
If internal . . .	
What is the internal number for the hotline?	(Internal #)
If external . . .	
What route do you want the telephone to use to access the external number?	(Facility) Use prime line, Use routing table Use <assigned line> <assigned line pool>
What is the external number for the hotline?	External #
Screen 7, User Preferences **Note:** Not all of these preferences appear for all models of telephones. Refer to "Defining user preferences" on page 415.	
• What model of telephone are you going to assign using this template? Choose **Multiple** if you want to use the template for different types of telephones, and you do not plan to perform any button programming.	(Set Model)
• When do you want calls to be logged at the telephone? **WARNING:** Do not choose **Log all calls**, as this will affect system speed and function. This setting is used on individual or small groups of telephones for testing purposes. If you allow any logging, ensure that the user activates autobumping (F815) to prevent the log files from filling up and locking.	(Call Log Options) No autologging/No one answered Unanswered by me/Log all calls
• How do you want the users to be able to dial?	(Dialing Options) Automatic dial, Standard dial, Pre-dial
• Choose the language in which you want the telephone to display the prompts. These choices depending on which region profile your system is running. Refer to "Languages" on page 846 for a list that cross-references regions and supported languages.	(Language)
• Choose the level of contrast for your telephone display. **Note:** Does not work for portable handsets.	(Contrast) (1-9)
• Choose how you want your telephone to ring. **Note:** This ring can be overridden by ring types assigned to lines or hunt groups if the values for lines or hunt groups is higher than the ring type, or if the ring type for a line was chosen after you assigned the ring type to the telephone.	(Ring Type) 1, 2, 3, 4

Table 81 Edit DN Record Template information (Continued)

• Do you want to determine button settings for the telephones? Refer to "Programming telephone buttons" on page 419.	(Perform Button Programming) No/Yes
If **No**, — If **Set model** is set to **Multiple**, the button programming for the selected DNs does not change. — If **Set model** on both the Wizard and the system telephone records (DNs) you selected in the Wizard are the same, there will be no change to existing button programming. — If **Set model** on the Wizard and **Set model** in the DNs on the system are different, the Wizard will overwrite the button programming for the telephone record with the default settings for the model specified in the Wizard. The exception to this is if a telephone with a different model identity is already plugged into the system, in which case the wizard will not change the button settings for that telephone.	
If **Yes**, — The button display for the telephone appears. Lines and intercom buttons will be indicated as read-only and cannot be changed. Refer to "Changing button programming in the wizard" on page 382 and "Default button assignments" on page 422. — When you apply this template, all current settings for the specified DNs are overwritten by the wizard entries. — For External Autodial numbers and features that use a dial-out, you will need to know which line, line pool, route, or prime line the telephone will use when the number is dialed.	(Button XX) Blank Internal Autodial External Autodial Feature

Creating telephone records with the Add Users Wizard

Use the Add Users Wizard to change the telephony settings for DN records. You can change a single DN or a group of DNs that require the same settings.

All the DN feature information can be entered when you run this Wizard, or you can indicate a pre-defined template that automatically sets up the DN features. Refer to "Editing DN Record Templates" on page 369. If you filled out the telephony forms from the Programming Records, you can use this information in the wizard if you did not create templates.

If you have a number of Business Communications Manager systems and you want to use the same templates for all your systems, you can define Edit DN Record templates on one system, and then use the remote template setting on the first page to access these templates from your remote systems. Refer to "Using remote templates" on page 384.

To determine what you need to enter for the DNs, refer to "What you need to know about the user" on page 376. Follow these steps to run the wizard:

1. From the first page of the Unified Manager, click the **Wizards** button.
2. When prompted, enter your system user ID and password.
3. Click the **Add Users** button.

4. Proceed through the Wizard and add or change the information, based on what you entered in "What you need to know about the user" on page 376.
   - Page 1: Choose DNs and a local or remote template, of no template.
   - Page 2: Enter Name (maximum seven characters). Choose target line assignment.
     - Target lines: either enter specific target line numbers for all the DNs, or use Auto Assign to allow the system to automatically assign sequential target line numbers
   - The following pages appear if you do not choose a template name on page 1.
     - Page 3: Indicate CallPilot Mailbox information (host system only)
     - Page 4: Line access
     - Page 5: Determine Capabilities
     - Page 6: Determine Call Forward and Hotline settings
     - Page 7: Set up User Preferences and determine button configurations
5. The last page provides a summary of the information you chose.
   If you need to make changes, use the **Back** button to navigate to the page where you need to make changes. Use the **Next** button to return to the **Summary** page when you have completed all your revisions. If you used a template name, you will need to make any changes you require for the telephone settings on the original template.
6. Click the **Apply** button.

7 After you configure the DNs, review each DN record and determine if you need to change any of the other settings. Refer to the detailed programming sections to identify each field under each heading.

Note: Not all DN records have the same programming options. For example, ISDN sets do not have a **Button Programming** option

What you need to know about the user

Before you fill out the Add Users Wizard, photocopy this list and fill out the information for each telephone or group of telephones. If you filled out the telephony forms in the Programming Records, use the information in these forms to answer the questions.

Table 82 Add Users wizard information

Screen 1, Add Users Refer to "Identifying the telephone (General heading)" on page 391.	
• What type of telephone records are you programming: Note: Companion and ISDN/DECT DNs have more limited functionality than Set DNs, therefore, not all the following pages will appear for these settings.	(DN type) Set DNs ISDN and DECT DNs Companion DNs
• What type of telephones are you configuring?	(Set model)
• How many telephones do you want to configure? Select: — a single DN — a range of DNs (hold down <SHIFT> key) — several DNs scattered across the list (hold down <CNTRL> key. **Warning:** When configuring M7324 telephones, ensure that you do not choose any DNs that are assigned to BTS Doorphones, unless the template you choose is for doorphone configuration.	(Choose one or more DNs)
• Do you want to use this wizard to define settings or use a preconfigured template?	(Use settings) Defined in this wizard From a Local DN Record Template From a Remote DN Record Template
If from Local DN Record Template . . .	
• Which template do you want to choose?	(Local DN Record Template) Template <number> - <template name>

Table 82 Add Users wizard information (Continued)

If from Remote DN Record Template . . .	
• What is the IP address for the remote server? • What is the access Port for the remote server? • What is the path to the file on the remote system • Do you want to add this remote repository? Refer to "Using remote templates" on page 384.	(Remote IP_Address) (Remote Port (default: 8600) (Remote Path (default:/) (Refresh button)
Screen 2, Per-DN settings Refer to "Assigning target lines" on page 287.	
• Enter the Name for each DN you are configuring.	(Template Name)
• If you want to create a target line, click the Show Target Lines link and fill out the line information. On the Per DN Settings screen for target lines, click Auto Assign to assign the values you choose in the header menus. Click Clear to exit from target lines. Refer to "Notes about Add Users target lines" on page 381.	Target line fields: Line Public # Appr type Appearances
Note: The following fields do not need to be changed if you applied a template on Screen 1.	
Screen 3, CallPilot Voice Messaging*	
*These settings are only for those systems actually running the CallPilot application. Connection to remote voice mail systems is set under **Telco Features** and **Target lines**. Refer also to "Configuring centralized voice mail" on page 559.	
• Do you want to subscribe a mailbox for the DNs you are defining?	(Enable voicemail?) No/Yes
If yes . . .	
• Do you want to put this telephone into the Auto Attendant directory?	(In directory?) No/Yes
• How do you want the telephone to dial out to voicemail? If Pool, you will be prompted to choose a Line pool. If Line, you will be prompted to choose a line	Pool Line Route None
Screen 4, Line Assignment Refer to "Configuring line access" on page 393.	
• Do you want the Prime line for your telephones to be the intercom button?	(Prime line) None, Pool (A to O), I/C (intercom) Line: <line number>
• How many intercom buttons do you want to assign to the telephone?	(Intercom Keys) 0 to 8
• Which line pools do you want assigned to this telephone?	(Pool) (enter line pool name)Add
• Which lines do you want this telephone to access?	(Line) (enter line number)Add

Table 82 Add Users wizard information (Continued)

Screen 5, Capabilities Refer to "Defining device capabilities" on page 405.	
• Do you want a second call to ring if the telephone is busy?	(DND on busy) No/Yes
• How do you want the handsfree feature to be activated?	(Handsfree) Auto/None/Standard
• Do you want to be able to answer a voice call without lifting the receiver or pressing the handsfree button on the telephone?	(HF Answerback) No/Yes
• Do you want to include this telephone into a pickup group?	(Pickup group) None or Group: 1- 9
• Which Page zone do you want this telephone to be in?	(Page zone) None or Zone: 1-6
• Do you want to allow the user of this telephone to access the Paging feature?	(Paging) No/Yes
• Which telephone, if any, do you want the telephone to dial when the direct dial number is entered on this telephone?	(Direct dial) None or Set: 1-5
• Do you want the user to be able to use the Priority call feature?	(Priority Call) No/Yes
• Do you want an active call to automatically be put on hold when another call comes in and is picked up?	(Auto hold) No/Yes
• Do you want this telephone to have access to an auxiliary ringer?	(Aux ringer) No/Yes
• Do you want to allow the line to be redirected?	(Allow redirect) No/Yes
• Do want redirected lines to ring at this telephone?	(Redirect ring) No/Yes
• Are you programming an analog telephone or a telephone attached through an ATA2 device?	(Receive short tones) No/Yes
Screen 6, Call Forward/Hotline Refer to "Assigning Call Forward" on page 409 and "Assigning a Hotline" on page 411.	
• If the call is not answered, where do you want to forward it to? (i.e. voicemail DN)	(Forward no answer to)
• How long do you want forward to delay on a call that is not answered? **Note:** This field appears after you enter a DN into the Forward no answer field.	(Forward no answer delay) 2, 3, 4, 6, 10
• If the telephone is busy, where do you want to forward the call? (i.e. voicemail DN)	(Forward on busy to)
• CallPilot Messaging DN (F985)	<DN number> (read-only)

Table 82 Add Users wizard information (Continued)

• Do you want the telephone to have access to a Hotline number? Refer to "Assigning a Hotline" on page 411.	(Type) None, Internal, External
If internal . . .	
What is the internal number for the hotline?	(Internal #)
If external . . .	
What route do you want the telephone to use to access the external number?	(Facility) Use prime line, Use routing table Use <assigned line>, <assigned line pool>
What is the external number for the hotline?	External #
Screen 7, User Preferences Note: Not all of these preferences appear for all models of telephones. Refer to "Defining user preferences" on page 415.	
• What model of telephone are you configuring? Choose **Multiple** if you want to configure different types of telephones, and you do not plan to perform any user preference programming.	(Set Model)
• When do you want calls to be logged at the telephone? **WARNING:** Do not choose **Log all calls**, as this will affect system speed and function. Use Log all calls only for testing single or small groups of telephones. If you allow any logging, ensure that the user activates autobumping (F815) to prevent the log files from filling up and locking.	(Call Log Options) No autologging, No one answered Unanswered by me, Log all calls
• How do you want the users to be able to dial?	(Dialing Options) Automatic dial, Standard dial, Pre-dial
• Choose the language in which you want the telephone to display the prompts. These choices depending on which region profile your system is running. Refer to "Languages" on page 846.	(Language)
• Choose the level of contrast for your telephone display.	(Contrast) (1-9)
• Choose how you want your telephone to ring.	(Ring Type) 1, 2, 3, 4

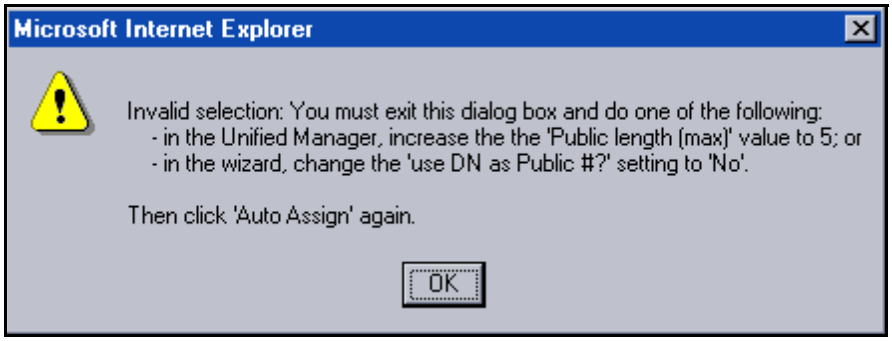
Table 82 Add Users wizard information (Continued)

• Do you want to determine what the button settings will be for the telephone?	(Perform Button Programming) No/Yes
If **No**, — If **Set model** is set to **Multiple**, the button programming for the DNs you selected will not change. — If **Set model** on both the Wizard and the system telephone records (DNs) you selected in the Wizard are the same, there will be no change to existing button programming. — If **Set model** on the Wizard and **Set model** on the system DN record are different, the Wizard overwrites the button programming for the telephone record with the default settings for the model specified in the Wizard. The exception to this is if a telephone with a different model identity is already plugged into the system, in which case the wizard will not change the button settings for that telephone.	
If **Yes**, — The button display for the telephone appears. Lines and intercom buttons will be indicated as read-only and cannot be changed. Refer to "Changing button programming in the wizard" on page 382 and "Default button assignments" on page 422. — When you apply this template, all current settings for the specified DNs are overwritten by the wizard entries. — For External Autodial numbers and features that use a dial-out, you will need to know which line, line pool, route, or Prime line the telephone will use when the number is dialed.	(Button XX) Blank Internal Autodial External Autodial Feature

Notes about Add Users target lines

If you choose to assign target lines to the DNs with the Add Users Wizard, there are a couple of points you need to be aware of:

- If your system DN # length is not the same as your system maximum Public length, you cannot auto assign public numbers when you set up these target lines. If these two parameters are not equal, and you attempt to use Auto Assign when the **use DN as Public #?** field of the Wizard is set to yes, the dialog box shown below appears. Click **OK** to exit the dialog.



  Click **OK** to return to the main screen, and perform whichever process you require.

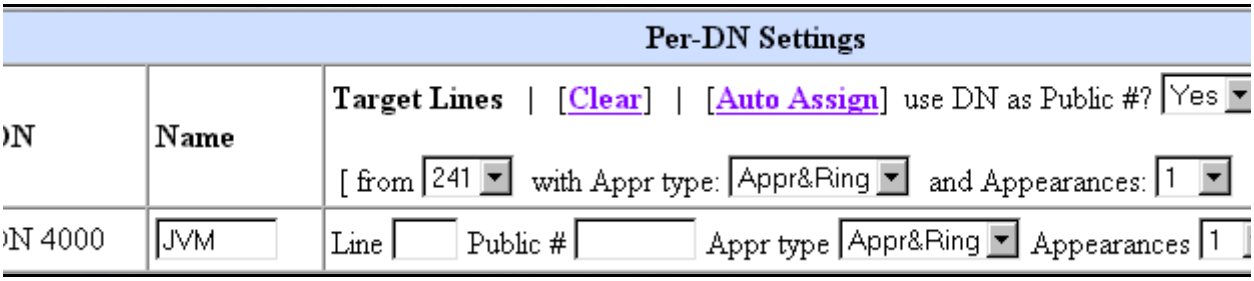
  Note: The value shown in the first bullet will reflect what you need to change the Public length setting to on your system. In the example, the system DN length is 5, so the system prompts that user to change the Public length to 5.

- If you want to change your **Public Length (max)** value to match the DN length, you can do so under **Services, Telephony Services, General settings, DN length, Received # length**. You can then return to the Wizard and use Auto Assign.

Warning: Before you attempt to change this value, ensure that you are aware of the other settings in your system that might be affected by the change.

- If you choose the Auto Assign, the wizard populates the **Line** field for each DN you have specified. Target line numbers are specified in sequence, starting with the number that you chose in the **from** field. The system also fills in the **with Appr type** and **Appearances** values specified at the top of the table.

Figure 111 Target line assignments in the Wizard



If **use DN as Public #** is set to Yes (the default), the wizard populates the **Public #** field for each DN with that DN. If the field is set to No, the **Public #** field will be blank so you can manually entered your preferred number.

Note: The Wizard does not know about any previously assigned target lines. If you choose a range of target lines in which lines have already been assigned to other DNs, the Wizard will still assign that line to a currently-selected DN. If this is not what you want, go into the DN record of the DN you do not want assigned to the line and assign another target line. Also check the target line record, to ensure that it still has the correct Received Number specified.

Changing button programming in the wizard

The button programming section of the wizard only appears if a specific type of telephone has been specified in the wizard or template. The changes you make to this table will overwrite any existing programming for these telephones connected to the ports associated with the DN records that you are changing with this wizard.

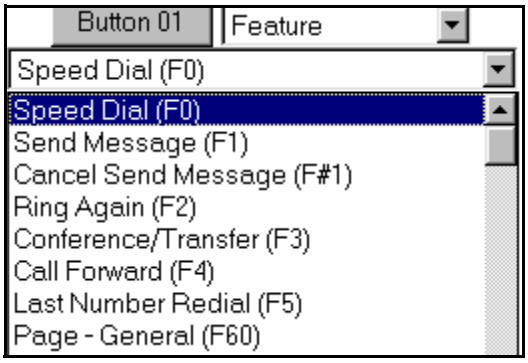
Line buttons, Answer DN, buttons, intercom buttons, and Hunt group designators cannot be reconfigured by the user at the telephone. They also appear as read-only fields in this table, since they are assigned to the buttons in other places. Feature and auto dial can be reconfigured by the user, if they have privileges to change memory buttons ("Defining telephone dialing restrictions" on page 442).

1 In the wizard, open the list beside the button you want to program.

2 Choose the action that you want to program onto the button.

- If you choose **Blank**, any existing programming on that button will be erased and the button will be empty. Use this setting for the buttons where you want to allow the user to indicate speed dial codes or other user-specific options.
- If you choose **Feature**, you will be presented with a list of all the available features. Refer to "Button programming features" on page 865 for descriptions of the available features.

Figure 112 Feature selection

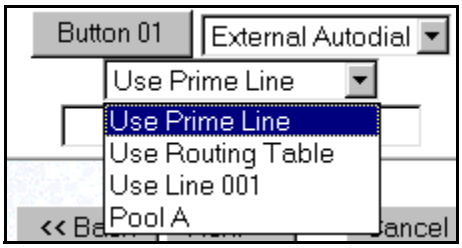


- If you choose **Internal Autodial**, you will be prompted to choose the DN of the telephone that will be dialed.

Figure 113 Internal autodial selection

- If you choose **External Autodial**, you will be prompted to choose the route the dialout will take. In the third field, enter the external dialed number.

Figure 114 External autodial selection



Notes about programming telephone buttons

When you choose a telephone model, then choose Perform button programming on the User Preferences page, the button layout for that telephone appears.

Each button can be programmed to be empty (Blank), to dial an internal or external number, or to activate a feature code. Note that the buttons that are configured for lines, intercom button*s*, and Handsfree are read-only

Refer to "Default button assignments" on page 422 for a description of the default settings for each type of telephone.

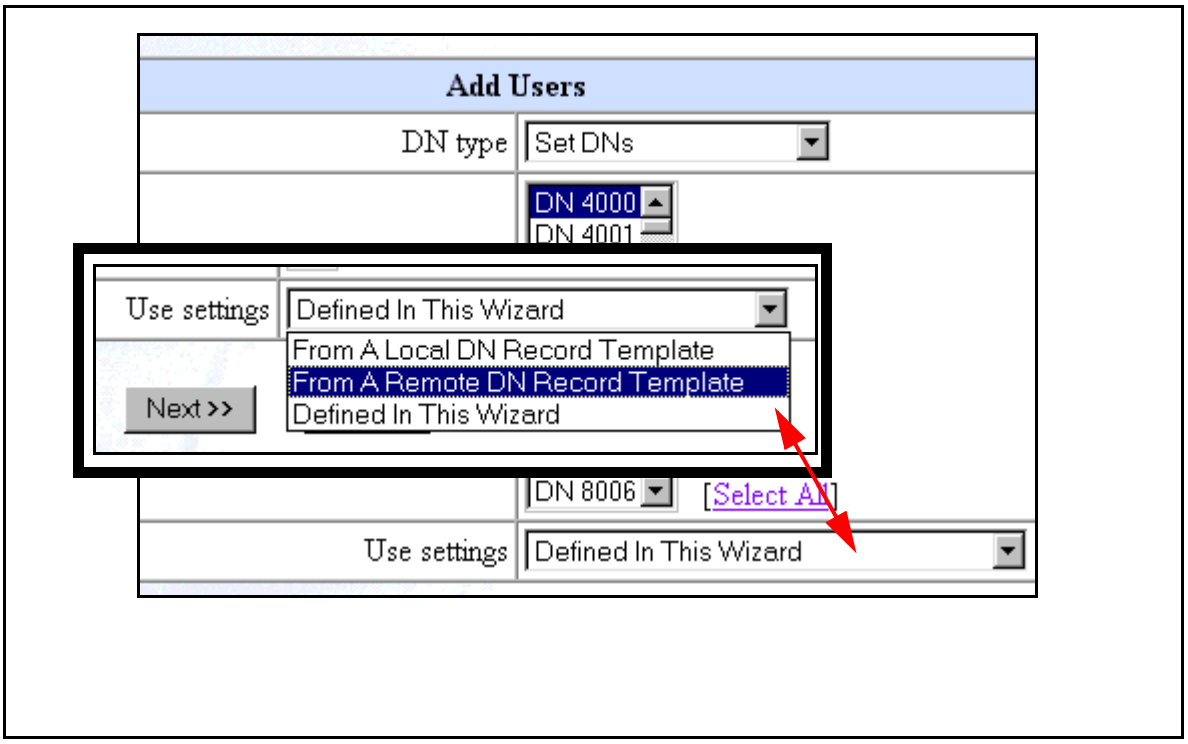
Using remote templates

If you have a group of Business Communications Managers in various locations, and you want to ensure consistency of telephone programming, you can configure DN Record Templates on one system, and then access the templates from the other systems by using the Add Users Wizard.

The templates can be stored on the originating Business Communications Manager or you can move the files to any HTTP web server. However, you can only edit the templates on the Business Communications Manager where they were created.

1 On the first page of the Add Users Wizard you will be prompted to choose the source for the template you want to use to configure telephones.

Figure 115 Add Users first page, choosing remote template



2 When you choose **From Remote DN Record Template**, a new set of fields display, and you will be prompted to enter the following information:

• What is the IP address for the remote server?	(Remote IP_Address)
• What is the access Port for the remote server?	(Remote Port (default: 8600)
• What is the path to the template file on the remote system?	(Remote Path (default:/)
• Do you want to add this remote repository?	(Refresh button)

Once the system connects to the remote site, and selects the template, press **Next** to move forward in the Add Users Wizard.

Saving wizard pages on your computer

If you want to save a copy of your button settings, or the summary page to your computer as part of your Programming Record files, you can use the **View Source** heading under the right-click menu.

1. Right click on the page you want to save.
2. Choose **View Source**.
   A Notepad screen appears.
3. On the Notepad screen, click **File**, then select **Save As**
4. In the **Save In** box at the top of the Save As screen, select where you want to save the file.
5. In the **File Name** box, type in a name for the page.
6. Change the .txt extension to **.htm**.
7. Click **Save**.

View the file through your browser.

Chapter 15
Configuring DNs for system devices

This section describes, in detail, the DN record screens that are used for configuring the telephones and equipment attached to the station modules on the Business Communications Manager screen-by-screen.

Refer also to the process map ("Understanding the configuration process" on page 354).

The Programming Records contain a number of forms for telephone programming. If you fill those forms out beforehand, you can easily create the templates and programming described in this section.

Task: To set up each telephone or device attached to your system:

- Copy settings from existing records: "Copying settings to other DNs" on page 389
- Configure each telephone record individually):
    - — Define the unique name for the telephone. ("Identifying the telephone (General heading)" on page 391).
    - — Assign lines or line pools to each telephone. ("Configuring line access" on page 393)
    - — Determine the Capabilities and User Preferences for each telephone, if applicable. ("Defining device capabilities" on page 405, "Defining user preferences" on page 415, "Programming telephone buttons" on page 419, "Configuring user speed dialing" on page 432)
    - — Determine the restrictions for each telephone. ("Programming restrictions for DNs" on page 441)
- Determine the call display and log options. ("Configuring telco features" on page 445)
- If you have optional voice mail active on your set, you will also see the active phone number for each telephone. ("Voice Mail settings" on page 446).
- If your attendants have M7324+eCAP telephones or BST T7316E+eKIM telephones, you need to assign these systems under "Setting up CAP stations" on page 434.

The Unified Manager navigation tree allows you to refine details about individual telephones. You can also use these DN records instead of the Add Users Wizard ("Configuring DNs using the Wizards" on page 369) to configure telephones. For general information about the DN headings and how to decide which records you need to use, and how to alter the number, refer to the information under "Configuring DN records, an overview" on page 353.

Note: This section discusses telephone DNs in terms of a default Start DN of 221, and a DN length equal to 3. These values are defined during system startup.
However, you can specify a different DN length or change the DN number ranges, depending on your system requirements. Note that changes to these settings, have a wide-ranging affect on your system and should be done before you do any other system programming. Refer to "Renumbering DNs" on page 366 and "Defining DN length" on page 284.

The figure below shows an overview of the top two levels of the System DNs headings. The DN records shown under the second-level headings are similar in structure, as shown in the second figure below, which shows a detailed view of the information under the DNs (DNxxx) headings. For a detailed explanation of the second-level DN headings, refer to "Digital telephones DN record matrices" on page 447.

Figure 116 First and second-level System DNs headings and features

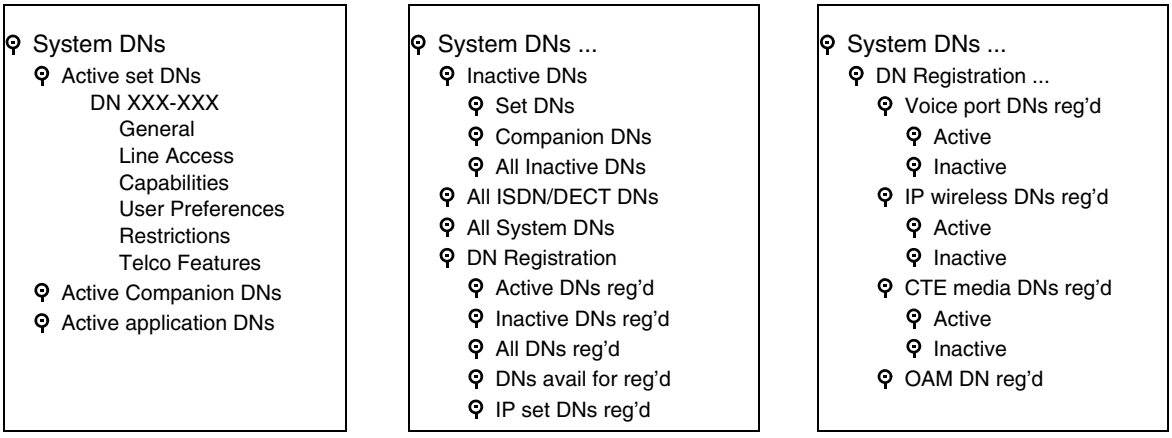
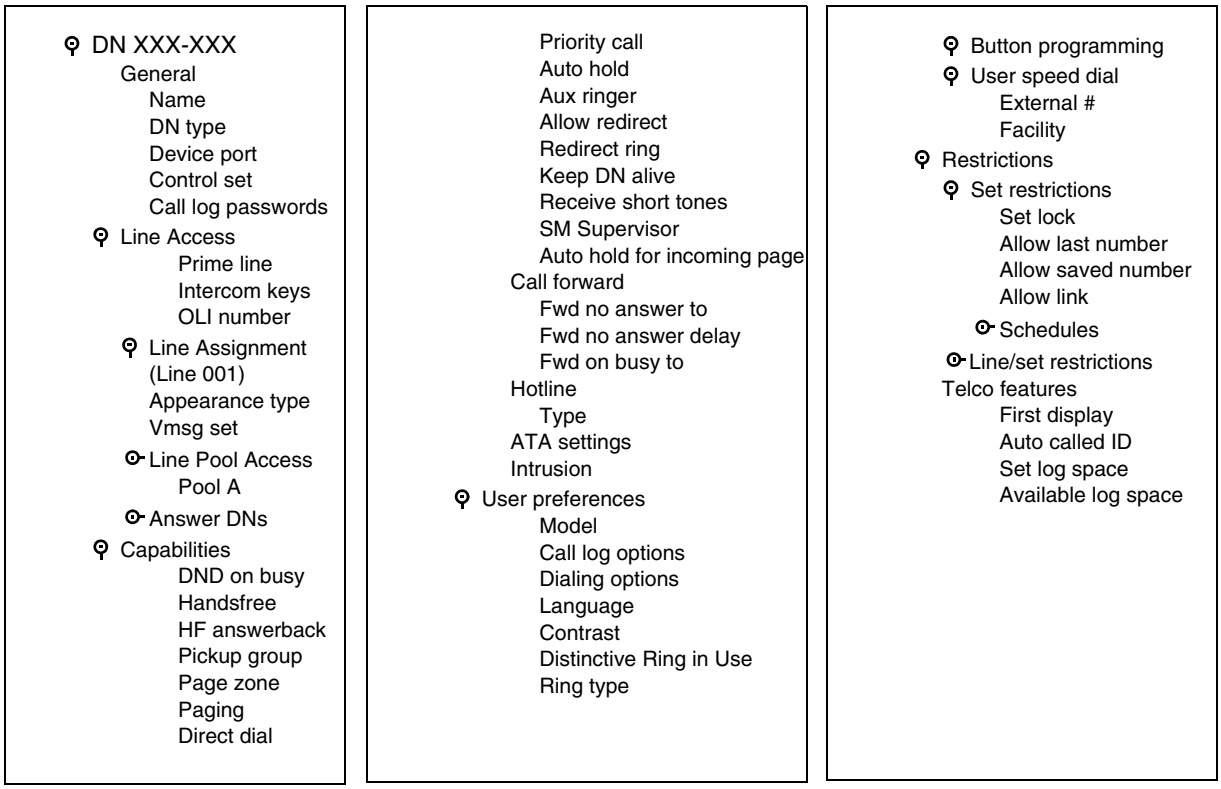


Figure 117 Headings found under typical DNXXX heading



Copying settings to other DNs

The **Copy** command allows you to duplicate programming for a telephone and apply it to another telephone, a range of telephones, or to all the telephones on the system. If information is copied to a record with an assigned telephone, the copy information replaces the existing settings.

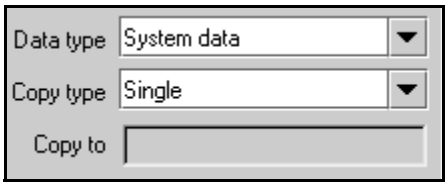
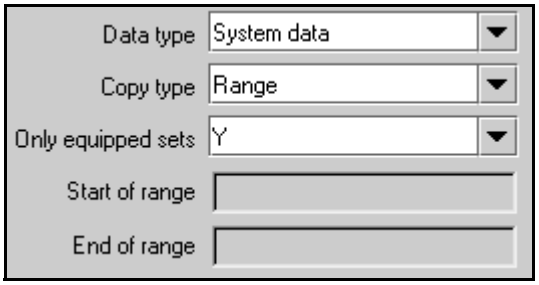
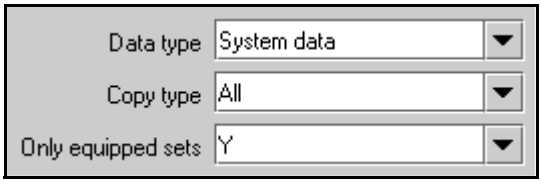
Note: Unique configurations, such as the Name, do not copy over.

Follow these steps to copy telephone configurations:

1. Click on the keys beside **Services, Telephony Services, System DNs,** and **Active Set DNs**.
2. Click the DN number for the record that has the settings you want to copy.
   If you want to copy a specific part of the record, open the DN record and pick the heading you want to copy, such as Line Access or Capabilities.
3. On the **Edit** menu, click **Copy**.
   The following screen appears, depending on which heading you selected:

4 The following table describes the fields that appear in the various copy screens. Choose the settings that will set up the system to copy the information you want to the DNs you specify.

Table 83 Copy values

Attribute	Value	Description
Data type	System data System+user data	Only available on DN copy screen. 
Copy Type	Single Range All	Single: copy to one DN record Range: copy to a range of DN records All: copy to all DN records
Copy to: If Copy type is single	<DN>	Enter the DN of the telephone to which you want to copy the information. Note that if this telephone is a different model than the copy DN, some of the information may not be copied.
Copy to: If Copy type is Range or All	no value	Click in the field. A new screen appears.  
Only equipped sets	Y, N	If you only want to copy information to DN records that have assigned telephones, choose Y. If you want to copy the information to all DN records or DN records specified in the range, choose N.
Start of range/End of Range	<DN>	If you specified a Copy type of Range, enter the first and last DNs of the range of telephones to which you want the information copied.

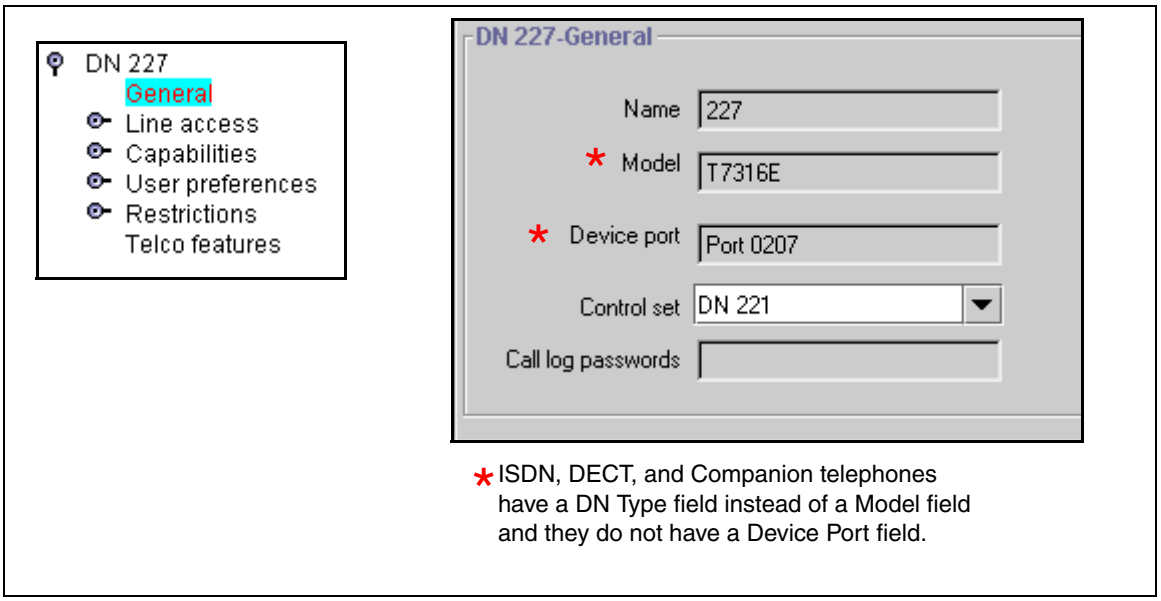
5 Click the **OK** button.
If you are copying to a number of records, this process could take some time to complete. Do not attempt to go in and make any adjustments to individual DN records until the copy process is finished.

Caution: Caller ID set (DNXXX, Line Access, Line Assignment, Line XXX).
You can only enable Caller ID Set (target lines and analog devices attached to an ASM8+) on a maximum of 30 telephones. If you attempt to copy an enabled setting to more than 30 sets, you will receive an error message.

Identifying the telephone (General heading)

The **General** heading allows you to assign the name, the DN type or model, a control telephone, and a call log password for a telephone. This record also shows you which physical port the telephone is accessing.

Figure 118 DN General screen for digital and IP telephones



Follow these steps to identify a new telephone, that has not yet been attached to the system:

1. Click on the keys beside **Services**, **Telephony Services**, **System DNs**, and **Inactive DNs**.
2. Click on the key beside the heading that indicates the type of telephone you are installing. For example, click on the key beside **Set DNs** to program digital telephones or IP telephones.
3. Click the telephone record (**DN XXX**).
4. Click **General**.

5 Use the information in the following table to choose the general settings for the telephone.

Table 84 General record values

Attribute	Value	Description
Name	<up to seven alphanumeric characters>	Use this field to provide a more specific description of the telephone, such as the last name of the user or the location, or the actual extension number if it is different than the DN number.
DN type	ISDN and DECT Companion	This heading only appears for DN records in the following ranges: Companion: 565 to 596 ISDN and DECT: 597 to 624
Model	M7000/T7000 M7100/T7100 M7208/T7208 M7310/T7316 M7324 i2004/i2050 i2002 IPWIs i2001 T7316E Other	This heading appears for telephones in the digital DN range, which starts at the Start DN (default:221) up to DN 433. Choose the setting that is appropriate for the telephone you want to configure. This field will be read-only if the telephone is already attached or registered to the system. • M7000/T7000 (European only), these models are used in specific non-North American markets • M7100/T7100: Use for M7100, M7100N, T7100 telephones • M7208/T7208: Use for M7208, M208N, and T7208 telephones • M7310/T7316: Use for M7310, M7310N, T7316, and T7406 telephones • M7324: Use for M7324, M7324N telephones and BST Doorphones • i2004/i2050: Use for i2004 IP telephones and the Nortel Networks i2050 Software Phone • i2002: Use for i2002 IP telephones • IPWIs: Use for NetVision and NetVision Data telephones • i2001: Use for i2001 IP telephones • T7316E: Use for T7316E telephones and T7316E telephones with KIMs • Other: Analog telephones, model 7000 telephones
Device port	<port number>	This number indicates the port number that this DN corresponds to. A group of port numbers relates to a specific station module installed in your Business Communications Manager. Station modules support 32 ports, which are assigned to the DNs related to each module in sequence. Refer to "DN mapping for digital telephones" on page 355 to see how the DN numbering corresponds to the type of station module that is installed in the system, and to the corresponding Bus numbers and ports for that bus. If you change the DN for a telephone, the port number remains the same. If you physically move a telephone with the relocation feature turned on, the DN transfers to the new port, and the DN for that port transfers to the vacated location. This field is not available or not shown for Companion and ISDN and DECT device records as these devices have a specific range of DNs to which they are assigned. **IP telephone** ports refer to virtual ports on the MSC. These ports are not static. An IP telephone grabs the first available port when it registers with the Business Communications Manager.

Table 84 General record values (Continued)

Attribute	Value	Description
Control set	DN: <any telephone DN> None DN:221<start DN>	The Control telephone attribute allows you to define a DN that will act as a control telephone. A control telephone is used to enable/disable Scheduled Services, such as Restriction Services, for the telephones to which it is assigned. For more information about services, see "Defining service schedules" on page 489. You can assign several control sets for your system but you can only assign one control telephone per DN. * If you changed the Start DN, this number reflects that change. Doorphone note: Ensure this DN does not belong to a doorphone.
	**TIPS: Control telephone** • You must program external lines and telephones with a control telephone to use the Scheduled Services: Ringing, Restriction, and Routing Services. • Nortel Networks recommends that the control telephone you assign for all telephones (DNs) is different from the control telephone you assign for the lines. • You can turn on a service manually or automatically for all telephones controlled by a given control telephone, but you cannot combine schedules. In other words, a service can only be active as normal service or one of the six schedules at any one time. You can have several schedules active, as long as they are using different services. The *Telephony Features Handbook* explains how to use schedules.	
Call Log Password	<four-digit alphanumeric or blank> Read-only.	If the user has entered a password, a row of asterisks appear. If a user forgets their password, you can reset it by erasing the asterisks and leaving this field blank.

Configuring line access

Line access allows you to assign lines or line pools to individual telephones.

This section includes the following information:

You can copy line settings to other telephones using the Copy utility or by using the Edit DN Record Template wizard. If you are assigning the same lines to a number of telephones, you can set up a template with the Edit DN Record Template Wizard, and use the Add Users Wizard to assign the settings to a range of telephones all at once. Refer to "Editing DN Record Templates" on page 369 and "Creating telephone records with the Add Users Wizard" on page 375.

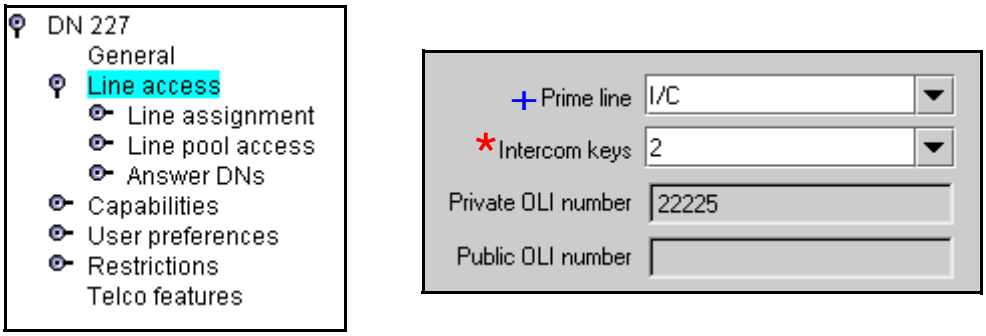
Assigning line access

The prime line for a telephone is the line that is automatically selected when a call is made from the telephone.

The default for all telephones is:

- Prime line: I/C (intercom)
- Intercom keys: 2

Figure 119 Line access fields



* ISDN, DECT, Companion, NetVision, 7000 and 7100 telephones do not have intercom keys

+ BST Doorphone: Ensure this is set to None before you install the BST Doorphone hardware.

If you want to change the prime line or intercom key settings, following these steps:

1. Choose the DN record you are assigning lines to.
2. Click on the **Line access** heading.
3. Use the table below to select the values for line access.

Table 85 Telephone line access fields

Attribute	Values	Description
Prime line	None, Pool (A to O), I/C (intercom), Line: <line number>	Choose the first line that the telephone selects when a call is made. PRI pools are not valid selections for a Prime line. When you assign a line pool as a prime line, the system searches automatically for an idle line in the pool. Also refer to "Rules about assigning prime lines" on page 395 **Doorphone:** Before you install the doorphone hardware, ensure that this line is set to None on the DN record you are assigning to the doorphone.

Table 85 Telephone line access fields (Continued)

Attribute	Values	Description
Intercom (I/C) keys	0 to 8	Assign the number of intercom buttons to a telephone. Intercom buttons provide a telephone with access to internal and external lines, and line pools. Refer to "Assigning intercom (I/C) buttons (keys)" on page 396. Doorphone: Before you install the doorphone hardware, assign one intercom key to the DN record you are assigning to the doorphone.
*Private OLI number		Define the originating line identification number (OLI) which appears on the telephone being called from this telephone over a private network. **Note:** On systems running DID, this field is automatically populated with the DN. Refer to "Private OLI notes" on page 396. On PBX systems, this field is only automatically populated if the DN length and the Received # length are the same. If the DN length or the Received # length are changed so they are different from each other, this field is cleared.
*Public OLI number	<up to 10 digits>	Define the originating line identification number (OLI) which appears on the telephone being called from this telephone over the public network. North America: 10-digit (National) European: digits equal to the public received number length **Note:** If line pools are not properly configured, an extension may use a line with a network range that does not include the OLI of the telephone, causing the network to present an incorrect CLID to the called party.
*If your system allows outgoing name and number blocking, the telephone must have a valid OLI.		

Rules about assigning prime lines

Read the following before you assign Prime lines to a telephone.

- You must assign an external line to the telephone in **Line assignment** before you can assign the line as the prime line to the telephone. Refer to "Determining line assignments" on page 397.
- You must assign a line pool to the telephone in **Line pool access** before you can assign a line pool as the prime line to the telephone. Refer to "Assigning line pool access" on page 402.
- A target line cannot be a prime line for a telephone because a target line is incoming-only.

  Note: Do not assign a T1 DID line as the prime line for a telephone. If assigned, the system treats it as if there is no prime line. The telephone displays the message **Select a line** when you lift the receiver.
- PRI lines are set to Auto Answer. You cannot change a PRI line to Manual Answer.
- VoIP line pools could be used for prime lines, but the lack of dial tone can cause user confusion.

Assigning intercom (I/C) buttons (keys)

The Intercom keys attribute assigns the number of intercom buttons that display on a telephone. Intercom buttons provide access to a maximum of eight internal and/or external lines and line pools. The user presses the intercom key to answer internal calls, or to select a line or line pool to make a call. Lines configured for ring-only also appear on intercom buttons.

- If you assign a prime line to an intercom key, when you press the button or pick up the handset you are immediately connected to a line and a line indicator appears beside the intercom button.
- When you assign each intercom button during programming, it automatically appears on the telephone. The intercom buttons appear starting at the lower-right button, or one button above it if the handsfree feature appears on the telephone. They overwrite any feature or line programming that existed on that button. They do not overwrite answer DNs. Instead, the answer DNs are pushed up one button.
- A telephone requires two intercom button to establish a conference call with two other Business Communications Manager telephones.
- You require only one intercom button if the button is used to make and receive internal calls, and to access line pools. Doorphones only require one intercom key.
- You require two intercom buttons for a telephone with several lines assigned to Ring only.
- Model 7000 and 7100 telephones and analog telephones are automatically assigned two intercom buttons. This allows users to toggle between two active calls using the **Hold** button.

Private OLI notes

Upgrade note: If you upgraded your system from a version of Business Communications Manager previous to BCM 3.6, the Private OLI field will autofill with the DN of the telephone. However, if the DN length of the system was different from the Received number length, this field will be blank after the upgrade.

Other settings to note:

- “Programming access codes” on page 310 (Public/Private DISA DNs and Auto DNs)
- “Defining DN length” on page 284
- “Notes about the Public and Private Received Numbers” on page 290

Determining line assignments

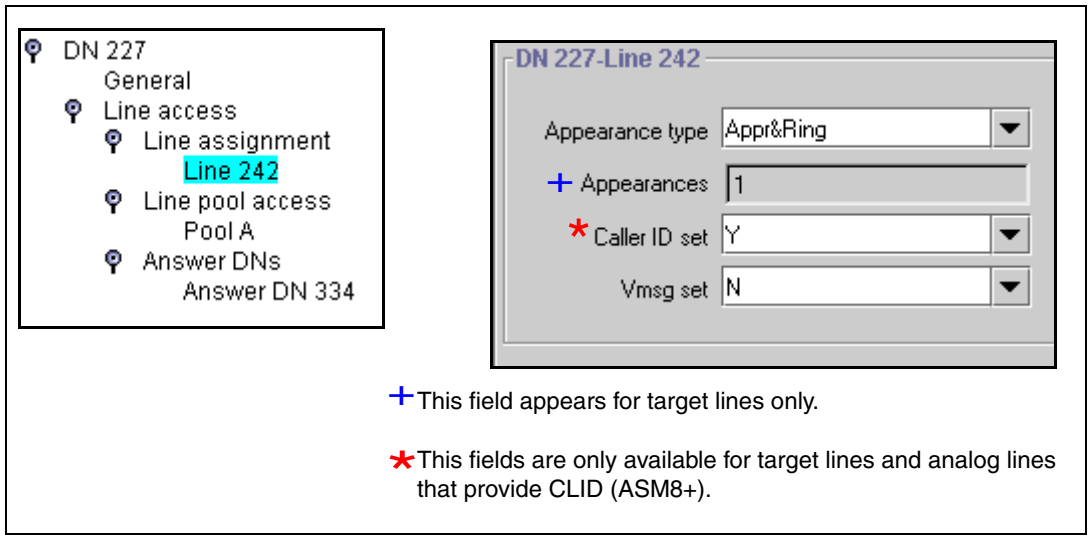
The line assignment setting allows you to assign physical trunks and target lines to each telephone. Target lines are incoming only. Other lines can be used to both make and answer calls if they are configured to do so.

Doorphone note: Before installing doorphone hardware, ensure that you delete any lines, line pools, or answer DNs assigned to the DN record you plan to use for the doorphone.

This section includes the following information:

- "Applying target lines (incoming calls only)" on page 397
- "Assigning lines to telephones" on page 398
- "Notes about assigning lines to telephones" on page 399

Figure 120 Assigning characteristics to each line



Applying target lines (incoming calls only)

You can assign and remove target lines (lines 241 to 492) in the same way that you assign other lines, under **Line access**. You can also use the Add Users Wizard to define target lines. Refer to "Creating telephone records with the Add Users Wizard" on page 375.

Refer also to "Notes about assigning lines to telephones" on page 399.

Assigning lines to telephones

Follow these steps to assign lines to telephones:

1. If you are not already in the DN record, click the telephone DN to which you want to assign a trunk or line.
2. Choose **Line access**. Click on the **Line assignment** heading.
3. Click the **Add** button.
4. Type a line number in the **Line** box.
5. Click the **Save** button.
6. On the navigation tree, click the **Line nnn** you just created.
7. Use the following table to define the line for the telephone.

Table 86 Telephone line assignment fields

Attribute	Values	Description
Appearance type	Ring only, Appear & Ring, Appear only	Select how a call on this line shows on the telephone. If you choose **Appear&Ring** or **Appear only**, you can have as many simultaneous DID calls as there are target line button appearances. If you choose **Ring only**, you can have as many simultaneous DID calls as you have intercom buttons.
		Note: The Business Communications Manager does not support a mixture of Appear only and Ring only appearances for the same line. NetVision, Companion, DECT, 7000 or 7100 telephones default to Ring Only.
Appearances (for target lines, only)	<1-10>	Select the number of appearances of a target line. **Note:** The number of appearances that can actually be assigned to a telephone, depends on how many buttons with indicators are available. Target line appearances cannot overwrite other line appearances, Answer DNs, Intercom buttons or and assigned Handsfree button.
Caller ID set	Y or N	Choosing **Y** enables the telephone to display call information on the telephone display, when it is available for a call. This setting also is used in conjunction with other settings to create the alpha tagging feature. Refer to "Using alpha tagging for name display" on page 455. Choosing **N** disables the telephone from receiving call display information. Choose this setting if the telephone does not have a display, or if you do not want call information displayed to the user. Disabling this function can reduce system resource requirements. This prompt only appears for target lines, and any analog lines that provide CLID through an ASM8+ (North America only). **Limitation:** Only 30 telephones can have this field enabled for any given line.

Table 86 Telephone line assignment fields (Continued)

Attribute	Values	Description
Vmsg set	N or Y	Select whether an indicator shows on the telephone for voice message waiting to an external voice message system. The line must appear on receiving telephone. Note: the Message Waiting Indicator (MWI) is currently supported exclusively by Meridian Mail and CallPilot. **MCDN note:** If your system is part of an MCDN network connected to a Meridian 1 system, and you are using the voice mail system off the Meridian 1, you need to set this field to Y. **Analog lines** connected to legacy analog ASM station modules, and analog telephones attached to an ATA device, do not provide visible message waiting indication. Analog telephones connected to a ASM8+ ((Global) Analog Station Module) support message indicators, if the telephone is set up to receive them.
	Note: Contact your voice message service provider to find out if your voice message service works with Business Communications Manager, or if you have any problems with your service.	

Caution: PRI Lines

Users cannot access PRI lines directly through line appearances.
PRI lines must be part of a line pool.

If you change a digital trunk module (DTM) to PRI, the system automatically removes all existing line appearances for that module.

Notes about assigning lines to telephones

Read these notes for more information about assigning lines to telephones.

- The Business Communications Manager Analog Terminal Adapter (ATA2), or a portable telephone cannot process more than two simultaneous calls.
- Nortel Networks recommends a maximum of four line buttons per telephone. You can program more than four line buttons on a telephone by programming less than four on other sets. For example, you might program 20 line buttons on a receptionist telephone equipped as a CAP station and only two lines on all other telephones.
- You can program a maximum of 93 telephones with a line appearance for a specific line, including VoIP and target line*s*. Above this maximum, you can configure more than one appearance per telephone of a target line.
- Do not assign auto-answer loop start trunks, auto-answer T1 E&M trunks and T1 DID trunks to telephones. If assigned, use them to monitor incoming call usage, or make outgoing calls (auto-answer loop start and T1 E&M trunks).
- You cannot assign a line that is configured to private to another telephone.
- Each line assigned to appear at a telephone must appear at a button with an indicator. The maximum number of line buttons is eight for the model 7208 telephones, 10 for the model 7310 and 7316 telephones, 16 for the 7316E telephone, and 24 for the model 7324 telephone. However, you need to also consider other button requirements such as intercom button*s* and

handsfree buttons. Line programming will not overwrite assigned intercom, Answer DN, handsfree, or Hunt group buttons. Refer to Figure 121.
Intercom buttons, on the other hand, will overwrite anything. (Figure 122) **Note:** You need at least two intercom buttons if you want to use the conference feature.
answer DNs will also overwrite line programming, but not Intercom buttons. Answer DNs appear above intercom appearances on the telephone buttons. If an intercom button is added after answer DNs are assigned, the intercom button pushes the answer DNs up. The top Answer DN overwrites whatever is above it. (Figure 123)

Figure 121 T7316E display button assignment protocol

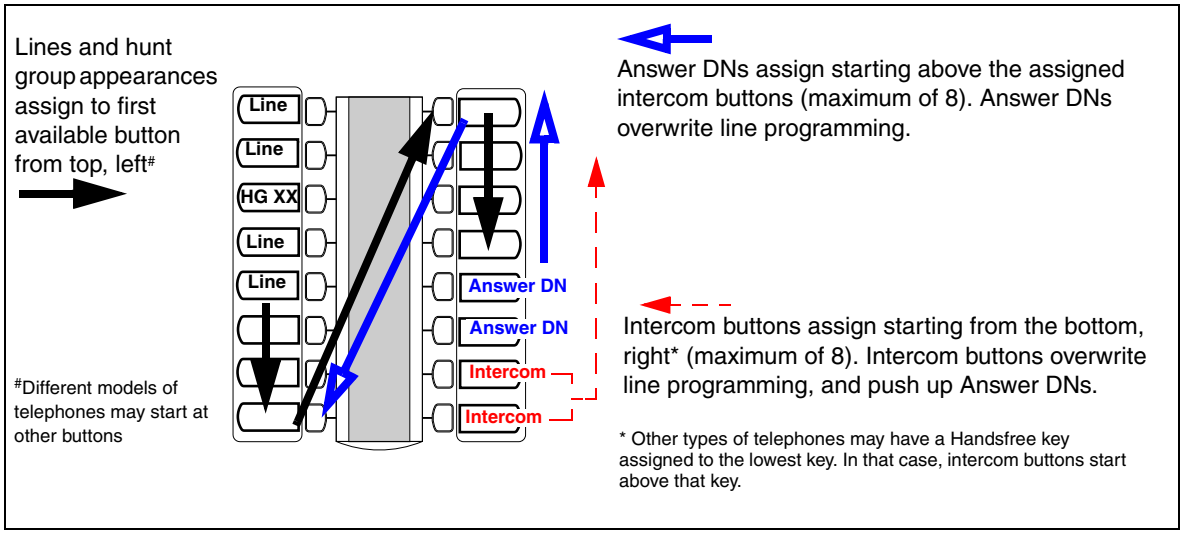


Figure 122 Adding an intercom button

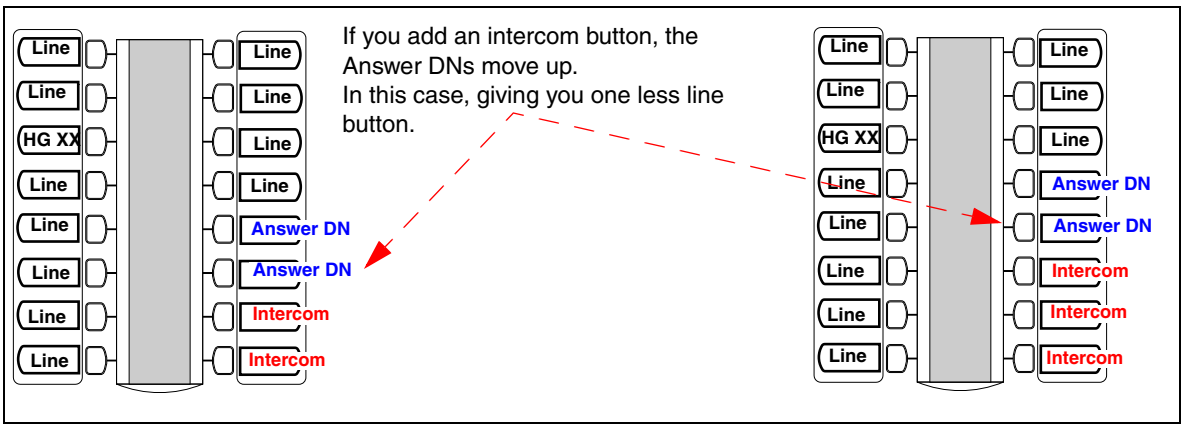
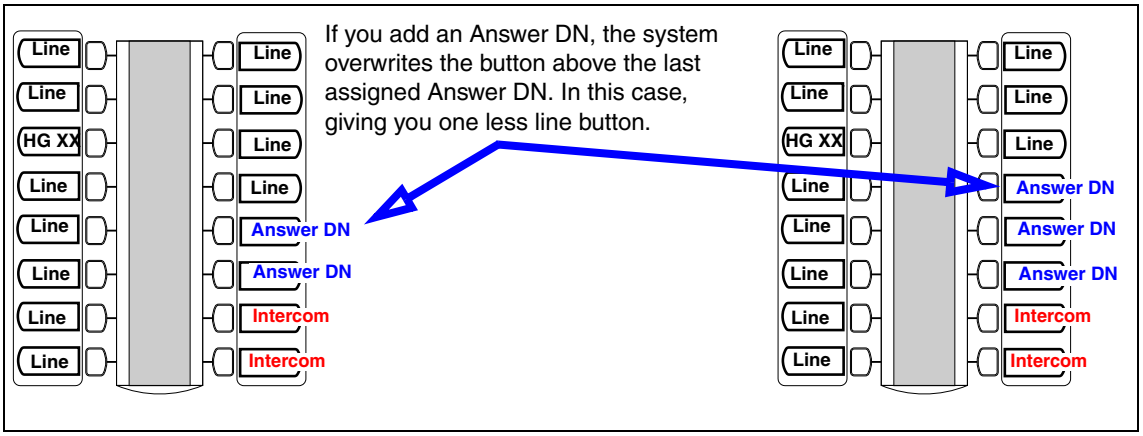


Figure 123 Adding an Answer DN



- If you set a line to Ring only, incoming calls appear on an intercom button. The model 7000, 7100, Companion, DECT, and NetVision telephones are exceptions. They have no line buttons, therefore, you can assign any number of lines, but only two lines can be answered at any one time. Assign the lines on these telephones to ring, otherwise, you cannot detect incoming calls on the lines.
- An enhanced central answering position (eCAP), with one or more modules, provides extra line button support if more than the number of lines are assigned than can assign to available buttons with indicators. The remaining lines assign to buttons on the module. The eKIM also supports hunt group designators, and multiple appearances of the same target line, which flow to the module if there are no available buttons with indicators on the T7316E.

Warning: ECAP programming issue on cold start reboot

If you do a Backup/Cold Start/Restore sequence on your Business Communications Manager, button programming on an enhanced CAP (ECAP) module is lost and the lines assigned to those buttons are assigned to the buttons on the telephone. They replace any programming on the telephone buttons, except answer DNs, intercom buttons, handsfree buttons, or Hunt group appearances. As well, even if there are no more buttons to assign lines to, the system still has the lines assigned to the telephone and it will ring when a call comes in on that line (if appear&ring is configured on the line).

To correct the issue, go into the DN records for the telephone and the CAP/KIM button programming, and reenter the correct programming.

- By using **FEATURE** *81 at the telephone, lines can be moved to other buttons on the telephone, except intercom, answer DN, or handsfree positions, or they can be moved to buttons on the modules on an eCAP. On telephones, the feature or line assigned to the button where the line is moved, moves to the original line button position. On eCAP modules, moved lines overwrite feature programming.

Assigning line pool access

The Line pool access heading allows you to define the line pools that the telephone will be able to access. These shared pools of lines allow many users to use fewer lines for connections where dedicated lines are not practical or not desirable. If all lines in the pool are taken, the user receives a busy signal.

Doorphone note: Before installing doorphone hardware, ensure that you delete any lines, line pools, or answer DNs assigned to the DN record you plan to use for the doorphone.

To assign a line pool to a telephone:

1. If you are not already in the DN record, click the telephone DN to which you want to assign a line pool.
2. Click **Line access**, then click **Line pool access.**
3. Click the **Add** button.
4. Enter a line pool identifier. <Digital and VoIP - **Pool A** to **O>** or **<PRI-A** to **PRI-F>**.
5. Click the **Save** button.
   The line pool identifier appears under the Line pool access heading.

About PRI line pools

PRI lines have special requirements when being used within line pools.

- Six exclusive line pools (PRI-A to PRI-F) are available for PRI lines.
- Only PRI or BRI ETSI QSIG lines can belong to a PRI pool.
- PRI lines cannot belong to Line Pools A through O.
- All lines on a single DTM (PRI) belong to the same pool. Lines from multiple DTMs (PRI) can belong to the same pool if the lines are configured with the same protocol.
- You can assign PRI lines to pools with the **Line type** setting.

Using Answer DNs

You can program a telephone to provide automatic call alerting and call answering for other telephones in the system. The DNs of the other telephones are referred to as answer DNs.

Every answer DN you assign to the telephone automatically designates an appearance on the answer telephone beside a button with an indicator. On the answer telephone, an indicator appears beside the answer button when a call comes in from the original telephone. If the call is answered at the originating telephone, the indicator disappears. Label the buttons to identify the telephone with a name or DN. More than one telephone can have an Answer button for the same DN.

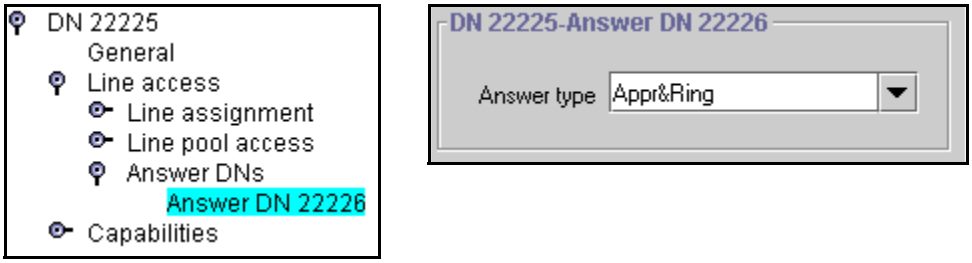
Refer to “Answer DN notes:” on page 403.

Assigning Answer DNs

Use these steps to assign answer DNs to a telephone:

1. If you are not already in the DN record, click the telephone DN to which you want to assign an answer DN.
2. Click the key beside **Line access**.
3. Click on the **Answer DNs** heading.
4. Click the **Add** button located above the navigation tree.
5. In the **Answer DN** field, type in the DN for the telephone you want to be able to answer.
6. Click the **Save** button.
7. On the navigation tree, click on the Answer DN you just created.

Figure 124 Answer condition for Answer DN



8. In the Answer type field, indicate who you want to be alerted to calls coming into the Answer DN telephone.
   - Appr & Ring: The call number or name will display and the telephone will ring
   - Appr only: The call number or name will display.

Answer DN notes:

You can assign a maximum number of eight answer DNs to a telephone. You can also determine what types of calls alert at the telephone where the answer DNs are assigned. Refer to "Answer key levels" on page 461.

You cannot assign answer DNs to 7000 or 7100 telephones because they do not have memory buttons.

Warning: Call Center restrictions: If you assign answer DNs, ensure that the **Answer Key** field (**General settings, Feature settings**) is set to **Basic**.

Mobility sets: Companion, DECT, T7406 telephones: You can twin desk sets with the portable sets by assigning one or more Companion, DECT, or T7406 or NetVision portable DNs to a desk telephone Answer DN.

Companion, DECT, and NetVision portable handsets do not have answer buttons, but you can assign a single Answer DN to each handset. If you want to share a portable telephone among users, use the Call Forward feature to temporarily call forward a desk telephone DN to the handset.

Warning: DECT security notice: Ensure that your DECT handset is set to answer calls manually. Otherwise, if a call is forwarded to the handset with appearance only, the handset will answer the call with no indication to the user that the line is open.

Doorphone note: Before installing doorphone hardware, ensure that you delete any lines, line pools, or answer DNs assigned to the DN record you plan to use for the doorphone.

Hunt group note: A linear Hunt group that has defined an overflow telephone does not support having the overflow telephone assigned as an Answer DN to any hunt group member. If this occurs, the Answer DN will not ring at the hunt group telephone when an overflow condition occurs.

Autodial function: Answer DNs can also act as an internal autodial link to the assigned telephone.

The answer DN must be idle for this feature to work. That is, there must be no active indicator showing beside the button.

The system still sees the key as an Answer DN, and any key press still interacts with other features in that way. Therefore, even though you are making an internal call, any other autodial actions do not occur. As well, none of the autodial visual prompts occur. That means that the button will still only prompt if a call is alerting at the other telephone, based on the answer key level assigned to the system. Refer to “Answer key levels” on page 461.

You can program both an Answer DN and an autodial key for the same DN on the same telephone.

Defining device capabilities

The **Capabilities** headings control how the system interacts with individual telephones, and how the telephones receive calls. The Capability heading itself has a set of feature settings, which determine how much functionality the telephone will have in terms of system features.

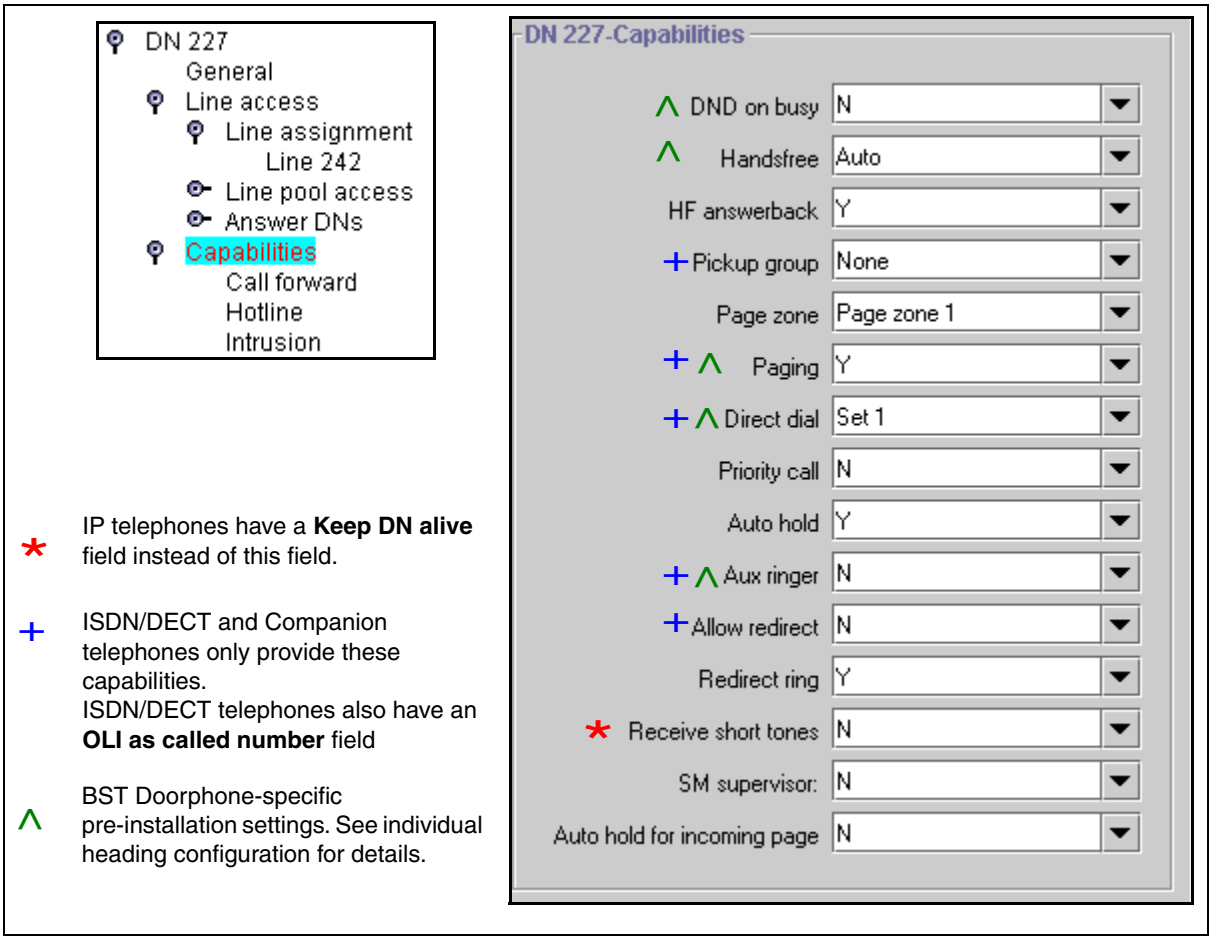
To configure capabilities settings, refer to "Configuring the Capabilities features" on page 406.

Under the Capabilities heading on the navigation tree, there are headings for setting **Call Forward**, **Hotline** numbers, and **Intrusion** controls. If an analog station module is connected to the system or a telephone is connected through an ATA2 module to a digital station module, the ATA settings heading also appears.

Refer to these sections:

- "Assigning Call Forward" on page 409
- "Assigning a Hotline" on page 411
- "Determining analog settings" on page 412
- "Setting intrusion controls" on page 414

Figure 125 Features that define telephone feature capabilities



Configuring the Capabilities features

1. If you are not already in the DN record, click the telephone DN to which you want to assign set capabilities.
2. Click the **Capabilities** heading.
3. Use the information in the following table to configure the telephone capabilities.

Table 87 Capabilities fields

Attribute	Values	Description
DND on busy	N or Y	Defines whether an incoming call rings if you are already on another call. BST doorphone note: Before you install the doorphone hardware, ensure this is set to N in the DN record you want to use for the doorphone.
Handsfree	Auto Standard None	**None**: The handsfree feature is not available to this telephone (7000, 7100, i2001 and any portable handset that does not have an external speaker). **Standard**: The handsfree feature is activated by pressing a button on the telephone. **Auto**: The handsfree feature is activated when the telephone receives a call. BST Doorphone note: Before you install the doorphone hardware, ensure this field is set to **Auto** in the DN record you want to use for the doorphone. **Note:** Handsfree must be enabled on any telephone that allows headsets. For T7316E telephones and DECT handsets, set **Handsfree** to **Auto**. BST T7406: Handsfree must be enabled for this handset to work. **Speaker volume:** Note that the speaker volume returns to the telephone default setting for each new handsfree call.
HF answerback	Y or N	Defines whether you can automatically answer a voice call without lifting the receiver or pressing the Handsfree button. Note: The feature is not available to model 7000 and 7100 telephones and wireless handsets. **Speaker volume:** Note that the speaker volume on the telephone returns to the default volume setting determined by the telephone for each new handsfree call.
Pickup group	None 1 to 9	Assigns this telephone to a pickup group. This is a group where all telephones ring until one is answered.
Page zone	Page Zone (1 to 6) None	Assigns this telephone to a page zone. A zone is any group of telephones that you want to group together for paging regardless of their location. You can assign one of six zones to each telephone. The maximum number of digital telephones in a page zone is 50. The maximum number of digital and IP telephones in a page zone is 60.
Paging	Y or N	Defines whether you can make paging announcements from this telephone. BST Doorphone note: Before you install the hardware, ensure this is set to Y in the DN record you want to use for the doorphone.
Direct dial	Set 1 to Set 5 None	Defines whether you can call the direct-dial telephone from this telephone using the direct-dial digit. BST Doorphone note: Before you install the doorphone hardware, ensure this is set to **None** in the DN record you want to use for the doorphone.
Priority call	N or Y	Defines whether this telephone can interrupt calls or override Do Not Disturb at another telephone.

Table 87 Capabilities fields (Continued)

Attribute	Values	Description
Auto hold	Y or N	This setting determines if the system will automatically put an active call on hold if you answer or initiate another call. If you choose No, the system drops the active call, unless you press the **HOLD** button first, if you answer a call or initiate another call. Default is Yes. The user can change the Auto Hold setting at their telephones by pressing **FEATURE 73.** **SWCA note:** Ensure this setting is set to Yes for any telephones with configured System-wide call appearance (SWCA) keys. Refer to "Configuring system-wide call appearance groups" on page 462.
Aux ringer	N or Y	Determine whether an auxiliary ringer (if installed) rings for incoming calls at this telephone. BST Doorphone note: Before you install the hardware, ensure this is set to N in the DN record you want to use for the doorphone.
Allow redirect	N or Y	Define whether this telephone will allow assigned lines to be redirected. This must be set to Yes to allow call forwarding outside the network (external call forward), including calls to a centralized voice mail system over a private network. Refer to "Line redirection notes" on page 408.
Redirect ring	Y or N	Define whether the telephone rings briefly when a call on one of its lines is redirected by the Line Redirection feature (**FEATURE 84**).
Keep DN alive	N or Y	This feature is only relevant to the i-series IP telephones (i20XX). Y (yes) allows the system to retain an IP telephone DN record even if the IP set becomes disconnected. This occurs as long as the IP set has completed the bootup process. This allows DN-specific features like Call Forward No Answer and Call Forward on Busy to continue to function even if the telephone is disconnected. **WARNING**: If the system is reset, and the IP telephone is disconnected, the feature remains inactive until the telephone is reconnected. **Note:** A delay of about 40 seconds occurs between when the IP telephone is disconnected and when Keep DN alive becomes active. During this period, incoming calls get a busy signal or are rerouted to the prime set, depending on system programming. The delay also occurs when the IP telephone is reconnected to the system. N (No) allows the DN record to become inactive if the IP telephone is disconnected, which produces a `Not in Service` prompt if any of the special features, such as Call Forward, are invoked.
Receive short tones	N or Y	Analog equipment that is connected to the system with an internal or external analog terminal adapter (ATA2), responds only to tone dialing signals. If you have analog equipment connected to an extension, set to **Yes**. Otherwise, leave Receive short tones set to **No**.
SM Supervision	N or Y	On two-line display telephones only, you can choose whether the telephone can be used to allow the Silent Monitor feature (*550). Select Y (yes) to allow this feature on this telephone. Refer to "Monitoring Hunt groups" on page 585 for information about setting up the system settings for the Silent Monitor feature, including determining how many telephones can be allowed to use this feature.

Table 87 Capabilities fields (Continued)

Attribute	Values	Description
Auto hold for incoming page	N or Y	N = if the telephone is active when a page comes in, the page will be put on queue until the user hangs up Y = if the telephone is active when a page comes in, the call is automatically put on hold and the page proceeds. **Note: Business Series Terminals (BST) telephones:** • **Condition:** This setting is Y, active call on mute when the page comes in. • **Results after page:** the call comes off hold, but is no longer muted.
OLI as Called Number		ISDN/DECT only.

Line redirection notes

This feature allows you to send your external calls to a telephone outside the office. You can decide to redirect all, or just some, of your external lines.

Warning: You redirect lines at a telephone, but after redirection programming, the lines redirect for the entire system.

Warning: While you are programming Line Redirection, you do not receive any indication of calls that do not actually ring at your telephone.

Warning: Be careful about redirection loops. For example, if you redirect your lines to your branch office and your branch office redirects its lines to you, you can create a redirection loop. If these calls are long distance, significant toll charges may result.

You can redirect only lines that appear at line buttons on your telephone. Since T7100, Companion, DECT, and NetVision telephones do not have line buttons, you cannot use this feature on those telephones. Also, you cannot use the feature on any telephone connected to an ATA2 or ASM (analog station modules).

You can answer the telephone if it rings while you are programming Line Redirection, however, none of the call handling features are available until the feature times out. If you need to use a feature to process the call, quit Line Redirection programming by pressing **FEATURE**. Do not press **RELEASE** or you disconnect the call you are trying to redirect.

In some conditions, callers can experience lower volume levels when you redirect calls to an external location.

Assigning Call Forward

The **Call Forward** setting under **Capabilities** allows you to define how the system handles calls when the call is unanswered or the line is busy.

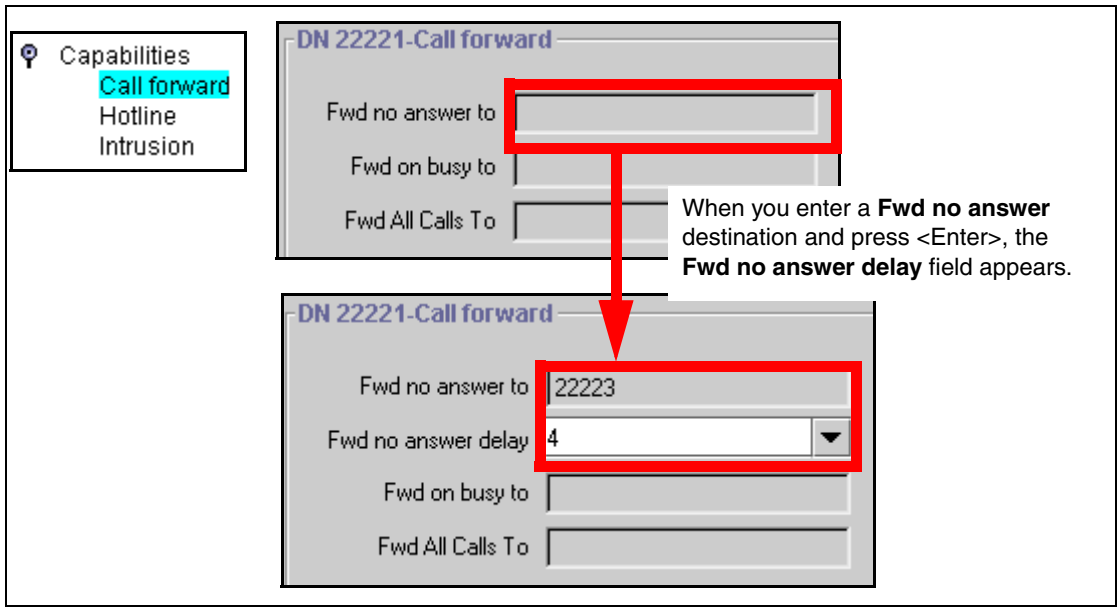
You can enter internal numbers, external numbers, and routing codes to process these calls. For instance, if your voice mail system is on a Meridian system, you would call forward unanswered calls to that number. The number you enter must include access codes, if required for network access.

BST Doorphone note: Before you install BST doorphone hardware, ensure that these fields are blank in the DN record you are planning to use for the doorphone.

Use these steps to set up the Call Forward feature on a telephone.

1. If you are not already in the DN record, click the key beside the telephone DN to which you want to assign Call Forward properties.
2. Click on the key beside **Capabilities**.
3. Click on **Call forward**.
   The Call forward screen appears.

Figure 126 Configuring call forward



4 Use the information in the following table to configure the call forward settings.

Table 88 Call forward fields

Attribute	Values	Description
Fwd no answer to	up to 24 digits	Enter the number to which you want to redirect unanswered incoming calls.
Fwd no answer delay	2, 3, 4, 6, 10	Define the number of rings before the system forwards an unanswered call. This heading only appears after you enter a Call Forward No Answer number and press **Enter**.
Fwd on busy to	up to 24 digits	Redirect incoming calls when this telephone is busy with another call.
Fwd all calls to	up to 24 digits	This setting is the same as using **FEATURE** 4 at a the telephone. When this feature is active, all calls to this telephone are forwarded to the destination entered in this field. If you are forwarding calls to a remote location, ensure that you include the required destination/access codes. A user can press **FEATURE** #4 to cancel this feature.

Private network, call forwarding voice mail: If you want to call forward to a voice mail system attached to an external system, you must treat the calls as call forward to external numbers. As well, **Allow redirect** must be set to Y (Yes) under **Capabilities**.

DPNSS notes

(UK only)

DPNSS lines connected to an Embark switch perform call redirection using the Call Forward feature to create a tandem link back to the switch.

Before you program Call Forwarding on lines on an Embark switch line, ensure that:

- The DTM is configured to DPNSS and the Host Node switch connection is set to Embark.
- Both real channels and virtual channels are provisioned.
- Destination code or line pool code are programmed for the DPNSS to Embark link.
- **Allow redirect** must be set to Y (Yes). This field is also located under **Capabilities**.

During telephone programming for **Call Forward No Answer** and **Call Forward on Busy**, when you enter the **Forward to:** digits, the system does a validation check with the switch on the number. If the validation does not succeed, the system displays one of the messages shown in the following table.

Table 89 Embark validation error messages

Message	Description
The number is invalid or the destination has rejected.	The destination telephone had DND programmed, or it was in an programming session.
There are no free virtual channels available for validation.	You either did not set up enough channels or there were no more available.
Destination may be out of service, no response received.	The system could not connect to the remote system.

Assigning a Hotline

The **Hotline** heading under **Capabilities** allows you to define a telephone number that automatically dials when you lift the receiver or press the Handsfree button on a telephone.

ISDN terminals, DECT handsets, NetVision: This feature is not supported for this equipment.

BST doorphone: Before you install the BST doorphone hardware, ensure there is no hotline assigned.

Use these steps to define an internal or external Hotline number.

1. If you are not already in the DN record, click on the key beside the telephone DN to which you want to assign a hotline.
2. Click on the key beside **Capabilities**.
3. Click on **Hotline**.
4. Use the information in the following table to configure the hotline setting for a telephone.

Table 90 Hotline values

Attribute	Values	Description
None		The telephone does not automatically dial any number.
Internal	Internal # Direct dial set DN:	Define the internal telephone you want to access. Direct dial set: Will automatically dial a telephone on the system defined as a direct dial telephone DN: the DN of the telephone that gets automatically dialed when the user picks up the handset
External	External # **Facility Value:** Use line nnn Use prime line Pool code Use routing table	Enter the complete call number for the external telephone you want to access. Enter the line you want the call to use. (This cannot be a target line.) **Use line nnn**: Refer to line assignment for this telephone. **Use prime line**: Refer to the General record for this telephone. **Pool code**: Refer to the line pool assignment for this telephone. **Use routing table**: Refer to the routing tables. The destination code for that table must be part of the External #.

Determining analog settings

The settings for analog devices under **Capabilities** allow you to define general settings for equipment connected to an analog media bay module or through an Analog Terminal Adaptor (ATA2), which connects an analog device to a digital media bay module (DSM). These settings apply to analog DNs only and are available to telephone DNs in the digital telephone range only.

Details about how to use an analog telephone are included in the *Analog Telephone User Guide*.

Note: These settings only appear if an analog station module or an ATA device is actually connected to the system.

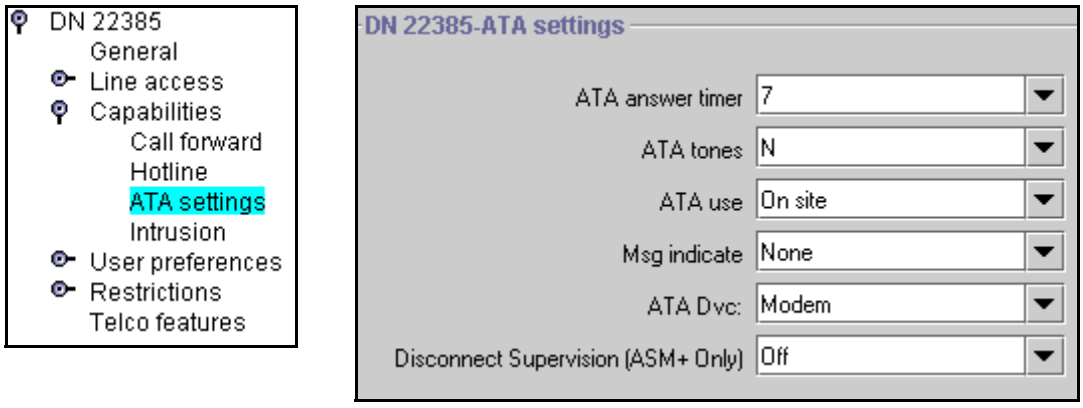
Follow these steps to configure the ATA settings:

1 If you are not already in the DN record, click the key beside the telephone DN to which you want to assign ATA settings to.

2 Click on the key beside **Capabilities**.

3 Click on **ATA settings**.
The ATA settings screen appears for that DN.

Figure 127 ATA settings for a DN



4 Use the information in the following table to configure ATA settings.

Table 91 ATA settings

Attribute	Values	Description
ATA answer timer	3, 5, 7, 10	Select the length of delay between the last digit you dial and when the ATA 2 device is ready to receive DTMF tone.
ATA tones	N, Y	N: No tones occur when a message is received (use for data equipment). Y: Tones occur when a message is received (use for analog telephones).
ATA use	On site Off site	Select the location of the ATA 2. **Note:** Only the ASM8+ supports off-site analog telephones.
Msg Indicate	None Tone Lamp	Tone sends a Message Tone through the telephone receiver when you receive a message. Lamp turns on the Message Lamp when you receive a message. (Refer to "MWI tone/lamp matrix" on page 413.)

Table 91 ATA settings (Continued)

Attribute	Values	Description
ATA Dvc	Modem Telephon	Default: Modem Devices connected to the system through an ATA can have connectivity issues over BRI/PRI lines. To alleviate this, you can specify the type of device attached to the analog line. **Modem** supports 3.1 Khz audio, which requires a higher quality of service on the ISDN trunks which modems and FAX machines require for reliable information transfer. If the trunks cannot provide the higher level of service, the call will fail. **Telephon** supports speech paths, which require less quality on the trunk; if used for FAX and/or modem, information transfer would be unreliable.
Disconnect Supervision (ASM8+ only)	N Y	Default: N If you have a modem or fax machine that does not automatically disconnect when the caller disconnects, you can set this field to Y and the system will disconnect the line from the device once it receives the disconnect signal from the far end. This feature is supported only by ASM8+ modules and only on the North American profile.

Tips: If you have a modem or fax machine, keep the ATA answer timer delay short. If a call to a fax machine or modem cannot connect, shorten the delay. If an individual dials the number for a fax machine or modem, make the delay a little longer.

MWI tone/lamp matrix

The following table outlines the availability of MWI signals for analog telephones on Business Communications Manager Systems.

Table 92

	ATA2	Norstar ASM via FEM	Norstar ASM-MW via FEM	ASM	ASM8+
Systems running software versions previous to BCM 3.6					
MWI tone	No	No	NA only	No	NA only
MWI lamp	No	No	NA only	No	NA only
Systems running BCM 3.6 or newer software					
MWI tone	Yes	Yes	Yes	Yes	Yes
MWI lamp	No	No	NA only	No	Yes
NA = North America					

Setting intrusion controls

If the break-in feature is allowed on any private network MCDN lines (PRI SL-1) assigned to the telephone, you need to define the level of intrusion for each telephone. This determines if the user can use the feature, and to what degree. This heading is found under **Capabilities**.

Follow these steps to set Intrusion levels.

1. If you are not already in the DN record, click on the key beside the telephone DN to which you want to set an intrusion level.
2. Click on the key beside **Capabilities**.
3. Click **Intrusion**.
4. In the **Protect lvl** field, choose an access level.
   There are four levels of access:

   - None — feature is turned off, user cannot break in on any calls
   - Low — user can only break into calls on other telephones with low level protection
   - Med(ium) — user can break into calls on other telephones with low and medium-level protection
   - High — user can break into calls on all other telephones with this feature

Defining user preferences

The User preferences headings allow you to program the same settings that users can perform at their telephones. These options are only available to digital/analog sets, IP telephones, and BST T7406 telephones.

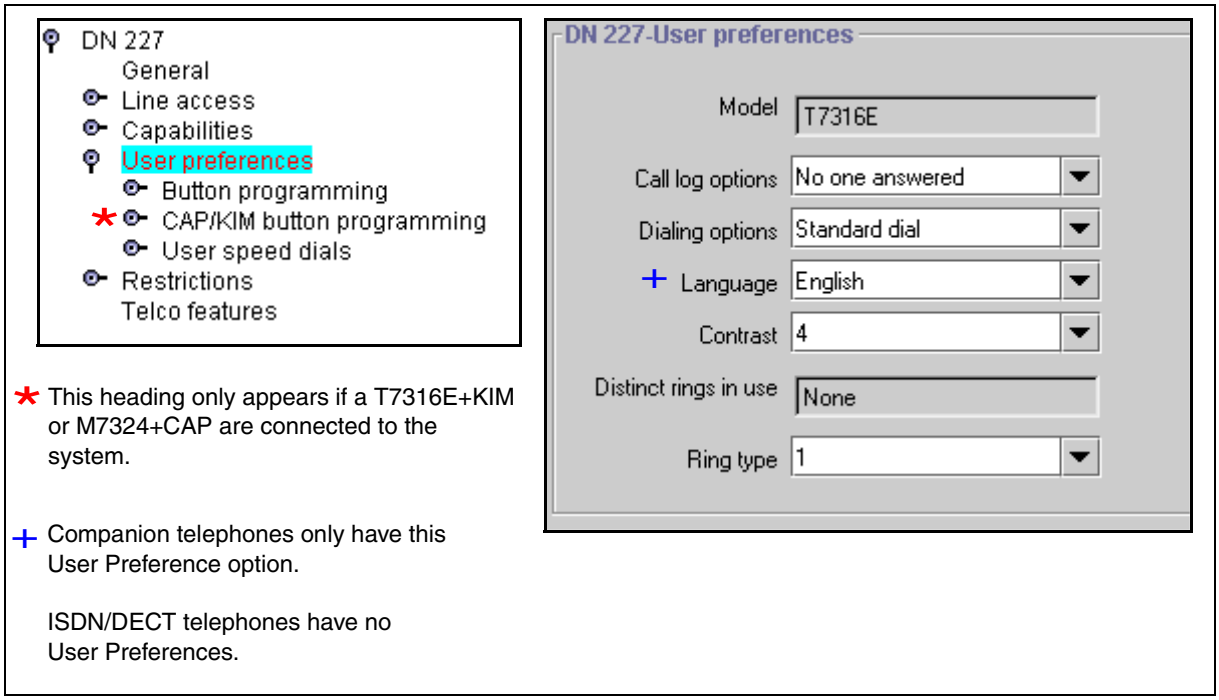
Notes about portable handsets:

- ISDN, DECT and Companion telephones do not have user preferences.
- Feature programming for the NetVision telephones occurs through a separate configuration process, with the exception of 10 programmable buttons, which are specifically used for two intercom positions, and eight SWCA key positions. Programming performed by users at their own sets, takes precedence over these settings. User telephone programming and feature programming for the NetVision telephones is described in the *IP Telephony Configuration Guide* and the *NetVision Phone Administrator Guide*.

This section includes information about:

- "Configuring user preferences" on page 416
- "Programming telephone buttons" on page 419
- "Configuring user speed dialing" on page 432
- "Setting up CAP stations" on page 434

Figure 128 User preference telephone settings



Configuring user preferences

Use these steps to program user preferences for a telephone.

1 If you are not already in the DN record, click the key beside the telephone DN to which you want to assign a user preferences.

2 Click the **User preferences** heading.

3 Use the information in the following table to configure user preferences.

Table 93 User preference choices

Setting	Values	Description
Model	M7100/T7100 M7208/T7208 M7310/T7316 T7316E M7324 i2004/i2050 i2002 IPWls i2001 T7316E	If you have not yet attached a telephone, choose the model of the telephone. This will create a number of defaults based on the telephone capabilities. This setting reflects whatever you set on the General page. Refer to "Identifying the telephone (General heading)" on page 391. This field will be read-only if the telephone is already attached or registered to the system. • T7310 also refers to the cordless T7406 telephones. • IPWls (**IP W**ire**l**ess) refers to the NetVision telephone • T7316E indicates both a stand-aloneT7316E telephone and a T7316E telephone connected to one or more KIMs (Key Indicator Modules). • T7324 also refers to the BST Doorphone
	Companion ISDN/DECT	These telephones have their own set of DN records. • Companion: refers to the Companion handsets • ISDN/DECT refer to DECT handsets or any ISDN equipment
	Other	This heading is used for the following types of devices: • analog telephones • Intl set (European only), is used for other types of compatible telephones used in specific non-North American markets, such as the model 7000 telephones
Call log options	Log all calls, No autologging, No one answered Unanswered by me	Select how you want the telephone to handle logging calls. **Log all calls**: All calls are noted in the call log. **No autologging**: No calls are automatically logged. **No one answered**: Unanswered calls are not logged. **Unanswered by me**: Unanswered calls are not logged. Refer to: "Call log notes" on page 417. Refer to the *Telephony Features Handbook* for information about using Call logging.
Dialing options	Standard dial Pre-dial Automatic dial	Determine how the telephone handles dialed information. **Standard:** Pick up the receiver and dial. **Pre-dial:** Dial the numbers, then pick up the receiver to allow the telephone to dial the number. **Automatic dial**: Use for devices like fax machines where you want the number to dial out without external cues. Note: Not all devices show all three options.

Table 93 User preference choices (Continued)

Setting	Values	Description
Language	Languages displayed are based on telephone capabilities and system software	Choose the language for the telephone display prompts.
Contrast	1, 2, 3,4, 5.....9	Adjust the contrast of the display.
Distinct rings in use	read only	This read-only field indicates the distinct ring patterns are currently in effect, if any, on any lines, telephones, or Hunt group*s* on the system. Refer to the Warning below.
Ring type	1, 2, 3, 4	Select a distinctive ring pattern type for the telephone. Default is 1.
	**Warning:** If you assign a distinctive ring pattern to a telephone, and that distinctive ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None. If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. Refer to "Assigning Trunk/line data" on page 236 for information about assigning a distinctive ring pattern to a line. You can also assign a distinctive ring pattern to a Hunt group. Refer to "Identifying a Hunt group" on page 575.	

Call log notes

If your system has the appropriate equipment, and you subscribe to the call information feature supplied by your service provider, you can record information about calls received from an external line. ISDN service packages that come with calling line identification (CLID) can supply the same feature.

Note: Your cordless and wireless telephones may not support this feature, or they may only support some of the functions of the feature.

Call Log creates a record of incoming external calls to a telephone even if the telephone does not have that line assigned. For each call, the log can contain:

- sequence number in the Call Log
- name and number of the caller
- indication if the call was long distance
- indication if the call was answered and by whom
- time and date of the call
- number of repeated calls from the same source
- name of the line on which the call came

Call Log can help to

- keep track of discarded calls or calls not answered
- track patterns for your callers (for example volume of calls and geographic area of calls)
- record caller information quickly and accurately
- build a personal telephone directory from log items

Information such as long distance indicator and the caller name and number, may not show in the log. The appearance depends on the Call Display services provided by your local telephone company and the local telephone company at the caller end.

Call logging limitations:

- A total of 600 log spaces are shared by all telephones assigned with call log space. To ensure that this list does not fill up and start rejecting logs, ensure that Autobumping is enabled (**FEATURE** 815).
- If you answer the call, then forward it, the call will log only at the forwarding telephone.
- If call forward is set, the calls will be logged at both the forwarding telephone and the target telephone, providing the target telephone answered the call.
- If the call is released by the telephone to which the call was forwarded, only the forwarding telephone logs the call.
- Hunt group calls are only logged once a call is answered.
- If a call is redirected to the Prime telephone, and it is answered at the prime telephone, then the call is logged at both the redirecting telephone and the prime telephone. If the call is answered by the intended telephone, then the call is logged only at that telephone.
- If the telephone is experiences a warm-reset, all log entries are flushed.
- If line has been redirected, calls will not be logged.

Programming telephone buttons

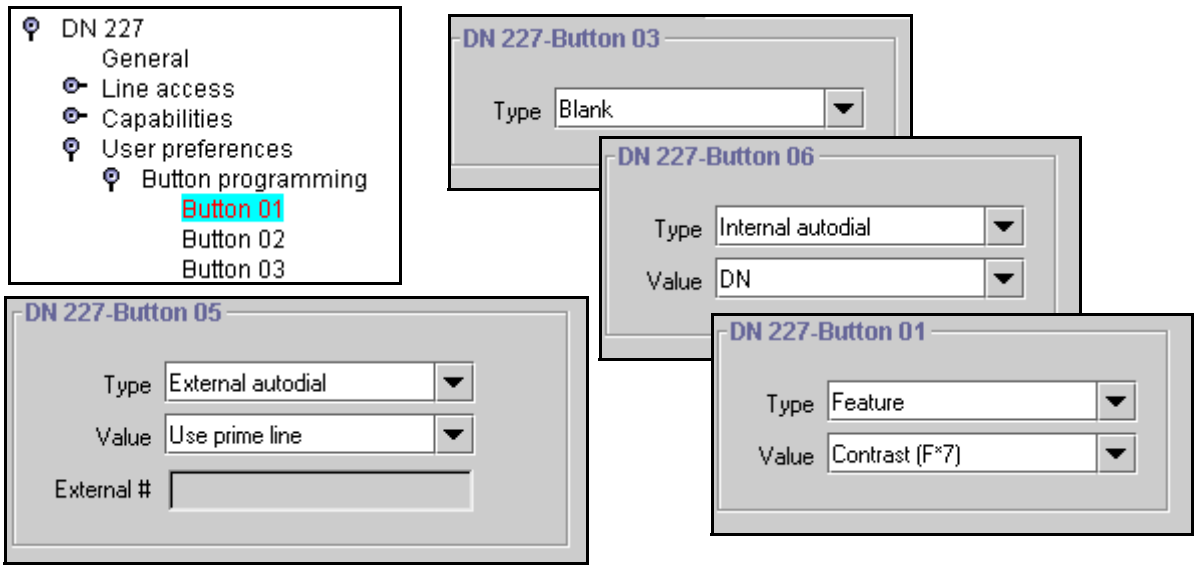
Button programming allows you to program the buttons on a telephone with internal and external autodialers and with programmed feature keys. You also can use these screens to remove programming from a button, making it blank. Assigned line, Hunt group designator, answer DNs buttons, intercom button*s*, and handsfree buttons cannot be changed through these screens. They appear in read-only format under Button Programming. ISDN terminals, Companion, and DECT portable systems do not have feature buttons that are programmable through this heading.

You can also program buttons using the Edit DN Record Templates Wizard or the Add User DN Wizard. Refer to "Editing DN Record Templates" on page 369 and "Creating telephone records with the Add Users Wizard" on page 375.

To view the default button mapping for each type of telephone, refer to "Default button assignments" on page 422.

To view a list of the available feature selections, refer to "Button programming features" on page 865. Note that not all telephones support all the features in this list. The *Telephony Features Handbook* describes how to use the features.

Figure 129 Button programming options



Configuring buttons from the DN record

Follow these steps to program the buttons on a telephone.

1. If you are not already in the DN record, click the key beside telephone DN where you want to program button features.
2. Click the key beside **User preferences**.
3. Click the key beside **Button programming**. The list of available buttons appears.
4. Click the button number that you want to program.
5. Use the information in the following table to configure button preferences.

Table 94 Button programming choices

Setting	Values	Description
Type	Blank Feature Internal autodial External autodial	Choose the type of feature that you want to program on the telephone buttons. Blank means that nothing is programmed on the button. Example: new KIM modules have all blank buttons when they are first installed.
Value field:		
Feature	<*feature name*>	Use the arrow to choose the feature you want to program on the button.
Internal autodial	<*Internal DN*>	Enter the DN number for the internal telephone you want the telephone to dial by pressing this button.
External autodial	Use prime line Pool Use routing table Use line	Choose the route the telephone will dial through. **Prime line**: the prime line assigned to the telephone **Pool X**: one of the pools assigned to the telephone **Routing table**: enter the destination code with the external phone number **Use line X**: one of the lines assigned to the telephone
External #		
External autodial	<*dialing codes plus dialout string*>	Enter the complete dial sequence for the external call. This sequence will depend on what you chose for the route in the Value field.

Notes about button programming:

- The number of available button positions, will depend on the model of telephone that you are programming.
- New button programming will overwrite any memory button programming performed at the telephone by the user. Conversely, any changes to memory button programming performed by the user at the telephone, after button programming, will overwrite memory keys programmed under Button programming or CAP/KIM button programming. The screens will reflect these changes.

- The T7316 telephone has disjointed button numbering, because it is patterned after the M7310 button programming, but has fewer available buttons. However, the Button programming heading shows all the keys available for a model 7310 telephone. Refer to the default button programming section and ensure that you program the correct button numbers. Refer to "T7316 Business Series Terminal button defaults" on page 424.
- IP telephones have three (i2001), nine (i2002) and 12 (i2004) programmable memory keys, as well as a display feature list that can contain up to 10 items. Refer to the *IP Telephony Configuration Guide* for information about setting up this list, and to the *Telephony Feature Handbook* for an explanation about how to use the telephone buttons to access the list. Refer to "IP telephone button defaults" on page 427 for a list of default settings, and the location of the buttons for each telephone. The model 2001 IP telephone has an additional five non-visible buttons that can be programmed with Answer DNs or SWCA controls.
- Although NetVision wireless IP telephones (model: IPWls) do not have any physical line or memory buttons, the DN record for this telephone provides 10 programming spaces to accommodate the SWCA feature and intercom assignments.

Replacing digital telephones

If you unplug a digital or IP telephone, the Business Communications Manager will retain the programming for that DN on these conditions:

- Set relocation is enabled on the Feature settings screen. Refer to table entry: *Set relocation* on page 459.
- The original telephone is replaced with the same model.
- The original telephone is plugged in somewhere else on the system before any other telephone is plugged into the jack from which the telephone was removed.
- IP telephones: Keep DN alive is enabled on the DN record. Refer to table entry: *Keep DN alive* on page 407.

If the KIM attached to a T7316E telephone becomes disconnected, the KIM loses any spillover line programming from the T7316E, and all the buttons revert to either Blank or an Internal autodial.

Button labeling

M-series telephones have paper labels that fit onto the keycaps, and printed keycaps.

T-series telephones have a paper strip of labels that can be customized and printed using the Desktop Assistant or Desktop Assistant Pro application. These applications are located under the Client Applications button on the first Unified Manager web page. Desktop Assistant Pro requires a LAN CTE keycode before it can be used.

IP telephones also have soft display labels. These feature labels can be changed under **Telephony Services, General Settings, Nortel IP Terminals, Feature labels**. The *IP Telephony Configuration Guide* describes this process in detail.

Default button assignments

During startup, the installer chooses one of the available telephony template (PBX or DID). Each profile has a default features set which assigns automatically to the programmable buttons on telephones plugged into the system, unless you configure different settings in the DN record. The default features are listed, by telephone model, in the following sections in this chapter.

Rules of default button assignment

- Line and intercom buttons assigned by default templates can be changed in programming. handsfree and answer DN buttons are not assigned by default. When these features are programmed, however, they are automatically assigned to specific buttons.
- Telephones can have a maximum of eight intercom button*s*. When Answer DNs are assigned, they appear above the handsfree button, if there is one, at the bottom right-hand corner on the telephone. The model 7000 and 7100 telephones, analog telephones, and portable telephones are automatically assigned two intercom.
- Default line button assignment starts on or near the top of the left column and descends. Default button programming does not necessarily provide default line assignments.

  Note: Companion, and DECT handsets do not have buttons that are programmable from these screens.
- Line assignments can be moved by the user to more convenient buttons. Refer to the *Telephony Features Handbook* for details.

T7316E Business Series Terminal button defaults

The default button assignments for the T7316E Business Series Terminal (BST) depend on the template applied. Refer to your Programming Records to identify the current button programming for each telephone or group of telephones.

- This telephone has individual handsfree, mute and headset buttons, located under the dialpad. Handsfree must be set to automatic for these buttons to work.
- The current incoming call on this telephone defaults to the voice path last used. For example, if you answered the previous call using your headset, the next call will come in over your headset.

- Line numbering starts on button 09.

Important note: The T7316E BST telephone buttons are mapped differently than the T7316 BST telephone. Therefore, if you replace a T7316 telephone with a T7316E telephone, the button programming will revert to the default settings for the T7316E, losing any keys programmed by the user at the telephone. Also, settings that are copied from one telephone to the other may be in a different location on the new telephone. This is consistent with how the system behaves if you switch any telephone model for a different model on the same connector.

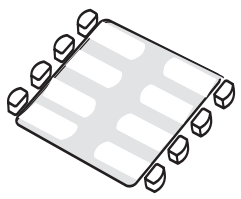
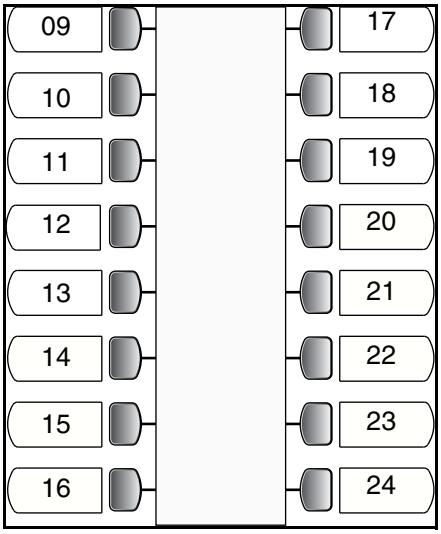
T7316E BST upper button defaults				
	Btn #		**Btn #**	
Contrast	01		05	Blank
Show time	02		06	(DID only) Sys Park
Blank	03		07	Send Message
Blank	04		08	Speed dial

Figure 130 T7316E lower button mapping



T7316E BTS lower button defaults				
Btn #	**PBX**	**DID**	**Btn #**	**PBX/DID**
09	Sys Park	Target line	17	Call Timer
10	Saved No.		18	Ring Again
11	Call Fwd		19	DND
12	Pick-up		20	Transfer
13	Page		21	Last No.
14	Transfer		22	Voice call
15	Time/Date		23	Intercom
16	Receive Msg.		24	Intercom

T7316 Business Series Terminal button defaults

Button mapping for the T7316 BST telephone is unique. Although the button is patterned after the M7310, the T7316 does not have a second level on its upper button group. Because of this, the numbering for the T7316 is not consecutive. Refer to the diagrams below.

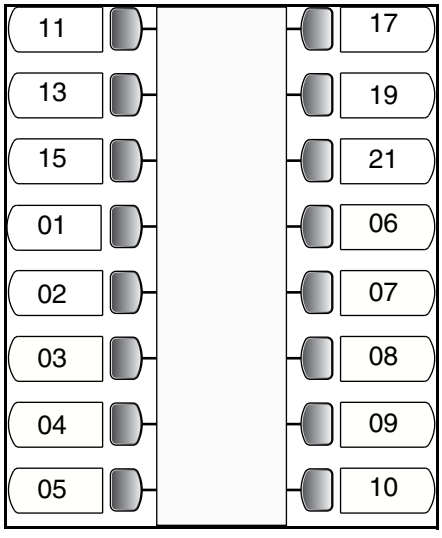
Internal autodial numbers are assigned to buttons 11, 13, 15, 17, 19, and 21 on the main button group. Programmed external line buttons descend down the lower left buttons, starting with button 01. When more than five external lines are programmed, assignment continues on the lower right buttons, starting at button 06.

Important note: The T7316E BST telephone buttons are mapped differently than the T7316 BST telephone. Therefore, if you replace a T7316 telephone with a T7316E telephone, the button programming will revert to the default settings for the T7316E, losing any keys programmed by the user at the telephone. Also, settings that are copied from one telephone to the other may be in a different location on the new telephone. This is consistent with how the system behaves if you switch any telephone model for a different model on the same connector.

The following figure shows the default button number assignments on the T7316 telephone.

T7316 BST upper buttons (PBX and DID) default button settings				
	Btn #		Btn #	
Autodial to 227	23		31	Autodial to 231
Autodial to 228	25		33	Autodial to 232
Autodial to 229	27		24	Autodial to 239
Autodial to 230	29		26	Autodial to 240

Figure 131 T7316 telephone button assignment

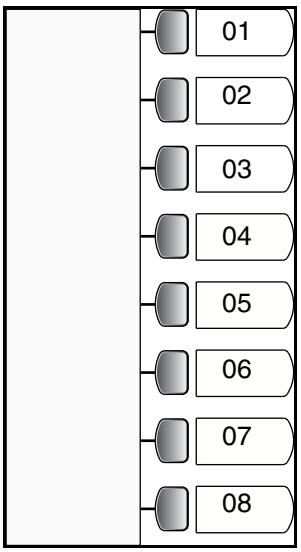


T7316 lower button defaults					
Btn #	PBX	DID	Btn #	PBX	DID
11	Autodial 221		17	Autodial to 224	
13	Autodial 222		19	Autodial to 225	
15	Autodial 223		21	Autodial to 226	
01	DND	Target Line	06	Conference	
02	Transfer		07	Last No. Redial	
03	Call Forward		08	Intercom	
04	Pick-Up		09	Intercom	
05	Page-General		10	Handsfree	

Model 7208 button defaults

The default button assignments for the model 7208 telephones depend on the template applied.

Figure 132 Model 7208 button mapping



Model 7208 default button mapping		
PBX	**Btn #**	**DID**
Pick-Up	01	Target line
Transfer	02	Transfer
Last No. Redial	03	Last No. Redial
Page-General	04	Page-General
Conference	05	Conference
Intercom	06	Intercom
Intercom	07	Intercom
Handsfree	08	Handsfree

Model 7100 telephone button defaults

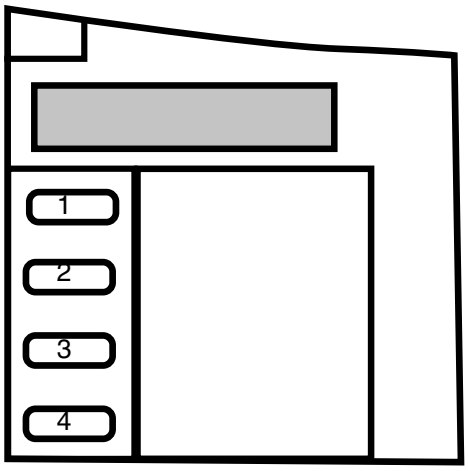
Model 7100 telephones are basic-function telephones with a single-line display. For all templates assigned to 7100 telephones, the one programmable button defaults to **Last Number Redial**.

This telephone cannot use features that require a speaker, such as Page.

Note: The default Page button activates the External Page option (**FEATURE 62**).

Model 7000 telephone button defaults*

Figure 133 Model 7000 button mapping



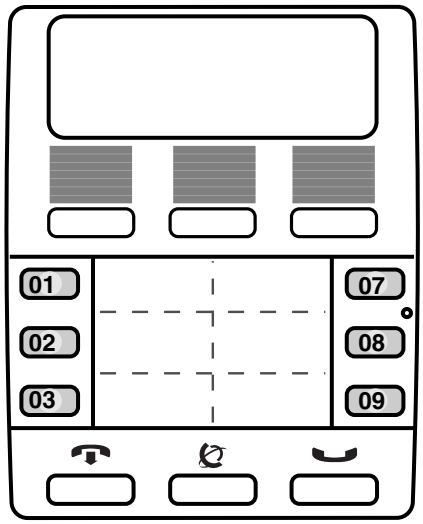
This basic-function telephone has four programmable memory keys (Figure 133) which default to the features shown in the table below. This telephone has no display and does not support features that require a speaker or a display.

* Only available in limited markets.

7000 button defaults		
PBX	**DID**	**Btn #**
Last Number Redial		1
Call Forward		2
Transfer		3
Conference/Transfer		4

T7406 Business Series Terminal button defaults

Figure 134 T7406 button defaults



The BST T7406 cordless handset is based on the T7316 telephone button numbering. However, the T7406 handset only has six memory buttons. These buttons map to specific T7316 button numbers: 01, 02, 03, 07, 08, 09.

Ensure that when you fill out the DN record, which shows 24 buttons for the T7316 telephone, that you only program these buttons. The handset can access any system features except for features that require a speaker, such as handsfree.

T7406 lower button defaults				
Btn #	**PBX**	**DID**	**Btn #**	**PBX/DID**
01	DND	Target line	07	Last No. Redial
02	Transfer		08	Intercom
03	Call Forward		09	Intercom

IP telephone button defaults

The i20XX models have fewer programmable buttons than the T7316 or T7316E, but they have access to a feature menu through the Services key (**FEATURE** *900) that greatly expands quick access to call features. Additionally, IP telephones support the hot desking feature, which allows the user to transfer telephone settings from one IP telephone to another to allow mobility without needing to relocate the physical telephone.

Both the features menu configuration and hot desking password reset are described in the *IP Telephony Configuration Guide*, which describes how to configure these telephones to the system. The *IP Telephony Configuration Guide* also describes how to move the telephones without losing voice mails, how to set the time zone, and how to change the feature labels that appear beside the keys next to the telephone display. The *Telephony Features Handbook* has a section that describes how to use Hot desking and the Services features list.

Model 2004 IP telephone and 2050 Software Phone button defaults

The 2004 telephone and the 2050 Software Phone have six memory buttons beside a display that provides soft labels for the buttons. These telephones also have six other buttons that can be programmed as memory buttons without display.

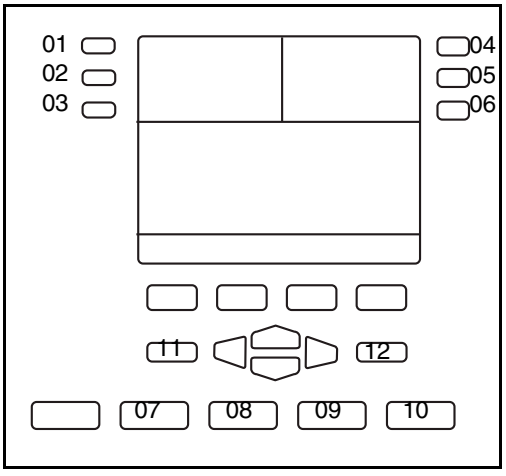


Figure 135 Models 2004/2050 default button programming

i2004 default button assignment		
Btn #	**PBX**	**DID**
01	Call Forward	Line XXX
02	Conference/Transfer	
03	Last # Redial	
04	Page - General	
05	Intercom	
06	Intercom	
07	Blank	
08	Voicemail login	
09	Express Messaging	
10	Service menu	
11	Blank	
12	Blank	

Model 2002 IP telephone button defaults

The model 2002 has four memory buttons beside a display that provides soft labels for the buttons. This telephone also has five other programmable buttons with no display.

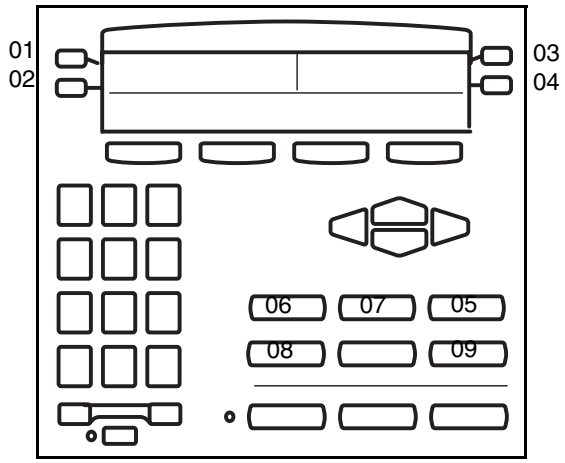
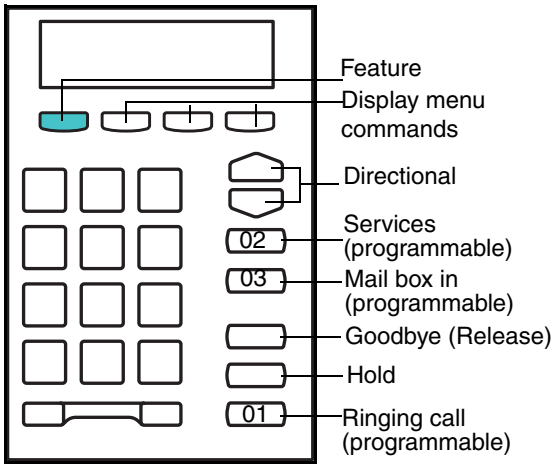


Figure 136 Model 2002 default button assignment

i2002 default button mapping		
Btn #	**PBX**	**DID**
01	Call Forward	Line XXX
02	Conference/Transfer	
03	Intercom	
04	Intercom	
05	Blank	
06	Voicemail login	
07	Express Messaging	
08	Service menu	
09	Blank	

2001 IP telephone button defaults

Figure 137 Model 2001 default button formatting



The model 2001 is a simple version of the IP telephone. None of the programmable buttons have indicator displays, so all incoming calls must be set to ring only. The figure shows the positions of the three programmable buttons and which button number corresponds to each of the three buttons.

Although two intercom lines are assigned to the telephone, there is no visible indicator of the lines, but a light at the top of the telephone blinks. The user presses the Hold key to toggle between two active calls, or to put one call on hold to make a second call.

Handsfree and mute are not available, since this telephone does not have an external speaker. It also does not support a headset. The only indicator on the telephone is the message waiting indicator (MWI) lamp.

Model 2001 feature buttons:

• Four display buttons appear under the telephone display screen. The first button defaults to act as the **Feature** button (green button). The other buttons provide access to menu commands that appear on the display, as with the other types of telephones on the system.

- The IP telephone Features list is accessible through the button that defaults to Services (**FEATURE** *900). This button can be programmed to another feature.
- One of the buttons defaults to the voice mail login (**FEATURE** 981). This program can be programmed to another feature, such as the dial string for a remote voice mail system.
- The Hold and Goodbye (release) features are automatically programmed above the Ringing call button, which is also programmable. The Ringing call button (**FEATURE** 807) provides call send and receive access, allows users to toggle between two calls using the Hold key, and is required if the Conference feature is allowed on the telephone.
- The telephone has an additional five hidden button assignments that can be programmed with Answer DNs or SWCA assignments. All assignments on the virtual buttons are ring-only. SWCA calls are accessed by using the feature code for each assigned button ("Parking and retrieving calls on SWCA keys" on page 467.)

2001 default button mapping		
Btn #	**PBX**	**DID**
01	Ringing Call (F807)	
02	IP Services List (F*900)	
03	Voice message access (F981)	

Hidden button assignments:		
Btn #	**PBX**	**DID**
04*	Blank	
05*	Blank	
06*	Blank	
07*	Blank	
08*	Blank	

* These buttons only support Answer DNs or SWCA controls.

- There are only two directional buttons (Up and Down) on this telephone. These buttons allow you to scroll through the Features list, which is access through the Services button or by entering **FEATURE** *900.

NetVision telephones

The NetVision telephone uses a display menu or feature code entry to access features. However, line assignments (intercom) and SWCA key assignments need to be entered into the button programming page on the DN record for these handsets for the feature to be active, even though the handsets do not have physical line or memory buttons.

Once the SWCA keys are assigned, the user enters the SWCA codes from the menu or enters the codes on the handset dial pad to access the SWCA keys. Refer to the *Telephony Features Handbook* for a detailed description of using SWCA keys.

NetVision default button configuration

Default	Button #	Default	Button #
SWCA 521	01	SWCA 526	06
SWCA 522	02	SWCA 527	07
SWCA 523	03	SWCA 528	08
SWCA 524	04	Intercom	09
SWCA 525	05	Intercom	10

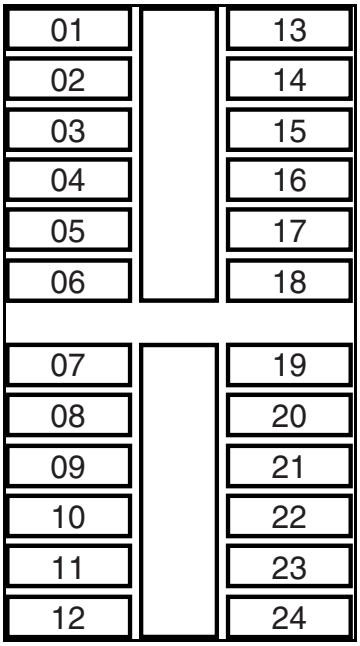
M7324(N) button defaults

Button mapping for the Nortel M7324(N) telephone is unique because this telephone has a different layout and more buttons than the other telephone types. Lines assigned to this telephone will first try to assign to button 01. If that button is not available, the line will assign to the next available button, scanning down the left button row, and then down the right button row.

Note: If there are no buttons available, the lines will still assign to the telephone, but they will have no appearance on the telephone, so ensure that these lines are configured to ring.

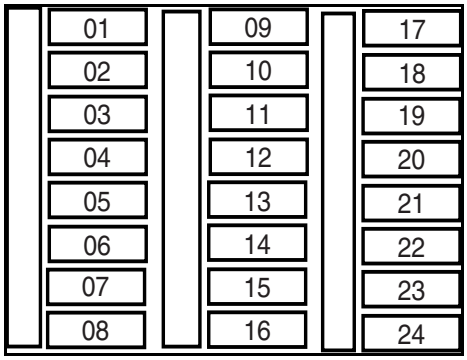
The table below shows the button assignment template for the M7324(N) telephone.

Note: The M7324N telephone has the 24 buttons lined up in three rows of eight buttons. Refer to the second figure below. This telephone is available in market profiles that do not support the M7324 telephone.



M7324(N) telephone default button assignment		
Button #	**PBX**	**DID**
01	Blank	Target line
02	Blank	Blank
03-12	Blank	
13	Call Forward	
14	Speed Dial	
15	Last Number Redial	
16	Saved Number	
17	Conference/Transfer	
18	Transfer	
19	DND	
20	Pickup	
21	Voice Call	
22	Intercom	
23	Intercom	
24	Handsfree/Mute	

Figure 138 M7324N defaults



Configuring user speed dialing

Speed dial numbers allow users to dial out a number with fewer button presses than dialing out the entire dial string.

User speed dial codes can be assigned to telephones using the following procedure.

1 Click the key beside the telephone DN if you are not already in the DN record for the telephone to which you want to assign the user speed dial.

2 Click the key beside **User preferences**.

3 Click the **User speed dial** heading.

4 Click the **Add** button, located above the navigation tree.
The Add User speed dials screen appears.

Figure 139 Add a user speed dial code to a telephone

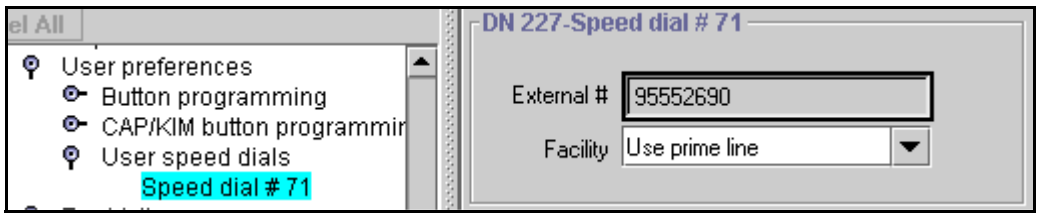
5 In the **Speed dial #** box, type a user speed dial code, from 71 to 94.

6 Click **Save**.

7 Click the key beside **User speed dial**.

8 Click the **Speed Dial # XX** heading you just created.
A DN XXX Speed Dial # XX screen appears.

Figure 140 Entering call parameters for a user speed dial



9 Use the information in the following table to set the speed dial number and route for the speed dial code.

Table 95 User speed dial settings

Setting	Values	Description
External #	<external phone number>	Enter the number the telephone will automatically dial when the user speed dial code is entered. Remember to include the access codes for the route you choose.
Facility	Use prime line Use line Pool Use routing table	Select the route you want the dialed number to take out of your system. **Note:** Any line numbers or line pool codes that you specify must be assigned to the telephone where the code is entered. If you choose prime line, a prime line must be assigned to the telephone where the code is entered. Refer to "Configuring line access" on page 393.

Entering user speed dials at the telephone

Users can add, change, or assign a memory button for user speed dials during button programming or at the telephone.

Press **FEATURE** *4 to add or change speed dials.

Press **FEATURE** *3 to add a speed dial to a memory button.

Refer to the *Telephony Features Handbook* for information about telephone operations for speed dials.

Setting up CAP stations

A CAP (Central Access Point) station acts as a central answering and monitoring point for a group or a business. You can configure quick dial numbers that allow the person at this station to monitor and answer call traffic into the group.

If you program the CAP to be an enhanced CAP (eCAP), lines, hunt group appearances, and multiple target line appearances can also be moved to the module. **Note:** Only T7316E/eKIM configurations support Hunt group appearances and multiple target line appearances.

This section includes this information:

- "Configuring CAP/KIM assignment" on page 436
- "Configuring a CAP or KIM module" on page 438
- "Programming CAP/KIM buttons" on page 438
- "Cold starting the KIM to erase programming" on page 440

Only two styles of telephones can be configured as CAP stations, with the addition of extra modules.

- The T7324(N) telephones connect to CAP(N) modules to provide auto dial or features. If this configuration is programmed to be an eCAP, it can also support line appearances.

  Note: International note: (N) refers to the version of the CAP module and M7324 telephone that is available to operations who cannot use the standard M-series terminals.

- The T7316E BST telephones connect to KIM (Key Indicator Module) modules to provide autodial buttons, system-wide call appearance (SWCA) buttons, and feature programming. If this configuration is programmed as an eCAP, it can also support extra lines, Hunt Group indicators and multiple target line appearances.

Figure 141 T7316E with KIM

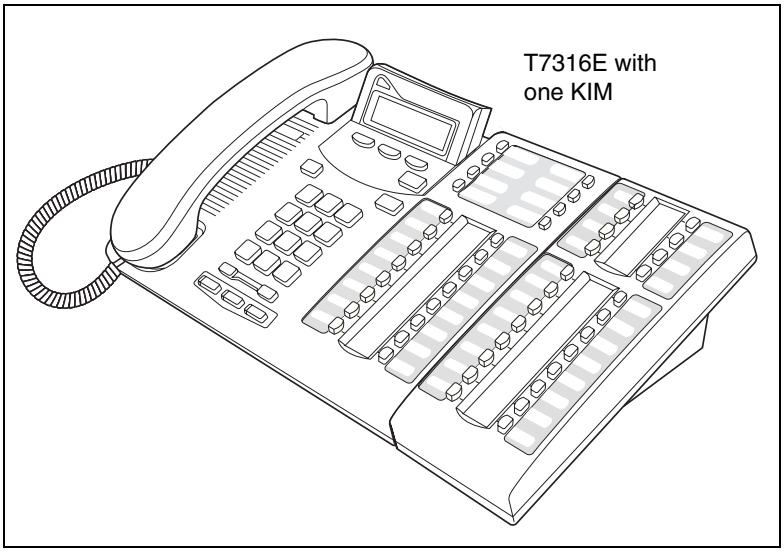
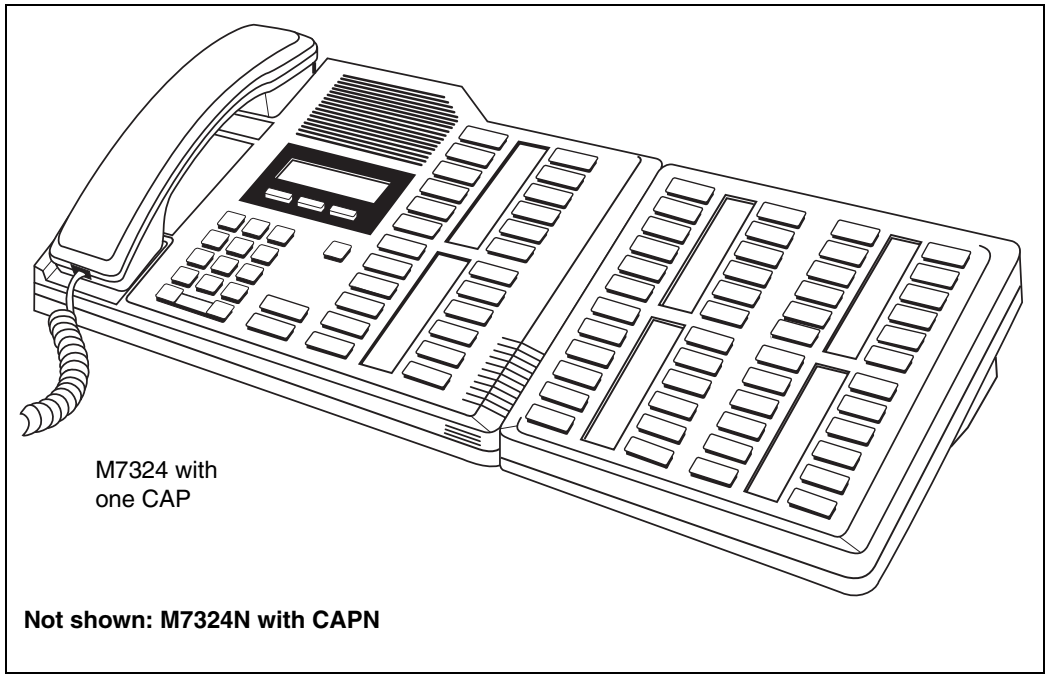


Figure 142 T7324 with CAP



You can configure a total of 12 CAP stations on a Business Communications Manager using the **CAP/KIM assignment** setting. Modules that have been configured like this will be referred to as eCAPs and eKIMs.

Note: If you do not use **CAP/KIM assignment** to designate a T7324(N)/CAP(N) or T7316E/KIM as a CAP station, there is no set limit to the number of these combinations that you can have on your system, resources permitting. However, you cannot assign lines or Hunt group indicators (T7316E/KIM) to the CAP or KIM modules unless the CAP stations have been assigned under **CAP/KIM assignment**.
If the T7316E/KIM is not configured under CAP/KIM assignment, the KIM module is known as an OKIM. This combination allows you to add additional direct dial keys or features to a T7316E. You can add up to nine KIM modules to a T7316E if they remain as OKIMs.

Use CAP stations to:

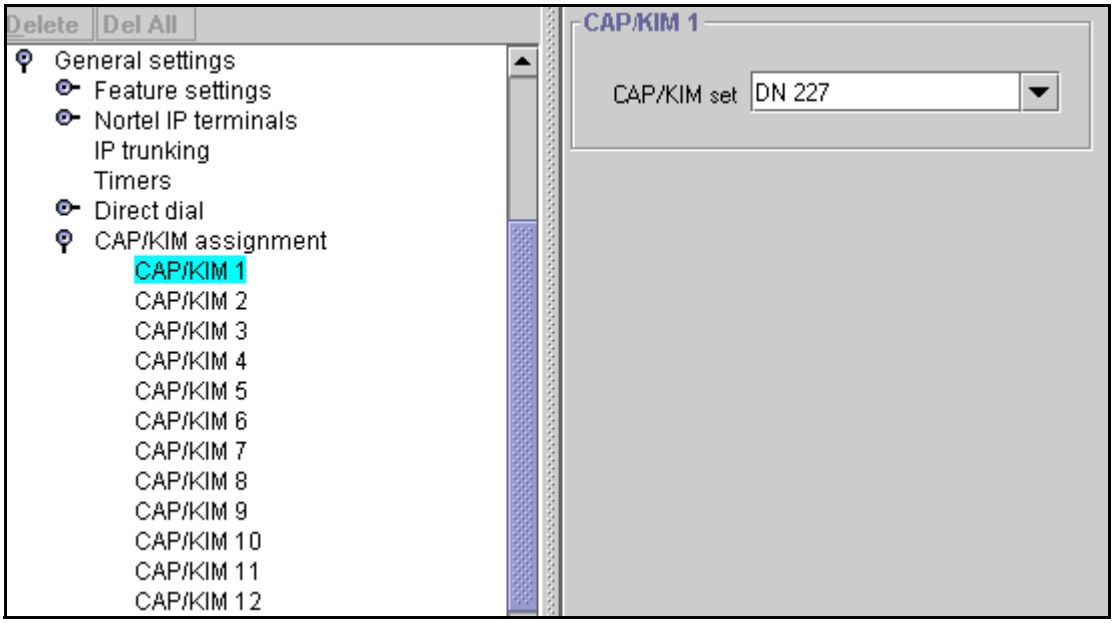
- monitor the busy/not busy and Do not disturb status of system telephones
- answer external calls on up to 120 lines on a CAP and 112 lines on a KIM, and extend calls to other Business Communications Manager telephones
- send up to 30 messages to other Business Communications Manager telephones
- provide extra memory buttons for the M7324(N) and T7316E telephones

Configuring CAP/KIM assignment

Follow these steps to create CAP stations:

1. Ensure that the telephone you want to use for a CAP station is configured and working.
2. Ensure that the CAP/KIM module has been installed on the appropriate telephone. Refer to the installation user card that came with the module, if in doubt.
3. In the Unified Manager, click on the keys beside **Services**, **Telephony Services**, and **General Settings**
4. Click on the key beside **CAP/KIM assignment**.
5. Click the CAP you want to program (**CAP/KIM 1** to **CAP/KIM 12**). The CAP # window appears.

Figure 143 CAP/KIM assignment, CAP/KIM 1 screen



6. Type the DN for the M7324 or T7316E telephone that you want to designate as a CAP station.
7. Click on the next CAP/KIM to add another CAP station, or click elsewhere on the navigation tree to save the setting.

   TIPS: If a CAP(N) module (or modules) is relocated with the M7324(N) telephone, the settings are retained.

Warning: ECAP programming issue on cold start reboot

If you do a Backup/Cold Start/Restore sequence on your Business Communications Manager, button programming on an ECAP module is lost and the lines assigned to those buttons are assigned to the buttons on the M7324 telephone. They replace any existing programming on the M7324. If there are no more buttons to assign lines to, the system still assign the lines without appearances, and they will ring when a call comes in on that line.

To correct the issue, go into the DN records for the telephone and the CAP programming records, and reenter the correct programming.

CAP/KIM notes:

- A station auxiliary power supply (SAPS) is required for M7324 telephones that have one or more CAP modules attached.
- A SAPs is not required for T7316E telephones attached to four or fewer KIMs. If the KIMs are designated as eKIMS, you can only attach a maximum of four modules to a T7316E telephone. If the KIMS are designated as OKIMs, you can attach up to nine modules to the T7316E. You must add a SAPS if more than four KIMs are added to the T7316E. Note also that the line loop to the CAP cannot be greater than 304.8 m (1000 feet).
- If a CAP/KIM module is relocated with the telephone, the settings are retained.
- If you replace an M7324+eCAP with a T7316E+eKIM, only the line assignments will be copied to the new telephone, but not to the eKIM. The telephone programming will revert to the default settings for other buttons. If you move an OKIM from one T7316E to another, the KIM will retain memory button programming. However, if you move an eKIM from one T7316E to another, programming will not follow.

Monitoring telephones with the CAP or KIM module

The indicators ▶ beside internal autodial buttons on your CAP module show the status of Norstar telephones. KIM modules have a more graphic set of icons that indicate various call states. Refer to the *Telephony Features Handbook* for details about KIM icons.

Configuring a CAP or KIM module

If the telephone/module set is programmed as a CAP station, you can move lines onto the module using **FEATURE** *81 on the telephone. Refer to the *Telephony Features Handbook* for detailed information about moving lines. You can also reassign Hunt group designators to the KIM module by using the same feature.

You can also force lines onto the CAP/KIM by entering more lines than the telephone buttons can support. Extra lines automatically flow over to the module, but they flow sequentially, starting on the top left at button 01. Also, they overwrite any existing programming on the KIM, except existing line or hunt group (KIM) assignments.

Any of the buttons on your CAP/KIM module that do not have assigned lines can be programmed to dial internal or external numbers automatically, or to access a feature. Refer to Programming CAP/KIM buttons.

Programming CAP/KIM buttons

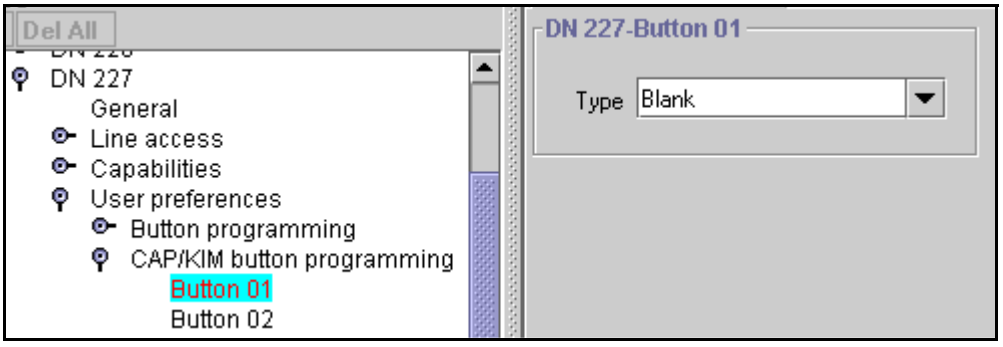
Designating features or autodial numbers to the eCAP/eKIM buttons can be performed using the **CAP/KIM button programming** heading located under **User Preferences**.

You cannot assign lines, target lines, or Hunt group indicators using button programming. This must be performed through adding lines to the telephone (Assigning lines to telephones), and, for hunt groups, configuring the telephone as a Hunt group member ("Adding a Hunt group member" on page 579). These lines are then either moved to the modules or overflow to the module if the telephone buttons cannot accommodate the number of lines.

To program the buttons, follow this procedure:

1. If you are not already in the DN record, click the key beside the telephone DN where you want to program button features.
2. Click the key beside **User preferences**.
3. Click the key beside **CAP/KIM button programming**.
   The following figure shows the programming field for button 01.

Figure 144 Programming a CAP/KIM button.



4. Click the button number that you want to program.

5 Use the information in the following table to configure button preferences.

Table 96 CAP/KIM feature button programming choices

Setting	Values	Description
Type	Blank Feature Internal autodial External autodial	Choose the type of feature that you want to program on the telephone buttons. Blank means that nothing is programmed on the button. New KIM modules, for instance have all blank buttons when they are newly-installed.
Value field:		
Feature	<*feature name*>	Use the arrow to choose the feature you want to program on the button.
Internal autodial	<*Internal DN*>	Enter the DN number for the internal telephone you want the telephone to dial by pressing this button.
External autodial	Use prime line Pool Use routing table Use line	Choose the route the telephone will dial through. **Prime line**: the prime line assigned to the telephone **Pool X**: one of the pools assigned to the telephone **Routing table**: enter the destination code with the external phone number **Use line X**: one of the lines assigned to the telephone
External #		
External autodial	<*dialing codes plus dialout string*>	Enter the complete dial sequence for the external call. This sequence will depend on what you chose for the route in the Value field.

Programming note: You cannot assign Hunt group DNs as an autodial button on the KIM modules.

Cold starting the KIM to erase programming

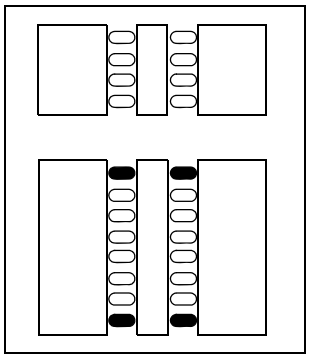
If your KIM fails, or if you want to erase programming on the KIM, there are two types of cold start.

Note: If you are cold starting an eKIM that has line or Hunt group assignments, the cold start will erase current programming, and insert the line appearances, starting with the top, left button. After all the line appearances are assigned to lines, the system adds target line or Hunt Group appearances. If any buttons are left, the system populates the buttons with autodialer assignments.

Use **FEATURE** *0 to view button assignments after a cold start.

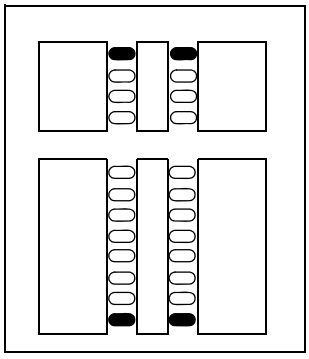
For both types of cold starts:

1. Unplug and replug the T7316E line cable.
   The telephone will restart and all the icons will flash. When the telephone icons stop flashing, the KIM module icons start flashing.
2. At this point, do one of the following:
   - **KIM single-module cold start**



If you just want to cold start an individual module, on that module, simultaneously press the two top and two bottom buttons on the lower button set, as shown in the diagram to the left. The KIM displays a random pattern of icons as the KIM resets.

   - **KIM multi-module cold start**
     If you want to cold start all the KIMs attached to your telephone, simultaneously press the top two buttons on the upper button set, and the bottom two buttons on the lower button set, as shown in the diagram to the right.



Programming restrictions for DNs

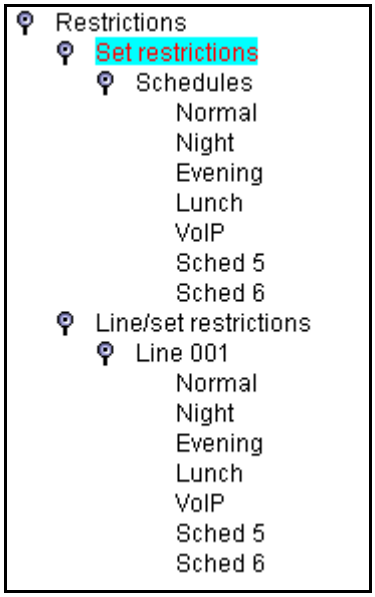
The Restrictions settings prevent callers from making certain kinds of calls from a specific telephone or from lines that are available at the telephone. You can also restrict some features.

You can copy the restriction settings you program on one telephone to other telephones.

TIPS: Remote access: Users dialing in from an external source are given a COS password to gain access to the system. When you define these passwords, you also define a specific set of restrictions for each password. For example, you may have a group password that provides general internal access only, however, you may have an individual password that is assigned to a top executive that has fewer restrictions that allow internal and external calls through the system. Refer to "Using COS passwords" on page 296.

This section includes information about:

Figure 145 Telephone-based dialing restrictions, menu



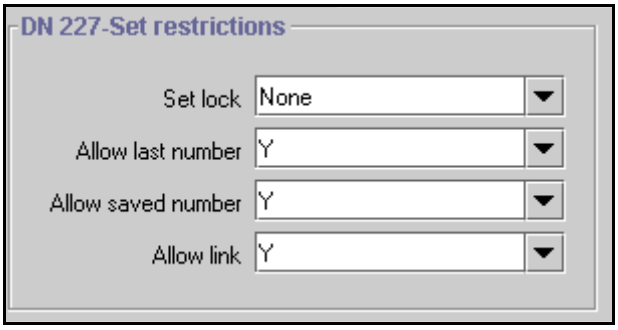
Defining telephone dialing restrictions

Set restrictions allow you to assign a restriction filter to a telephone to prevent certain numbers from being dialed from that telephone and prevent the use of some features.

Follow these steps to create or change set restrictions:

1. If you are not already in the DN record, click the key beside the telephone DN for which you want to assign set restrictions.
2. Click the key beside **Restrictions.**
3. Click on **Set restrictions**.
   In the right frame a list of general restriction settings appears.

Figure 146 General restrictions for telephones



4. Use the information in the table below to configure telephone restrictions.

Table 97 Telephone restriction fields

Setting	Values	Description	
Set lock	None Partial Full	Choose the option that sets the amount of programming and customizing the user can do with this telephone.	
		None allows access to all features.	
		Partial prevents: • programming autodial buttons • programming user speed dial numbers • programming feature buttons • moving line buttons • changing the display language • changing dialing modes (Automatic, Pre-, and Standard Dial) • using Voice Call Deny • saving a number with Saved Number Redial	**Full** restricts all the Partial settings, plus: • changing background music • changing Privacy • changing Do Not Disturb • using Ring Again • using Call Forward all calls • using Send Message • using Trunk Answer • activating Services
Allow last number	Y or N	Allow or disallow access to the Last Number Redial feature.	
Allow saved number	Y or N	Allow or disallow access to the Saved Number Redial feature.	
Allow link	Y or N	Allow or disallow access to the Link feature, which is a host signaling option.	

ISDN terminals/cordless handsets notes:

- Set lock is not supported.
- Allowed last number redial is supported on some handsets. Refer to the user manual for your telephone.
- Allowed saved number redial is not supported
- Allow link is supported on some sets. Refer to the user manual for your telephone.

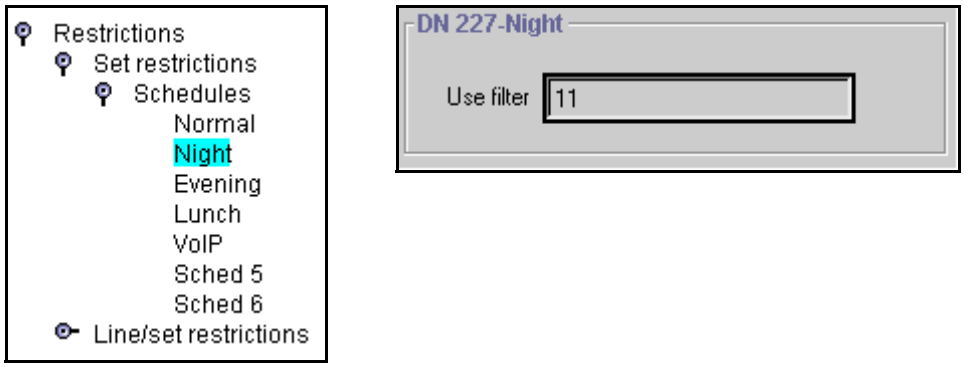
Setting restriction schedules for telephones

You can assign a different restriction filter for normal service and for each of six other schedules. See "Defining service schedules" on page 489 for more information about the schedules.

Follow these steps to configure Set Restriction schedules:

1. If you are not already in the DN record, click the key beside the telephone DN for which you want to assign set restrictions schedules.
2. Click on the keys beside **Restrictions, Set restrictions, Schedules**.
3. Click on the schedule you want to program. For example, **Evening**.

Figure 147 Defining set restrictions for the Night schedule



4. In the **Use filter** box, type in the number of the restriction filter you want to assign to the telephone.
   Refer to the table below for a list of default settings.

Table 98 Schedule filter defaults

Schedule	Restriction filter (defaults)	Schedule	Restriction filter (defaults)
Normal	02	Schedule 4	00
Schedule 1 (Night)	11	Schedule 5	00
Schedule 2 (Evening)	12	Schedule 6	00
Schedule 3 (Lunch)	13		

For example, if you enter a set of restrictions for filter 11, the restrictions will automatically apply for the Night schedule.

Defining line/set restrictions

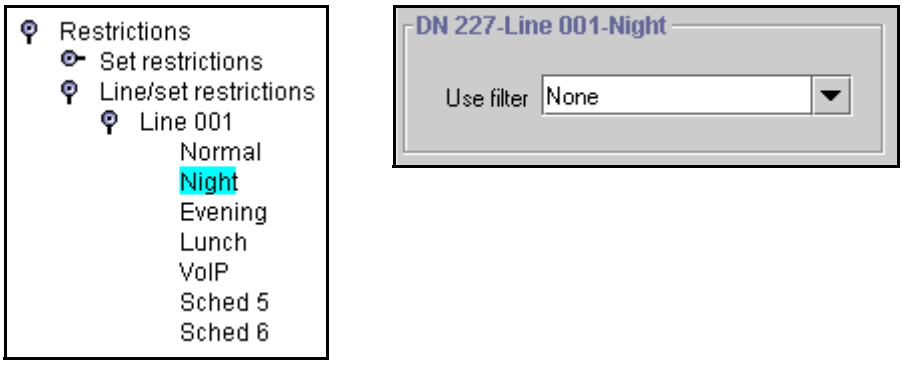
The **Line/set restrictions** settings allow you to assign a restriction filter to a specific line for outgoing calls at a specific telephone. This type of filter replaces any line or set restriction filters that can otherwise apply. Line/set restrictions restrict the numbers the user can dial on a line, but only from that telephone. The same line on another telephone can have different restrictions.

You can apply a different line restriction for normal service and for each of the six schedules.

Follow these steps to configure Line/set restrictions settings:

1. If you are not already in the DN record, click the key beside the telephone DN for which you want to assign line/set restrictions.
2. Click on the keys beside **Restrictions, Line/set restrictions.**
3. Click the key beside the **Line** number you want to configure.
   The list of schedules expands on the navigation tree.
4. Click the schedule name that you want to configure.
   For example, select **Night**. The Night schedule window appears.

Figure 148 Defining Line/set restrictions for line 001, Night schedule



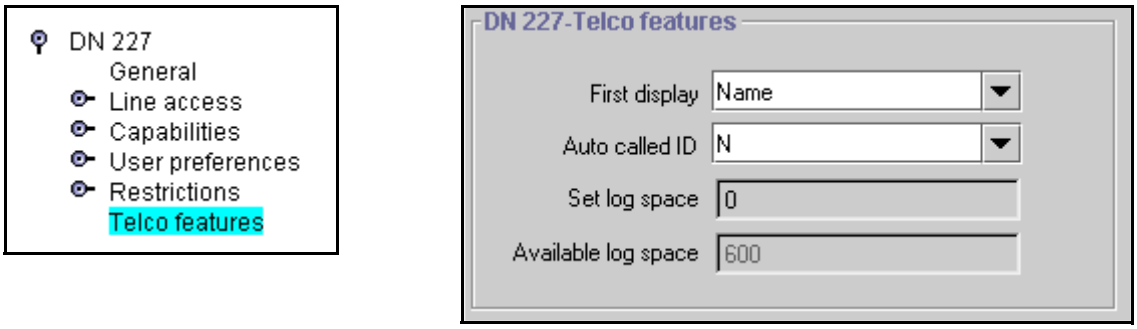
5. In the **Use filter** box, choose **None** or **Filter:**
   If you choose Filter:, enter the number you want to assign as the Line/set restriction for this schedule and press the **Enter** key. There are no default Line/set restrictions.

   TIPS: You can apply a maximum of 255 line/set restrictions to lines at telephones.
   If you assign a Line/set restriction to a line at a particular telephone, it overrides any line restrictions or telephone restrictions that might otherwise apply.
   If no Line/set restrictions are defined, the system checks the numbers dialed against the telephone restrictions and the line restrictions, if either of these are defined.
   The numbers dialed can be rejected by either restriction.

Configuring telco features

The Telco features heading allows you to program how the Business Communications Manager works with the public network or other outside features and services to supply Call Display.

Figure 149 DN Telco Features fields



You can copy the Telco features settings you program on one telephone to other telephones.

Follow these steps to configure Telco features settings:

1. If you are not already in the DN record, click the key beside the telephone **DN** for which you want to assign telco features.
2. Click on **Telco features**.
3. Use the information in the following table to configure Telco features.

Table 99 Telco features settings

Setting	Values	Description
First display	Name Number Line	Determine what call display information appears first. This feature depends on which services you subscribe to. Call Display information may contain the name of the caller, the number of the caller, the name of the line in your Business Communications Manager system that the call is on, or all. For each telephone, you can determine what information displays first.
	Tips: The Call Information feature displays and toggles between the name and line number for Call Display information. Unknown number appears on the display if the information is not available from your telephone company. You may see Private number on the display if the caller blocks that information. **Alpha tagging:** If you are using the alpha tagging feature, choose **Name**. Refer to "Using alpha tagging for name display" on page 455.	
Auto called ID	Y or N	Select whether you want to see the extension number and name of the telephone you call on your display. The Auto called ID set for target lines is the same telephone that has an appearance on that target line.
Set log space	<amount of space remaining on the log>	This setting indicates the amount of space that the user has to store call log items for the telephone. Default: 20.

Table 99 Telco features settings (Continued)

Setting	Values	Description
Available log space (read only)	<total amount of log space that is available>	This setting indicates the total amount of space available for call logging on the system.

DECT handsets note: DECT handsets display numbers for incoming calls from outside the local network, and displays the telephone name for incoming calls from internal sets.

Voice Mail settings

Systems with voice mail have an additional screen that can be used to change the display and outdial for the voice mailbox for each telephone.

Note: This screen is generated when you use the Add Users Wizard to configure DNs. The DN must appear under the Active DNs heading before this screen appears.

1. Click on the keys beside **Services, Telephony Services, System DNs, Active set DNs**.
2. Click on the DN you want to set voice mail parameters for (DNXXX).
   The Voice Mail screen appears in the right frame.
3. Use the information in the following table to change the Voice Mail display features.

Table 100 DN voice mail settings

Setting	Values	Description
Last name	<alphanumeric>	Last name of the person who owns the mailbox
First name	<alphanumeric>	First name of the person who owns the mailbox.
Display in directory	Yes or No	Indicates whether this name will display in the company directory.
Outdial type	None, Line, Pool, Route	Indicates how the outdial occurs to reach the mailbox. Hint: If your voice mail system is physically attached to another system on the network, you need to indicate an external path (line, pool, or route).

Deleting a mailbox

If you want to delete the mailbox for this DN: On the top menu, click **Configuration** and select **Delete**.

Digital telephones DN record matrices

Transfer the following information to a spreadsheet and fill out the values for each telephone you provision.

Table 101 DN equipment identification

Name or location	DN type/Model	BLF	CAP	ATA	Port No.	Default DN (max. 7 digits)
	Companion ISDN/DECT					
Model (digital and IP sets only)	M7324(N) M7100/T7100 T7316E i2001	M7310/T7316 (T7406) i2004/i2050 IPWI (NetVision) Other (ATA, 7000, BST doorphone)			M7208(/T7208 i2002 CAP(N)	
Control set (default is start DN)						
Call log passwords						

Table 102 General and Line access settings for DNs

Line Access			
Prime Line	None I/C Line # __ Pool _____	Line pool access	___ (A-O) or PRI ___
Intercom Keys	0 1 2 3 4 5 6 7 8	Answer DNs	Enter DNs of telephones to be answered and circle Answer type: AR = Appear&Ring A = Appear only
OLI#	None #	Appearances (target lines)	#
Line assignment List three- digit line number and circle line assignment. AR = Appear&Ring A = Appear only R = Ring only blank = Unassigned	001 A R 002 A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R	Caller ID set (target lines/ analog CLID lines)	Y N
		Vmsg set	Y N

Table 103 Capabilities

Telephone DN					
Capabilities					
DND on Busy	Y N		Priority call	Y N	
Handsfree	Auto Std None		Auto hold	Y N	
			Aux. ringer	Y N	
HF answerback	Y N		Allow redirect	Y N	
Pickup grp	1 2 3 4 5 6 7 8 9 None		Redirect ring	Y N	
Page zone	1 2 3 4 5 6 None		Keep DN alive	Y N	
Paging	Y N		Receive short tones	Y N	
D-Dial	Set1 Set __ None		SM Supervisor	Y N	
			Auto hold for incoming page	Y N	
Call Forward			ATA settings		
Fwd no answer	None to:		ATA answer timer	3 5 7 10	
Fwd delay	2 3 4 6 10		ATA use	On site Off site	
Fwd on busy	None to:		Msg indicate	None Tone Lamp	
Hotline			Intrusion		
None			Protect lvl	None Low Med High	
Internal	Internal #				
External	Facility Prime	Pool ____	Use Routing Table	External #	

Table 104 User preferences

DNs: (max. 7 digits)				
Model			Call log opt'ns	Log all calls... No autologging... No one answered... Unanswered by me...
Dialing opt'ns	Standard dial/Pre-dial		Display cntrst	1 2 3 4 5 6 7 8 9
Language			Ring type	1 2 3 4

Table 105 Button programming

Model				
Button number	Blank	External Autodial	Internal Autodial	Feature
		External #: Use Line: Use Prime Line Use Pool Use Routing Table	DN DN:	

Table 106 User speed dial settings

Spd# (71-94)	Speed dial number (max. 24 digits)	Use prime line Use line: ____	Pool code ____ Use routing table

Table 107 Telephone (set) Restrictions

Restrn flt	Restrn		Default Overrides	
	(Number)	(Value)	(Number)	(Value)
00		No restrictions (cannot be changed)		
01	01	0		
	02	1	001	1800
			002	1877
			003	1888
	03	911	001	911
	04	411		
	05	976		
	06	1976		
	07	1•••976		
	08	1900		
	09	1•••900		
	10	5551212		
02-99 . . .				
Restrn flt	Restrn nn		Override	
(01-99)	# (two digits)	Restriction (max. 15 #)	# (three digits)	Overrides (max. 16 #)
Set lock	None/ Partial /Full			
Allow last number	Y N			
Allow saved number	Y N			
Allow link	Y N			

Table 108 Telephone restriction schedules and line/set restrictions

Sets: (max. 7 digits)					
Names: (max. 7 char.)					
Set restriction schedules				Line/set restrictions	
Filters					
Normal	02	02,		Normal	None
Night	11	11,		Night	None
Evening	12	12,		Evening	None
Lunch	13	13,		Lunch	None
Sched 4	00	00,		Sched 4	None
Sched 5	00	00,		Sched 5	None
Sched 6	00	00,		Sched 6	None

Table 109 DN record, Telco features

Telephone DN		Auto Called ID	
names:		Set log space	
First display	Name/ Number/ Line	Available log space	

Chapter 16
Configuring system settings

Some settings affect all telephones in the system, which have the specific feature. This section describes the call-related Telephony services settings found under **General Settings**, **System Speed dial** and **Telco features** headings.

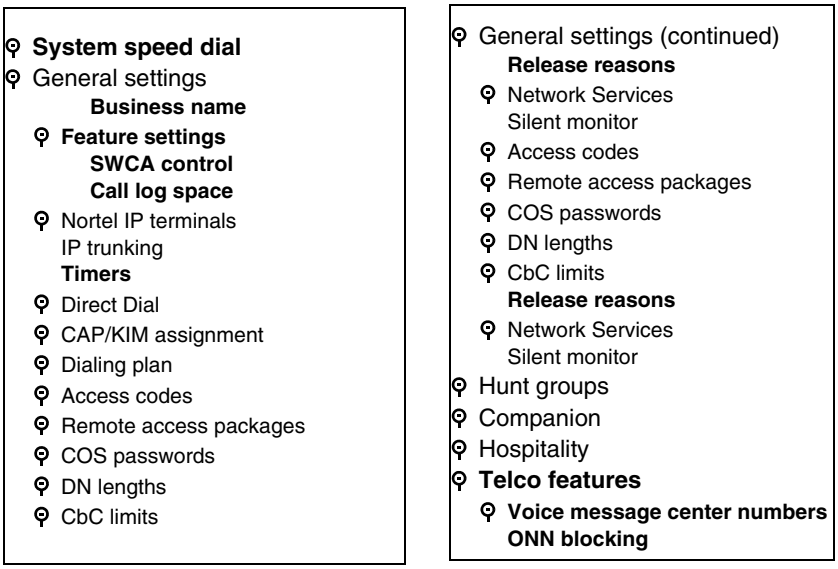
TASKS:	
Define system-wide settings (General settings) that affect how all the telephones in the system use certain features, or perform in specific ways. Note that some of the General headings listed below are discussed in other sections of the *Programming Operations Guide* because they apply to a more specific process.	
Define system speed dial numbers. Also use these assignments to apply alpha tagging. "Configuring system speed dial numbers" on page 475	
Define a system external voice mail system. Also, define ONN codes for lines that require them to allow the name and number blocking feature. "Setting system telco features" on page 478	
General settings	
Business name	"Programming Business name display", defines the screen where you enter the banner name that displays as part of the outgoing Name, Number and Line display.
Feature settings	"Programming Feature settings" on page 457 deals with configuring: • hold/call parked features: — "Background music" — "On hold" (what caller hears while on a call) — "Park mode" — "Held line reminder" — also under Feature settings is the heading that allows you configure SWCA keys "Configuring system-wide call appearance groups" on page 462 • transferred calls — "Delayed Ring Transfer" (how long telephone will ring before transferring to prime set or voice mail) — "Directed pickup" • handset volume ("Receiver volume") • page feature ("Page tone") • alarm recording/display ("Alarm set") • relocating wired telephones ("Set relocation") • message waiting indicator for analog telephones ("Message reply enhancement") • answer DN alert levels ("Ans key")

	• feature activation while on an active call ("Force auto/spd dial over ic/conf") • incoming caller ID — "Clid Match Length" — "Maximum CLI per Line" • system speed dial list size ("Maximum System Speed Dials") • system call log space ("Resetting call log space" on page 470).
Nortel IP terminals	*IP Telephony Configuration Guide*
IP trunking	The fields on the screen are described under "Configuring special IP trunking interoperability" on page 541. "Message Waiting Indication" on page 565 and Chapter 22, "Configuring centralized voice mail (Chapter 22, "Configuring centralized voice mail) Allow outgoing caller name over the VoIP trunks ("Enabling/disabling outgoing name display" on page 454) Private Network ID and Zone ID are required for specific interoperability situations between the Business Communications Manager and systems that use Bandwidth Management, such as Succession 1000/M.
Timers	"Setting system timers" on page 472
Direct Dial	"Creating Direct Dial sets" on page 313 (Chapter 12, "Configuring outgoing calls)
CAP/KIM assignment	"Setting up CAP stations" on page 434 (Chapter 15, "Configuring DNs for system devices)
Dialing plan	"Configuring the public and private dialing plans" on page 302 (Chapter 12, "Configuring outgoing calls)
Access codes	"Understanding access codes" on page 309 (Chapter 12, "Configuring outgoing calls)
Remote access packages	"Configuring for remote access" on page 291 (Chapter 11, "Controlling access into the system)
COS passwords	"Using COS passwords" on page 296 (Chapter 11, "Controlling access into the system)
DN lengths	"Changing the DN length" on page 285 (Chapter 11, "Controlling access into the system)
CbC limits	"Configuring Call by Call services" on page 339 (Chapter 12, "Configuring outgoing calls)
Release reasons	"Define release reason levels" on page 474
Network Services	Network Services: "Configuring private networks with SL-1 MCDN" on page 519 and "Configuring ETSI QSIG and DPNSS network services" on page 543 (Chapter 20, "Configuring private networks with SL-1 MCDN and Chapter 21, "Configuring ETSI QSIG and DPNSS network services)

Silent monitor "Setting up Silent Monitoring" on page 585 (Chapter 23, "Configuring Hunt groups)

The following figure shows the headings discussed in this section in bold.

Figure 150 General Settings headings and fields



Network name display

Business Communications Manager displays the name of the calling party, when available, on both Private or Public ISDN PRI interfaces. The displayed name can include the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. Refer to "Receiving and sending calling party name" on page 454.

If only a number is available for CLI on an incoming call, you can program a system speed dial in such a way that a name displays when that number calls in. Refer to "Using alpha tagging for name display" on page 455.

The outgoing name display consists of the Business name and the telephone name. Refer to "Programming Business name display" on page 455.

The following table provides a list of the name/number display features and the list of ISDN interfaces that support each feature.

Table 110 Call features/interface list

Feature	Interface					
	NI PRI	DMS Custom PRI	SL-1 (MCDN)	NI-BRI	ETSI Euro (PRI/BRI)	ETSI QSIG
Receiving Calling Name	Supported	Supported	Supported	Supported		Supported
Receiving Redirected Name	Supported		Supported	Supported		

Table 110 Call features/interface list

Feature	Interface					
	NI PRI	DMS Custom PRI	SL-1 (MCDN)	NI-BRI	ETSI Euro (PRI/BRI)	ETSI QSIG
Receiving Connected Name		Supported	Supported			Supported
Sending Calling Party Name	Supported	Supported	Supported			Supported
Sending Connected Name		Supported	Supported			Supported

Note: Network Name Display is an optional feature that is available based on the interface you subscribe to.

MCDN note: MCDN networks fully support name display features.

Receiving and sending calling party name

Network Name Display allows the name of an incoming PRI/BRI, analog with CLID, or VoIP with MCDN call to appear on the Business Communications Manager telephone receiving the call.

Calling Party Name with status of Private can appear on the Called Party telephone as **Private name**. If the incoming Calling Name is defined by the CO as a private name, then **Private name** appears on the answering telephone. If the Calling Party Name is unavailable it can appear on the Called Party telephone as **Unknown name**.

If the call is answered by a Hunt group, the hunt group name appears instead of the telephone name in forming the connected name.

The Connected Name is a transient display that appears for approximately three seconds. The Connected Name is sent only if the OLI is programmed ("Configuring line access" on page 393). You can program both a public and private OLI. The system uses the one appropriate to the type of call.

Network name display interactions

Calling and Connected Name information (if available) passes between trunks with Selective Line Redirection (SLR). Only Calling Name information passes between trunks in cases where Direct System Inward Access (DISA) results in tandeming of trunks.

Enabling/disabling outgoing name display

You can set up the trunks to disallow name display to be sent out on PRI, BRI, and VoIP trunks. Use this for trunks where the connecting switch does not support outgoing line display. Default is enabled (Y).

PRI lines: "Configuring the trunk module to line type" on page 131 (see the field "Send Name Display" on page 134.) Can with set for PRI trunks with these protocols: SL-1, NI, DMS100, DMS250, or PRI QSIG

BRI loops: "Identifying BRI T-loops (ETSI, QSIG)" on page 271 (see the field "Send Name Display (Type: QSIG trunks only)" on page 272). Can be set for T-loop and BRI-QSIG trunks.

VoIP trunks: The field for allowing outgoing name display for VoIP trunks, affecting all trunks, is under **Services**, **General settings**, **IP Trunking**.

Programming Business name display

Nortel Networks recommends that you use a blank space for the last character of the Business name to act as a separator between the Business name and telephone name.

Note, that if you leave this field blank, no name appears.

To program the Business Name:

1. Click on the keys beside **Services**, **Telephony services.**
2. Click on **General settings.**
3. In the **Business name** box, type the Business name you want to appear on receiving telephones (a maximum of eight characters).
4. Other areas that you must programmed include:
   - The **OLI number**. Refer to "Configuring line access" on page 393.
   - Under **Telco Features**, the **Auto Called ID** must be set to **Yes**. Refer to "Configuring telco features" on page 445.

Using alpha tagging for name display

You can configure your system to display a caller name for incoming lines that provide number-only CLID, such as target lines and analog CLID lines.
Note: Lines that provide name and number CLID, such as PRI lines, use that name for display, rather than the alpha tagging feature.

You use a combination of fields within the Unified Manager to set up this feature.

- To determine the name to display, you add a system speed dial for the number, entering a display name. Refer to "Configuring system speed dial numbers" on page 475.
- You can increase the default number of system speed dials from 70 to 255 if you want to provide an extensive CLID list. Refer to table entry: *Maximum System Speed Dials* on page 460.
- To determine how many digits of the dialed number and the system speed dial must match before a name is displayed, you set the **Clid match length** setting. Refer to table entry: *Clid Match Length* on page 460.
- In order for the telephone to display the name, it must have **CLID name display** (table entry: *Caller ID set* on page 398) enabled for the assigned line, and **First display** must be set to **Name** (table entry: *First display* on page 445).

Limitations:

- Due to system resource limitations, only 30 telephones can be assigned to provide alpha tagging CLID per line. Refer to table entry: *Maximum CLI per Line* on page 460.
- If the incoming number only partially matches the CLID match length, no name displays.
- If the number matches more than one speed dial, which have different names, the telephone displays the name of the first match.
- ISDN devices do not support the alpha tagging feature.

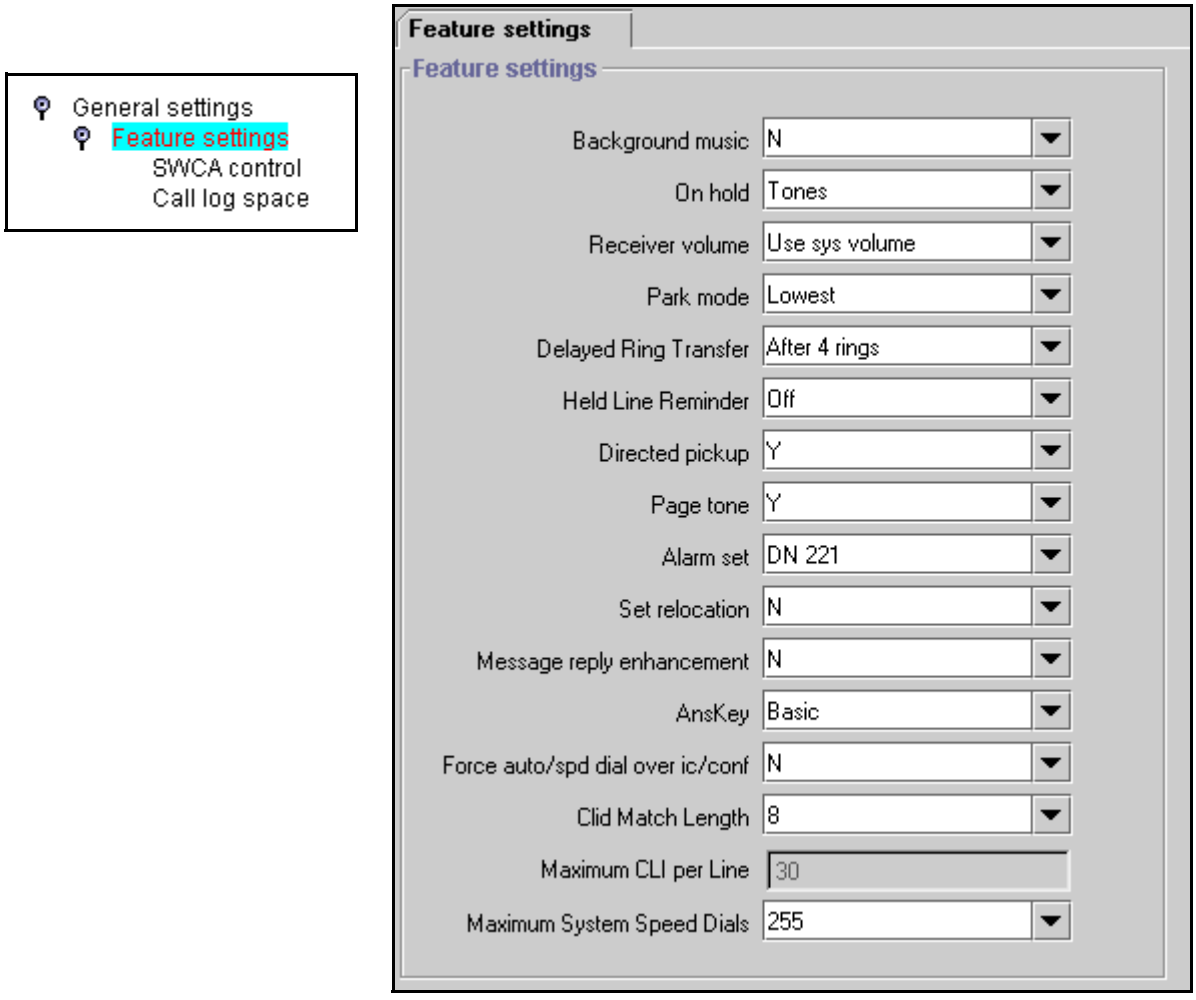
Programming Feature settings

The Feature settings heading allows you to program a number of features that apply to all telephones connected to Business Communications Manager.

Follow these steps to define feature settings on a specific telephone:

1. On the navigation tree, click on the keys beside **Services**, **Telephony services**, and **General settings**.
2. Click on **Feature settings**.
   The Feature Settings screen appears in the right frame.

Figure 151 Feature settings screen



3. Use the values in the following table to set the features you have on your system.

Table 111 Set feature values

Attribute	Value	Description
Background music	Y or N	Allows you to listen to music through your telephone speaker after pressing **FEATURE** 86 on your telephone. A music source must be connected to Business Communications Manager or IP music must be configured. Refer to "Background and on-hold music sourcing" on page 460.
On hold	Tones Music Silence	Allows you to choose what a caller hears on an external line when the line is put on hold. **Tones** provides a periodic tone. **Music** provides any signal from a source such as a radio connected to Business Communications Manager or streaming audio, using the IP Music feature. "Background and on-hold music sourcing" on page 460 **Silence** provides no audio feedback.
Receiver volume	Use sys volume Use set volume	Allows you to specify if the volume level of a receiver or headset returns to the system default level when a call ends or is put on hold, or if it remains at the volume level set at the individual telephone.
Park mode	Lowest Cycle	Allows you to determine how the system assigns a retrieval code to parked calls. **Lowest**, the system chooses the lowest code that is available when the call is parked. **Cycle**, the system will choose the codes in a sequence, from lowest to highest, until all the codes have been used, then start at the lowest code again.
Delayed Ring Transfer	Off After 1 ring After 2 rings After 3 rings After 4 rings After 6 rings After 10 rings	Defines whether unanswered external calls are automatically forwarded to a prime telephone after this timer expires. You must assign a prime telephone for this feature to operate. Refer to "Assigning Trunk/line data" on page 236.
Held line reminder	Off Immediate After 30 seconds After 60 seconds After 90 seconds After 120 seconds After 150 seconds After 180 seconds	Reminds you that an external call at your telephone is still on Hold. You periodically hear two tones from your telephone until you take the call off Hold. Note: These tones can be heard by the caller.
Directed pickup	Y or N	Y (yes) allows anyone to answer any calls by specifying the internal number (DN), where the call is ringing. Directed pickup is useful when not all the telephones have the same lines, but you want to allow co-workers to answer a call on any external line. **Note:** Do not confuse Directed pickup with the Group pickup feature. Group pickup allows you to answer a call at any telephone within a specific group without specifying the internal number (DN) of the ringing telephone.
Page tone	Y or N	Y (yes) determines that a tone sounds before a page begins.

Table 111 Set feature values (Continued)

Attribute	Value	Description
Alarm set	None DN: <number>	Allows you to assign a device on which alarm messages appear when a problem has been detected in the system. Alarms are recorded in the Windows NT event log.
Set relocation	Y or N	**Activate** Set relocation after you perform the telephone installation and programming, for more flexibility in testing equipment. This allows you to move any digital telephone to a new location without losing the directory number, autodial settings, personal speed dial codes, and any programming for that telephone. If you **deactivate** Set relocation while moving a telephone, the internal number and programming data remain with the physical port on Business Communications Manager. When you connect the telephone somewhere else, it does not receive the original programming. A telephone that is plugged into the original jack would download the programming. If the new telephone is a different model, it would download that part of the programming that is the same for both models.
Message reply enhancement	Y or N	Y (yes) allows you to automatically deactivate the message waiting indicator on analog telephones connected to an analog station media bay module (ASM), if the reply call from the analog telephone to the direct-dial telephone is answered. It does not matter where the call is answered from by the user. This feature also functions if the user invokes the Call pickup feature to answer the reply call from the analog telephone. It does not, however, work with the Retrieve parked call feature.
		Tips Direct-dial telephones are the only telephones that can send messages (using F1) to analog telephones connected to an ASM. The direct-dial set must be the designated direct-dial telephone for the analog telephone receiving a message.
Ans key	Basic Enhanced Extended	The **Answer key** setting allows you to determine what types of calls alert at a telephone that has answer DNs assigned. Answer key changes do not apply to portables. **WARNING:** Do not change the default setting (Basic) if you have **Call Center** active on your system. Refer to "Answer key levels" on page 461 for attributes of each setting. Also refer to "Phantom DNs" on page 461.
Force auto/spd dial over ic/ conf	Y or N	This feature allows you to determine if Auto and Speed dial codes can be transmitted during an active call. This feature works during either a one-to-one call, or during a conference call. If set to N: When the user presses a memory key for a speed dial, the current call will automatically be put on Hold, and the second call will be dialed. If set to Y: When the user presses a programmed auto dial or speed dial key, the system dials out the number while maintaining the current call.
*Conference Tone	Y or N	This setting determines whether a conference tone is heard by participants at the beginning of the conference. *Not available in all region profiles.

Table 111 Set feature values (Continued)

Attribute	Value	Description
*Network Callback Timer	<XX seconds>	This timeout value determines when a transfer attempt will stop and then attempt a retry of the transfer. *Not available in all region profiles.
Clid Match Length	None, <3-8>	Set this number to the number of digits that you want an incoming number and a system speed dial number to match before displaying a name on the telephone receiving the call. If you choose **None**, the feature is disabled. **Note:** Number matching starts from the end of the dial string. Refer to "Using alpha tagging for name display" on page 455.
Maximum CLI per Line	30 (read-only)	This setting indicates the maximum number of telephones that will display CLID simultaneously for an incoming call.
Maximum System Speed Dials	70 or 255	Determine how many system speed dials you want to be able to assign. If you plan to use an extensive alpha tagging list, choose the 255 setting. Refer to "Using alpha tagging for name display" on page 455 and "Configuring system speed dial numbers" on page 475.

Background and on-hold music sourcing

If there is an music source connected to your system, you can listen to music through the speaker on the telephone (**FEATURE 86**), and/or you can allow the music to be heard by callers with calls on hold.

External source: The Business Communications Manager allows you to attach an external music source to the hardware. Refer to the hardware installation guides for details about connecting the source.

IP music: On systems running BCM version 3.5 or newer software, you can use the IP music feature to configure a list of .wav or .au files to use as background music and music on hold. Refer to Chapter 25, "Configuring the music source," on page 601.

Warning: According to U.S. copyright law, a license can be required from the American Society of Composers, Authors and Publishers or a similar organization if radio or TV broadcasts are transmitted through the Background Music feature of this telecommunication system.
Nortel Networks hereby disclaims any liability occurring as a result of failure to obtain a license.

NetVision note: NetVision telephones do not allow this feature. Attempting to invoke the feature will produce an error message on the display.

Answer key levels

The following table shows what functions are provided by each level of the answer key settings. The Xs indicate the call types which will ring at answer DN telephones.

Table 112 Answer keys

Answer keys	Basic	Enhanced*	Extended*
Prime set call capture			X
Overflow call routing calls		X	X
Call forwarded calls			X
Ringing service calls			X
Callbacks			X
Blind transferred calls	X		X
Other answer key calls			
Priority calls			
Voice calls			
All other calls	X	X	X

*__Call Center warning__: If you assign Answer DNs to Call Center telephones, ensure that your system Answer key is set to **Basic**.

Overflow routing note: This feature is only supported on Answer DN telephones when systems are set to **Enhanced** or **Extended** settings.
Hunt group overflow DN note: Ensure that a DN used for Hunt group overflow is not part of the hunt group if it has answer DNs for the hunt group members. Answer key must also be set to **Extended**.

Portable handset note: Answer Key settings do not affect NetVision, DECT, or Companion handsets.

Phantom DNs

A Phantom DN is a DN record for a telephone that does not physically exist. You can assign lines to the telephone that can be programmed to Appear and Ring. This allows you to assign an Answer key from the non-existent telephone to an existing telephone. This might be used in the case where a customer number has been changed, but the number still gets used. Rather than assign a telephone to the line, you can create a phantom DN and assign an Answer key to an active telephone.

Configuring system-wide call appearance groups

These sections describe the system wide call appearance (SWCA) feature in detail:

When you use the SWCA feature, your system gains extended flexibility in making and answering calls between telephones within the system.

Note: Your telephone must have auto hold enabled if you want to use SWCA lines so that an active call automatically gets placed on Hold if the user answers a second call. You must also ensure that a Call Park code has been assigned ("Understanding access codes" on page 309), and that a Park timeout has been specified ("Setting system timers" on page 472).

There are 16 SWCA codes that can be assigned to buttons when the telephone is being programmed. Buttons are programmed under **Services, Telephony services, System DNs, DN<group DN>, User preferences, Button programming**. They can also be assigned by the user at the telephone, using the button programming feature code (**FEATURE *3**) and feature codes **FEATURE *521** to **FEATURE *536**. Usually these buttons are programmed onto buttons that have a display icon.

You also can assign SWCA codes to a Key Interface Module (KIM) Refer to "Programming CAP/KIM buttons" on page 438.

Telephones do not need to have SWCA buttons defined to retrieve or park SWCA calls. The feature codes can be entered directly onto the handset to retrieve or park the calls.

Finding SWCA calls

These three feature codes allow you to navigate through the SWCA codes and current calls parked on SWCA keys. These codes only work for telephones that have SWCA keys defined, and only search across the range of codes that are assigned for that telephone.

FEATURE *520 searches for the next available SWCA code. If the system finds an available code, the call is associated with the code and parked. If no code is available, the call remains active on the current telephone, and unassigned to any SWCA button. If the call was already associated with a SWCA code, the call is simply reparked on that code.

FEATURE *537 retrieves the oldest SWCA call. The call becomes active on the telephone that invoked the code, and the indicator on all other telephones becomes solid.

FEATURE *538 retrieves the most recent SWCA call. The call becomes active on the telephone that invoked the code, and the indicator on all other telephones becomes solid.

Programming SWCA controls for your system

This section describes the screen where SWCA controls are defined for the SWCA feature.

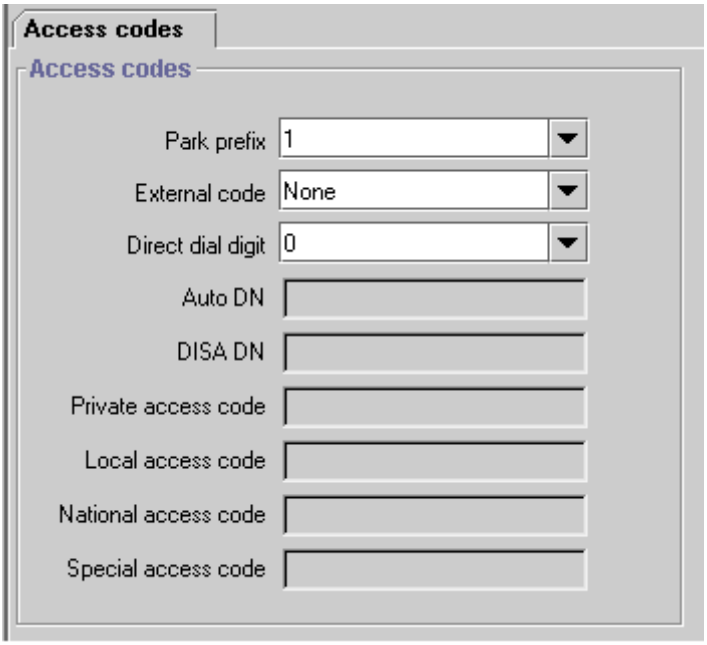
On this screen, you need to determine two things:

- You need to determine how calls will be assigned to SWCA keys, and whether you want intercom (I/C) calls to be treated in the same way.
- As well, you need to determine if using the Hold button will interact with the SWCA features and with intercom calls, and how.

Follow these steps to set the SWCA controls for your system:

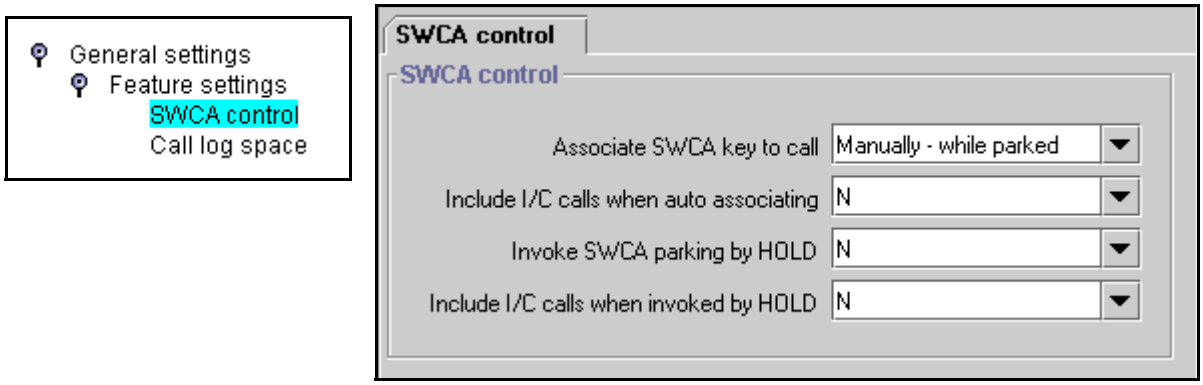
1. On the navigation tree, click on the keys beside **Services**, **Telephony Services**, **General** Settings.
2. Click on **Access codes**.

Figure 152 Checking for Park prefix



3. Ensure that Park prefix has a number beside it. If this access code is set to **None**, SWCA keys will not work.
4. On the navigation tree, click on the keys beside **Services**, **Telephony Services**, **General Settings**, and **Feature settings**.
5. Click on **SWCA Controls**.
   The SWCA Controls screen appears in the right frame.

Figure 153 Setting SWCA controls



6 Use the values in the following table to set the SWCA controls.

Table 113 SWCA controls

Attribute/Value	Description
Associate SWCA key to call Manually - while parked Manually - life of call Automatically - life of call	Choose how a call will be parked on a SWCA key.
Manually - while parked: The user either presses a free SWCA key on the telephone, or dials the feature code for a free key. Once the call is retrieved, it is unassigned from the SWCA key. Manually - life of call: The user either presses a free SWCA key on the telephone, or dials the feature code for a free key. When the call is retrieved, it remains assigned to the SWCA key. The key is freed only after the call is terminated. Automatically - life of call: When a call is answered, it will automatically be assigned to a free SWCA key, starting with the lowest available number. When the call is retrieved, it remains assigned to the SWCA key. The key is freed when the call is terminated.	
Include I/C calls when auto associating Y or N	Decide if you want intercom calls to automatically park on SWCA keys.
If you choose Y (yes) ... **Associate SWCA key to call** must be set to **Automatically - Life of call** for this feature to work. When the user makes a call using the intercom button, the call automatically associates with a free SWCA key, and remains assigned for the duration of the call. If you choose N (no) ... The user must manually assign an intercom call to a SWCA key. The call will otherwise behave by the rules of the choice made for **Associate SWCA key to call**.	

Table 113 SWCA controls (Continued)

Attribute/Value	Description
Invoke SWCA parking by Hold Y or N	Choose whether calls that are put on hold will automatically assign to a SWCA key.
If you choose Y (yes) ... When the user presses Hold, the system attempts to repark the call on the current SWCA key assigned to the call, or on a free SWCA key programmed on the telephone. If no SWCA is currently associated with the call (Automatically - life of call is not turned on), and there is no free SWCA key to assign to the call, the call remains on Hold on the line it came in on. Note: In this case, the call is not available to other telephones in the group until it can be assigned to a SWCA key or unless they have the same line appearance as the held call. If you choose N (no) ... There is no interaction with SWCA keys. The call remains on Hold on the line it came in on and is not available to other telephones in the SWCA group unless the user manually assigns the call to a SWCA key or unless those telephones have the same line appearance as the held call.	
Include I/C calls when invoking by Hold Y or N	Choose whether intercom calls put on Hold will automatically assign to a SWCA key.
If you choose Y (yes) ... Invoke SWCA parking by Hold must be set to Yes to activate this feature. When the user makes an intercom call, and puts it on Hold, the call works the same ways as described in Invoke SWCA parking by Hold, Yes. If you choose N (no) ... Intercom calls will be held on the local line, regardless of what you chose in Invoke SWCA parking by Hold. If the intercom call was assigned to a SWCA key automatically, you can press the SWCA key to repark the call and make it available to other telephones in the group. If you manually assign the intercom call to a SWCA key, the call is automatically parked, and it becomes available to the rest of the group.	

SWCA notes:

Refer to "Programming telephone buttons" on page 419 for details about programming the memory buttons in each DN record.

- A telephone must either have a line appearance of the call or a free intercom button to be able to retrieve a parked SWCA call.
- The number of SWCAs that can be assigned will depend on available programmable buttons on the telephone.
- Companion and DECT cordless telephones do not have programmable buttons and cannot have programmed SWCAs.

NetVision telephone interactions with SWCA keys

For NetVision handsets that do not have physical programmable buttons you can program the three SWCA search codes onto the feature menu through the NetVision Phone Administrator (NVPA). Refer to the *NetVision Phone Administrator Guide* for details.

SWCA park and retrieve codes must then be assigned under **User Preferences**, **Button Programming** on the DN record for the handset to provide the search codes with a range of local SWCA codes from which to park and retrieve calls. Users can also park and retrieve calls using SWCA codes that are not assigned to the handset, by manually entering that code on the handset using the **FCT**/Feature sequence. Refer to the NetVision Feature Card for details about using the **FCT** menu Feature listing.

How SWCA works in a call group

The SWCA feature displays call appearances on any telephones in the system which have buttons with displays assigned for the same SWCA answer keys.

If you want to assign sets of SWCA answer keys to specific call groups, the same buttons on each telephone in a group should be programmed with the same SWCA feature code, to allow for consistent service across the group.

When calls are parked on a SWCA key, the call can be answered by anyone in the group.

- A solid indicator means that someone has control of the call.
- A blinking indicator means the call is parked and can be answered by anyone in the group.

The following two figures show how the indicators change, depending on the state of the call.

Figure 154 SWCA indicators, incoming call from a line (auto SWCA association is on)

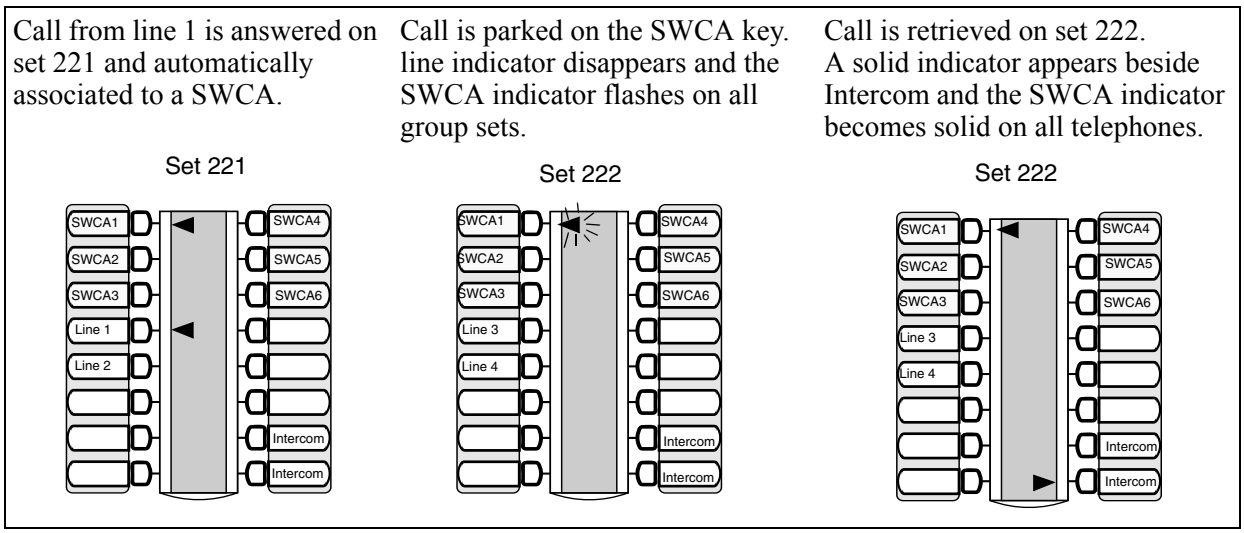
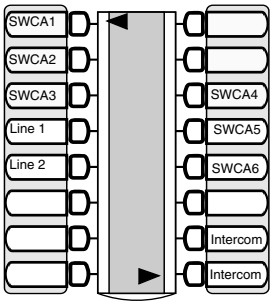
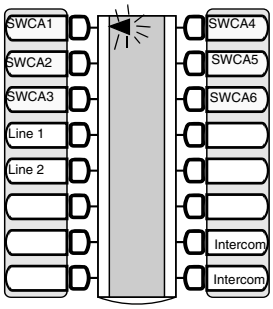
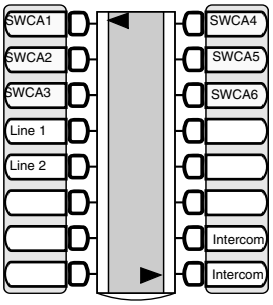


Figure 155 SWCA indicators, incoming call from an intercom (auto SWCA association for intercom is on)

Call is answered and automatically associated to a SWCA.	Call is parked on the SWCA. Intercom indicator disappears and the SWCA indicator flashes.	Call is retrieved. A solid indicator appears beside Intercom and the SWCA indicator becomes solid on all telephones.
		

Transferring calls between SWCA groups

Calls can still be transferred between groups. If a call received at one group seems more appropriate for a different group, the user manually enters a SWCA code that applies to the other group. Once the call successfully transfers, it is dropped from the SWCA key of the first group.

If the call needs to be handled by a telephone without SWCA key assignments, the call can be left parked on the original associated SWCA key. The user who wants to take the call then dials the SWCA feature code for the call. At this point, the call is dropped from the SWCA key on all telephones. If the call needs to be assigned back to the group, the user manually enters a SWCA code for the group to repark the call.

Parking and retrieving calls on SWCA keys

The system administrator determines whether calls automatically associate with free SWCA keys, or whether the user must manually assign the call, either by pressing a SWCA key, by dialing a SWCA code, or by pressing the Hold button (refer to "Hold" on page 469).

The system settings also determine if the call is associated with the SWCA key for the duration of the call or only while the call is parked on the SWCA key.

Manually associating a call

On the M/T-series telephones and the IP i-series telephones, there are three ways of manually associating a call to a SWCA key. Note that in all three cases, once the call is parked, the call must be retrieved to make it active again.

1. If the telephone has assigned SWCA keys, press one of the keys that has no indicator showing.
2. Enter a SWCA dial code on the dialpad. If the telephone has a key programmed for that code, a flashing indicator will appear beside the button.
3. Enter **FEATURE *520** and allow the system to automatically assign the call to one of the defined SWCA keys on your telephone.

Parking a call to a SWCA key

If a call is manually assigned to an SWCA key, the call automatically goes into park mode.

If a call is automatically assigned to an SWCA key when it is answered, you have three choices for parking the call:

1. Press the SWCA key the call is assigned to. A flashing indicator fill appear beside the button.
2. Enter a SWCA dial code on the dialpad. If the telephone has a key programmed for that code, a flashing indicator will appear beside the button.
3. Enter **FEATURE *520** and allow the system to automatically assign the call to one of the defined SWCA keys on your telephone, although, not necessarily the same SWCA it was originally assigned to.

Retrieving a parked call from a SWCA key

You can only retrieve a call if your telephone has an intercom (I/C) button that is free. Refer to "How SWCA works in a call group" on page 466.

There are four ways to retrieve a parked SWCA call:

1. Press a SWCA key beside any flashing indicator.
2. Dial the SWCA code that you know has a call parked on it. (**FEATURE *521** to **FEATURE *536**)
3. Dial **FEATURE *537** to retrieve the oldest parked call on your telephone.
4. Dial **FEATURE *538** to retrieve the most recently-parked call on your telephone.

   Note: If you retrieve a call, and then repark it. That call becomes the most recently-parked call, regardless of where it stood on the original stack of calls.
   Internal calls: You cannot retrieve a SWCA call at a telephone that originated the intercom call.

Call interactions with SWCA controls

Some call features have impacts when activated from or to a call assigned to a SWCA key.

Transferring calls

If you transfer the call to a telephone that does not have the same SWCA keys assigned, the call will disappear from the SWCA key on your telephone once the call is transferred. If the call needs to be reassigned to your group, the person who answered the call would manually enter a SWCA control code that is assigned to your group, to repark the call on a SWCA key.

Conference calls

A conference call cannot be parked on a SWCA key.

You cannot conference a call that is parked on a SWCA key. To conference such a call, you need to retrieve the call, and then put it on hold, and then create the conference.

If a conference call is created from two SWCA-associated calls, and then a transfer occurs by the conference master releasing, the remaining call between the two conference slaves will move to being associated to only the currently associated SWCA keys (if any) on the slaves.

If a conference call is created from two SWCA-associated external calls, and then a transfer occurs by the conference master releasing, the remaining call between the lines/trunks will not be associated with any SWCA keys.

Hold

Only active calls can be assigned to SWCA keys. If you want to move a call on hold to a SWCA key, you must un-hold the call, and then assign the call to a SWCA key.

Your system administrator can set a SWCA system control to force a call to attempt to assign to a SWCA key when you press hold for an active call. If the call cannot be assigned to a SWCA key, such as the case where all keys are already assigned, the call remains on hold at your telephone.

Auto hold

If auto hold is enabled for the telephone, and you press a SWCA key with a parked call while you are still on an active call, the active call will automatically be put on hold at your telephone, assuming that an intercom resource is available for the call.

If auto hold is not enabled for the telephone, and you press a SWCA key with a parked call while you are still on an active call, the active call gets dropped.

You can change this setting at the telephone using **FEATURE 73** to enable the feature or **FEATURE #73** to disable the feature. Or your system administrator can change the setting through the Unified Manager under **Capabilities** for each telephone.

Resetting call log space

The Call log space heading allows you to reallocate the Call log space equally to all telephones in your system.

Warning: Use this heading only if you want to allocate an equal amount of log space to all the telephones in your system.
Reallocating Call log space may destroy Call log data at telephones that lose space. There are 600 Call log spaces available in the system. There are no spaces allocated by default. Changing the space allocation using Log defaults defines the log space available to all telephones in the system.

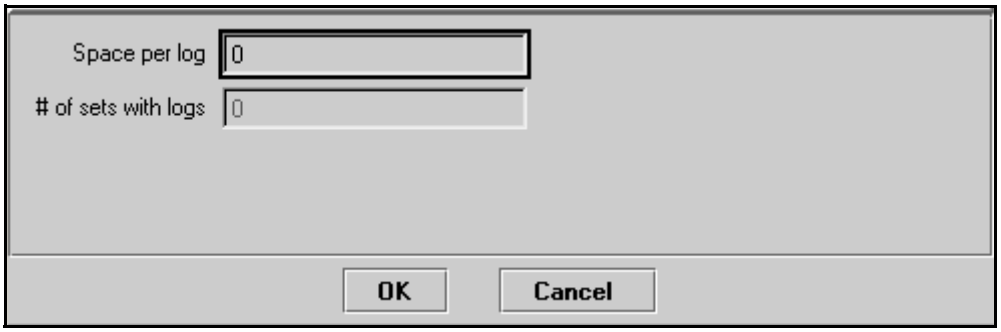
To reset call log space, follow these steps:

1 Click the keys beside **Services**, **Telephony services**, **General settings**, **Feature settings.**

2 Click on **Call log space**.

3 On the menu at the top, click **Configuration**.

4 Click **Reset logs**.
A dialog appears.

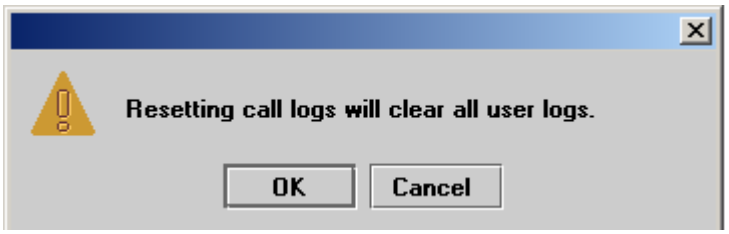


5 The following table explains the type of content for the two fields in the dialog box.

Table 114 Call log options

Attribute	Value	Description
Space per log	<*three digits*>	Type a three-digit number, for example, 020, to give each set 20 spaces
# of sets with logs	Read-only	Lists the number of sets that have logs. If you click **OK** on this dialog, these logs will be deleted.

6 Click **OK**.
A dialog box appears, warning you that all existing logs will be cleared if you reset logs.



7 Click **OK** to reallocate the log space and clear all user logs.
Click **Cancel** if you do not want to clear user logs. In this case, the call log space will not be reallocated.

System features matrix

To help you identify your system feature settings, transfer the following information to a spreadsheet and fill out the values.

Table 115 System features

Background music	Y or N	Set relocation	Y or N
On hold	Tones Music Silence	Message reply enhancement	Y or N
		Answer key	Basic Enhanced Extended
Receiver volume	Use sys volume Use set volume		
Park mode	Lowest or Cycle	Force auto/spd dial over ic/conf	Y or N
Delayed Ring Transfer	1 2 3 4 6 10	Conference Tone	Y or N
Held line reminder	Off 30 60 90 120 150 180 seconds	Network Callback timer	
		Clid Match Length	3-8, None
Directed pickup	Y or N	Maximum CLI per line	30 (read-only)
Page tone	Y or N	Maximum System Speed dial	70 or 255
Alarm set	None DN: DN <control set>		
Call log space			
Space per log		# of sets with logs	
SWCA controls			
Associate SWCA key to call	Manually - while parked Manually - life of call Automatically - life of call		
Include I/C calls when auto associating	Y or N		
Invoke SWCA parking by Hold	Y or N		
Include I/C calls when invoking by Hold	Y or N		

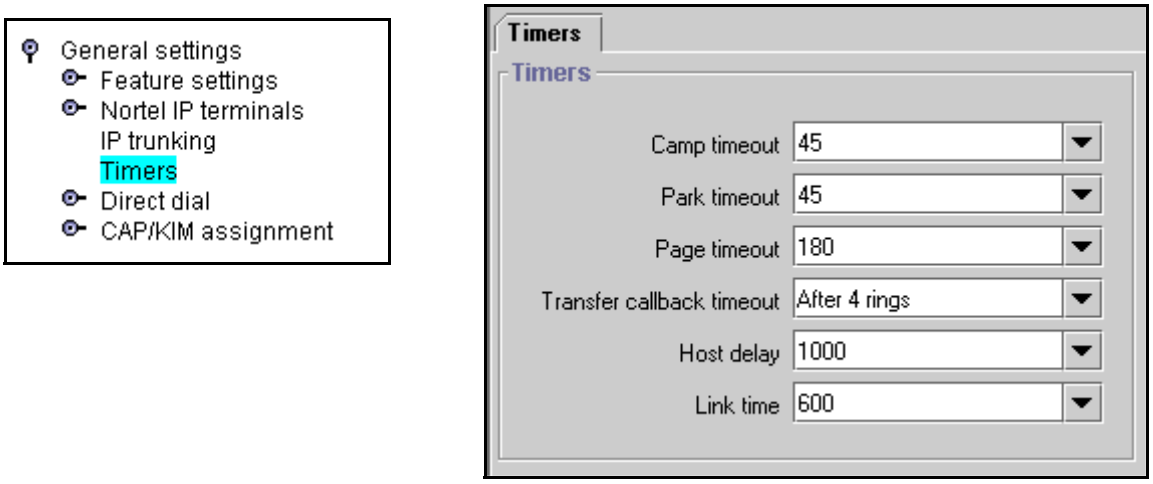
Setting system timers

The settings under Timers allows you to define a number of timed features for your Business Communications Manager system. These settings apply to all telephones connected to the Business Communications Manager system.

1 Click the keys beside **Services**, **Telephony Services**, and **General Settings**.

2 Click on **Timers**.
The Timers window appears in the right frame.

Figure 156 Setting system timers



3 The possible settings are described in the following table.

Table 116 Timer values

Attribute	Values	Description
Camp timeout	30, 45, 60, 90,120, 150 or 180 seconds	Assign the number of seconds before an unanswered camped call returns to the telephone that camped the call.
Park timeout	30, 45, 60, 90, 120, 150, 180, 300 or 600 seconds	Assign the number of seconds before a parked call on an external line returns to the telephone which parked the call. This interval is used for SWCA lines as well.
Page timeout	15, 30, 60, 120, 180, 300, 600 2700 seconds	Define the period of time after which the paging feature automatically disconnects.
Transfer callback timeout	Off after 3 rings after 4 rings after 5 rings after 6 rings after 12 rings	Specify the number of rings before a callback occurs on a transferred call. You can estimate the delay in seconds if you multiply the number of rings by six. Note: This setting can affect transferred calls from voice mail and should be configured accordingly.

Table 116 Timer values (Continued)

Host delay	200, 400, 600, 800, 1000, 1200, 1400, 1600, 1800 or 2000 milliseconds	Assign the delay between the moment an outgoing line is selected to make an external call (for example, by lifting the receiver off the telephone) and the moment that Business Communications Manager sends dialed digits or codes on the line.This ensures that a dial tone is present before the dialing sequence is sent. Minimizing this delay provides faster access to the requested features.
Link time	100, 200, 300, 400, 500, 600, 700, 800, 900 or 1000 milliseconds	Specify the duration of a signal required to access a feature through a remote system. The Link time depends on the requirements of the host switching system. For example, to program external dialing through a Centrex system requires a Link time of 400 ms. Link is another name for recall or flash.

Timers matrix

To help you identify your system timing settings, transfer the following information to a spreadsheet and fill out the values.

Table 117 Timer fields

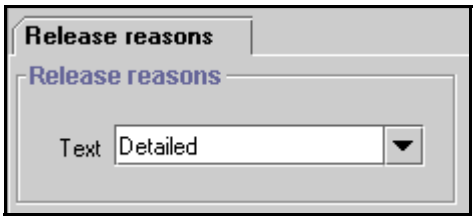
Camp timeout	Transfer callback timeout
Park timeout	Host delay
Page timeout	Link time

Define release reason levels

The **Release reasons** heading allows you to determine the level of system reporting you require for released ISDN calls. You can choose to have no text, a simple explanation, or a detailed explanation.

To set **Release reasons**, follow these steps:

1. Click on the keys beside **Services**, **Telephony services**, and **General settings**.
2. Click on **Release reasons**.
   The Release Reasons screen appears.



3. The following table lists the possible values for Release reasons.

Table 118 Release reason values

Attribute	Values	Description
None	Default value	No text will accompany a dropped call notification.
Simple	Cause code: Off On	 Off: no text is provided. On: the code only is provided. Note: If you select Simple text, you must turn off the Cause code. This is for diagnostics purposes, only.
Detailed	No settings	A detailed explanation of the cause code is provided.

Configuring system speed dial numbers

The System speed dial heading accesses screens that allow you to assign speed dial codes to external numbers that can be dialed from any telephone on the system. Examples of system speed dials might include telephone numbers of regional sales offices within your organization or key customers that you call frequently.

The *Programming Records* document contains a table where you can note all the codes you enter so that you can provide copies to your users.

TASK: Set up the system so users can dial frequently-called numbers using two or three digits. ("Assigning numbers to system speed dial codes" on page 476)

You have two choices about how many system speed dials you want to make available to the system.

- The default is 70 speed dial codes from 01 to 70. This is the number of codes available in all legacy software.
- If you have the number of speed dial codes set to 255, the codes are 001 to 255.

  If you want to use alpha tagging ("Using alpha tagging for name display" on page 455), you may need to increase the number of codes to allow for more matching possibilities for incoming calls. For information about setting this the maximum speed dials for your system to 255, refer to table entry: *Maximum System Speed Dials* on page 460.

Speed dial codes can be programmed onto memory keys by the installer during button programming. Refer to "Programming telephone buttons" on page 419. Also, each user can assign speed dial codes to memory buttons directly on the telephone. Refer to the *Telephony Features Handbook* and the *Feature User Card* for instructions about using memory keys.

These speed dial codes are the same for all users. You can also configure a set of codes specific to a telephone using User speed dial programming when you program the DN for each set. Refer to "Configuring user speed dialing" on page 432.

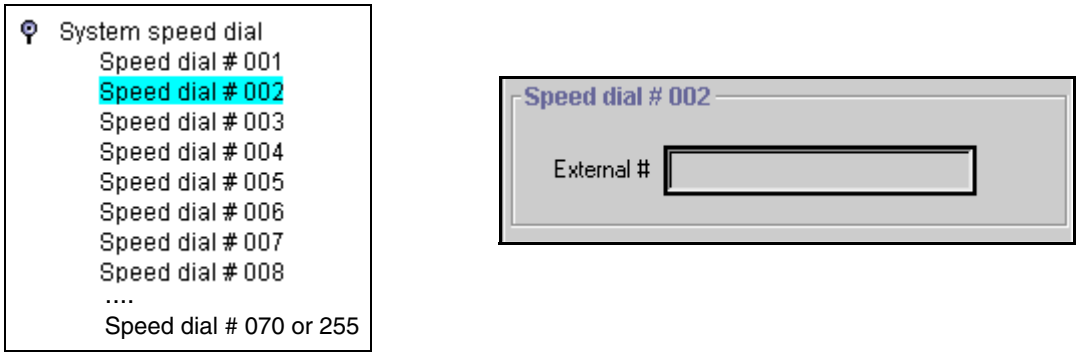
Assigning numbers to system speed dial codes

Follow these steps to create a speed dial code for quick-access to an external number:

1 Click on the keys beside **Services**, **Telephony services**, and **System speed dial**.

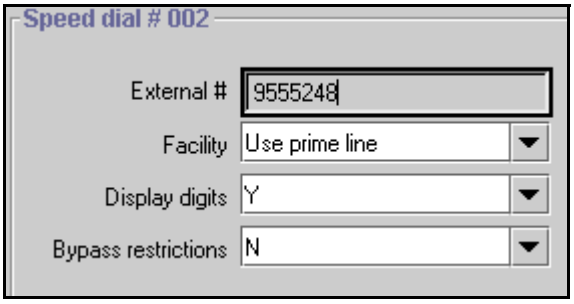
2 Click a **Speed dial number** (Speed dial # XXX).

Figure 157 Undefined speed dial screen



3 In the **External #** box, type the telephone number (up to 24 digits), and then press **Enter**. If this is a new speed dial, more fields appear after you press Enter.

Figure 158 Expanded speed dial screen

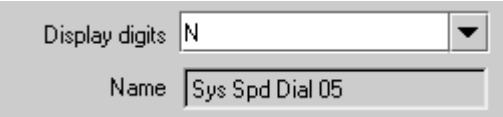


4 Use the following table for the possible speed dial parameters.

Table 119 Release reason values

Attribute	Values	Description
Facility	Use prime line Use line: Pool code Use routing table	Select the route you want the dialed number to take out of your system. Note: Any lines or pool codes that you specify must be assigned to the telephone where the code is entered. If you choose prime line, a prime line must be assigned to the telephone where the code is entered. Refer to "Assigning line access" on page 394.

Table 119 Release reason values (Continued)

Display Digits Name	Y or N If N is selected: <alphanumeric>	Y = the speed dial number displays N = the name defined for the speed dial displays  In the Name field, enter the name you want to display for alpha tagging.
Bypass restrictions	N or Y	N = the dialed number will use the line and set restrictions Y = the dialed number will bypass any line and set restrictions

Caution: Resource issue:

Entering a large number of system speed dials at one time can impact system performance. Therefore, it would be best to perform this activity during low-user periods, where possible.

System speed dial matrix

To help you organize your system speed dial information, transfer the following information to a spreadsheet.

Table 120 System speed dial matrix

Speed dial #:	External #	Facility	Display digits	Bypass restr'n
		Use prime line Pool code:___ Use routing tabl:___ Use Line: ___	Y N	Y N

Setting system telco features

The Telco features commands found under the **General** heading allow you to define settings for voice message center numbers and outgoing name and number blocking (ONN).

Task:

- Set up voice message access and control strings ("Defining Voice Message Center numbers" on page 478)
- Set up the method for blocking outgoing set identification ("Setting outgoing name and number blocking" on page 479)

Defining Voice Message Center numbers

If you subscribe to a voice message service outside your office, you can access it through your Business Communications Manager system. You can specify what voice message center you use for each external line that receives message waiting indication. This setting specifies the external telephone numbers that the Message feature dials to retrieve voice messages.

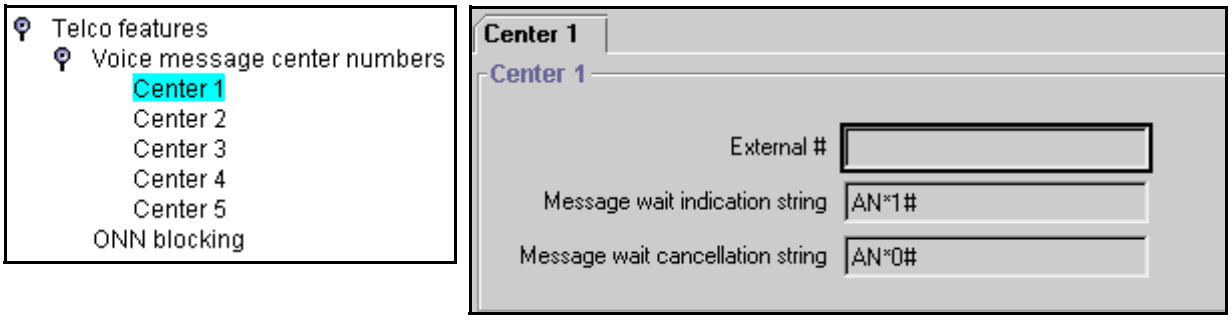
Note: If you have an MCDN network link set up with a Meridian 1 voice mail service, for example, you need to ensure that the number of the voice mail system is entered here, complete with external dialing requirements.

1 Click on the keys beside **Services**, **Telephony services**, and **Telco features.**

2 Click on the key beside Voice message center numbers.

3 Click the Center number you want to program. For example, **Center 1**.
The Center 1 screen appears.

Figure 159 Voice message center programming



4 The following table explains the settings for the Center # screen.

Table 121 Voice message center settings

Field	Values	Description
External #	<phone number>	Enter the telephone access number of the remote voice message system.
Message wait indicate string	<string>	indicates that the message center has a message in the mailbox. This is a default NSI string for message waiting.

Table 121 Voice message center settings (Continued)

Field	Values	Description
Message wait cancellation string	<string>	indicates that the voice messages have been retrieved. This is a default NSI string for message waiting.

5 Repeat for each center you want to identify.

TIPS:

- A telephone does not show that external voice messages are waiting unless you enable **VMSG set** for the lines assigned to each telephone under **Line Assignment**. Refer to table entry: *Vmsg set* on page 399.
- Analog telephones connected to an ASM8+ on systems running BCM 3.6 or newer software can receive message waiting indicators if the analog line supports CLID. MWI indicator settings for analog telephones or for analog telephones attached to ATA2s, are set under the ATA heading. Refer to "Determining analog settings" on page 412.
- You can program up to five voice message center numbers, but many systems require only one.

Setting outgoing name and number blocking

When you activate Outgoing name and number blocking (ONN), a user presses **FEATURE 819** to block the outgoing name and number on a per-call basis. The system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call.

ETSI note: ETSI lines may use the Calling Line Information Restriction (CLIR) supplementary service to provide this feature.
ETSI PRI lines do not use a VSC. The line always uses Suppression bit to invoke the CLIR supplementary service.

Business Communications Manager alerts the CO by two methods. The method used depends on the type of trunk involved in placing the outgoing call.

- Analog trunks use a dialing digit sequence called a Vertical Service Code (VSC). The VSC differs from region to region and must be programmed. Analog trunks with both tone and pulse dialing trunks can have separate VSCs. Refer to "Configuring ONN blocking service codes" on page 480.
- PRI trunks have only one VSC. No specific system programming is required. See ETSI note, above.
- BRI trunks can be set to either:
  - provide ONN using a suppression bit, which provides a notice from the system to the central office to withhold CLI.
  - provide ONN using a VCS, which is dialed out in front of the dialed digits (optional on ETSI trunks). Refer to "Configuring ONN blocking service codes" on page 480.

  BRI trunk ONN settings are located under the loops settings. Refer to "Identifying BRI T-loops (T1 profiles)" on page 267 or "Identifying BRI T-loops (ETSI, QSIG)" on page 271.

Programming note: Ensure that users who have access to this feature have telephones with valid OLI numbers. Refer to "Assigning line access" on page 394.

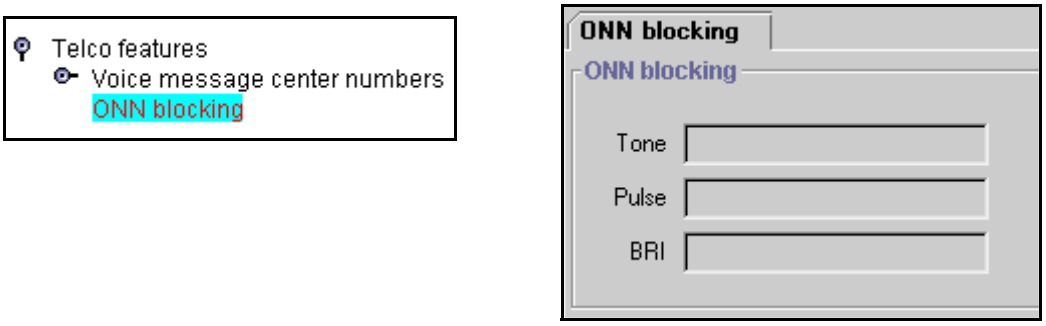
Configuring ONN blocking service codes

Follow these steps to configure an ONN setting:

1 Click on the keys beside **Services**, **Telephony services**, and **Telco features.**

2 Click on **ONN blocking.**

Figure 160 ONN blocking parameters



3 The following table explains the possible choices for ONN blocking.

Table 122 ONN blocking settings

Field	Values	Description
Tone	F78(0 to 9, *, #)	For analog trunks, enter a digit or character to determine what code the user will enter to activate this service.
Pulse	F78(0 to 9, *, #)	For digital trunks, except BRI, enter a digit or character to determine what code the user will enter to activate this service.
BRI	F78(0 to 9, *, #)	For BRI trunks, enter a digit or character to determine what code the user will enter to activate this service.

Note: When ONN is active, set and set/line restrictions are ignored. The CO call back feature is also disabled until the feature is cancelled.

Telco features matrix

To help you organize your voice message center information, transfer the following information to a spreadsheet.

Table 123 Telco features matrix

Voice Message Center numbers	ONN Blocking (F78)	
VMsg center 1-5	Tone	<blank>F780123456789*#
External Number	Pulse	<blank>F780123456789*#

Table 123 Telco features matrix

Message Wait Indication String	BRI	<blank>F780123456789*#
Message Wait Cancellation String		

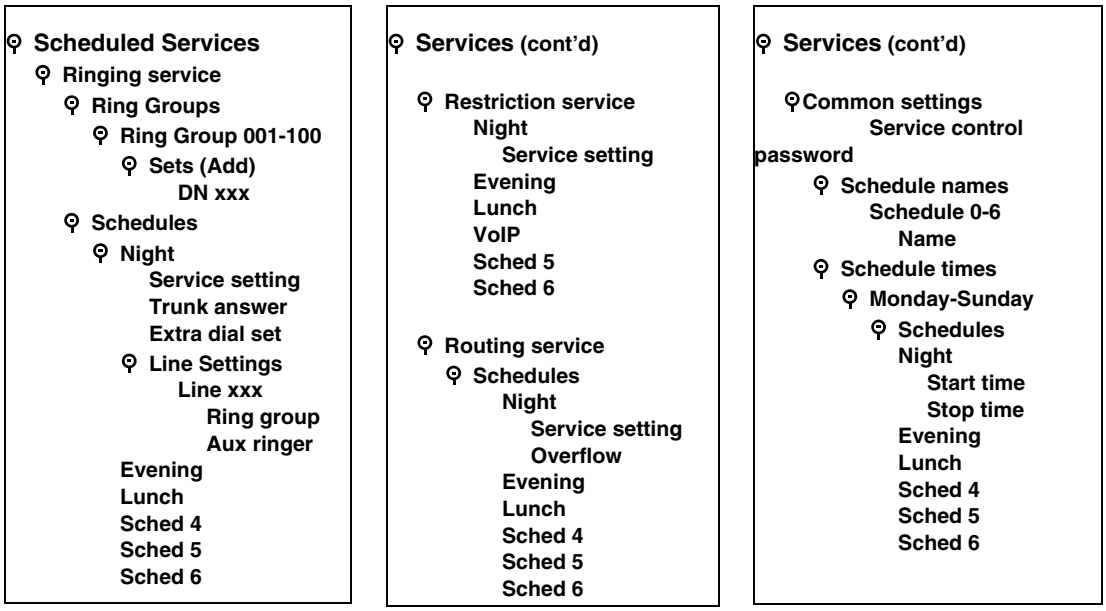
Chapter 17
Configuring schedules

This section describes the headings where you configure system-wide schedules. The information discussed in this chapter is found under the Telephony Services heading **Scheduled services**.

Task:
• Understand how to activate and deactivate schedules from a control telephone ("Turn services on and off" on page 484)
• Set up the common headings and times for the schedules ("Defining common schedule settings" on page 485)
• Configure Ringing, Restriction, and Routing schedules. ("Defining service schedules" on page 489)
• Define Service control password ("Defining the service control password" on page 485)

The following figure shows the Scheduled Services navigation tree headings:

Figure 161 Scheduled Services headings



Turn services on and off

You can manage schedules from a control telephone using the feature codes shown in the table below. This section provides step-by-step instructions for turning services on and off on one-line and two-line display telephones.

Table 124 Turning services on and off

On: **FEATURE** 871 Off: **FEATURE** #871	Controls Ringing service schedules. When used at the direct dial telephone, it activates the alternate direct dial telephone (extra dial telephone).
On: **FEATURE** 872 Off: **FEATURE** #872	Controls Restriction service schedules. This feature requires a service control password. Refer to "Defining the service control password" on page 485.
On: **FEATURE** 873 Off: **FEATURE** #873	Controls Routing service schedules. This feature requires a service control password. Refer to "Defining the service control password" on page 485.

1. Enter the appropriate feature code from a control telephone.
2. For the Restriction service or Routing service, you will be prompted for a Password. Enter the **Service Control Password**.
   Contact your system administrator for the current password if the default password does not work. (Default: 23646).
3. Access the schedule list, and choose the schedule:
   Two-line display:
   When a service is active, the control telephone display shows `Services ON`.
   a. Press `LIST`. The display shows the first active service and the schedule in use.
   b. If there are several active services, press `NEXT` to view all of the services.
   c. Press `OK` to select the setting, or press `QUIT` to exit the feature

   One-line display:
   a. Press **FEATURE 870**. The display shows the first active service.
   b. Press # to move through the active schedule.
   c. Press **RELEASE** to exit. Services that turn on automatically have an asterisk (*) appearing before the name on the display. You cannot manually activate or cancel scheduled services. However, you can override a schedule service by manually activating another schedule.

To turn a service off, enter the appropriate feature code from a control telephone.

Caution: Assigning a service as Normal is not the same as cancelling a service using a feature code. If you assign the service as Normal, the Normal schedule version of a service overrides any automatic schedule and remains until you manually cancel it. When you cancel service by feature code, you return to the automatic schedule.

Overriding services with a Control telephone

The control telephone can override services turned on and off according to a schedule by entering a Services feature code, and then by selecting a different schedule. This override remains until canceled. If you select a schedule with an asterisk (*), the next automatic service schedule comes into effect at the programmed time.

Direct-dial telephone ringing service

Direct-dial calls to a direct-dial telephone ring at the extra dial telephone when you enter the Ringing service feature code (**FEATURE 871**) at that direct dial telephone. The installer assigns the extra dial telephone. Note that only the extra dial telephone is activated, not the actual Ringing service (unless that direct-dial telephone is a control telephone).

Defining common schedule settings

The **Common settings** heading allows you to define the common names and times for the services schedules. You also define the service control password under this heading.

- "Defining the service control password" on page 485
- "Changing schedule names" on page 486
- "Changing schedule times" on page 487

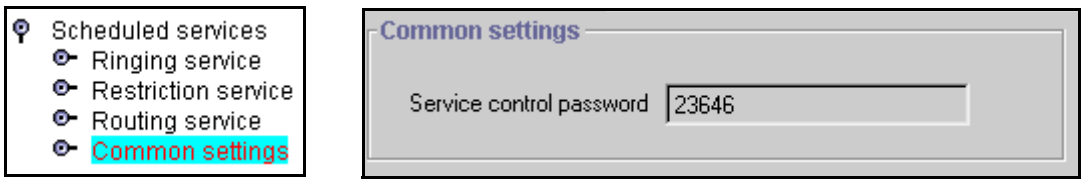
Defining the service control password

Use these steps to locate and confirm or change the password users will need to access the services feature from a control telephone to change Restriction or Routing service settings.

1 Click the keys beside **Services**, **Telephony services**, **Scheduled services.**

2 Click on **Common settings**.

Figure 162 Entering the Service control password



3 In the **Service control password** field, the default is set at 23646. You can change this, as required.

Security note: Change the default password once you have your system set up and have tested the services features. Keep the password in a safe place.

Changing schedule names

Schedules have been given default names. However, if you change the purpose of your schedules, you can also change the name to reflect this.

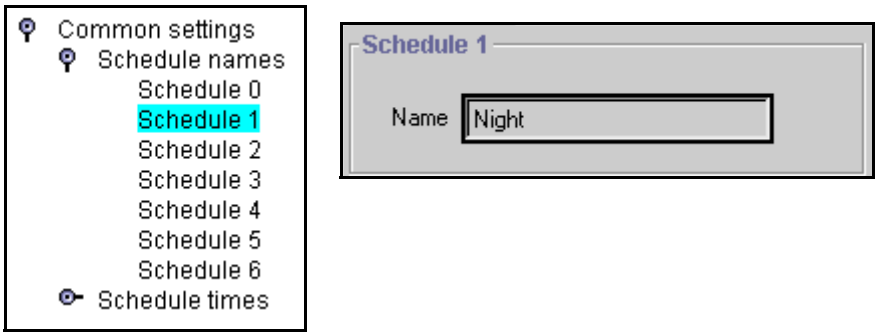
Use these steps if you want to change the name of a schedule.

1 Click on the **Common settings** key and on the **Schedule names** key.
A list of seven schedule records displays.

Note: Schedule 0 is named Normal and cannot be changed. Schedule 1 to 6 have default names which can be changed to meet your requirements.

2 Click on the schedule for which you want to change the name.
Note: Schedule 0 (Normal) cannot be changed.

Figure 163 Entering schedule names



3 Type in a new name for the schedule.

4 Press <**Tab**> to save the change.

TIPS: Reserve a couple of schedules (i.e. 5, and 6) for alternate call routing.

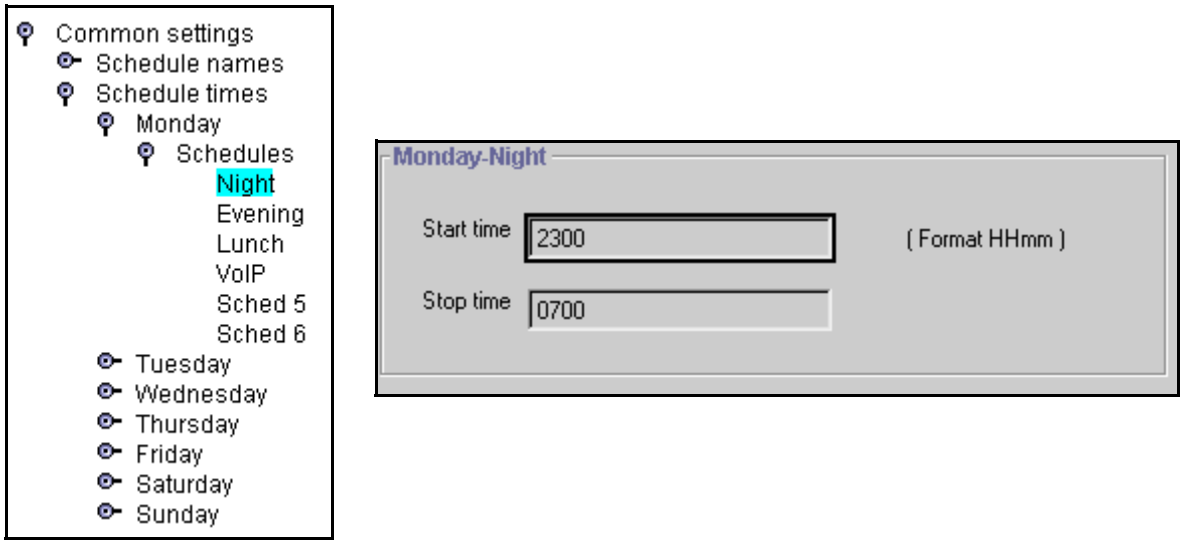
An example: If you have specific lines for which you want to allow fallback to a specific route, you must define a 24-hour schedule for the preferred lines destination code. To do this, you can rename schedule 5, or 6 to PRIME, so that you know which schedule to use when you are assigning the feature to telephones.

Changing schedule times

Schedule start and stop times are set at times you are most likely to want each service to be active.

1. Click the keys beside **Services**, **Telephony services**, and **Scheduled services,** and **Schedule times**.
2. Click the key beside the day you want to program (for example, **Monday**).
3. Click the key beside **Schedules**.
   The programming menu expands to display all the schedules.
4. Click the schedule you want to program. The Day-Schedule window appears.

Figure 164 Entering schedule time parameters



5. Type the start and stop times for each schedule on each day.
   The following table provides a list of the default times for each schedule.

Table 125 Default schedule times

Schedule	Start time	Stop time
Schedule 1: Night	23:00	07:00
Schedule 2: Evening	17:00	23:00
Schedule 3: Lunch	12:00	13:00

Schedule	Start time	Stop time
Schedule 4:	00:00	00:00
Schedule 5:	00:00	00:00
Schedule 6:	00:00	00:00

About start and stop times

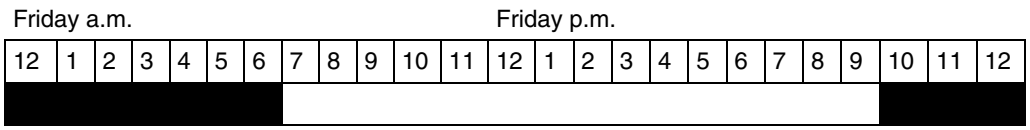
Here are some general rules about setting start and stop times:

- It is only necessary to program start and stop times for schedules that are activated automatically.
- The time may be entered in either 12 or 24-hour format. If the display is in English, and the hour entered is less than 13, the display prompts you to specify **AM** or **PM**.
- If you assign identical start and stop times for a schedule, for example, 04:00 start and 04:00 stop, the schedule is in effect all day. The only exception to this is a start and stop time of 00:00; in this case the schedule is off for the day.
- You may assign overlapping times. For example, if schedule 1 is assigned from 9:00 a.m. to 4:00 p.m. and schedule 2 is assigned from 1:00 p.m. to 5:00 p.m., then the start time of the second schedule is treated as a stop time for the first schedule.
  This is also true if two schedules have the same start time but different stop times. The stop time of the shorter schedule is treated as the start time of the longer schedule.
- If one schedule starts and stops within the times of another schedule, the first service temporarily ends when the second service starts. The first service then resumes when the second service has ended.
- Some schedules start and stop at the same times each day: use **COPY** to copy the start and stop times from one day to the next.

Warning: Start and stop times do not span days.
When you program a schedule to start in the evening and stop in the morning, it does not carry over into the next day. For example, if you program Night service for Friday (22:00 to 6:00), the system turns on Night service from midnight to 6 am on Friday, and then again from 10 p.m. to midnight on Friday, as shown in the diagram below.

Friday schedule:

- Start time: 22:00
- Stop time: 06:00



Defining service schedules

The **Scheduled services** headings access records that allow you to define service by the time of day and day of week for the following services:

- "Configuring ringing service" on page 490
- "Configuring restriction service" on page 493
- "Configuring routing service" on page 495

The headings found under "Defining common schedule settings" on page 485 allow you to determine the schedule names and times for the scheduled services.

Note: To use scheduled services, you must define a control telephone for the telephone you want to use to turn on schedules. Control sets are defined in the DN records under **System DNs**.

Each of the three services has six schedules that you can customize. The names and start/stop times of schedules are the same for all services. For example, if a Monday schedule is set to run the Night schedule from 18:00 to 24:00, it will run this schedule for all services that have Night schedules set to Automatic, and which have been turned on at the control telephone.

For example, you may want to combine alternate call ringing with alternate dialing restrictions for lunchtime, evenings, and weekends (Schedules 1, 2, and 3). Then you may want to run alternate call routing using three separate schedules.

Once you have programmed the different services and schedules, you can turn each of the services on separately. For example, the Night schedule might control both Ringing service and Restriction service. But you can turn on just the Ringing service part of the Night schedule if you wish.

You can activate the services from the designated control telephone for each telephone and line in your system. You can have one control telephone for the whole system, or different control telephones for different telephones and lines.

If you want to have several services active at the same time, simply program them on for the same schedule.

Note: To program services from a telephone, you require an access code. Refer to "Defining the service control password" on page 485.

Configuring ringing service

At certain times or in certain situations, you may want additional telephones to ring for incoming lines. The most common use of this feature is when a security desk telephone rings for incoming lines after 5:00 p.m., a practice often called *night service*.

Each non-auto-answer and target line can be assigned a ringing group for each schedule. If no schedule is set for ringing services, lines ring at any telephones that have the lines assigned.

Note: VoIP trunking lines and PRI lines are automatically set to auto-answer and, therefore, require target lines. BRI lines that are set to auto-answer also ring at target lines. Therefore, by specifying target lines in a ring group, all auto-answer lines can be forwarded to the telephone(s) indicated.

You define ringing services with the following features:

- "Defining ring groups" on page 490
- "Defining ringing service schedules" on page 491
- "Assigning ringing groups to lines" on page 492

Defining ring groups

Ring groups allows you to define groups of extended ringing telephones. A group can be assigned to any line for any of the schedules. You can define up to 100 ring groups with up to 30 telephones for each ring group.

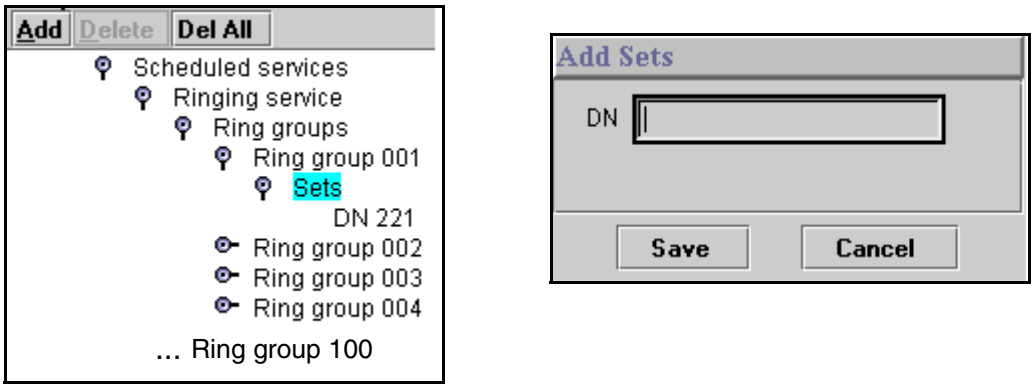
1 Click the keys besides **Services**, **Telephony services**, **Scheduled services**, **Ringing service**, and **Ring groups**.
A list of ring groups displays.

2 Click the key beside the ring group you want to program. The subheading **Sets** appears.

3 To add DNs, click on **Sets**, and then click the **Add** button, located at the top of the column.

4 In the Add Sets window, type the DN of the set you want to assign to this ring group.

Figure 165 Adding a telephone to a ring group



TIPS: You can assign any telephone on the Business Communications Manager system to a ring group. The assigned control telephone for each schedule is added to each ring group. A telephone can belong to more than one ring group.

5 Click **Save** to enter the DN.

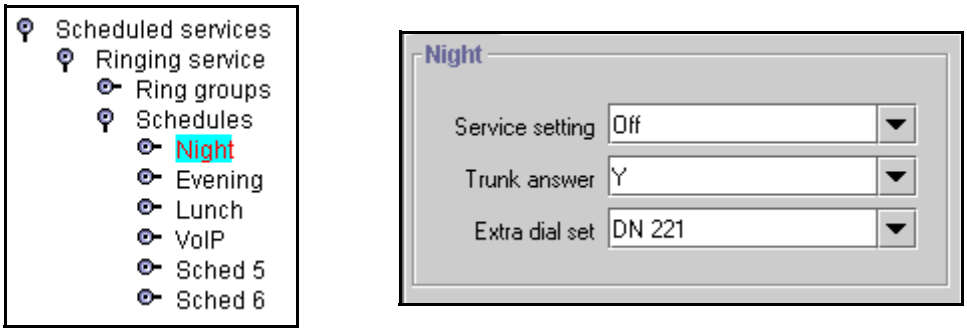
Defining ringing service schedules

Use the following process to indicate how Ringing service should be activated for each of the schedules:

1 Click the keys beside **Services**, **Telephony services**, **Scheduled services**, **Ringing service**, and **Schedules**.

2 Click a schedule name (for example, **Night**). The window for that schedule appears.

Figure 166 Defining ring schedule parameters



3 The following table shows the possible settings for each schedule day.

Table 126 Ringing group schedule values

Attribute	Value	Description
Service setting	Off Manual Auto	**Manual** allows you to turn the service on and off at any time from a control telephone. This setting overrides any automatically-running schedules. Example: You may have a restriction service Night schedule that prevents callers from making long distance calls. Since the Manual setting does not recognize any timing schedules, you can turn this service on at any time and it will be in effect immediately. To allow long distance calls, you would turn this service off at the control telephone, or specify a different schedule that contains a different set of restrictions. **Auto** allows you to program a stop and start time for a service under the Common Settings heading. These times are then automatically executed when the service is active. Example: If you want your evening calls to be routed through a different carrier, you can create the timing for this on one of the spare schedules. You would then find the same schedule under Routing Service and set it to automatic. When you turn Routing Service on, and choose this schedule, the telephone will automatically route all calls through the alternate carrier for the times specified. **Off** prevents the service from being activated.

Table 126 Ringing group schedule values (Continued)

Attribute	Value	Description
Trunk answer	Y or N	Trunk answer allows you to answer, from any telephone, an external call that is ringing at another telephone in your office if the Ringing Service is active on that line at the time of the call. If the service is not active, you cannot answer the call. This is useful if the other telephones are not assigned the same lines as the telephone you are using to answer the call. **Note:** You can change the Trunk Answer setting only if Ringing service is set to Manual or Automatic.
Extra dial set	None DN <XX> DN <control set>	The Extra dial set attribute allows you to assign an additional telephone to receive calls for each schedule. **Note:** The extra dial set is activated during a schedule by entering the Ringing service feature code from the assigned direct-dial telephone. This does not activate the Ringing service unless the direct-dial telephone is also a control set. Refer also to "Creating Direct Dial sets" on page 313. **Doorphone note:** Ensure that this DN does not belong to a doorphone.

Assigning ringing groups to lines

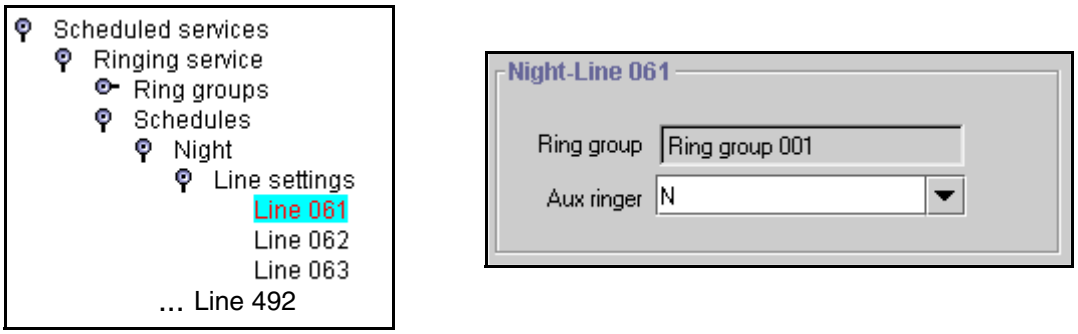
Each line must be assigned a Ringing service for ring group and auxiliary ringer.

Note: If the lines are not set up yet, skip this step until you have defined all the lines.

1 Within each ring schedule, click on the key beside **Line settings** to display the list of lines.

2 Click on each line in turn, or a specific line you want to adjust.

Figure 167 Defining ring service schedule line settings



3 The following table shows the possible settings for each schedule day.

Table 127 Ringing group schedule line values

Attribute	Value	Description
Ring group	Ring group <XXX>	Type in a ring group number (001-100) to choose a different ring group assignment. Only one ring group can be assigned to a line for each schedule. To combine groups of ringing sets, you must create a new ring group which contains all the sets you want to ring and assign it to the line.

Table 127 Ringing group schedule line values (Continued)

Attribute	Value	Description
Aux ringer	Y or N	This variable indicates whether the auxiliary ringer (if installed) also rings when Ringing service is on. **TIPS:** • The default ringing telephone is 221 (Start DN). This means that all lines ring at telephone 221 when Ringing service is on. • You can copy Ringing set and Auxiliary ringer programming from one line to another. • If you have an auxiliary ringer programmed to ring for calls on an external line and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

Configuring restriction service

Restriction service prevents a user from dialing some types of calls from a telephone or from lines that are available at the telephone during the duration of the selected schedule. The installer programs restrictions.

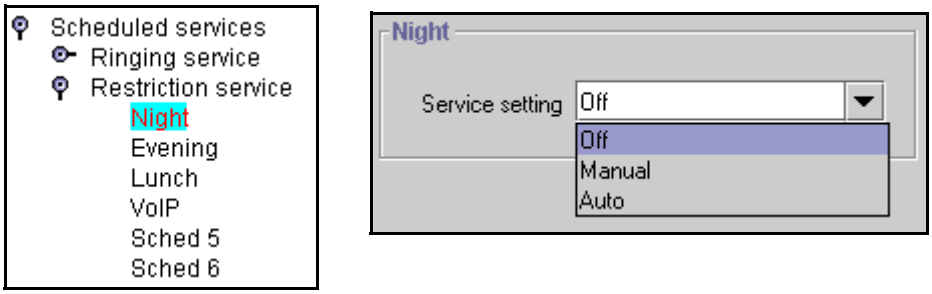
Use these commands to indicate how the alternate dialing restrictions become active for each schedule.

1 Ensure the correct scheduling has been set up for each telephone. (Services, Telephony Services, System DNs, Active DNs, DN XXXX, Restrictions)

2 Click the keys beside **Services**, **Telephony Services**, **Scheduled services,** and **Restriction service**.

3 Select the schedule you want to program, (for example, **Night**).
The schedule window appears.

Figure 168 Defining restriction service setting



4 The following table shows the possible settings for each schedule day.

Table 128 Restriction schedule values

Attribute	Value	Description
Service setting	Off Auto Manual	**Off** prevents the service from being activated.
		Auto allows you to program a stop and start time for a service under the Common Settings heading. These times are then automatically executed when the service is active. Example: If you want your evening calls to be routed through a different carrier, you can create the timing for this on one of the spare schedules. You would then find the same schedule under Routing Service and set it to automatic. When you turn Routing Service on, and choose this schedule, the telephone will automatically route all calls through the alternate carrier for the times specified.
		Manual allows you to turn the service on and off at any time from a control telephone. This setting overrides any automatically-running schedules. Example: You may have a restriction service Night schedule that prevents callers from making long distance calls. Since the Manual setting does not recognize any timing schedules, you can turn this service on at any time and it will be in effect immediately. To allow long distance calls, you would turn this service off at the control telephone, or specify a different schedule that contains a different set of restrictions.

Programming note: This service requires the user to enter a service control password before it can be accessed. Users obtain this password from their system coordinator. Refer to "Defining the service control password" on page 485.

Notes about restriction service filters

These filters are assigned for both telephones and lines. If no restriction filter has been assigned for a telephone or line for the schedule that you make active, then no restrictions will apply to that telephone or line while the schedule is in effect.

Line filters apply to all telephones which have that line assigned.

However, a group of telephones can have different filters for the same schedule. Therefore, you need to be aware of what services you are allowing or disallowing for all telephones assigned to the control telephone you are using. If you are unsure, or want to change a filter for a telephone, you must open a programming session on the Unified Manager and check the DN record for the telephone. Refer to the *Programming Operations Guide* for details about setting up telephone restrictions. For easier administration, you might consider making the filters the same for all telephones connected to a control telephone, with the exception of the control telephone.

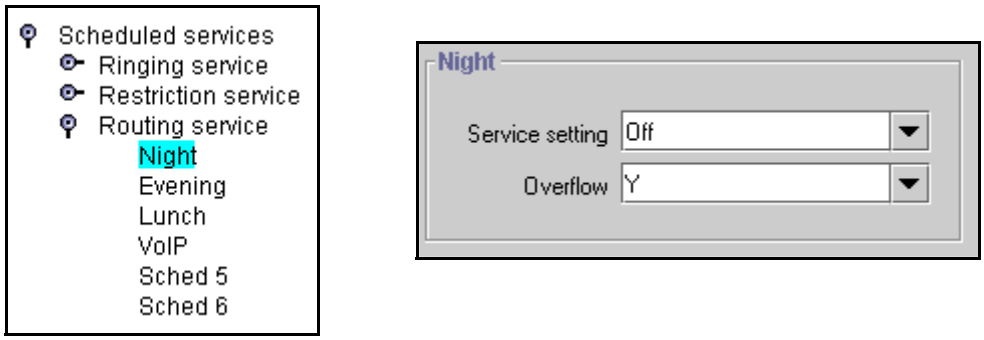
Configuring routing service

Routing service allows you to assign alternate routes to calls. You can take advantage of lower costs available on selected routes for some days and at some times. You can also use this service to set up overflow routing, to allow calls that come into line pools that have no available lines to be answered through an alternate line pool. IP telephones use this service to route calls over a ground line if the VoIP trunk signal is not strong enough to support a call.

Use these steps to activate routing tables for each of the schedules.

1. Ensure the correct scheduling has been set up for each route. (Services, Telephony Services, Call Routing, Destination Codes)
2. Click the keys beside **Services**, **Telephony services**, **Scheduled services**, and **Routing service**. Schedule names display.
3. Select the schedule you want to program, for example, **Night**. The schedule window appears.

Figure 169 Defining routing service settings



4. The following table shows the possible settings for each schedule day.

Table 129 Routing service schedule values

Attribute	Value	Description
Service setting	Off Auto Manual	**Manual** allows you to turn the service on and off at any time from a control telephone. This setting overrides any automatically-running schedules. Example: You may have a restriction service Night schedule that prevents callers from making long distance calls. Since the Manual setting does not recognize any timing schedules, you can turn this service on at any time and it will be in effect immediately. To allow long distance calls, you would turn this service off at the control set, or specify a different schedule that contains a different set of restrictions. **Auto** allows you to program a stop and start time for a service under the Common Settings heading. These times are then automatically executed when the service is active. Example: If you want your evening calls to be routed through a different carrier, you can create the timing for this on one of the spare schedules. You would then find the same schedule under Routing Service and set it to automatic. When you turn Routing Service on, and choose this schedule, the telephone will automatically route all calls through the alternate carrier for the times specified. **Off** prevents the service from being activated.

Table 129 Routing service schedule values (Continued)

Attribute	Value	Description
Overflow routing	Y or N	If all the lines used by a route are busy when a call is made, you can program Routing service to overflow to the route used for normal mode. If this happens, the telephone sounds a warning tone and displays the message **`Expensive route`**. The caller can then release the call to avoid the toll charges, or continue. **TIPS:** A schedule must be active for overflow routing to be in effect. Overflow routing is not available in normal mode. You must create an overflow route to be used with each destination code. In this way, every route used with a scheduled mode that has overflow service must have an alternate route in normal service.

Programming note: This service requires the user to enter a service control password before it can be accessed. Users obtain this password from their system coordinator. Refer to "Defining the service control password" on page 485.

Services matrix

To help you with your services planning, transfer the following information to a spreadsheet and fill out the values for each type of service.

Table 130 Ringing and Scheduling Services

Ringing Services	
Ring grp #	Sets

Scheduling Services		
Schedule	1 2 3 4 5 6	
Ctrl set:	221	
Service setting	Off Auto Manual	
Trunk answer	Y N	
ExtraDial	221	
Line settings		
Line #	Ring group (name)	Aux ringer
		Y N

Table 131 Restriction and Routing Services

Restriction Service	
Schedule	1 2 3 4 5 6
Service setting	Off Auto Manual

Routing Service	
Schedule	1 2 3 4 5 6
Service setting	Off Auto Manual
Overflow	Y N

Table 132 Common settings: Schedule Name

Common settings: Service control password					
Schedule Name					
Schedule 0	Normal		Schedule 4	Sched 4	
Schedule 1	Night		Schedule 5	Sched 5	
Schedule 2	Evening		Schedule 6	Sched 6	
Schedule 3	Lunch				

Table 133 Common settings: Schedule times

Common settings: Service control password			
Schedule Times			
Monday Tuesday Wednesday Thursday Friday Saturday Sunday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time

Chapter 18
Configuring public networks

This section describes the ways of networking Business Communications Managers across a public network. Different countries have different trunk types, therefore, these descriptions are also region based. Refer to "Media bay module availability by region" on page 849 for more information.

This section includes information about:

These are the protocols that the Business Communications Manager supports for public networking:

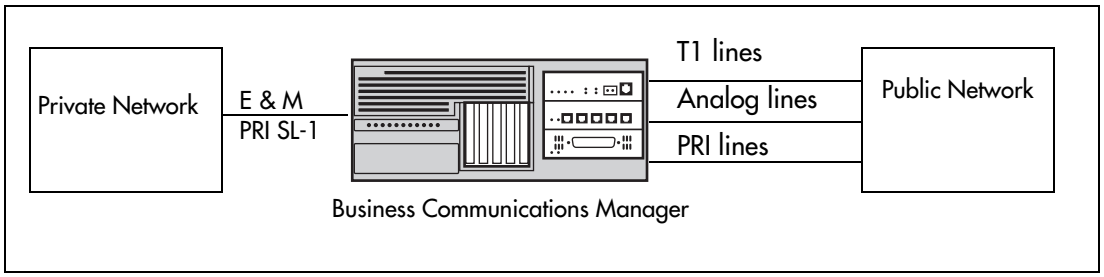
- PRI: ETSI Euro, NI, DMS100, DMS250, and 4ESS
- DASS2
- BRI: ETSI Euro, NI
- T1: Loop

TIPS: Most of the diagrams in this section use the BCM1000. The BCM400 and BCM200 can be used in any of these situations, as well. Keep in mind that the BCM200 only supports two PECs, and, therefore, has less processing capacity than the other two units. This affects both networking and IP telephony functions.

Simple networking

In the simplest form of networking, the Business Communications Manager acts as a routing station between a private network and the public network, as shown in the following figure.

Figure 170 Connection to a private network



In the above example, there are three types of callers:

Each type of caller has a specific method of accessing the other two systems.

Callers using Business Communications Manager

These callers can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the Business Communications Manager features

Callers in the public network

These callers use the public lines to:

- call directly to one or more Business Communications Manager telephones
- call into Business Communications Manager and select an outgoing tie line to access a private network
- call into Business Communications Manager and select an outgoing central office line to access the public network
- call into Business Communications Manager and use remote features

Callers in the private network

These callers use private lines to:

- call directly to one or more Business Communications Manager telephones
- call into Business Communications Manager and select an outgoing tie line to access other nodes in a private network
- call into Business Communications Manager and select an outgoing central office line to access the public network
- call into Business Communications Manager and use remote features

Dialing plans for T1 lines

Business Communications Manager has a routing feature that allows you to set up a coordinated dialing plan with other systems in the public network. The goal is to have a network-wide dialing plan where all telephone numbers are unique and of a uniform length.

Typically, you use coordinated dialing plans with a network of systems with a three to seven digit dialing access between them.

Any programming for routing must be carefully planned using tables. For more information about routing and destination codes, see "Configuring call routing" on page 320.

This section deals with applying the programming in network situations.

Dialing plan using public lines

The following illustrations provide an example of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax and Vancouver. Without routing, a Business Communications Manager user in Toronto would have to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial out, P stands for pause, a host system signaling option. Press **FEATURE 78** to insert a 1.5-second pause in the dialing string.

Figure 171 Routing service record: use pool

Routing Services (Services: Routing Service)

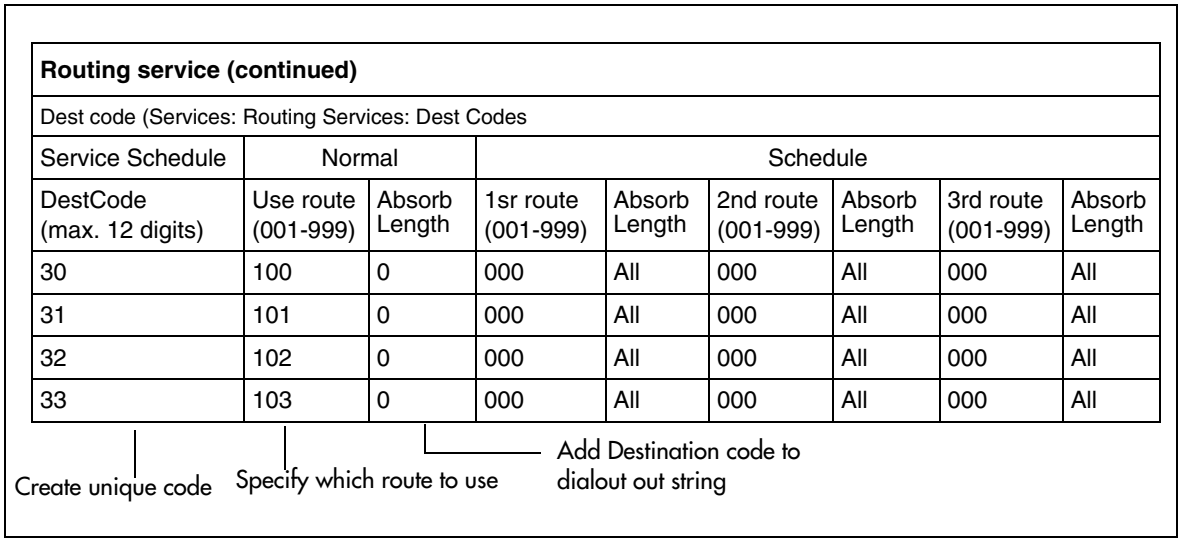
Route # (000-999)	Dialout (if required) (max. 24 digits or characters)	Use Pool
100	1-2-902-585	A B C
101	1-2-902-585	A B C
102	1-2-604-645	A B C
103	1-2-604-645	A B C

Create unique route number

Specify dial out digits

Route through Pool A

Figure 172 Routing service record: Destination code



Routing service (continued)								
Dest code (Services: Routing Services: Dest Codes								
Service Schedule	Normal		Schedule					
DestCode (max. 12 digits)	Use route (001-999)	Absorb Length	1sr route (001-999)	Absorb Length	2nd route (001-999)	Absorb Length	3rd route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Destination code numbering in a network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 134 Destination code leading digits

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
8	Call Park Prefix
9	All PSTN Calls

In the table shown above, 4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 can also be used for this purpose

TIPS: When programming a button to dial a Network number automatically (autodial), network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.
Routes generally define the path between the Business Communications Manager system and another switch in the network, not other individual telephones on that switch.

Other programming that affects public networking

Besides the line programming, these topics cover other areas that affect how calls are sent or received over the public network.

- "Controlling access into the system" on page 283 (Public Received Number Length, Target lines and remote access)
- "Configuring outgoing calls" on page 301 (dialing plans, access codes and routing, restriction filters)
- "Assigning line access" on page 394 (Public OLI)
- "Network name display" on page 453
- "Setting outgoing name and number blocking" on page 479

Chapter 19
Configuring private networks

This section describes the basic requirements for private networking Business Communications Managers. As well, four simple private networks are described.

Private networking using the MCDN protocol is described in “Configuring private networks with SL-1 MCDN” on page 519 and “Configuring ETSI QSIG and DPNSS network services” on page 543.

Different systems support different trunk types, depending on the market profile installed on the system. The examples in this chapter are based on the trunks available for North American-based profiles. Refer to “Media bay module availability by region” on page 849 for more information about which trunks are support in which profile.

This section includes information about:

TIPS: Most of the diagrams in this section use the BCM1000 base unit. The BCM400 and BCM200 can be used in any of these situations, as well. Keep in mind that the BCM200 only supports two PECs, and therefore, has less processing capacity than the other two units. This affects both networking and IP telephony deployment.

Private network programming parameters

The following section provides an overview of the values in the system that affect private networking, including:

Private networking protocols

These are the protocols that the Business Communications Manager supports for private networking:

- PRI: ETSI QSIG, MCDN
- DPNSS
- BRI: ETSI QSIG
- T1: E&M
- VoIP trunks (Refer to the *IP Telephony Configuration Guide* for details)

Business Communications Manager systems can be networked together using Tie lines or E&M connections. Larger networks, or networks that are geographically spread out, can be chained together through faster PRI SL-1 connections or with voice over IP (VoIP) trunk lines. SL-1 lines and VoIP trunks also offer the opportunity to use the MCDN protocol, which provides enhanced trunking features and end-to-end user identification. If a Meridian 1 is part of the MCDN network, the network can also provide centralized voice mail and auto attendant off the Meridian.

MCDN note: MCDN networking requires all nodes on the network to use a common Universal Dialing plan (UDP) or a Coordinated Dialing Plan (CDP). Refer to "Configuring the public and private dialing plans" on page 302 and "System numbering plans" on page 520.

Keycode requirements

Keycodes are required to activate the protocols that are used to create private networking, including:

- PRI keycodes, if you are using PRI lines for your network
- IP trunks, if you want additional IP trunks
- an MCDN keycode, if you want to use the MCDN protocol between the systems

You must purchase and install these keycode*s* before you can create any of the networks described in this chapter. Consult with your Nortel Networks distributor to ensure you order the correct keycodes for the type of network you want to create.

Remote access to the network

Authorized users can access tie lines, central office lines, and Business Communications Manager features from outside the system. Remote users accessing a private network configured over a large geographical area, can potentially also place long-distance calls through the network and avoid toll charges.

Note: You cannot program a Private DISA DN or Private Auto DN to a VoIP trunk, as they act as auto-answer trunks from one private network to the next. However, you can configure VoIP line pools with remote access packages so that callers can access telephones or the local PSTN on remote nodes on a tandemed network that use VoIP trunks between systems.

Lines used for networking

External (trunk) lines provide the physical connection between Business Communications Manager and other systems in a private or public network.

The Business Communications Manager numbers physical lines from 061 to 233/240. Default numbering depends on the trunk module positioning within the Business Communications Manager.

Refer to "Explaining the Media Bay Modules headings" on page 124.

VoIP trunks: Although a VoIP gateway does not require physical trunk lines, it is simpler to think of them in the same way as actual trunk lines. Therefore, in the Business Communications Manager, lines 001 to 060 are used for VoIP trunk functionality. Refer to the *IP Telephony Configuration Guide* for details about configuring VoIP trunks.

Business Communications Manager networking configurations that use PRI lines, require specific modules, depending on the type of lines chosen.

- DTMs configured for PRI are used for incoming and outgoing calls (two-way DID). Incoming calls are routed directly to a Business Communications Manager telephone. Outgoing calls are made using the intercom button and dialing destination codes.
- DTMs configured for T1 have digital lines that are configured as Groundstart, E&M, Loop, or DID.

Target lines are virtual communication paths between trunks and telephones on the Business Communications Manager system. They are incoming lines only, and cannot be selected for outgoing calls or networking applications. With target line*s*, you can concentrate incoming calls on fewer trunks. This type of concentration is an advantage of DID lines. Business Communications Manager target lines allow you to direct each DID number to one or more telephones. VoIP trunks also require target lines to direct incoming traffic. Target lines are numbered 241 to 492.

Telephones can be configured to have an appearance of any type of trunk and line or line pool (including target lines, excluding PRI trunks which can only be configured into PRI line pools and configured into routes with destination codes).

Other programming that affects private networking

Besides the line programming, these links connect to other programming that affect affects or is affected by private networks.

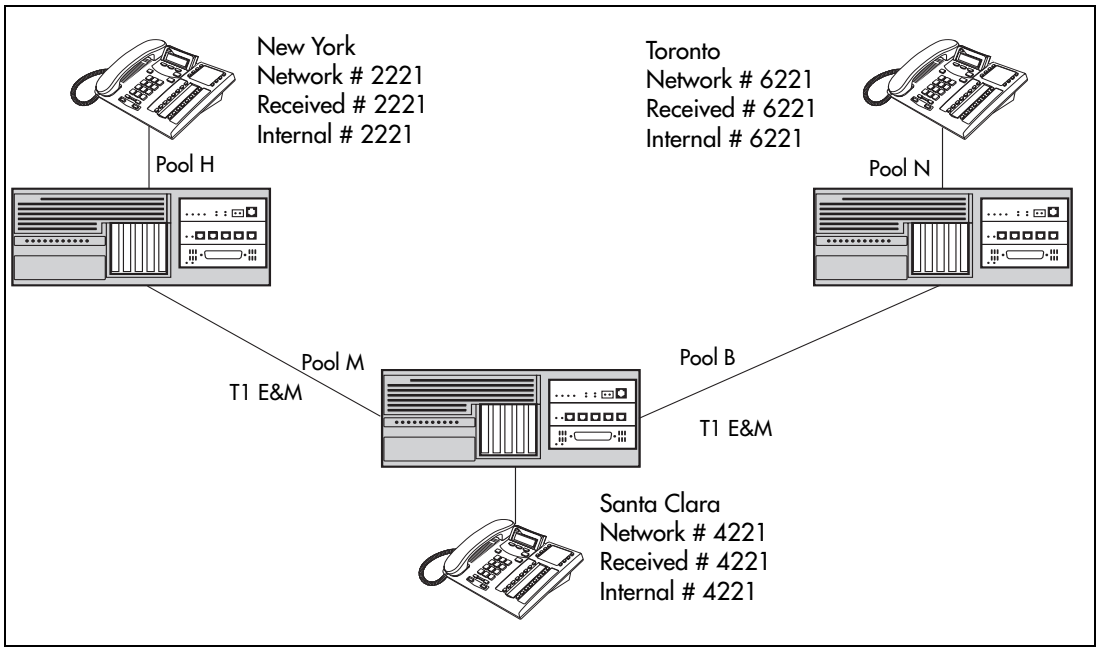
- "Controlling access into the system" on page 283 (Received Number Length, Target lines and remote access)
- "Configuring outgoing calls" on page 301 (dialing plans, access codes, routing, restrictions)
- "Assigning line access" on page 394 (Private OLI)
- "Network name display" on page 453
- "Setting outgoing name and number blocking" on page 479

Using routing to create networking

By properly planning and programming routing tables and destination codes, an installer can create a numbering plan where T1 E&M lines between Business Communications Manager systems are available to other systems in the network

The following figure shows a network of three Business Communications Manager systems. Two remote systems connect to a central system.

Figure 173 Dialing plan for T1 E and M routing network



Each system must be running Business Communications Manager software. Each system must be equipped with target lines and Business Communications Manager with a DTM with at least one T1 E&M line or the appropriate Norstar trunk module configuration ported in through a Fiber Expansion module (FEM). Programming information for this network is shown in the following table.

Table 135 E and M routing for a Business Communications Manager network

New York office:		
Parameter	**Setting**	
Trunk/Line Data		
Network line (external)		
Line 061	T1 E&M	
Answer Mode	Auto	
Line type	Pool H	
Target line (internal)		
Line 241	Target line	
Private Received #	2221	
Line Access (set)		
Set 2221	L241: Ring only	
Line pool access	Line pool H	
Routing service		
Route	001	
Use	Pool H	
External #	None	
Routing Destinations	**Office #1**	**Office #2**
Routing to	Santa Clara	Toronto
Destination Code	4	6
Normal route	001	001
Absorb	None	None
Dialed number:	4221	6221

Table 135 E and M routing for a Business Communications Manager network (Continued)

Santa Clara office:

Parameter	Setting
Network line (external to New York)	
Line 091	T1 E&M
Answer Mode	Auto
Line type	Pool M
Network line (external to Santa Clara)	
Line 092	T1 E&M
Answer Mode	Auto
Line type	Pool B
Target line (internal to Toronto telephone)	
Line 251	Target line
Private Received #	4221
Line Access	
DN 4221	L251: Ring only
Line pool access	Line pool B Line pool M

Routing Destinations	Office #1	Office #2
Routing to	New York	Toronto
Route	001	002
Use	Pool M	Pool B
External #	None	None
Destination Code	2	6
Absorb	None	None
Normal route	001	002

Remote access	
Rem access pkgs	01
Line pool access	Pool M: ON
Rem access pkgs	02
Line pool access	Pool B: ON
Line abilities	049
Remote pkg	01
Line abilities	050
Remote pkg	02

Table 135 E and M routing for a Business Communications Manager network (Continued)

Toronto office:		
Parameter	**Setting**	
Trunk/Line Data (external)		
Line 093	T1 E&M	
Answer Mode	Auto	
Line type	Pool N	
Target line (internal)		
Line 300	Target line	
Private Received #	6221	
Line Access		
DN 6221	L300: Ring only	
Line pool access	Line pool N	
Routing Destinations	**Office #1**	**Office #2**
Routing to	New York	Santa Clara
Route	001	
Use	Pool N	
External #	None	
Destination Code	4	2
Absorb	None	None
Normal route	001	001

If a user in New York wants to call Toronto within the network, they dial 6221. The local Business Communications Manager checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the auto answer line on the Business Communications Manager in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 002 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line Private received number. The call now alerts at telephone 6221 in Toronto.

Note: Network calls that use routes are subject to any restriction filters in effect.
If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the intercom button to the Line button.
The telephone used to make a network call must have access to the line pool used by the route.
Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.
When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal telephone numbers.
Routes generally define the path between your Business Communications Manager switch and another switch in your network, not other individual telephones on that switch.

Using shared line pools to create a network

Using shared line pools is a powerful and efficient way to create a coordinated dialing plan for a small network. If the Business Communications Manager systems are close to each other geographically, you can conserve resources by not duplicating long-distance access. For example, system A, B, and C are all within the same area code. System A has a line pool to Santa Clara, System B has a line pool to Montreal, and system C has a line pool to Miami. An Business Communications Manager user in system A can reach Miami by calling system C and using their line pool to Miami.

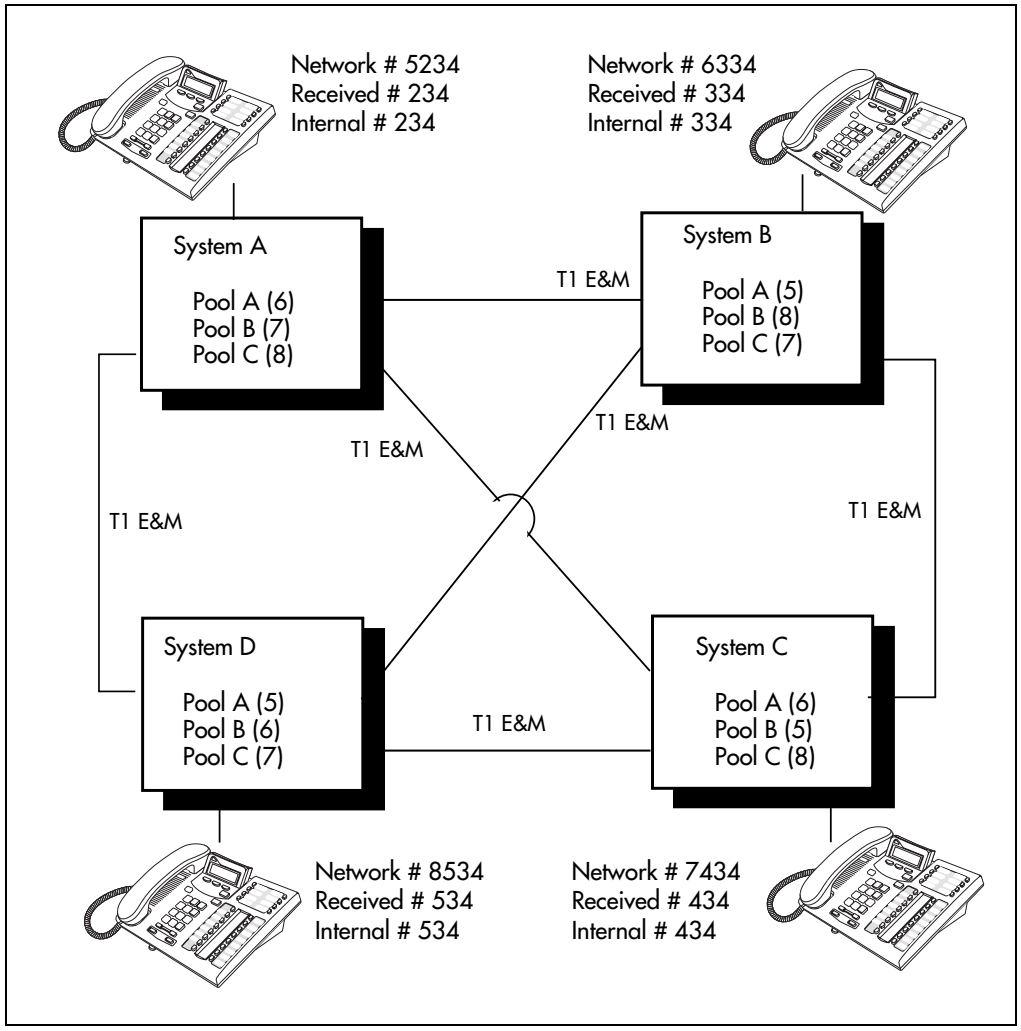
To simplify access between Business Communications Manager systems, all line pools that go to the same destination should have the same line pool access code. For example, system A and system B both have a line pool to Ottawa. You can configure both systems with the same line pool access code for the Ottawa line pool.

A dialing plan similar to the one in the following figure allows you to create a company directory that uses line pool access codes and unique DNs of a uniform length

In this example, the person on system A at telephone 234 can press an intercom button and dial 7434.

This means that telephone 234 has dialed the line pool access code of the trunk to system C, and will receive the dial tone of system C. The digits 434 then map to the Private received number 434, and ring telephone 434 with an appearance of the associated target line.

Figure 174 Network example using shared line pools



The following table shows the system coding for each system to set up a line pool-based coordinated dialing plan.

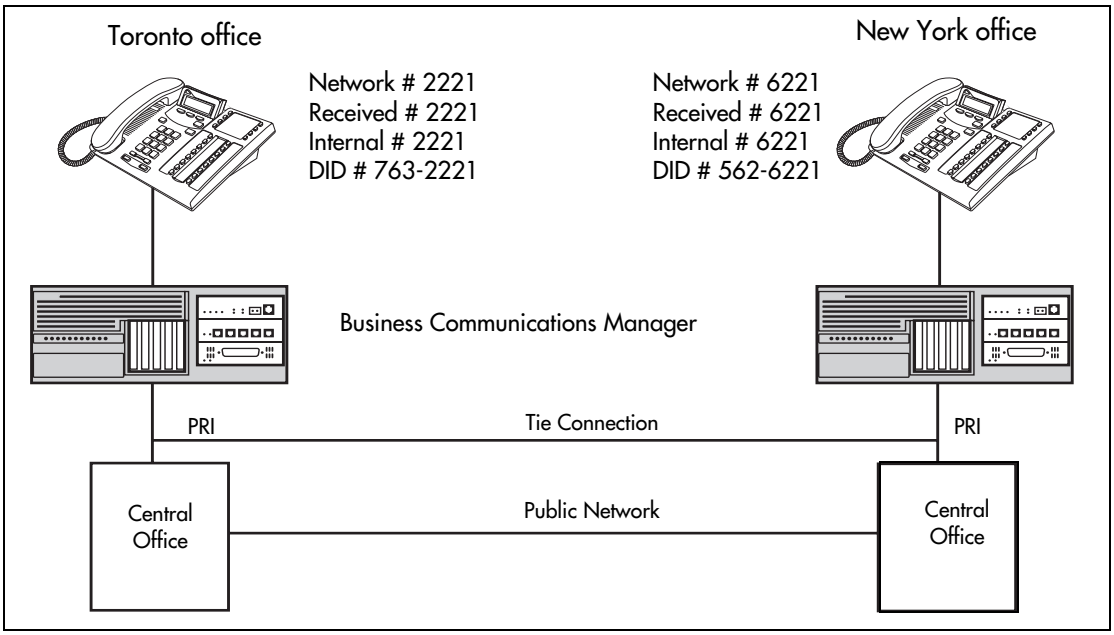
Table 136 Creating a coordinated dialing plan using line pools

Route from System A to:	**System**		**B**	**C**	**D**
Lines, Trunk/Line Data	Assign lines that connect with each system to a line pool		Pool A	Pool B	Pool C
General Setting, Access Codes, Line Pool Codes	Create an line pool access code for the pool		6	7	8
Dialout:			6334	7434	8534
Route from System B to	**System**	**A**		**C**	**D**
Lines, Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool A		Pool C	Pool B
General Setting, Access Codes, Line Pool Codes	Create an line pool access code for the pool	5		7	8
Dialout:		5234		7434	8534
Route from System C to	**System**	**A**	**B**		**D**
Lines, Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool B	Pool A		Pool C
General Setting, Access Codes, Line Pool Codes	Create an line pool access code for the pool	5	6		8
Dialout		5234	6334		8534
Route from System D to	**System**	**A**	**B**	**C**	
Lines, Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool A	Pool B	Pool C	
General Setting, Access Codes, Line Pool Codes	Create an line pool access code for the pool	5	6	7	
Dialout:		5234	6334	7434	

PRI networking using Call-by-Call services

The example shown in the following figure highlights the use of PRI Call-by-Call services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with a Business Communications Manager system and a PRI line. Each office has to handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office.

Figure 175 PRI networking using Call-by Call Services



To reduce long distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle interoffice traffic. Refer to "Configuring the public and private dialing plans" on page 302.

If call-by-call services were *not* used, each Business Communications Manager system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic.
- eight T1 E&M lines needed to handle inter-office calls.
- eight lines needed to handle outgoing public calls

The total required is thus 28 lines. If the Business Communications Manager systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time will generally be less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines will be low.

With PRI Call-by-call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private Tie, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than

two T1 spans. With PRI Call-by-call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each Business Communications Manager site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the four-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using Tie service with a private numbering plan.

Incoming Tie calls are routed to telephones based on the digits received by the network, which in this case will be the four-digit private DN.

If a user in either location wishes to dial an external number, they dial 9, followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls will be routed to telephones, based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network will deliver digits 4167632221. The Business Communications Manager will route the call using the last four digits, 2221.

Refer to the following table for a description of the settings required for this type of routing service.

Table 137 PRI call-by-call services routing information

Parameter	Home System Settings	
Hardware		
DTM	PRI	
Protocol	NI-2	
Trunk/Line Data		
Line 245	Target line	
Private/Public Received #	2221	
Line Access		
DN 2221	L245:Ring only	
Line pool access	Line pool PRI-A	
Routing Services	**Private Network**	**Public network**
	New York:	**Public network**
Route	001	002
External #	No number	No number
Use	Pool PRI-A	Pool PRI-A
Service type	Tie	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	6	9
Normal route	001	002
Absorb	0	ALL

Table 137 PRI call-by-call services routing information (Continued)

New York office:		
Parameter	**Home System Settings**	
Hardware		
DTM	PRI	
Protocol	NI-2	
Trunk/Line Data		
Line 245	Target line	
Private/Public Received #	6221	
Line Access		
DN 6221	L245:Ring only	
Line pool access	Line pool PRI-A	
Routing Services	**Private Network**	**Public Network**
	Toronto	Public Network
Route	001	002
External #	No number	No number
Use	Pool PRI-A	Pool PRI-A
ServiceType	Tie	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	2	9
Normal route	001	002
Absorb	0	ALL

Chapter 20
Configuring private networks with SL-1 MCDN

This section describes how to network Business Communications Managers together in a private network using PRI SL-1 lines with or without the MCDN protocol. When Business Communications Managers are networked with other call services, such as Meridian 1, using the MCDN protocol, the network can also support centralized voice mail.

This chapter discusses SL-1 and MCDN networking based on North American trunks (PRI SL-1). ETSI-QSIG and DPNSS private networking is configured very similarly, although network features may be supported slightly differently. Private networking and network features on these trunks is described in "Configuring ETSI QSIG and DPNSS network services" on page 543.

The following section describe the different aspects of SL-1 and MCDN private networking.

Refer to the previous chapter "Configuring private networks" on page 505 for general requirements and directions for setting up non-PRI private networks.

TIPS: Most of the diagrams in this section use the BCM1000 base unit. The BCM400 and BCM200 can be used in any of these situations, as well. Keep in mind that the BCM200 only supports two PECs, and therefore, has less processing capacity than the other two units. This affects both networking and IP telephony deployment.

The type of network you require depends on the equipment you are networking to, and how you want to use the network.

- You can tie a set of Business Communications Manager systems together to create a tandem network. This type of network provides the additional advantage of providing private line access to local PSTN*s* for all the nodes on the network.
- You can tie one or more Business Communications Manager systems to a Meridian 1 system and use the Meridian voice mail or auto attendant system for centralized call management, as well as providing reduced toll calling across the private lines.

You require PRI and MCDN keycode*s* to create either of these networking configurations. Note, however, that to use the MCDN features, your network must include a Meridian system as a controlling system.

System numbering plans

Both these types of networks require similar setups for dialing plans and routing. Each node must have a way to route external calls to the adjacent node or nodes. To do this, all nodes must have the same Private DN lengths.

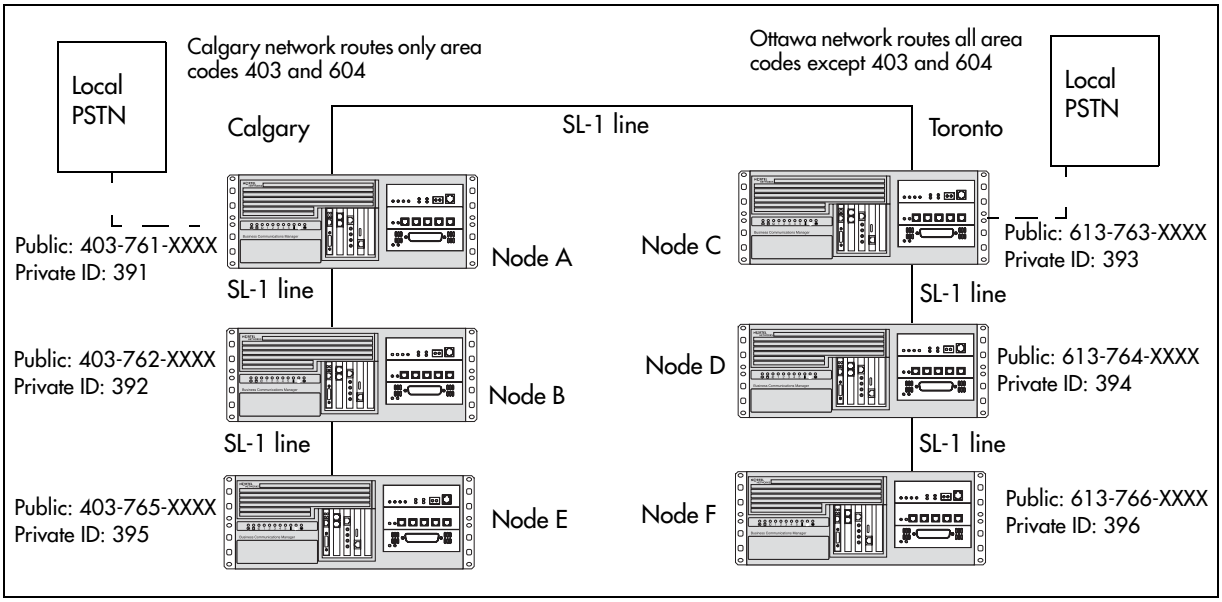
You use routing and a private dialing plan to control calls over the network. Refer to "Configuring the public and private dialing plans" on page 302 for a description of the two types of dialing plans available for private networking over SL-1 and SL-1 MCDN networks. Each example in this section describes the routing configurations that are required to support calls over the network.

Depending on the type of dialing plan you choose, each node must also have a unique location or steering code so the calls can be correctly routed through the nodes of the network. MCDN networks also require a Private Network ID, which is supplied by the Meridian network administrator to define how the Meridian system identifies each node.

Creating tandem private networks

You can tie a number of Business Communications Manager systems together with SL-1 lines. This tandem network provides you with the benefits of end-to-end name display and toll-free calling over the SL-1 private link. Each Business Communications Manager becomes a node in the network. The following figure demonstrates a tandem configuration.

Figure 176 Private tandem network of Business Communications Managers



In this type of network, you must ensure that each Business Communications Manager system, known as a node of the network, is set up to route calls internally as well as to other nodes on the system. This means, each node must have a route to the immediately-adjacent node, and the correct codes to distribute the called numbers. Each node must have a unique identification number, which is determined by the type of dialing plan chosen for the network.

As well, you can save costs by having a public network connection to only one or two nodes, and routing external calls from other nodes out through the local PSTN, thus avoiding toll charges for single calls.

This section includes the following:

- "Calls originating from the public network" on page 521
- "Calls originating in the private network" on page 524
- "Routing for tandem networks" on page 526

VoIP note: You can also use VoIP trunks between some or all of the nodes. The setup is the same, except that you need to create gateway records for each end of the trunk, and routing tables to accommodate the gateway codes. Refer to the *IP Telephony Configuration Guide* for information about setting up VoIP trunks and gateway programming.

Calls originating from the public network

The following table describes who each node handles calls originated from the public network into the system.

Table 138 Call originating from the public network to a tandem network

Received	Destination	Description
Node A	Node A	User in Calgary dials 761-xxxx number Incoming interface: Public DN type: Public Node A receives the call and identifies it as terminating locally. Uses target line to route call (Public received #). Destination: Local (target line)
Node A	Node B	User in Calgary dials a 762-xxxx number DN type: Public Node A receives it and identifies it as being for node B. Uses private trunk to route it to B. Incoming interface: Public Destination: Remote Node Outgoing interface: Private Node B receives the call and identifies it as terminating locally. Uses target line to route call (Private received #). Incoming interface: Private Destination: Local (target line)

Table 138 Call originating from the public network to a tandem network (Continued)

Received	Destination	Description
Node A	Node E	User in Calgary dials a 765-xxxx number. DN type: Public Node A receives it and identifies it as being for B. Uses private trunk to route call to B. Incoming interface: Public Destination: Remote node Outgoing interface: Private Node B receives it and identifies it as being for E. Uses private trunk to route call to E. Incoming interface: Private Destination: Remote node Outgoing interface: Private Node E receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)
Node A	Node C	User in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN) User enters a COS password and a private DN for Node C i.e. 6 + 393-xxxx DN type: Private Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Table 138 Call originating from the public network to a tandem network (Continued)

Received	Destination	Description
Node A	Node D	User in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN) User enters a COS password and a private DN for Node D, i.e. 6 + 394-xxxx DN type: Private Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node Node C receives it and identifies it as being the responsibility of D. Uses private trunk to route call to D. Incoming interface: Private Destination: Remote node Node D receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)
Node A	Ottawa PSTN	User in Calgary dials a 761-xxxx number which is answered with DISA. User enters a COS password and an Ottawa public network number. Incoming interface: Public DN type: Public Destination: Local (DISA DN) Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: Local (DISA user) Destination: Remote PSTN Node C receives the call and identifies it as a public number and routes it out over the local PSTN. Incoming interface: Private Destination: Local PSTN

Calls originating in the private network

The following table describes who each node handles calls originated in the public network.

Table 139 Calls originating from the private network within a tandem network

Received	Destination	Description
Node B	Node B	DN is internal, therefore no trunk routing is required. Incoming interface: Intercom DN type: Local Destination: Local
Node A	Ottawa PSTN	User in Node A dials the private network access code for Node C, followed by an Ottawa public number. Incoming interface: Intercom DN type: public Destination: Remote PSTN Node C receives the call and identifies it as being for the public network. Node C routes the call over the local public network. Incoming interface: Private DN type: Public Destination: Local PSTN
Node B	Calgary PSTN	User on Node B dials a public DN. Node B recognizes it as being the responsibility of Node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node Node A receives the call and identifies it as being for the public network. Node A routes the call over the local public network. Incoming interface: Private Destination: Remote PSTN
Node B	Node A	User in Node B dials a private DN for a user on A. DN type: Private Node B recognizes it as being for Node A. Uses the private trunk to route the call the call to A. Incoming interface: Intercom Destination: Remote node Node B receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Table 139 Calls originating from the private network within a tandem network (Continued)

Received	Destination	Description
Node B	Node C	User on Node B dials a private DN for a user on C. DN type: Private Node B recognizes it as being the responsibility of Node A and routes the call over the private trunk to A. Incoming interface: Intercom Destination: Remote node Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)
Node B	Node D	User on B dials a private DN for node D. DN type: Private Node B identifies it as being for node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node Node C receives it and identifies it as being for D. Uses the private trunk to route call to D. Incoming interface: Private Destination: Remote node Node D receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Table 139 Calls originating from the private network within a tandem network (Continued)

Received	Destination	Description
Node B	Node F	User on B dials a private DN for node F. DN type: Private Node B identifies it as being for node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Intercom Destination: Remote node Node C receives it and identifies it as being for D. Uses the private trunk to route call to D. Incoming interface: Intercom Destination: Remote node Node D receives it and identifies it as being for F. Uses the private trunk to route call to F. Incoming interface: Intercom Destination: Remote node Node F receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Routing for tandem networks

In tandem networks each node needs to know how to route calls that do not terminate locally. To do this, you set up routes for each connecting node by defining destination codes for each route.

If the node is also connected to the public network, the usual routing is required for that connection.

The following tables show the routing tables for Node A and Node C for external and internal terminating calls.

Note: The PRI lines are enbloc dialing lines, so all dialed digits are collected before being dialed out.

Table 140 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91604
3 (Node B)	0	91403762 (Node B)
3 (Node B)	0	91403765 (Node E)
4 (PSTN)	1	9140376* (not internal network)
4 (PSTN)	1	914037* (not internal network)
4 (PSTN)	1	91403* (not internal network)
4 (PSTN)	1	9* (not internal network)
* This wild card represents a single digit.		

Table 141 Node A destination code table, internal termination

Route	Absorb length	Destination code (private DNs)
3 (Node B)	0	392 (Node B)
3 (Node B)	0	395 (Node E)
5 (Node C)	0	393 (Node C)
5 (Node C)	0	394 (Node D)
5 (Node C)	0	396 (Node F)

Table 142 Node C destination code table, external termination

Route	Absorb length	Destination code (Public DNs)
3 (Node B)	0	91613764 (Node D)
3 (Node B)	0	91613766 (Node F)
4 (PSTN)	1	9161376* (not internal network)
4 (PSTN)	1	916137* (not internal network)
4 (PSTN)	1	91613* (not internal network)
4 (PSTN)	1	9161* (not internal network)
4 (PSTN)	1	916* (not internal network)
4 (PSTN)	1	91* (not internal network)
4 (PSTN)	1	9 (not internal network)

Table 143 Node C destination code table, internal termination

Route	Absorb length	Destination code (Private DNs)
3 (Node D)	0	394 (Node D)
3 (Node D)	0	396 (Node F)
5 (Node A)	0	391 (Node A)
5 (Node A)	0	392 (Node B)
5 (Node A)	0	395 (Node E)

Understanding MCDN network features

When you connect your Business Communications Manager systems through an SL-1 and use the MCDN protocol, your network provides a number of network call features. You can use this protocol to network other Business Communications Manager systems, such as the tandem system, shown in the previous section, Norstar systems, or Meridian 1 systems.

Note: For information about networking voice over IP (VoIP) trunks using MCDN, refer to the *IP Telephony Configuration Guide*.

The following table lists the MCDN features that are provided by all networks connected with SL-1 lines, with MCDN active. The features affect call redirection and trunking functions.

Table 144 MCDN network features

Centralized messaging	• "Network Call Redirection Information" on page 528 (NCRI)
Centralize trunking	• "ISDN Call Connection Limitation" on page 530 (ICCL) • "Trunk Route Optimization" on page 531 (TRO) • "Trunk Anti-tromboning" on page 532 (TAT)

Network Call Redirection Information

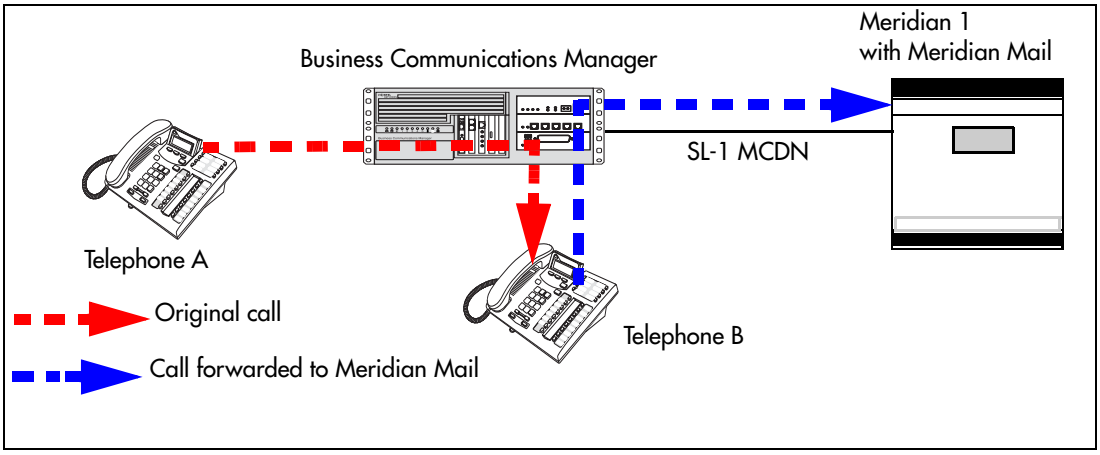
NCRI builds on the following Business Communications Manager features:

- External Call Forward
- Call Transfer
- Call Forward

NCRI adds the ability to redirect a call across an MCDN network using Call Forward (all calls, no answer, busy) and Call Transfer features. The call destination also receives the necessary redirection information. This feature allows the system to automatically redirect calls from within a Business Communications Manager system to the mail system, such as Meridian Mail, which resides outside the Business Communications Manager system on the Meridian 1.

The following figure shows an example of this situation, where user A calls user B on the same Business Communications Manager. If user B is busy or not answering, the call automatically gets transferred to a Meridian Mail number (user C) across an MCDN link between the Business Communications Manager system and the Meridian 1 system where the mailboxes are set up. Refer to "Assigning Call Forward" on page 409

Figure 177 Network call redirection path



If you are using the centralized voice message system from a Meridian 1 system, you require the following programming on the M1:

M1 programming in LD 17

- NASA set to Yes
- NCRD set to Yes

Verifying NASA is Active • Overlay 22, LD 22 • REQ: PRT • TYPE: ADAN DCH (slot number) • NASA should be set to yes			
If NASA is not on:	Disable the D channel • Overlay 96, LD 96 • REQ: CHG • TYPE:DISDCH	Disable the loop • Overlay 60, LD 60 • REQ: CHG • TYPE: DISL (slot number)	Program the D channel • Overlay 17, LD 17 • REQ: CHG • TYPE: ADAN • ADAN: CHG DCH (slot number) • Keep pressing enter until you get to NASA • TYPE: yes • TYPE: end
Verifying NCRD • Overlay 20, LD 20 • REQ: PRT • TYPE: TIE • CUST: 0 • Route: Enter the route defined in LD 20 • Keep pressing enter until all values are displayed. Check if NCRD is yes.		If NCRD is set to no • Overlay 16, LD 16 • REQ: CHG • TYPE: RDB • CUST: 0 • ROUT: (route number) from LD 20 • Keep pressing enter until you get NCRD and type Yes • Keep pressing enter until you get the REQ prompt again • TYPE: end	

ISDN Call Connection Limitation

The ICCL feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.

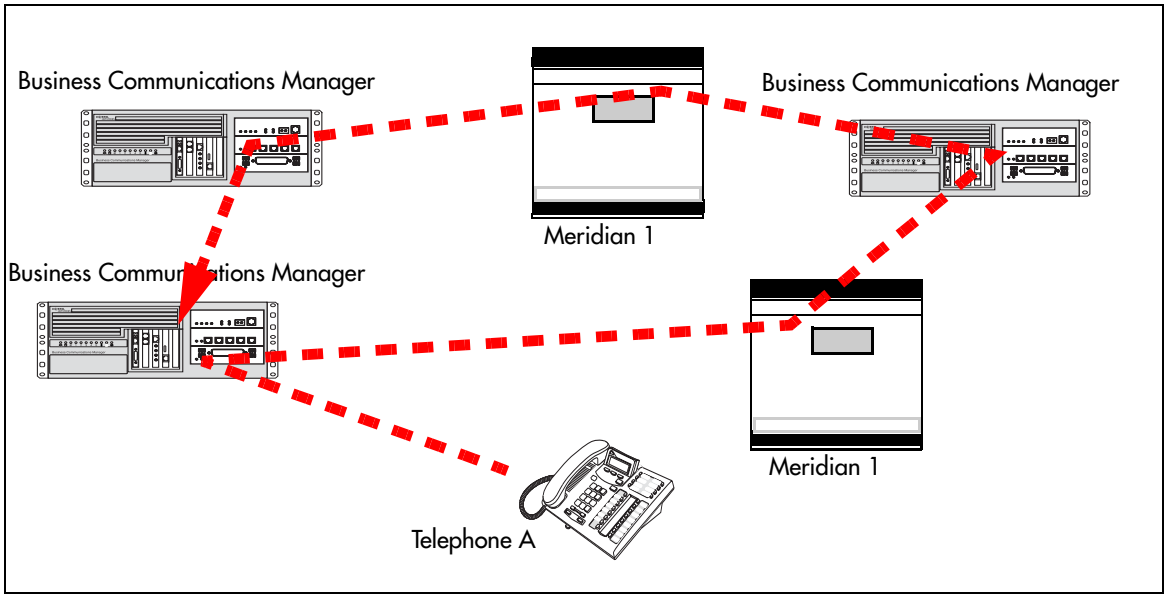
This feature adds a transit/tandem counter to a call setup message. This counter is compared at each transit PBX with a value programmed into the transit PBX, in a range from 0 to 31. If the call setup counter is higher than the PBX value, the call will be blocked at the PBX system and cleared back to the network. This prevents calls from creating loops that tie up lines.

Business Communications Manager configurations:

- Under **Network Services, MCDN**, set **NtwkICCL** to Y(yes).
- Under the media bay module record for the trunk module, define Maximum transits.

The following figure demonstrates how a call might loop through a network if the system is not set up with ICCL.

Figure 178 Call loop on system without ICCL



Trunk Route Optimization

TRO finds the most direct route through the network to send a call between nodes. This function occurs during the initial alerting phase of a call.

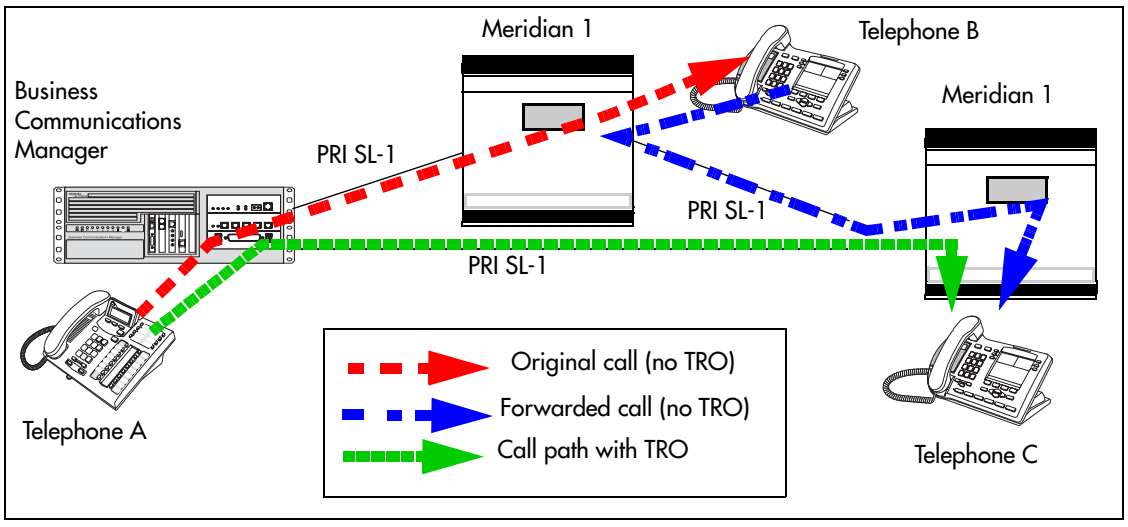
Business Communications Manager configurations:

- Under **Network Services, MCDN**, set **TRO** to Y(yes).
- Configure call routing for all optimal routes.
- Configure call forward (All Calls, No Answer, Busy) or Selective Line Redirection to use the optimal routes.

This feature avoids the following situation: A call originating from a Business Communications Manager system may be networked to a Meridian system, which, in turn, is networked to another Meridian system, which is the destination for the call. If the call routes through the first Meridian (M1) to reach the second Meridian (M2), two trunks are required for the call. An optimal choice is a straight connection to M2. This finds these connections and overrides the less-efficient setup.

The following figure shows two call paths. The first route, through the Meridian, demonstrates how a call might route if TRO is not active. The second route, that bypasses the Meridian, demonstrates how TRO selects the optimum routing for a call.

Figure 179 Call paths with and without TRO



If you are using a Meridian 1 system as part of the network, you need the following programming for each system:

```
M1 TRO set to yes for BCM route:
LD 16
TYPE: RDB
Cust: xx
Rout: 0-511
TRO: Yes
```

Trunk Anti-tromboning

TAT is a call-reroute feature that works to find better routes during a transfer of an active call. This feature acts to prevent unnecessary tandeming and tromboning of trunks.

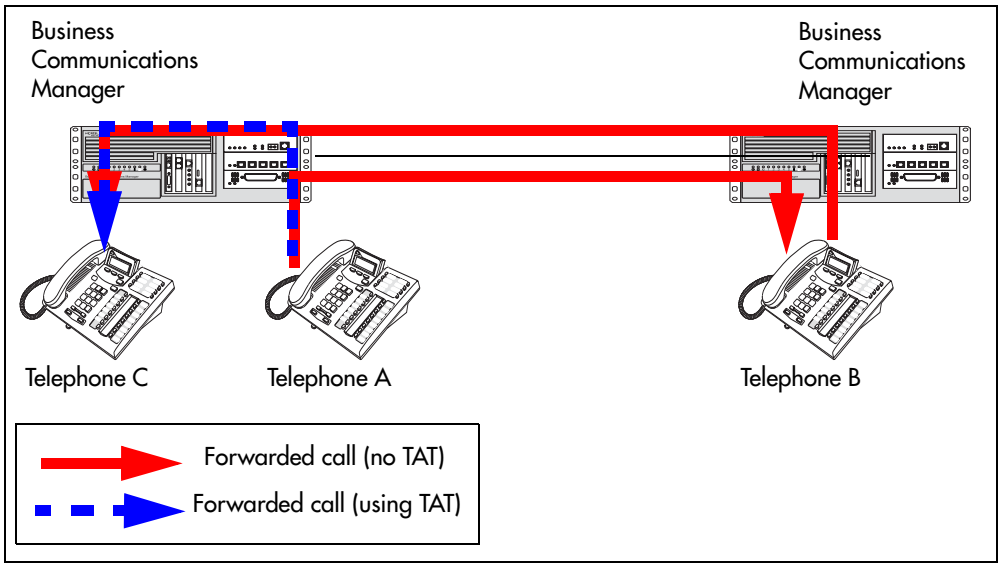
TIPS: This feature is not applicable for alerting calls.

Business Communications Manager configurations:

- Under **Network Services, MCDN**, set **TAT** to Y(yes).

The following figure shows how TAT reduces the line requirements. The solid line shows Telephone A calling Telephone B and being transferred over an additional PRI line to Telephone C. With TAT active, the same call is transferred to Telephone C over the same PRI line.

Figure 180 Call paths with and without TAT



Using SL-1 with MCDN to network with a Meridian system

When you connect your Business Communications Manager systems through the SL-1 MCDN protocol to a Meridian 1, the Meridian system manages several aspects of the network, including voice mail, auto attendant services, and system timing.

Programming note: For information about networking voice over IP (VoIP) trunks, which also can be set to use MCDN, refer to the *IP Telephony Configuration Guide*. For networks running Business Communications Manager BCM 3.5 software or newer, the trunk protocol for Meridian 1 IPT connection should be set to CSE.

This section includes the follow information about setting up an MCDN network:

- "Meridian system requirements"
- "MCDN networking checklist" on page 534

An example of an MCDN system and the Business Communications Manager programming to support it, is given in "An example of a private network with Meridian 1" on page 537.

Meridian system requirements

When setting up networking with Meridian, the Meridian systems must provide the following:

- the correct software version to allow MCDN features (If your Meridian system administrator cannot confirm this, call your technical support center (TSC) or 1-800-4NORTEL.)

  The Meridian must provide the following:

  — end-to-end signaling (option 10)
  — message center (option 46) and an IVMS link (option 35)
  — Meridian Mail link (option 77 and 85)
  — basic Attendant Console Directory features (options 40, 45, and 83)
  — ISDN PRI or ISDN Signaling link (option 145 and 146 or 145 and 147)
  — advanced ISDN features (option 148)
  — network message services (option 175)
- act as the timing master for the private network connections
- use descending mode for PRI B-channel selection
- recognize dial codes for all nodes in the network.
- provide routing tables that direct incoming calls to the correct nodes on the network, including DID calls from the public network
- recognize the destination code (usually 9) that indicates a public network call, regardless of where in the network the number was dialed from.

Note: For MCDN over VoIP trunks, the Meridian uses the IPT trunk card (introduced in BCM 3.5). Both systems must have remote gateways pointed to correct system types and protocols. Refer to the *IP Telephony Configuration Guide* for information about Remote Gateways for the Business Communications Manager system.

Software requirements

These additional software packages may be required to activate all the options on the Meridian:

For a new M1 (option 81C, 61C or 51C) on X11 Rls 25, the following additional packages are required to provide the software options listed above:

- SW0059B
- SW0052D
- SW0221C
- SW0051B

For a new M1 Option 11C or 11C Mini or X11 Rel. 25, order one of the following:

- Enterprise software package
- NAS/VNS software package

MCDN networking checklist

The following points provide a quick check for the system prerequisite settings for MCDN networking.

Select the dialing plan to be used:

- **UDP (Universal Dialing Plan)**
  - DNs on the same node are dialed directly.
  - DNs on other nodes are called by first dialing an Access Code and an ESN.
  - Each node has its own ESN.
- **CDP (Coordinated Dialing Plan)**
  - DNs on all nodes are dialed directly.

Ensure the following common programming is configured:

- **Business Communications Manager Programming**
  - Configure the system DN length to match the DN length used in the rest of the private network (i.e. the M1).
  - Program the private Route: Type=Private, Dial=None.
  - Program the public Route: Type=Public, Dial=None.
  - Enable the MCDN Supplementary Services; TRO=Yes, ICCL=Yes, TAT=Yes.
  - Program telephones with a target line that specifies the system DN of the telephone in the **Private received number** field.

Note: If you have public DNs set up for your telephones that are different from the system-assigned DN, each telephone would need two target lines to accommodate both public and private networks.

- **Meridian 1 Programming**
  - — Program the system PNI and the PNIs for the routes.
  - — Program the Meridian Voice Mail mailboxes (if required).
  - — Enable the MCDN Supplementary Services; RCAP=[ND2,TRO,MWI], NASA=YES.

Set up the specific programming for the dialing plan the system requires:

UDP-specific programming

Business Communications Manager UDP programming		
• Private Dialing Plan:	Type=UDP, HomeLoc=<three-digit prefix>	
• Private Access Code	<unique code>	
• Private DN length	<total of Private Access Code + Location Code + DN length> Example: if dialing string is 6 393 2222, then set private DN to 8	
• Program the DestCodes for the other nodes	AccessCode plus the ESN, absorb the AccessCode. Example: For AccessCode=6; DestCode=6393[Absorb=1]	

M1 UDP programming		
• Private Access Code	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: ESN	To change Private Access Code: Overlay 86, LD 86 REQ: CHG CUST: 0 FEAT: ESN, keep pressing until you reach the AC1 prompt At the AC1 prompt, make your choice
• Check UDP programming	Overlay 90, LD 90 REQ: PRT CUST: 0 FEAT: NET TYPE: LOC LOC: press enter, all the programmed location codes are listed HLOC is the home location of the M1	
• Program UDP values to route	Overlay 90, LD 90 REQ: CHG CUST: 0 FEAT: NET TYPE: AC1 LOC: (enter a number) RLI: (enter the RLI corresponding to the route	

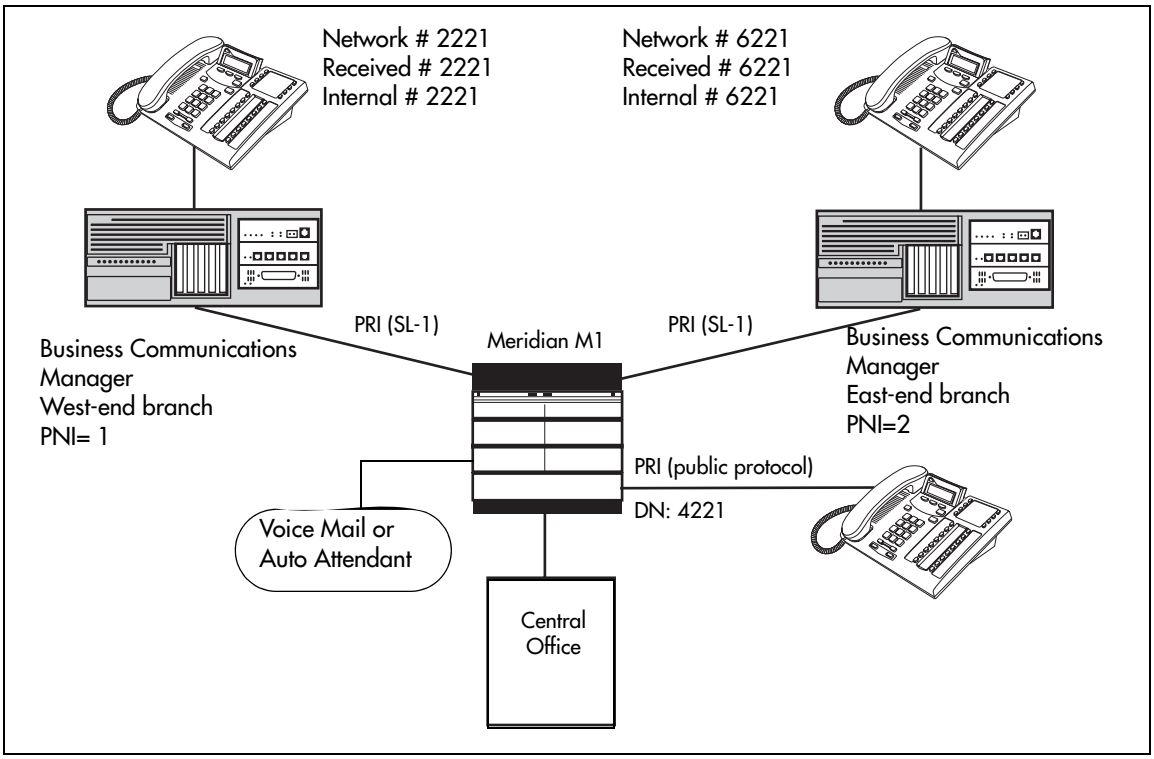
CDP-specific programming

Business Communications Manager CDP programming		
• Private Dialing Plan: Private Access Code <unique code>.	Type=CDP	
• Private DN length	<system DN length>	
• PNI	<number assigned from M1 (1-128)>	LD 16, RDB - PNI in M1 programming LD 15 - Net - PNI in M1 programming set to PNI of switch
• Program the DestCodes for the other nodes	use Steering code as part of dial string	
M1 CDP programming		
• Distant Steering Codes	Overlay 87, LD 87 REQ: PRT CUST: 0 FEAT: CDP TYPE: DSC (Distant Steering Code) DSC: press enter (lists all DSC programmed)	
• Check RLI (Route Line Index)	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: RLB PLI: press enter (displays all the RLIs)	
• Program new CDP value to route	Overlay 87, LD 87 REQ: CHG CUST: 0 FEAT: CDP TYPE: DSP DSC: enter number (enter common Business Communications Manager system number, for example if DNs are 4XX, enter 4) RLI: enter the RLI that corresponds to the route	

An example of a private network with Meridian 1

The following figure shows a private network composed of one central Meridian 1, and two sites with Business Communications Manager systems all connected by SL-1, with MCDN activated on all sites. This example uses a coordinated dialing plan (CDP). The DNs consist of four digits. The first digit is a destination code which is specific to each system. The last three digits are unique to each telephone within that system. Refer to Chapter 11, "Controlling access into the system," on page 283 for a description of the dialing plans available to private networks.

Figure 181 MCDN networking, with a common public network connection



This example could represent a large head office (the Meridian 1) connected to several smaller branch offices (the two Business Communications Managers). In this network, only the head office has trunks connected to the public network.

The branch offices access the public network via the PRI to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing 9, followed by the public number. For example, a user in the West End branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Business Communications Manager routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Note that the Private Network Identifier (PNI) is programmed at each end of the links. The PNI identifies the Business Communications Manager to the Meridian 1 system.

Routing is set up such that network calls are made by dialing a four-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221. The figure above illustrates this example.

The implications on the configuration on each node to access the PSTN through one network node:

- Each node must have the Private Network Access Code set to the value 9.
- Each node must have destination code(s) that match the Private Network Access Code plus digits corresponding to calls terminating in the local PSTN. For example, if the Private Network Access Code is 9, the node in Ottawa would require a destination code of 91613. Similarly, Toronto would require the following destination code: 91416.

Business Communications Manager module settings: The following table lists the module settings that are required to set up the network described in the previous figure. Refer to "Configuring resources — media bay modules" on page 123.

Table 145 Module settings for MCDN network

West End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
East End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary

Business Communications Manager dialing plan settings: The following table lists the dialing plan settings that are required to set up the network described in the figure in the previous section. Also refer to "Configuring the public and private dialing plans" on page 302.

Table 146 MCDN dialing plan settings

West End office:		
Dialing Plan programming	Type	UDP
	Private Network ID	1
	Location Code	<unique three digits> (becomes part of destination code)
	Private DN Length	4
	Public DN Length	7

Table 146 MCDN dialing plan settings (Continued)

East End office:		
Dialing Plan programming	Type	UDP
	Private Network ID	2
	Location Code	<unique three digits> (becomes part of destination code)
	Private DN Length	4
	Public DN Length	7

Business Communications Manager routing information: The following table lists the lines and routing information required to set up the network shown in Figure 181 on page 537.

Table 147 Network routing information

West End office:			
Trunk/Line Data	Line 245	Target line	
	Private Received #	2221	
Line Access	DN 2221	L245:Ring only	
	Line pool access	Line pool PRI-A	
Routing Services	Private Network		Public Network
	Head Office and East end		
Route	001		002
External #	No number		No number
Use	Pool PRI-A		Pool PRI-A
DN type	Private		Public
Destination codes for routes to:	Head office to M1	Head office to East End	
Destination Code	4 (includes location code)	6	9
Normal route	001	001	002
Absorb	0	0	0

Table 147 Network routing information (Continued)

East End office:			
Trunk/Line Data	Line 245	Target line	
	Private Received #	6221	
Line Access	DN 6221	L245:Ring only	
	Line pool access	Line pool PRI-A	
Routing Services	Private Network		Public Network
	Head Office to West End		
Route	001		002
Dial out #	No number		No number
Use	Pool PRI-A		Pool PRI-A
DN type	Private		Public
	Head Office to M1	Head Office to West End	Call terminates at M1
Destination Code	4 (contains location code)	2	9
Normal route	001	001	002
Absorb	0	0	0

VoIP networking

When you choose voice over IP (VoIP) trunks to make network connections, the process is very much the same as using land lines, except that you must also create a Remote Gateway record which identifies the IP address for the target system. Note: If the IP system has a Gatekeeper, the Remote Gateway record is not required. You need to supply the IP parameters of your system to the Gatekeeper administrator instead.

You also need a VoIP keycode before you can activate VoIP trunks.

MCDN networking over VoIP, which is always between a Meridian 1 and one or more Business Communications Managers, is set up and 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. Refer to "Understanding MCDN network features" on page 528.

The major difference between a PRI MCDN line and a VoIP MCDN connection is that the VoIP trunk requires Local and Remote Gateway settings. Under **Services**, **IP Telephony**, **H.323 Trunks**, **Remote Gateway**, ensure that **Gateway Protocol** is set to **CSE** if you want MCDN functionality for the VoIP connection to the Meridian system (BCM 3.5 and newer software). The **Gateway Type** would be set to **IPT** (M1 IP Telephony), as it would for any non-MCDN VoIP connection to a Meridian system. You can also use MCDN VoIP to other Business Communications Managers. There is a Gateway Type for each version of Business Communications Manager software that supports this function.

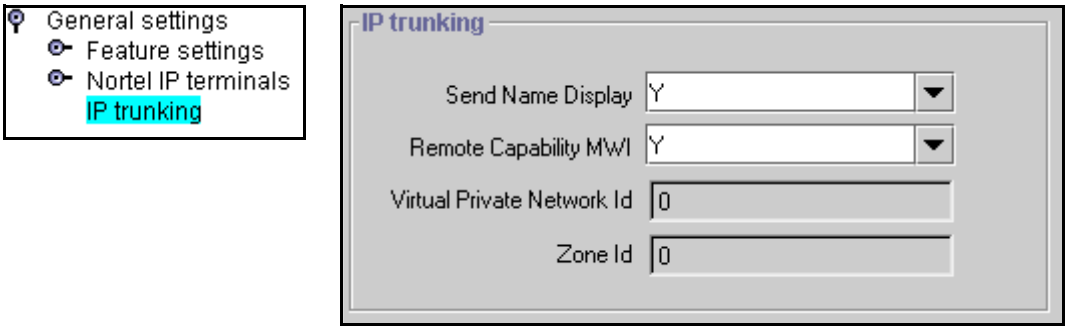
For details about setting up gateways and configuring VoIP trunks, refer to the *IP Telephony Configuration Guide.*

Configuring special IP trunking interoperability

Under Services, Telephony Services, General settings, IP trunking, there are four fields that may need to be filled out to specify specific parameters of the VoIP trunk between your system and a system such as Meridian 1 or Succession 1000/M, which may have special network requirements, such as Bandwidth Management or zone dialing.

1 Click on **IP trunking**.

Figure 182 IP trunking interoperability fields



2 Enter or confirm the required parameters supplied by the system administrator of the remote system.

The following table describes the field properties for each item.

Table 148 IP trunking interoperability fields

Field	Value	Description
Send Name Display	Y, N	If the remote voice mail system resides on a Meridian 1 system, that system should have the MWI package to allow message waiting indicators to occur on network telephones. In this case, the IP trunking Remote Capability MWI field should be set to Yes (the default), to indicate that the Business Communications Manager is compatible with the M1. If the M1 does not have the MWI package, you need to set the IP trunking Remote Capability MWI field to No, to indicate that there is no compatibility. Note: SIP trunks do not support MWI.
Remote Capability MWI	Y, N	The public or private OLI (outgoing line identification) are separately configurable for each telephone, under Line Access. Therefore, when the VoIP trunks allow name display on outgoing calls (Send Name Display), the system will send the appropriate OLI, based on line type (Public or Private). Default is Y.

Table 148 IP trunking interoperability fields (Continued)

Field	Value	Description
Virtual Private Network ID	<digits>	Default:0 This is the VPN ID for a remote system, such as Succession 1000/M. In some applications, such as for the Survivable Remote Gateway (SRG) acting as a Branch Office, this ID is required to ensure that Bandwidth Management is handled correctly for calls coming into the Succession 1000/M from your system.
Zone ID	<digits>	Default:0 A remote system, such as Succession 1000/M, may configure your system into a separate zone to accommodate specific dialing requirements, such as for an SRG system acting as a Branch Office to a Succession 1000/M system. The system administrator of the Succession 1000/M system provides the Zone ID. Enter that number here and include it in any destination codes directed to or through that system so that the remote system can correctly direct incoming calls.

3 Click anywhere off the IP trunking dialog to save the changes.

Chapter 21
Configuring ETSI QSIG and DPNSS network services

This section describes the network services for ETSI QSIG and DPNSS private networks. ETSI-QSIG and DPNSS private networking is configured in the same way as described in "Configuring private networks with SL-1 MCDN" on page 519.

Refer to "Configuring private networks" on page 505 for general requirements and directions for setting up private networks.

This section includes information about:

Networking with ETSI QSIG

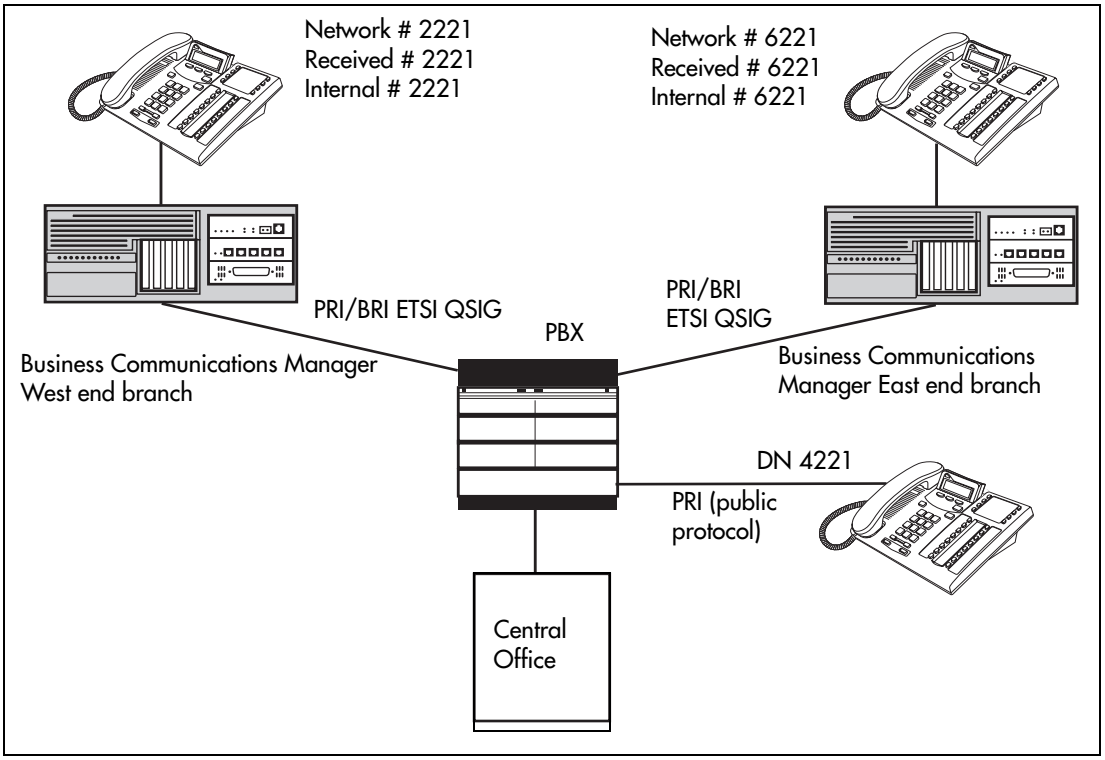
(International systems only)

ETSI QSIG is the European standard signaling protocol for multi-vendor peer-to-peer communications between PBX system*s* and/or central offices.

Other information in this section: "ETSI Euro network services" on page 545

The following figure illustrates an ETSI QSIG network. Note that this is exactly the same setup as that shown in the MCDN section for North America, in "An example of a private network with Meridian 1" on page 537, which describes PRI SL-1 networking. The exception in the configuration is for the hardware configuration because the trunk lines are different. The hardware programming for ETSI QSIG is described below the following diagram. All other configurations are the same as those shown in the MCDN section for North America, in "Configuring private networks with SL-1 MCDN" on page 519.

Figure 183 ETSI QSIG networking



The following table lists the settings for some of the hardware parameters for ETSI QSIG networking example shown above.

Table 149 Hardware programming for branch offices

West End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

East End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

ETSI Euro network services

If your system has ETSI ISDN BRI/PRI lines, you can activate the malicious call identification (MCID) and Network Diversion features. Advice of charge-end call (AOCE) is active if your service provider has activated that service on the line.

When the features are activated, users can:

- display a call charge
- redirect calls over the ETSI ISDN BRI/PRI line to the outside network
- tag malicious calls

Advice of Charge-End of Call (AOCE) — AOCE is a supplementary service available from your service provider on ETSI ISDN BRI/PRI links. This feature allows the Business Communications Manager user to view the charges for an outgoing call once the call completes. This information is also reported to the Call Detail Reporting Application. The information can be provided in currency or charging units, depending on how the feature is set up by your service provider.

To invoke the feature, the user presses **FEATURE 818**.

To set up MCID and network diversion, you can access the **Network Services** heading on the Unified Manager, as described in these steps:

1. Click the keys beside **Services**, **Telephony services**, **General settings,** and **Network services**.
2. Click on **ETSI**.
3. The following table lists the possible values for ETSI.
   The **Description** column of the table describes the feature and how the user activates each feature from their telephone.

Table 150 ETSI network values

Attribute	Values	Description
Netwrk Diversion	Y or N	Allows you to choose if you want to allow calls to be redirected to an outside network.
MCID	Y or N	Malicious Call Identification If you set this feature to Y, the called party can use FEATURE 897 to request the network to record the identity of an incoming call. including: • called party number • calling party number • local time and date of the activity • calling party sub-address, if provided by the calling user
MCID note		The feature code must be entered within 25 seconds of the caller hanging up (a 25-second busy tone occurs). If the called party hangs up first, there is no opportunity to use the feature. Note: The call identification comes from your service provider, not the Business Communications Manager. You must have the service activated by the CO before the feature is active for the user, regardless of the setting in this field.

DPNSS 1 services

The Digital Private Network Signaling System (DPNSS 1) is a networking protocol enhancement that extends the private networking capabilities of existing Business Communications Manager systems. It is designed to offer greater centralized functionality for operators, giving them access to Business Communications Manager features over multiple combined networks.

Note: The DPNSS feature is dependent on which region loaded on your system at startup and that a software keycode was entered to enable the feature.

Other information in this section includes:

- "DPNSS 1 capabilities" on page 547
- "DPNSS 1 features" on page 548
- "Private networking with DPNSS" on page 555

DPNSS 1 allows a Business Communications Manager local node, acting as a terminating node, to communicate with other PBXs over the network. For example, corporate offices separated geographically can be linked over DPNSS 1 to other Business Communications Manager nodes, bypassing the restrictions of the PSTN*s* to which they may be connected. This allows connected Business Communications Manager nodes to function like a private network, with all features of Business Communications Manager accessible.

TIPS: Business Communications Manager DPNSS 1 works as a terminating node only. Business Communications Manager to Business Communications Manager DPNSS is not supported.

DPNSS 1 features can be used on any Business Communications Manager telephone. On most Business Communications Manager telephone, you must use specific keys and/or enter a number code to access the features.

DPNSS 1 capabilities

A single Business Communications Manager node, acting as a terminating node on the network, supports the following capabilities over DPNSS 1 lines:

- Direct Dial Inward (DDI) for incoming calls.
- Originating Line Identification (OLI) for incoming and outgoing calls:
  - For incoming calls, the Calling Line Identification (CLI/CLID) information is displayed to the user on telephones with line display This must be configured in programming.
  - For outgoing calls, the directory number of the originating party is sent out as OLI.
- Terminal Line Identification (TLI) for incoming and outgoing calls. Referred to as Called Line Identification.
- Selective Line Redirect (SLR) and External Call Forward (ECF) implemented on calls between DPNSS 1, and BRI/PRI, DASS2, and Analog lines.

- These remote access features are supported on DPNSS: DDI, line pool access code, destination Codes and remote page feature codes.

Software Keys are required to enable DPNSS 1.

DPNSS to Embark connections

DPNSS lines connected to an Embark switch perform call redirection/diversion using the Call Forward feature to create a tandem link back to the switch. Since this is different from other switches, you must select the type of switch DPNSS will be connecting to when you do module programming. Refer to "Defining trunk module types and settings" on page 130.

Before you program Call Forwarding ensure that:

- Both real channels and virtual channels are provisioned.
- Destination or line pool codes are programmed for the DPNSS to Embark link.

Also, during programming for Call Forward No Answer and Call Forward on Busy, when you enter the **Forward to:** digits, the system does a validation check with the switch on the number. (**Telephony features, System DNs, Active/Inactive DNs, DN XXXX, Capabilities**)

DPNSS 1 features

The following features are available and can be programmed over DPNSS lines:

- "Three party service" on page 549
- Diversion ("Using the diversion feature" on page 549)
- Redirection ("Using the Redirection feature" on page 551)
- "Executive intrusion" on page 551
- "Call offer" on page 553
- "Route optimization" on page 554
- "Loop avoidance" on page 555
- Message Waiting Indication ("Configuring MWI on DPNSS 1 networks" on page 569 in the chapter "Configuring centralized voice mail" on page 559

The following parameters can be configured for DPNNS 1 lines:

- Line type
- Prime set
- CLID set
- Auto privacy
- Answer mode
- Auxiliary ringer
- Full autohold

Some features are transparent to the user, but must be programmed to be activated. Others are available for end-user programming at the telephone. Details about these features are given below.

Three party service

Three Party Service is a DPNSS 1 feature for Business Communications Manager that is similar to the Business Communications Manager Conference feature.

The Three Party Service allows a user, usually an operator, to establish a three-party conference by calling two other parties from one telephone. Once the connection is made, the controlling party can hang up, leaving the other two connected. The controlling party can even put one party on hold, and talk to the other party.

Note: Business Communications Manager does not support Hold over the DPNSS link itself. This means that the conferenced party on the distance end of the network cannot place a Three Party Service call on Hold.

This feature is basically designed to allow operators to assist in the connection of calls from one main location.

Making a conference call

To initiate or disconnect from a conference call on a Business Communications Manager system over DPNSS 1, use the procedure described in the *Business Communications Manager Feature Programming Telephone Guide*.

Note: Three Party Service is supported on model 7000 telephones, but in a receive-only fashion. These telephone types cannot initiate Three Party Service. For more information about these telephone types, see the Business Communications Manager T7000 User Card.

Using the diversion feature

Diversion is a DPNSS 1 feature for Business Communications Manager that allows users to forward their calls to a third party on the DPNSS 1 network. This feature is similar to call forward on Business Communications Manager, but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion. These variations are described below:

- Diversion Immediate diverts all calls to an alternate telephone. This function is programmed by the user at their telephone.
- Diversion On Busy diverts all calls to an alternate telephone when a telephone is busy. This feature is programmed in the Unified Manager.

- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Unified Manager.
- Bypass Call Diversion overrides all call forward features active on a telephone over a DPNSS line. An incoming call to the telephone will not be forwarded; instead, the telephone will continue to ring as if call forward were not active. This feature is used to force a call to be answered at that location. Bypass Call Diversion is a receive-only feature on Business Communications Manager, and cannot be used from a Business Communications Manager telephone.
- Follow-me Diversion is also a receive-only feature. It allows the call forwarded destination to remotely change the Business Communications Manager call forwarding programming (Call Forward All Calls (CFAC) feature) to a different telephone.

  TIPS: Business Communications Manager CFAC must be active and the destination set/PBX system must support the feature.

  For example, user A forwards all calls to telephone B, a temporary office. Later, user A moves on to location C. The user does not have to be at telephone A to forward calls to location C. Using telephone B and Follow-me Diversion, the user can forward calls from A to location C.

  Follow-me diversion can be cancelled from the forwarded location.
- Diversion on Busy and Diversion on No Reply cannot be cancelled from the forwarded telephone. These are programmable only by an installer and not by the user.
- If multiple telephones are programmed to take a call, the first telephone to respond will act. All other telephones responding are ignored. Therefore, if the first telephone to respond has Diversion enabled, this feature will be invoked.

Restrictions by telephone type

- all variations supported on Business Communications Manager digital and IP telephones
- ATA2/ASM8+—all variations supported on an ATA
- ISDN—all variations supported on ISDN telephones, except Diversion on Busy and CFWD Busy
- Portables—all variations supported on portable telephones

Setting Diversion

You set Diversion for DPNSS in the same way as call forward, see “Assigning Call Forward” on page 409. You will need to enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

Using the Redirection feature

Redirection is a DPNSS 1 feature similar to Business Communications Manager Transfer Callback. Redirection lets a call awaiting connection, or re-connection, be redirected by the originating party to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Note: The address to redirect depends on the history of the call. Calls that have been transferred are redirected to the party that transferred them. In all other cases, the address to redirect is the one registered at the PBX system originating the redirection.

Note: Business Communications Manager does not support the redirection of Business Communications Manager originated calls, even over DPNSS 1.

The Diversion on No Reply feature takes precedence over Redirection.

Restrictions by telephone type

- For telephones without displays, the # key acts as MORE and the * key acts as VIEW
- ATA2/ASM8+—not supported
- ISDN—all variations supported on ISDN telephones
- Portables—all variations supported on portable telephones

Setting redirection

The timer used for the network Callback Feature is also used for redirection.

Executive intrusion

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. An example of the use of this feature is to make an important announcement when the recipient is on another call.

EI is similar in functionality to Business Communications Manager Priority Call, but it is a receive-only feature on Business Communications Manager telephones. EI cannot be initiated from a Business Communications Manager telephone. The person using this feature must be on another PBX system on the DPNSS 1 network.

When EI is used to intrude on a call in progress, a three-way connection is established between the originating party and the two parties on the call. The result is very much like a conference call. When one of the three parties clears the line, the other two remain connected, and EI is terminated.

Restrictions by telephone type

- ATA2/ASM8+—supported
- ISDN—not supported
- Portables—not supported

The telephone receiving the intrusion displays `Intrusion Call`. A warning indication tone will sound after intrusion has taken place, and the standard conference call tone will sound every 20 seconds.

Intrusion levels

Whether or not a telephone will accept or reject an Executive Intrusion request depends on the level of intrusion protection programmed. Each telephone (DN) has an Intrusion Capability Level (ICL) and four Intrusion Protection Levels (IPL).

When the ICL of the intruding telephone is higher than the IPLs of *both* telephones on the active call, EI will occur. It is best to set the IPLs of most the Business Communications Manager telephone to the default of **None**, or Low or Medium.

Intrusion levels are described as follows:

- ICL: determines the ability of the attendant to intrude. As long as the ICL is higher than the IPL of the wanted party, EI is allowed. Since EI is a receive-only feature, the ICL cannot be set on Business Communications Manager.
- IPL: determines the ability of the attendant to refuse intrusion. If the IPL is lower than the ICL of the originating party, EI is allowed. For general purposes setting the IPL to None, Low or Medium is recommended, unless intrusion is not wanted.

Programming IPL on a telephone

1. Click on the keys beside **Services, Telephony Services, System DNs, Active Set DNs, DN ##,** and **Capabilities**.
2. Choose **Intrusion**.
3. Click a **Protection level**: None, Low, Med, or High.
   If the level of intrusion protection is set to **High** no intrusions will be allowed. The default is **None**.

Call offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the telephone. The intended recipient can ignore, accept, or decline the offered call. Call Offer is useful in increasing the call-coverage capability of a Business Communications Manager system, and helps to lift the network processing load. It is a receive-only capability on Business Communications Manager: incoming calls would be initiated at another PBX system on the DPNSS 1 network.

An example of Call Offer in use is an operator or attendant who has a number of calls coming in at once. The operator can call offer one call and move to the next without waiting for the first call to be answered.

Call Offer Displays

When a Call Offer is made by the originating exchange, the target telephone displays a message, and a tone is heard. When an offered call arrives on telephones with line display, the user sees `XX...X wtng` if the calling party ID is available and CLID is enabled. If CLID is not available or CLID is disabled, `Line XXX waiting` appears (the line name associated with the call). If there are more than 11 digits in the incoming number, only the last 10 will display.

If Call Queuing is programmed for the system, the display shows `Release Line XXX`.

This is the line name of the highest-priority queued call if it is an offered call.

Restrictions by telephone type

- model 7000 telephone — associated LED or LCD flashes, and a tone is heard
- ATA2/ASM8+—Call Offer is supported as a Camp On feature, and a tone is heard
- ISDN—not supported
- Portables—not supported

Note the following general conditions and restrictions:

- DND on busy must be programmed as N (**DN ##/Capabilities**) for a telephone to accept Call Offer.
- If CF on busy is programmed for the telephone, Call Offer is not accepted.
- The target line for the telephone must be set to: If **busy: busy tone**, which is the default. Refer to “Assigning Trunk/line data” on page 236.
- Call Offer does not work if sent over Manual answer lines. It is recommended that the lines be left at the default: **Auto**.

User actions

The party receiving a Call Offer has three choices:

- Ignore it. After a programmed time interval, the Offer request is removed.
- Reject it. If the user activates Do Not Disturb on Busy (DND) when the Call Offer request is made, the request is removed from the telephone. The calling party is informed of the rejection.

  A call cannot be offered to a telephone with DND active. The line indicator for external incoming calls still flashes.
- Accept it. The Offer is accepted by releasing the active call.

Note: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route optimization

Route Optimization is a DPNSS 1 feature for Business Communications Manager that allows calls to follow the optimum route between two end PBXs. This allows efficient use of network resources.

Route Optimization is initiated by the system and is transparent to the user. However, the user may see a call switch from an appearance on the telephone to another appearance key or from an intercom button to the appearance key or vice versa. This occurs when Business Communications Manager receives a Route Optimization request and initiates a new call to follow the optimal route.

If a telephone is active on a private line call, the Route Optimization call being established may go on a public line. This will cause a loss of privacy on that line.

Data calls are rejected by Route Optimization in order to ensure the data transmission is not affected.

Certain situations result in Route Optimization not taking place. For example, calls that are using Hold, Parking or Camp features do not undergo Route Optimization, and if a Route Optimization call undergoes Diversion, the Route Optimization is dropped.

Setting Route Optimization

There is no system programming required for the feature when Business Communications Manager is working as a terminating PBX system. However, Business Communications Manager must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, Allow redirect must be set to **Y**. For more information, see "Defining device capabilities" on page 405.

Loop avoidance

Errors in the configuration of a network may make it possible for a call to be misrouted, and arrive at a PBX system through which it has already passed. This would continue, causing a loop which would eventually use up all of the available channels. The Loop Avoidance service permits counting of DPNSS 1 transit PBXs and rejecting a call when the count exceeds a predetermined limit.

Programming loop avoidance

To set Loop avoidance during hardware configuration:

1. Click the keys beside **Resources, Media Bay Modules**, **Bus 02 - 07**, **Modules on Bus.**
2. Select **Module 1.**
3. Choose **Module type DPNSS**.
4. Type a value (0-25) in the Maximum transits box.
   The default value is 25.

Private networking with DPNSS
(International only)

DPNSS supports the Universal Dialing Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a dialing number includes the following:

- a Private Access Code, programmed into the system as part of the destination code table to prevent conflicts with the internal numbering system. (**Access Codes**)
- a Home Location Code (HLC) assigned to each PBX system, and configured as part of the destination code (a maximum of seven digits). For each HLC, a routing code must be programmed in the system. (**Dialing plan, UDP, Location code**)
- a Directory Number (DNs) assigned to each extension as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, 1111 is the DN.

A typical Private Number, using a private access code and dialed from another site on the network, appears below.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating Business Communications Manager system. Each site has its own HLC and a range of DNs. The figure below illustrates this example.

Calls are dialed and identified to the system as follows:

- To reach a telephone inside the Private Network, at the Business Communications Manager site, the user dials the DN of choice.
- To reach a telephone inside the Private Network, from another site, the user dials HLC + DN.
- To reach a telephone outside the Private Network, the user dials an Access Code + HLC + DN

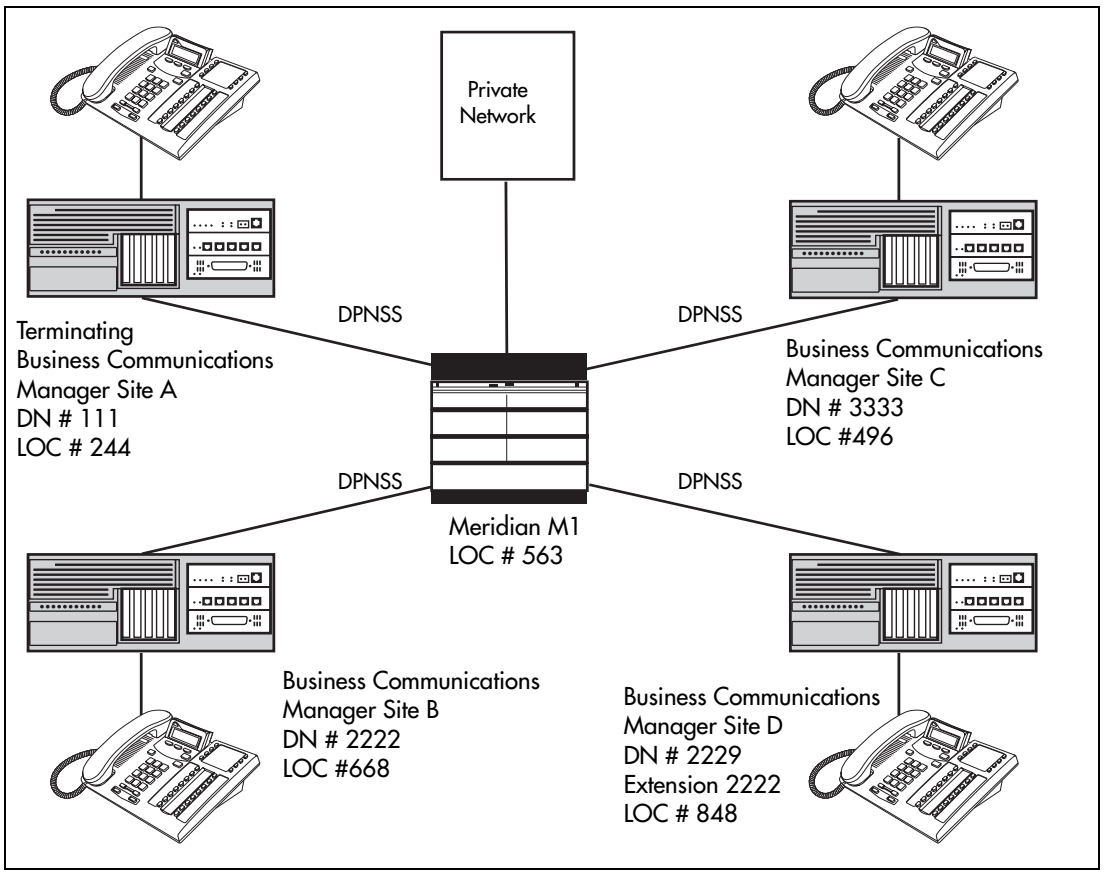
  Each node has its own destination (dest) codes which includes the appropriate access and HLC codes to route the call appropriately.

The table below shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 151 Calling numbers required for DPNSS network example

Calling Site	LOC/HLC	Calling Party Number	Called Site	Dialing String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Figure 184 DPNSS networking



The table below shows examples of the routing required to set up the network shown in the figure above. Note that 6 is the Private Access code.

Table 152 Routing for DPNSS network

Private Network: (for each branch Business Communications Manager)			
Routing service to		**Private network**	**Public network**
	Route	001	002
	Dial out #	No number	No number
	Use	Pool N	Pool N
	DN type	none (private access code 6 is programmed)	public
	Destination Code	6	9
	Normal route	001	002
	Absorb	1	1

Guidelines for creating a private numbering plan with DPNSS

Use the following guidelines when creating a private numbering plan with DPNSS.

- When creating HLCs for the nodes in your system, avoid numbering conflicts between network nodes and internal DNs, Hunt group DNs.
- Program a Private Access Code into your destination routing tables to avoid conflicts with your internal HLC and dest code numbering plan. For example, if a dialout HLC is 848, but this number already exists in the Business Communications Manager system for an extension, the routing tables should add a Private Access Code to the dest code. If the code is programmed as 6, the dest code becomes 6848. 6848 uses a route to dial out 848 using the DPNSS line pool, allowing the call to be placed.

  Note that a Private Access Code is required only for specific DPNSS features such as Diversion, Route Optimization, and Redirection.

Customizing the DPNSS routing service

You can customize the routing service using the following restrictions:

- Direct Inward Access (DIA) lines allow incoming calls on private circuits to be directed to telephones without going through the normal call reception. Each DIA line is assigned to one or more extensions and is given a distinct Private Received number. When someone on another system on the network dials the Private Received number on a DPNSS line, the Business Communications Manager system checks all received digits, compares the digits to an internal table and routes the call to the appropriate DIA line. All extensions programmed to have access to that DIA line will then alert for the incoming call.
- Dialing restrictions can be added to lines in line pools. Filters can restrict the use of the line to specific area codes.
- You can use host system signaling codes as part of the dial out for a route. Routing can also be used as an alternate method for a direct-dial digit. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1. Because overflow routing directs calls using alternate line pools, a call may be affected by different line restrictions when it is handled by overflow routing.

Chapter 22
Configuring centralized voice mail

This section describes how to set up the Business Communications Manager to support centralized voice mail or call attendant over a private network.

The Business Communications Manager supports voice mail configuration either from the local source or by accessing a remote voice mail system located on another Business Communications Manager or attached to a Meridian 1 system. The system can be configured to more than one voice mail system. However, each telephone can only be configured to one system.

BCM 3.6 and newer software: The Business Communications Manager can also support centralized voice mail on a DMS100/SL100 switch through a PRI-DMS100 connection. The system also supports centralized voice mail on the switch through an indirect connection through an M1, where the DMS100/SL100 is connected by PRI-DMS100 to the M1 and the M1 is connected to a Business Communications Manager through a PRI-MCDN connection. The DMS100/SL100 can use either the Public number or Private number of a Business Communications Manager telephone to designate the mailbox number on the voice mail system.

To configure centralized voice mail, the system must be using a CDP dialing plan and be running on a private network created using either PRI SL-1 or VoIP trunking set up with MCDN. Private network configuration and features are discussed in "Configuring private networks with SL-1 MCDN" on page 519 (North American profile) and "Configuring ETSI QSIG and DPNSS network services" on page 543 (ETSI profiles) and in the *IP Telephony Configuration Guide* (VoIP trunks).

Note: For centralized voice mail from a DMS100/SL100 system, configure the Business Communications Manager dialing plan as either CDP or UDP.

This section includes this information:

Business Communications Manager as host

A Business Communications Manager that acts as a central voice mail location must be running at least BCM version 3.5 or newer software. Other systems on the network can be running older software, as long as that software supports MCDN. In the case of another Business Communications Manager system, this would require BCM version 2.5 or newer software. You can add up to 1000 mailboxes on Business Communications Manager voice mail, providing you have entered adequate keycode*s*.

CallPilot constraints:

- To allow use of the auto attendant feature, you must ensure that the **Allow Network Transfers** check box is selected in the CallPilot Manager.
- To allow use of voice mail, you must ensure that the **Enabled Redirected DN** check box is selected in the CallPilot Manager.

For details about setting up the CallPilot parameters and features, refer to the *CallPilot Manager Set Up and Operation Guide* and the other CallPilot supporting documentation.

Meridian system as host

If you are using a voice mail system connected to a Meridian 1 as a host system, ensure that the systems are set up to be compatible with each other:

CallPilot compatibility

If you are planning to use M-1 based CallPilot software for the voice mail system, there are no compatibility issues.

Meridian Mail compatibility issues

If you are using Meridian Mail as the host system, ensure that the Meridian has the following:

- Meridian Mail rel. 7 (MM7) or above
- the appropriate number of PRI cards and D-channel handlers to support the PRI links to all the Business Communications Managers using the system.

Special requirements:

- Over a PRI SL-1 line: Meridian 1 must be on Release 19 or greater.
- Over VoIP: Meridian one must be installed with an IPT card version 3.0 or newer
- Meridian 1 requires the network ID of the Business Communications Manager, which is defined under **Dialing Plan, Private Network** in the Unified Manager. This is a number between 1 and 27, and is defined by the Meridian system administrator.

Refer also to "System set up for satellite systems" for specific call features available from a Meridian 1-based voice mail system.

System set up for host Business Communications Manager

The Business Communications Manager that hosts the voice mail needs to ensure that incoming calls are directed to the voice mail service.

Process assumptions:

- Private network has been set up, with MCDN, between any nodes that need to access voice mail on this system.
- That all systems are using the CDP dialing plan, and you set up the correct routing to these systems.
- CallPilot or auto attendant is setup and is running for the local system.
- You obtain a list of DNs from the remote systems that require mailboxes.

Follow these steps to configure the host system:

1. Obtain the Voice Mail DN by pressing **FEATURE** 985 on a system telephone.
2. If this setting matches the DN scheme for your system dialing plan, go to step 3.

   If this setting does not match the DN scheme for your system dialing plan:

   a. In the Unified Manager, click on the keys beside **Services**, **Telephony Services.**
   b. Click on **General Settings**.
   c. On the top menu, click on **Configuration**, and select **Change DNs**.
   d. In the Old DN field, enter the number you obtained in step 1.
   e. In the New DN field, enter the voice mail DN that fits your system dialing scheme.
   f. Click **OK**.
3. Click on the keys beside **Lines**, **Target lines**, **Line XXX** (the target line you want to assign to the Voice Mail DN), and **Trunk/Line data**.
4. Click on **Received number**.
5. Enter the voice mail DN.

CallPilot programming:

6. Set up CallPilot for voice mail or auto attendant answering:
   - **Voice mail:** In CallPilot Manager click on **Configuration** and **System Properties**. Ensure that the **Enable Redirected DN** box is enabled.
   - **Auto-Attendant:** Under the **Auto-Attendant** heading, click the line record you specified in step 4 and set the Auto-Attendant to answer after 0 (zero) rings.
7. To activate these settings, reboot the system when it is convenient for your users.

VoIP networking note: If you are using H.323 VoIP trunks for central voice mail, you need to set the following:

- Ensure that the local gateway protocol is set to SL-1 or CSE (BCM 3.0 or newer software), based on the version of the satellite systems.
- Ensure that the remote gateways are programmed to route using CDP.
- Ensure that the remote gateway protocols are set to SL-1 or CSE (BCM 3.0 or newer software), based on the version of the satellite system.
- Do not use SIP trunks for centralized voice mail.

System set up for satellite systems

Business Communications Managers that are remote to the voice mail system need to ensure that outgoing calls are correctly directed to the voice mail service on the host Business Communications Manager.

Process assumptions:

- Private network has been set up, with MCDN, between the satellite and host system.
- The correct routing to the host system is set up and working.
- You supplied a list of DNs to the host system administrator that require mailboxes.

Follow this process to set up a satellite Business Communications Manager for voice mail:

1. In the Unified Manager, click on the keys beside **Services**, **Telephony Services**, **Telco Features**, **Voice message center numbers**.
2. Click on the voice center number that you want to assign to the remote voice mail system.
3. In the **External #** field, enter the voice mail DN assigned by the host system.

Configuring the Target lines:

4. If the telephone does not already have a target line assigned:
   a. Click on the keys beside **Lines**, **Target Lines**.
   b. Select a the first target line assigned to the telephones you want to access the remote voice mail.
   c. Click on **Telco Features**.
   d. Beside the Voice message center field, use the drop list and choose the same center number that you chose in step 2.
5. On the top menu, click on **Edit** and select **Copy**.
6. In the Copy dialog box, enter the next target line you want to change.
7. Click **OK**.
8. Repeat steps 9 and 10 for all the target lines you want to change.

Configuring the telephone records:

9 Click on the keys beside **System DNs**, **Active set DNs**, **DN YYY** (the telephone you associated with the voice mail target line), **Line access**, **Line assignment**.

10 Click on **Line XXX** (the target line you programmed for the telephone.

11 Set the **Vmsg set** field to **Y** (yes).

MWI note: If you require answer DNs to provide messaging waiting indicators (MWI), the telephone with the DN must be assigned with a target line, and Vmsg set must be set to Y on the telephone record.

Configuring Call forward to go to voice mail:

12 In the same DN, click on **Capabilities**.

13 Set the **Allow redirect** field to **Y** (yes).

14 Under **Capabilities**, click on **Call Forward**.

15 Enter the Voice Mail DN in both the **Fwd no answer to** and the **Fwd on busy** fields.

16 Repeat steps 12 to 18 for each of the DNs you want to assign to the remote voice mail.

17 Test the system.

VoIP networking note: If you are using H.323 VoIP trunks for central voice mail, you need to set the following:

- Ensure that the local gateway protocol is set to CSE, based on the version of the satellite systems.
- Ensure that the remote gateways are programmed to route using CDP.
- Ensure that the remote gateway protocols are set to CSE, based on the version of the satellite system.
- Do not use SIP trunks for centralized voice mail.

Configuring the system for centralized voice mail

MCDN is supported over a PRI (SL-1) line or VoIP trunks between your Business Communications Manager and other systems, such as a Meridian 1, Norstar, or other Business Communications Managers. This section describes the specific programming for remote voice mail over PRI lines.

Apart from line configuration, MCDN over VoIP has the same system configuration.

To set up a PRI connection on the Business Communications Manager, you need to:

1. Ensure that the remote voice mail system is set up to accommodate your system on the network.
2. Ensure that your dialing plan coordinates with what the other nodes on the network are using. **Services, Telephony services, General settings, Dialing plans, Private network, UDP or CDP.**
3. Enter the network system identifier the Meridian system administrator supplied (between 1 and 27), if you are networked with a Meridian 1 somewhere in the network. **Services, Telephony services, General settings, Dialing plans, Private network, UDP or CDP**
4. Install a DTM module to connect to the appropriate PRI SL-1 trunk, or enter the keycode for the required number of VoIP trunks.
5. Configure the lines you plan to use, assigning them to the same line pool. Refer to "Configuring lines" on page 227 (PRI lines) and the IP *Telephony Configuration Guide* (VoIP trunks).
6. Enter the MCDN keycode.
7. Choose the MCDN network features that you want to use.
   Services, **Telephony services**, **General settings**, **Network Services**, **MCDN**
8. Set up routing to target the PRI or VoIP line pool you set up.
9. Set up your numbering plan to recognize the network system identifiers of the other nodes on the system, so your system can pass them along, as required.
10. Assign the pool to any telephones you want to allow to use this line.
11. Program target lines and assign to telephones.
12. Set up the voice mail DN for the system that is being used as the host voice mail system for your network.
13. Test the link.
14. Refer to the CallPilot documentation to set up the mail boxes or auto attendant features and other voice mail parameters.

Meridian MCDN call features over PRI SL-1 lines

Besides the general MCDN features described in Understanding MCDN network features on page 528, an MCDN connection with a Meridian 1 voice mail system, also provides some special call features, which are listed in the following table:

Table 153 MCDN feature enhancements

Centralized messaging	• "Message Waiting Indication" on page 565 (MWI)
Centralized Attendant	• "Camp-on" on page 567 • "Break-in" on page 568

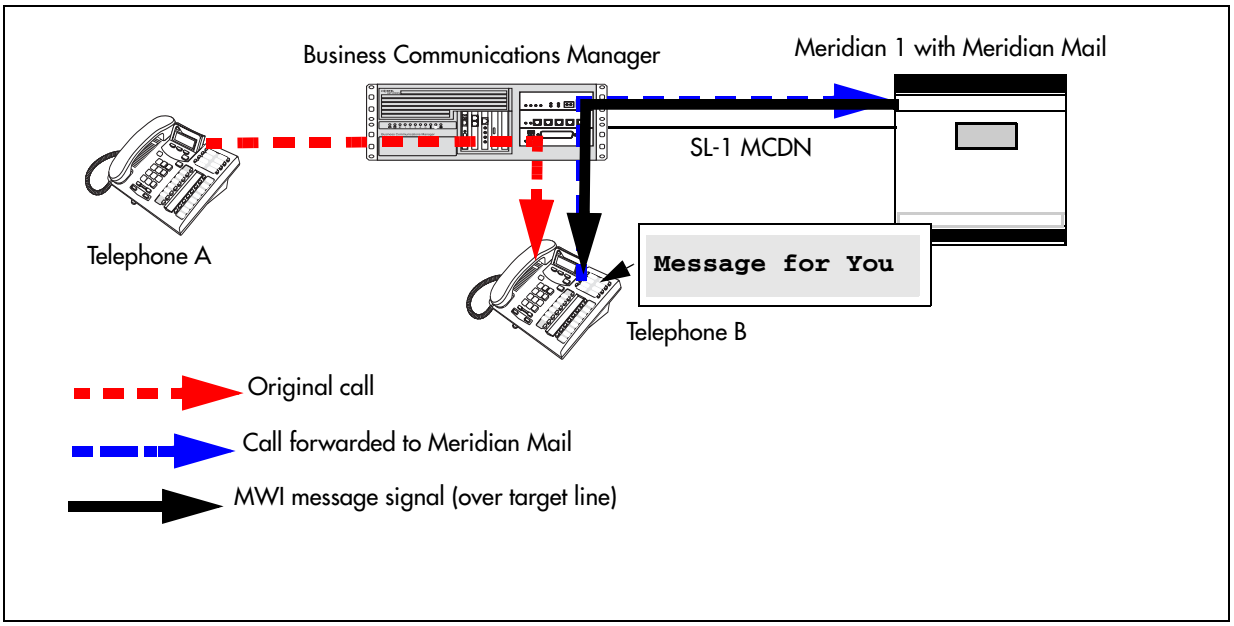
Message Waiting Indication

MWI allows the voice mail host system (Meridian 1) telephone that is designated to receive messages to notify a target telephone on the Business Communications Manager of a call waiting using the MIK and MCK message indicators on the Meridian telephones. This feature works for both Nortel and third-party voice mail systems. Messages are received at a centralized location, to a pre-determined telephone, where they are processed and forwarded to the target telephone.

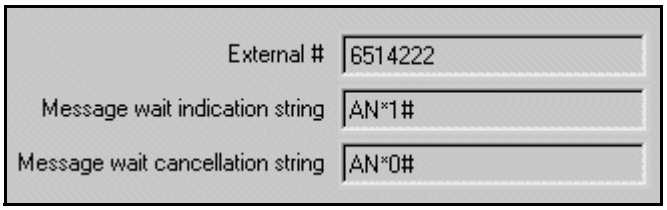
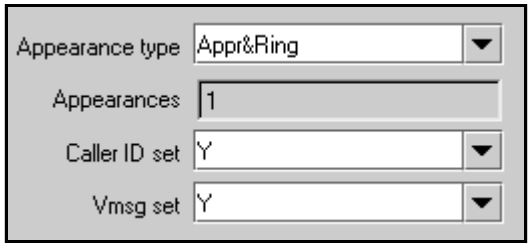
MWI allows the user to reply or call back to the message center. The procedure for retrieving messages is described in the Telephone Features Handbook.

The following figure demonstrates how the Meridian responds when a call is forwarded to a Meridian Mail mailbox.

Figure 185 Message waiting indication message



Programming notes

Business Communications Manager programming
To select Remote Capability for MWI on a per-loop basis for PRI: Resources, Media Bay Modules, Bus XX, Modules on bus, Module X: Remote Capability MWI = Y (if M1 has MWI package, with RCAP set to MWI)
Turning on the service for IP trunks: Services, General Settings, IP Trunking: Remote Capability MWI = Y (if M1 has MWI package, with RCAP set to MWI)
Telco features, VMsg Ctr Tel Numbers: • Voice Message Center 1 set to DES code plus M1 voice mail DN 
Lines (target line), Telco features: • choose Voice message Center 1 
System DNs, Active set DNs, Line access, Line assignment: • assign target line to each set • in target line, VMsg set to Y 

M1 programming
1. Disable the PBX D-channel associated with IPT (LD96). 2. Add MWI to the RCAP of the D-channel (LD 17 RCAP MWI) 3. Ensure the RLS ID is a minimum of 25 (RLS ID 25). 4. Re-enabled the PBX D-channel. Note: Package 219 is required on the Meridian PBX to allow RCAP MWI. Note: If IP routing is being used, you must complete this procedure on all the D-channels in the private network.

Camp-on

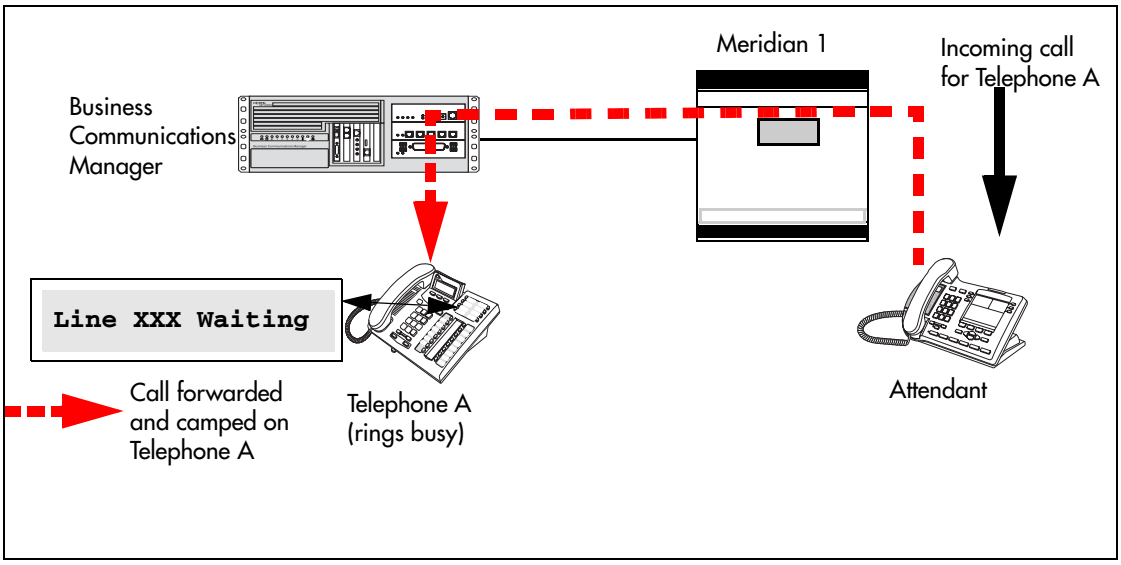
A call received by the Meridian attendant can be assigned to a telephone anywhere in the MCDN network, when the following situations are valid:

- the target telephone rings busy when the attendant calls
- no free keys on target telephone
- DND regular feature is inactive
- DND on busy feature is inactive

The target user sees that there is a call camped on the telephone. The called user can then clear a busy lines and take the call, or the user can choose to reject the call, using F814, or the user can indicate Do Not Disturb, using F85.

The following figure demonstrates the call path for a Meridian attendant to camp a call on a telephone in the Business Communications Manager system.

Figure 186 Camping a call

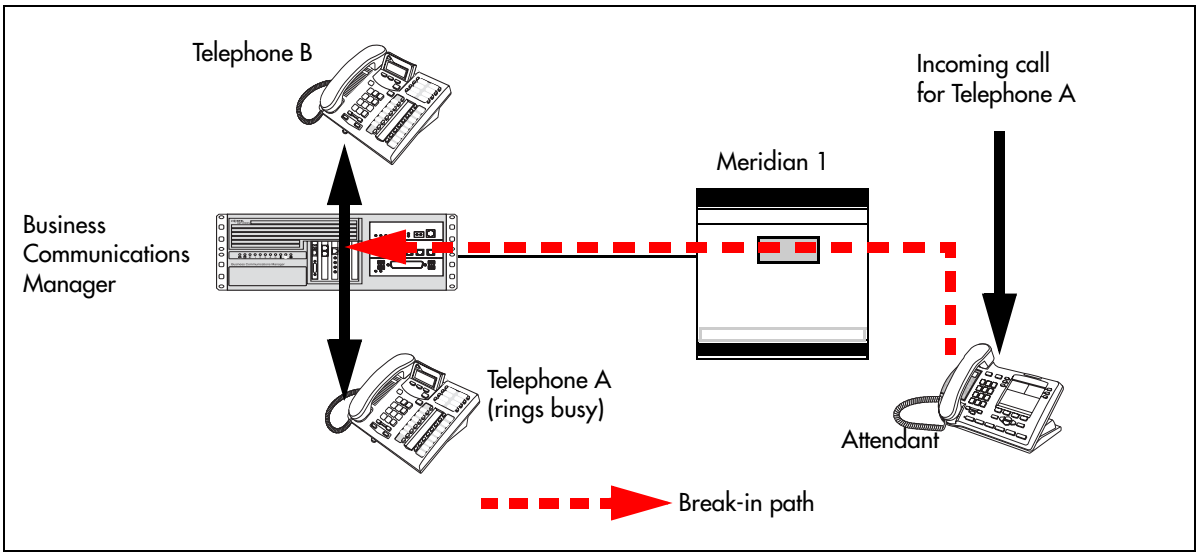


Break-in

The Meridian attendant can use the break-in feature to interrupt an on-going call from a telephone in the Business Communications Manager system.

The following figure demonstrates the call path for a Meridian attendant to break into a call between telephones in the Business Communications Manager system.

Figure 187 Breaking into a Business Communications Manager call path



Break-in can occur when these situations are valid:

- Target Business Communications Manager telephone is busy but still has a free intercom or line key.
- There is no camped call on the target telephone.
- DND on busy is turned on.
- prime set is also busy, with no free key, and with DND turned on.
- Attendant capability is high (2), and higher than either the target telephone or the caller the target telephone owner is busy with.

Only post-dial break-in is supported by MCDN:

1. Attendant dials destination number.
2. If a busy tone is heard, the attendant presses the BKI button.
   Attendant is given access to the conversation.

You can set a level of priority that will determine if a telephone will allow an attendant to break in. This is referred to as setting the Intrusion level. Use the following rules to configure the break-in feature.

- Set the Intrusion level for each telephone (under Capabilities). Refer to "Setting intrusion controls" on page 414.

How the intrusion hierarchy works:

— Break-in is allowed if Attendant telephone is High and caller telephone is Medium.

— Break-in is not allowed if Attendant telephone is Medium and caller telephone is high.

Configuring MWI on DPNSS 1 networks

Message Waiting Indication (MWI) is a DPNSS 1 feature for Business Communications Manager Call Services. Messages are received at a centralized location, to a pre-determined telephone, where they are processed and forwarded to the target telephone. This centralization relieves the network processing load, making the system more efficient. MWI provides users with the ability to scroll through, erase and reply to messages.

When there are messages to retrieve, `Message for you` appears on the telephone display. After all the messages are retrieved by the user, a Message Waiting Cancellation (MWC) is sent from the message center, and the user telephone no longer displays an MWI message.

MWI allows the user to reply or call back to the message center.

This feature is only supported on Business Communications Manager target lines.

Restrictions by telephone type:

- M7000—associated LED flashes
- ATA2—not supported.
- ASM8+ — supported
- ISDN— not supported.
- Portables—not supported.

The following sections describe how to set Message Waiting Indication:

- Assign message center to a line ("Assigning message centers to a line" on page 569).
- Select message center for use. ("Selecting a message center" on page 571)
- Assign the line to a telephone to Appear and/or Ring. ("Setting Message Waiting Indication" on page 572)

Assigning message centers to a line

You need to assign any one of five, or None, of the message centers to the line. There can be as many as five message centers in a network; that is, five telephones on the Business Communications Manager system can act as mailboxes in the message centers offered by five different PBX systems on the network. These PBXs may also be from different manufacturers.

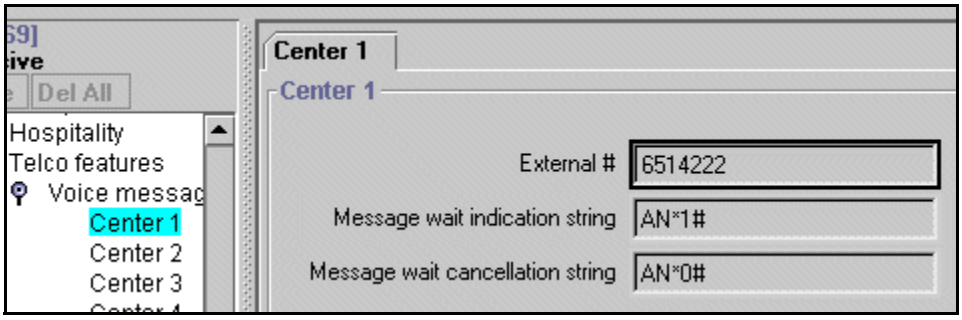
Thus, for each message center there may be different:

- numbers to be dialed to reach the mailbox from the telephone
- MWI strings received, indicating that the center has a message in the mailbox
- MWC strings received, indicating that the voice mails have been retrieved

To assign a message center:

1 Click the keys beside **Services**, **Telco Features**.

Figure 188 Telco features Voice message center



2 Click **Voice message center numbers**.

3 Choose a Voice message center: **1** to **5**.
The existing telephone (DN) for Message Waiting appears if available, as **Tel#:XXXX**.

4 Type the new target number, starting with an access code, if required, or **None**. For example: **65142222**.

The display shows **MWI:AN*1#**. This is a string sent by the PBX holding the message center.

5 Program the number that the user will dial on the IC key to retrieve a message from the messaging center.

6 Program the Non-Specified Information (NSI) string for the MWI that is expected from the particular message center.
The display shows **MWC:AN*0#**. See the next procedure: "Programming MWI and MWC".

7 Program the NSI string for the MWC that is expected from the message center.

Note: The line must be programmed to Appear and/or Ring at the telephone.

When assigning message centers, you can program all three parameters for each. Remember that the following procedure is not to select a message center, but to program any or all of the five available message centers. This is similar to the Direct Dial functionality.

Note: The MWI and MWC strings used in this procedure are default NSI strings for Message Waiting.
*58B*AN*1# – Message Waiting Indication
*58B*AN*0# – Message Waiting Cancellation
This provides the information required to program the strings as:
AN*1# for MWI, and
AN*0# for MWC
Private network strings will differ with different message centers. These should only be changed on the advice of your customer service representative.

Programming MWI and MWC

MWI and MWC information is received from the network in the form of NSI strings. The NSI strings in DPNSS are dependent on the supplier of the PBX. Therefore, the strings vary depending on the originating PBX system.

Each string has the following default structure: *58XYYYYY.*

The following table describes each part of the NSI string:

Table 154 Parts of the NSI string

String Component	Description
*58	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY..	Manufacturer specific string, which can contain any sequence of alphanumeric digits or *.
#	Marks the end of the identifier.

Only the YYYYY.. # portion of the string must be programmed for MWI and MWC. The procedure is similar to Set Name/Line Name.

The following criteria must be met when programming NSI strings for MWI/MWC:

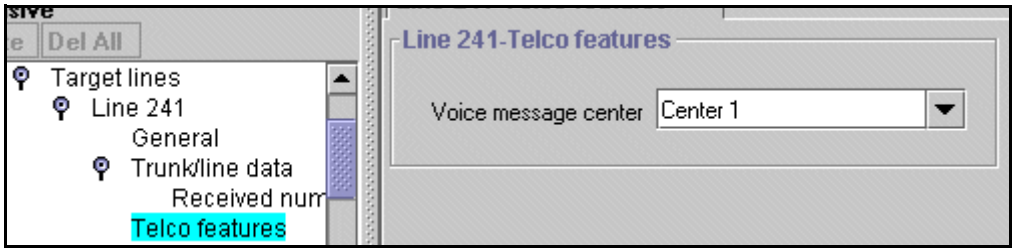
- No spaces are allowed, including spaces at the end of the string.
- A # must be present at the end.
- A # or a * cannot be present in the first character.

Selecting a message center

With a message center programmed on a selected line, you must set the message center for use:

1. Click the keys beside **Services**, **Telephony services**, **Lines**, **Target lines**.
2. Click a target line number (Line 241 to 492).
3. Click the key beside **Telco features**, then click on **Voice message center numbers**.
4. Choose a **Voice Message center**: **1** to **5**.

Figure 189 Target line Telco features voice message center

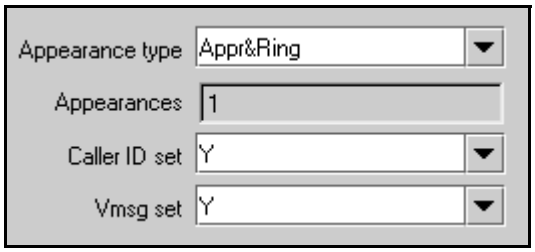


Setting Message Waiting Indication

Follow these steps to set the MWI:

1. Ensure that you have programmed a telephone to access target lines for receiving messages. For information on access to target lines, refer to "Assigning message centers to a line" on page 569.
2. Click on the keys beside **Services**, **Telephony Services**, **System DNs**, and **Active Set DNs.**
3. Click a DN (DN 221-528).
4. Click on the key beside **Line access and Line assignment.**
5. Select the target line you specified in Selecting a message center.

Figure 190 Setting Target line voice mail settings for the telephone



6. Click **Y** to enable Vmsg set.

   When Vmsg is enabled for a target line on a telephone, the telephone logs Message Waiting Indication/Cancellation received for the corresponding target lines to the user.

Chapter 23
Configuring Hunt groups

This section explains how to create hunt groups using the Hunt Group headings in the Unified Manager.

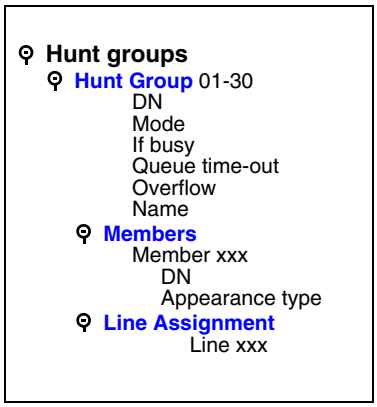
Hunt groups are designed to provide a service where incoming calls appear on a targeted group of telephones called a Hunt group ("How to use Hunt groups" on page 574). When you designate a Hunt group, you define the group as a unique DN. This DN receives and distributes calls to the telephones assigned to the group. The telephones receiving the call provide a line indication that a call has come in. How the calls are distributed can also be defined.

There can be a maximum of 30 Hunt groups assigned on a Business Communications Manager.

Tasks:
• Identify the Hunt group ("Identifying a Hunt group" on page 575)
• Determine Hunt group members ("Adding a Hunt group member" on page 579)
• Determine the lines for the group ("Programming Hunt group lines" on page 582
• Determine how the calls will be handled and distributed ("Feature operation within Hunt groups" on page 584)
• Monitor active Hunt group calls ("Monitoring Hunt groups" on page 585)
• Monitor Hunt group activity ("Using Hunt group metrics" on page 587)

The following figure shows a detailed view of the Hunt groups headings on the navigation tree.

Figure 191 Hunt groups menus and fields



How to use Hunt groups

You can use hunt groups to route calls to a support service such as a Help Line for a software company. For example, specialists handling Product A can be in one group, and specialists handling Product B can be in another group. Incoming calls hunt for the next available set in the group. If no set is available, the system places the call in a queue or the call gets routed to an overflow set.

Some typical uses of Hunt groups are:

- a sales department answering questions on product prices or availability
- a support department answering questions concerning the operation of a product
- an emergency department answering calls for help

Each Hunt Group has its own unique system DN that can be called from any set on the same system. When the Hunt group DN is called, the incoming call is treated in the same fashion as calls received from outside lines.

A Hunt group can receive a call in one of two ways:

- from one of the lines assigned to the Hunt group
- from an internal system call to the Hunt group DN

Hunt group tips:

Some of the things you need to note about Hunt group programming:

- calls on queue provide Ringback only (no on-hold music or tones)
- ensure the **General Settings, Timers, Transfer Callback Timer** is set correctly for Hunt group configuration. Refer to "Setting system timers" on page 472.
- Do not program videophones as members of a Hunt group. Hunt groups allow one B channel connection at a time and videophones use two B-channel*s*.
- Hunt group DNs cannot be assigned as an auto dial on a Key Indicator Module (KIM), attached to a T7316E telephone.

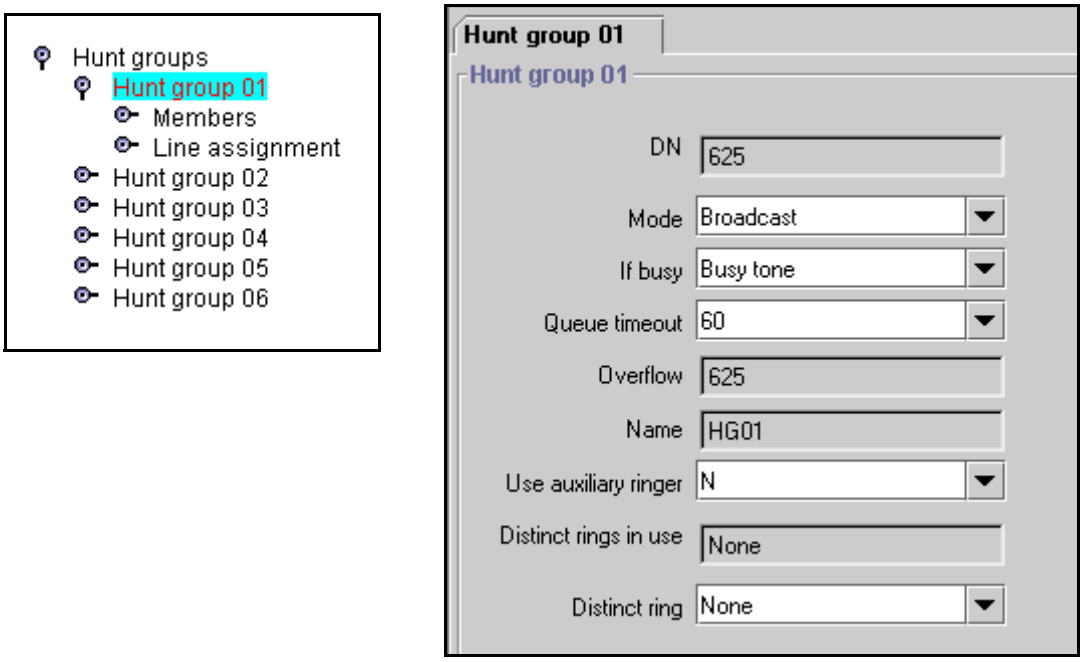
Identifying a Hunt group

When you first set up a Hunt group, you need to identify how a call will be handled among the group.

1 Click the keys beside **Services**, **Telephony Services**, and **Hunt groups**.

2 Click on a Hunt group (**Hunt group 1-30**).
The Hung group ## screen appears in the right frame.

Figure 192 Hunt group XX screen



3 The following table describes the settings that define how a hunt group handles calls:

Table 155 Hunt group settings

Field	Values	Description
DN	Read-only (625-654)	Hunt group DNs begin at 625. This value cannot be altered.
Mode	Broadcast Linear Rotary Default: Broadcast	Choose how you want the line to present to the group. **Broadcast**—simultaneously rings at each non-busy telephone in the hunt group. All telephones receiving the call also display the calling line identification from the line, if the telephone or line has been configured to offer that service. Any of the alerted telephones can access the call. Only one call can be presented to a hunt group at a time. Other calls are queued until the first call is answered. Then the next call rings on the remaining non-busy telephones. This feature allows the call load to be continuously spread across the entire member group.

Table 155 Hunt group settings (Continued)

Field	Values	Description
Mode (continued)	Refer to "Hunt group modes" on page 577	**Linear**—rings the first telephone in the hunt group list. If that telephone is busy, the system continues down the hunt group priority list until a non-busy telephone takes the call. In this case, all incoming calls are processed simultaneously and delivered based on the priority list. With this feature, you can program your top salesperson to be the first member of the Hunt group to receive incoming calls. **Rotary**—the call starts at the member telephone that appears on the list after the telephone that answered the last call. If that telephone is busy, the system proceeds down the priority list until a non-busy telephone is reached. As many incoming calls can be processed as there are available telephones to accept the call, each call being presented in the described round-robin fashion.
Hunt Delay	1-10 (seconds)	If Mode is either Linear or Rotary, Hunt Delay specifies how much time to delay offering a Queued call to a member telephone once that telephone becomes available. This is to provide a break period for the users between calls. The default is four seconds.
If busy	Busy tone Queue Overflow Default: busy tone	Choose how you want the system to respond if all lines appear as busy. **Busy tone**: If all lines are busy, the user receives a busy tone. **Queue**: If all lines are busy, the user is put on hold for the next available agent. **Overflow** - If all members of the Hunt Group are busy on a call from that Hunt Group, then route this call to the Hunt Group overflow DN. Overflow is only available if the overflow DN is different than the hunt group DN. Refer to the Overflow field, below.
Queue time-out	15, 30, 45, 60, 120, 180 (seconds) Default: 60	Choose the time in seconds for a call to remain in the Hunt Group. This value defines the maximum time a call remains queued, and the maximum time to offer a call before sending it to overflow if it is not answered. If the queue times out before the call connects to a member telephone, the call is terminated. If the call has been offered to a member telephone, but is not answered when the queue times out, the call is rerouted to the overflow DN.
Overflow	<any system DN> (including a Hunt Group DN) Default: hunt group DN	This setting determines where unanswered calls are routed after the Queue timeout occurs. If a call gets overflowed back to the same Hunt Group, the call goes to the bottom of the queue and is treated as a new call. **Answer DNs:** A linear hunt group that has defined an overflow telephone does not support having the overflow telephone assigned as an Answer DN to any hunt group member. If this occurs, the Answer DN will not ring at the hunt group telephone when an overflow condition occurs. Answer DNs are set up under the **Line Access** heading for each DN. Refer to "Assigning Answer DNs" on page 403. Answer key must be set to **Extended** for overflow to work correctly. Refer to "Answer key levels" on page 461.

Table 155 Hunt group settings (Continued)

Field	Values	Description
Name	<an alpha-numeric string naming the Hunt Group>	Provides a unique name for the Hunt Group. The default is HGxx, where xx is the Hunt Group number 01-30.
Aux ringer	Y or N	Defines whether an auxiliary ringer (if installed) rings for incoming calls to a hunt group (Y). If set to N, the control of the auxiliary ringer falls back to control defined on a per telephone or per line basis.
Distinct rings in use	read only	This field indicates the distinct ring patterns are currently in effect, if any, on any lines, telephones, or hunt groups on the system.
Distinct ring	None Pattern 2, 3 or 4	Select a ring pattern for the hunt group. Default is None.
⚠	**Warning:** If you assign a distinctive ring pattern for a Hunt Group, all calls offered to telephones in the group will use the assigned ring pattern. If no pattern is assigned, or if the ring pattern is lower in status than the ring pattern of the line or the telephone setting, the call will use the ring pattern with the highest status setting. Refer to the sections which describe configuring Lines and DNs for information about assigning distinctive ring patterns to lines and telephones.	

Hunt group modes

The following three figures graphically demonstrate each of the three modes described in the following table that are available to Hunt groups.

Figure 193 Broadcast call mode

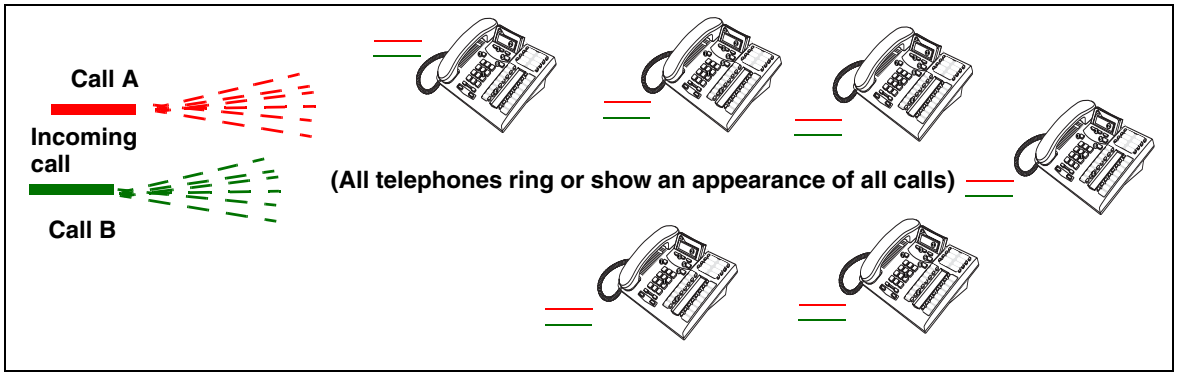


Figure 194 Linear call mode

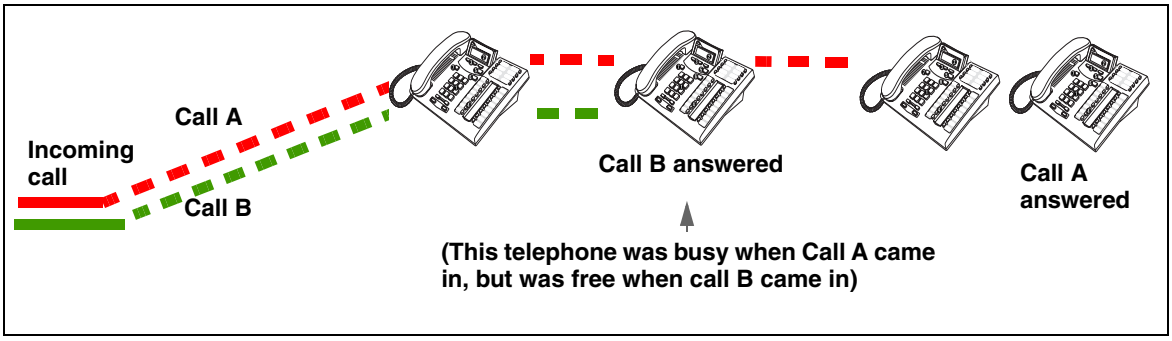
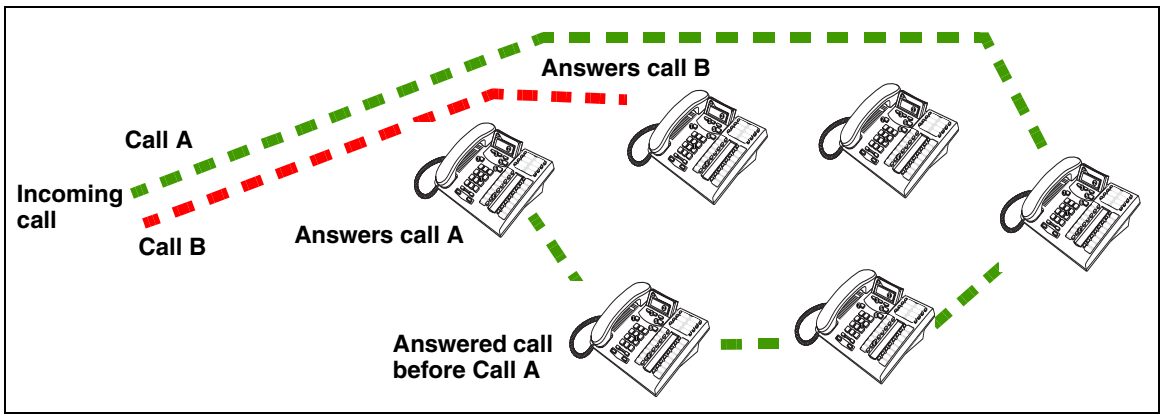


Figure 195 Rotary call mode



Hunt group members

After you determine the hunt group, you then assign members to the group.

This section includes information about:

- "Adding a Hunt group member" on page 579
- "Moving members" on page 581

The following limitations apply to adding member DNs to a Hunt Group:

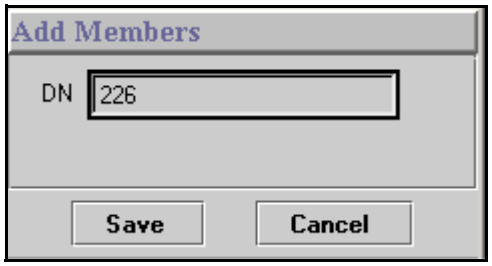
- Any system telephone or portable can be a member of a Hunt group.
- A telephone can be in more than one Hunt group. If a telephone is assigned to multiple groups, the telephone is considered a member in each Hunt group, which increases the total number of members in the system.
- There can be only one appearance of the same Hunt group on a telephone.
- Hunt group DNs cannot be members of other Hunt groups.

There are no default members to hunt groups. When a Hunt Group menu entry is first opened, there will be no entries under the Members node.

Adding a Hunt group member

Follow these steps to add a hunt group member:

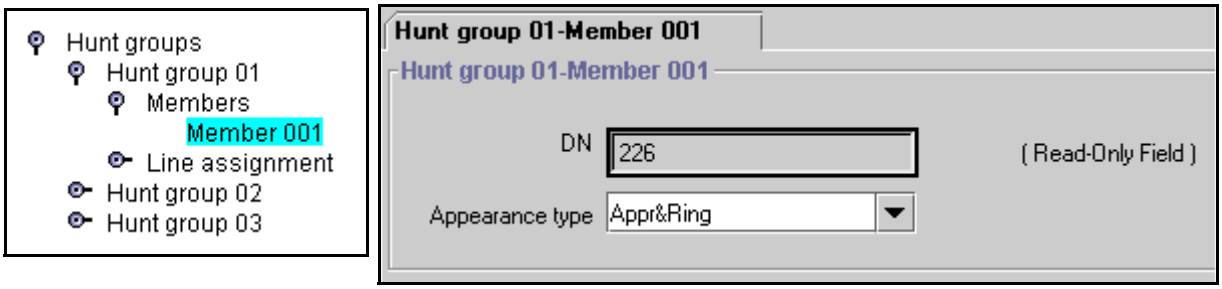
1. Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.
2. Click the key beside a **Hunt group** (**Hunt group 1-30**).
3. Click on **Members**.
4. At the top of the navigation tree, click the **Add** button.



5. Type a set number in the **DN number** box.

   TIPS: If you are assigning DECT DNs, ensure that you only assign a maximum of four DECT handsets that are registered with the same base station. DECT base stations can only handle a maximum of four calls at one time.
6. Click the **Save** button.
7. On the navigation tree, click the member number you created or that you want to change. The Hunt Group ## - Member ### screen appears.

Figure 196 Hunt group XX screen



8 Choose the Appearance type to define how the call appears on the set.

Table 156 Hunt group member settings

Field	Values	Description
DN	(read-only)	The DN of the telephone designated as this member of the hunt group.
Appearance type	Appr&Ring Ring only Appr only	**Appr&Ring (default)**: The call number appears on the display and the handset rings. **Ring only**: The incoming call rings at the set, but no number is displayed. **Appr only**: The incoming call displays on the set, but the set does not ring.

Removing a Hunt group member

Follow these steps to remove a Hunt group member:

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click the key beside the **Hunt group** (**Hunt group 1-30**).

3 Click on **Members**.

4 Click the member (for example, Member 001) to be removed.

5 Go to the top of the navigation tree and click the **Delete** button.

Removing all members from a Hunt group

Follow these steps to clear out the Hunt group members list:

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click the key beside the **Hunt group** (**Hunt group 1-30**) from which you want to remove the members.

3 Click **Members**.

4 Go to the top of the navigation tree and click the **Delete All** button.

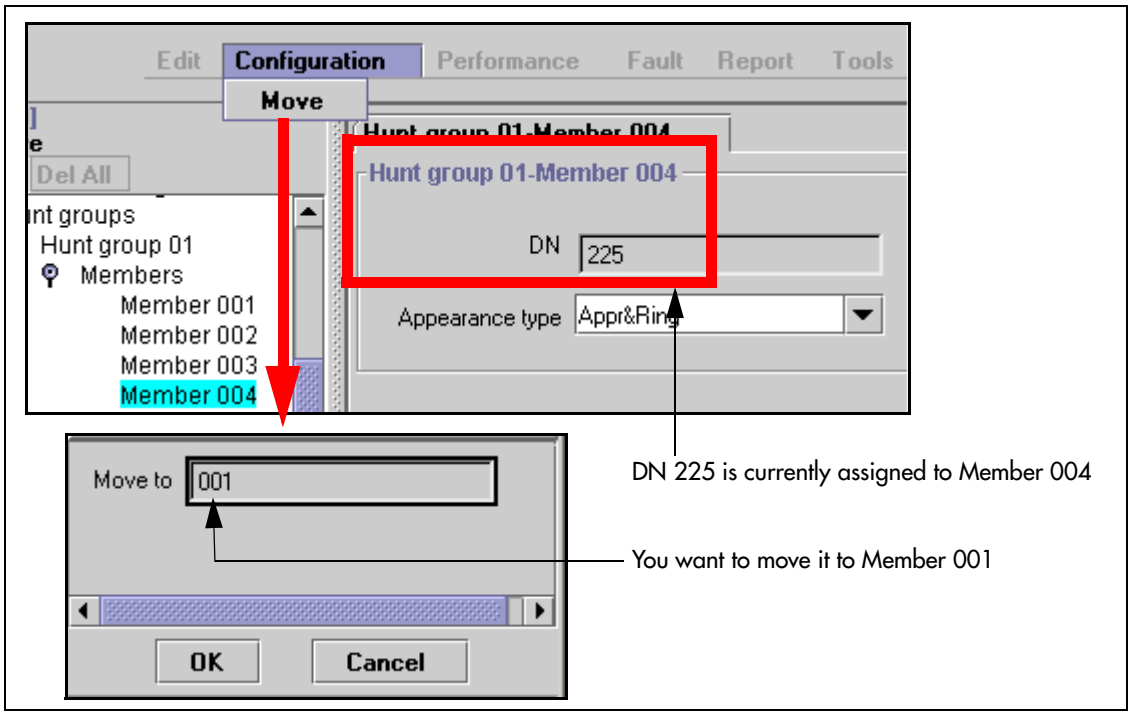
Moving members

Member order within a Hunt group is important. The member order determines how a call routes through a Hunt group when the group is set to either linear or rotary mode.

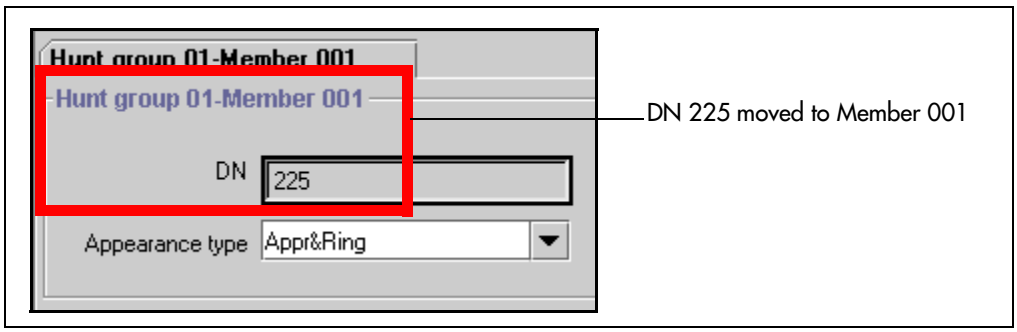
To move a member within a Hunt group:

1. Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.
2. Click a **Hunt group** (Hunt group 1-30).
3. Click on the key beside **Members**.
4. Click a member from the member list.
   For example DN 225, which is currently in Member 004 position.
5. On the **Configuration** menu, click **Move**.

Figure 197 Moving hunt group members



6. Type the new member number (001, 002, etc.) in the **Move to** box.
7. Click the **OK** button.
   The system automatically reorders the list.



Programming Hunt group lines

Multiple lines can be assigned to Hunt groups. However, a line can only exist in one Hunt group.

When you assign lines to Hunt groups, you must ensure that there is no interruptions to the call before the Hunt group DN handles the call. One of the settings that you need to check, is the designated prime set. This must be set to None. This prevents calls coming on that line from transferring to a prime set before the Hunt group can handle the call.

For more information about programming line settings, refer to "Assigning Trunk/line data" on page 236.

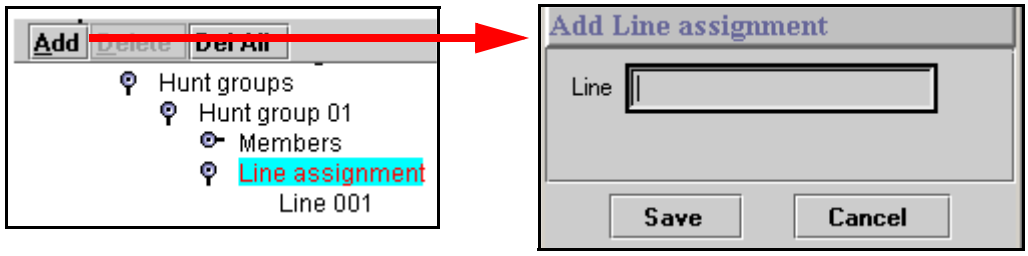
Programming note: Lines assigned to line buttons on individual telephones take precedence over the lines assigned to Hunt group buttons. Therefore, we recommend that you do not assign lines to individual telephone DN records for telephones that are part of a Hunt group.

Assigning a line to a hunt group

Assign the lines that you want calls to come in on:

1. Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. At the top of the navigation tree, click the **Add** button.

Figure 198 Adding lines to hunt groups



5. Type a line number (for example 061) in the **Line number** box.
6. Click the **Save** button.
   The new line number displays under **Line assignment**.

Unassigning a line

Remove lines that you no longer want to alert at the hunt group:

1. Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. Click the line number (for example, **Line 061**) to be deleted.
5. At the top of the navigation tree, click the **Delete** button.

Unassigning all lines

Remove all currently-assigned hunt group lines.

1. Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. At the top of the navigation tree, click the **Delete All** button.

Feature operation within Hunt groups

The operation of some features varies if the Business Communications Manager telephone is part of a Hunt group. The following table shows the affected features.

Table 157 Hunt group feature operation

Feature	Description
Call Forward All Calls	The system ignores Call Forward All Calls feature and the Hunt group call rings at the telephone.
Call Forward No Answer	The system ignores Call Forward No Answer and the Hunt group call continues to ring until the hunt time expires.
Call Forward on Busy	The system ignores Call Forward on Busy and the Hunt group call continues to ring until the hunt time expires.
Do not Disturb on Busy	If this feature is active, the set will not receive notification of incoming Hunt group calls.
Group Pickup	If a set is part of a Hunt group and a call pickup group, then an incoming Hunt group call can be picked up from any set that is in the call pickup group.
Transfer via Hold	The system supports transfer for Hunt group sets. However, you cannot Transfer via Hold. Once you answer a call on a Hunt group set, its appearance disappears from all other sets in the Hunt group. This means that other calls can come in on the same line.
Priority Call	You cannot make Priority calls to Hunt group DNs.
Ring Again	You cannot use Ring Again when calling a Hunt group DN.
Line Redirection	The Allow redirect attribute should be set to N for lines assigned to Hunt groups. For more information, see “Defining device capabilities” on page 405.
Page Zones	You cannot include Hunt group DNs in a Page zone.
Voice Call	Hunt groups cannot accept voice calls. Answer buttons have no appearances for voice calls, and the set does not ring.

Hunt group matrix

To help you organize your hunt group information, transfer the information in the following table to a spreadsheet and fill it out as you add Hunt groups.

Table 158 Hunt group matrix fields

Hunt Group #					
Hunt group name:	Hunt Group DN	Mode Broadcast Linear Rotary	If busy: Busy Tone Queue	Queue timeout (in seconds) 15 30 45 60 120 180	Overflow DN
Member #	DN, Appr only, Appr&Ring, Ring only				
Line assignment					

Monitoring Hunt groups

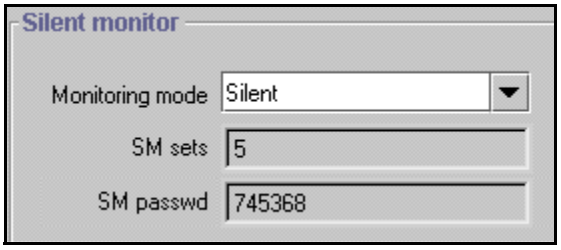
The Business Communications Manager system offers two ways to monitor hunt group activity. You can use Silent Monitor ("Setting up Silent Monitoring" on page 585) to actively monitor current calls or you can use the Hunt Metrics tables ("Using Hunt group metrics" on page 587) to get an overview of how each hunt group is performing.

Setting up Silent Monitoring

To set up Silent Monitoring for your system:

1. Click on the keys beside **Services**, **Telephony Services,** and **General Settings**.
2. Click on Silent Monitor.
   The Silent Monitor screen appears in the right frame.

Figure 199 Silent Monitoring system settings



3. The following table describes the settings that define how the silent monitor feature will work on your system:

Table 159 Silent monitor system settings

Field	Values	Description
Monitoring mode	Silent Non silent	Choose **Silent** if you want supervisors to be able to break into a hunt group conversation without giving an indicator of their presence. Choose **Non silent** if you want the hunt group member and the caller to hear a conference tone when a supervisor breaks into a hunt group conversation. **Note:** Initial monitoring is muted at the supervisor set. If the supervisor wants to speak within the conversation, a display key on the two-line display becomes available, once the connection is established. The default changes based on country profile.
SM sets	1 to 30	Indicate the number of two-line telephones in your system that you will allow to be used as supervisory telephones. (Default: 5)
SM passwd	XXXXXX	A six-digit set that must be entered after the supervisor presses **FEATURE** *550. To maintain system security, change this password frequently. (Default: 745368 (SILENT))

Security Note: Change the password regularly.

Using Silent Monitor

You can set up a number of two-line telephones on your system to use as supervisory telephones to monitor active hunt group calls from external numbers.

Only telephones that have been designated as monitoring devices have access to the **FEATURE** *550 code, which activates the monitoring session. Once the session is established, a number of display key prompts allows the supervisor to silently monitor the call, or break into the call to provide support or instruction. Refer to "Defining device capabilities" on page 405 for information about designating two-line display telephones as supervisor telephones.

Refer to the *Telephony Features Handbook* for a detailed description of the monitoring process and the display prompts.

Monitoring with IP telephones: On calls over an VoIP trunk, where both the Hunt group call and the monitoring call are from IP telephones (full IP domain calls), the agent will hear a click when supervisor starts and ends monitor session.

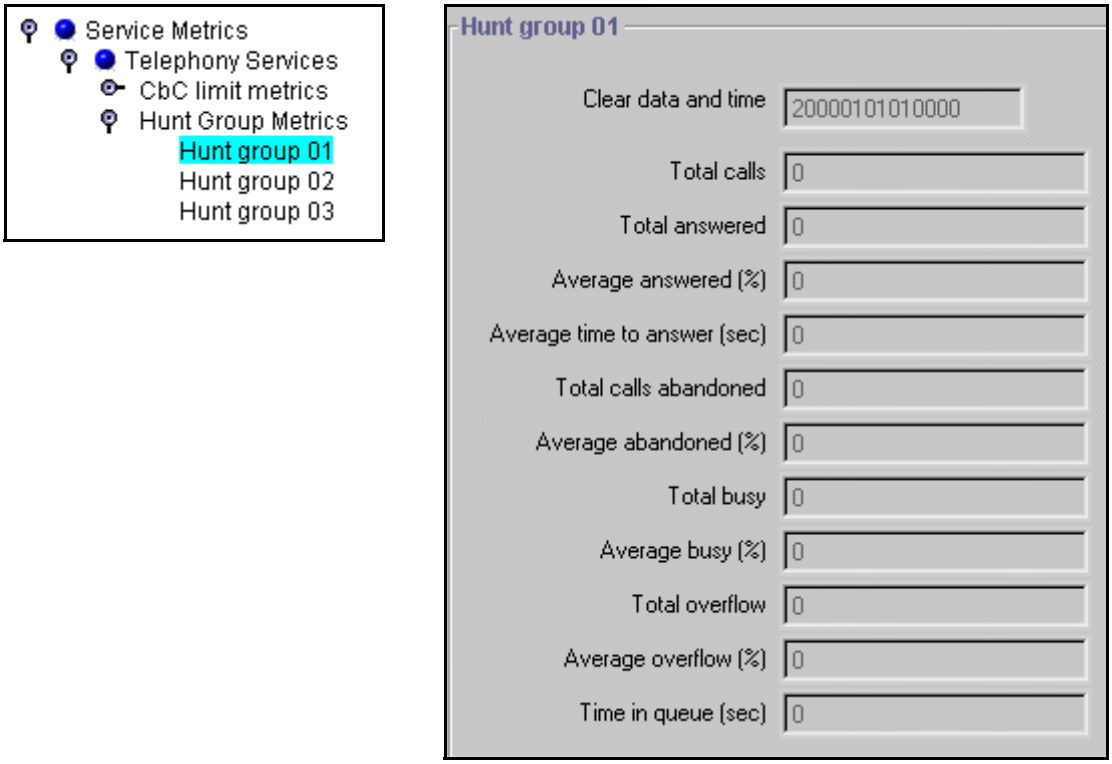
Using Hunt group metrics

The Hunt Group Metrics tables are located under **Diagnostics, Service Metrics** in the Unified Manager. Each Hunt group has a separate listing of group data that gives you a quick overview of activity and potential trouble spots.

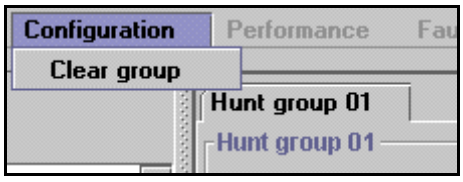
To access these screens:

1. Click on the keys beside **Diagnostics**, **Service Metrics**, and **Hunt Group Metrics**.
2. Click on the Hunt group you want to observe.
   As shown in the figure below, the Hunt group XX screen appears, where XX is the hunt group number.

Figure 200 Hunt Group Metrics screen for Hunt group 01



All the fields are read-only, however you can reset the statistics by clicking on **Clear Group** which is found under the **Configuration** menu item.



Chapter 24
Configuring Hospitality Services

This section describes the Hospitality headings. These records allow facilities such as hotels, motels, and hospitals to control telephone access to external lines, to provide alarm clock services on internal telephones, and to monitor room serviced status.

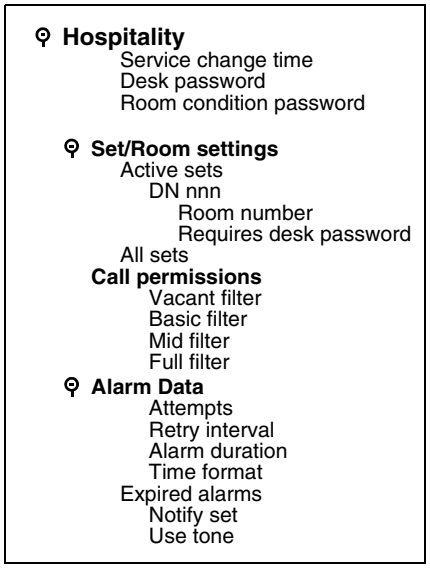
Tasks:

- Understand how the system operates ("About the Hospitality feature" on page 590)
- Determine hospitality service change times and passwords. ("Setting up Hospitality services" on page 591)
- Determine room numbers for telephones and whether the user requires a password to access administrative-level services. ("Identifying room telephones" on page 592)
- Determine call permissions for each of the four room occupancy levels. ("Identifying Call Permissions" on page 593)
- Determine how the system will deal with alarms. ("Programming Alarm data" on page 594)

Using the features: "Using the Hospitality Services Admin telephone" on page 596 and "Using the Hospitality services room telephone" on page 598 provide instructions for using the hospitality features on Administrative and room telephones.

The following figure shows the Hospitality headings on the navigation tree.

Figure 201 Hospitality commands and settings



About the Hospitality feature

In a temporary room occupancy setting, such as hotels or hospitals, guests gain improved services through immediate access to basic functions like:

- wake-up services or reminders via alarms on the room telephones
- accurate tracking of the room service requirements, such as cleaning schedules and occupancy

As well, telephones in specific areas have specific functions ("Hospitality telephone definitions" on page 590) and have access to specific alarm features ("Alarm Time (AL) feature" on page 590).

Hospitality telephone definitions

The system classifies telephones as one of three types of telephones:

Common set: This type of telephone can be found in a lobby, office, or common area. It is not associated with a room and does not have access to all of the hospitality features. These telephones are Business Communications Manager telephones or analog telephones connected to an analog terminal adapter (ATA2), or an analog station module (ASM).

Room set: This type of telephone is assigned to a room. You can assign up to five telephones to the same room (they all share the same room number). These telephones can be any Business Communications Manager telephone or an analog telephone connected to an ATA2 or an ASM.

Hospitality Services (HS) admin set: This type of telephone is any two-line display Business Communications Manager telephone. You can program a hospitality services telephone to require a Administrative desk password before the system grants access to hospitality administrative-level service control.

Alarm Time (AL) feature

The Alarm time feature provides an alarm clock capability. You can program both room telephones and common telephones to sound an audible alert at a time you request.

- You can program one Alarm time within a 24-hour period on a room or common telephone.
- You must program the alarm daily to have the alarm sound every day.
- When the alarm sounds, all telephones in a given room alert.
- When you cancel the alarm on any telephone, the alarm is cancelled on all the telephones associated with that room.
- A new Alarm time entered on a room or common telephone overwrites any previously-set alarm.
- You can determine a re-ring timer (snooze alarm) which determines when the alarm will ring again if the user paused the alarm by pressing the **HOLD** key (digital telephones) or by lifting the receiver (analog telephones).
- At all times, the Business Communications Manager system allows up to a maximum of 25 telephones that can alert at the same time.

Power failures

If the Business Communications Manager system experiences a power failure, the failure can result in lost Alarm times. When the Business Communications Manager system resumes running, and the system time resets, the missed Alarm times alert.

Setting up Hospitality services

The Hospitality heading allows you to enter the time when occupied rooms change state from Service done to Service required. The Service change time is a primary part of the Room condition (RC) feature.

Security Note: Change the desk and room condition passwords regularly.

As well, you will enter desk and room passwords for the system.

1 Click the keys beside **Services** and **Telephony Services**.

2 Click on **Hospitality**.
The Hospitality screen appears in the right frame.

Figure 202 Hospitality service times and passwords

3 The following table explains the possible settings for the hospitality record.

Table 160 Hospitality main settings

Field	Values	Description
Services change time	<24 hour digital time>	Identify when the occupied rooms will change from service done to service required. Format: HHMM, i.e. 1400 = 2 p.m. where HH = 0 to 23; MM = 0 to 59
Desk password	<up to six digits>	Enter the password that will be required to access all the Hospitality administrative features. Default password: 4677 (HOSP) **Security**: We strongly recommend that you change the default password, and frequently change the desk password to prevent unauthorized entry.
Room condition password.	<up to six digits>	Set the password that will allow access to the Room condition feature (**FEATURE 876**). Default password: None

Identifying room telephones

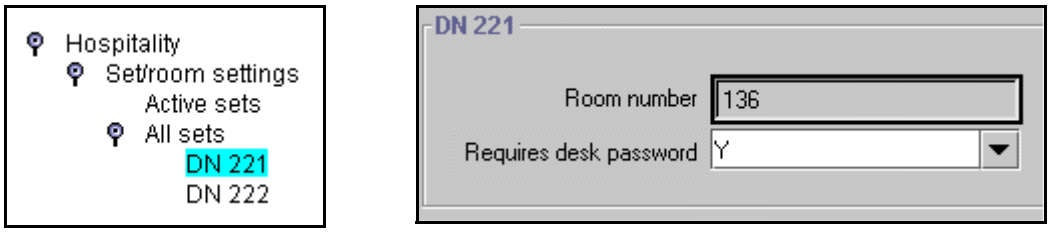
The Set/room settings allow you to assign one or more telephones to a room. This menu also enables access control to hospitality administrative features.

1 Under the **Hospitality** heading, click on the key beside **Set/room settings**.

2 Click on the key beside **Active sets** if you are configuring a telephone that has already been set up. Click on **All sets** if you need to locate a DN for a new telephone.

3 Click a DN number.
The room and password assignment fields appear in the right frame.

Figure 203 Hospitality room settings



4 The following table describes the two fields on the DN ### screen.

Table 161 Room settings

Field	Values	Description
Room number	<any digit from 1 to 32767>	Enter the room that contains the telephone with this DN.
Requires desk password	Y, N	If set to yes, the telephone requires a password to access administrative-level hospitality features (features 877-879). If set to no, the telephone does not require any passwords to access the features. Desk passwords are created using the main Hospitality command.

Identifying Call Permissions

The **Call Permissions** heading allows you to define dialing filters for room telephones based on the room occupancy status.

The dialing filters are standard Business Communications Manager Restriction filters (Filters 00-99). For more information, refer to "Defining restriction filters" on page 344.

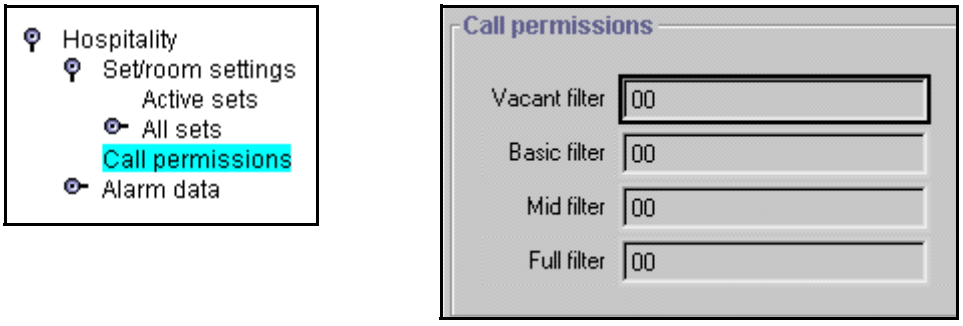
Setting room restriction filters

Follow these steps to create room restriction filters.

1 Click the keys beside **Services**, **Telephony Services**, **Hospitality**.

2 Click the **Call permissions** heading.
The Call permissions screen appears in the right frame.

Figure 204 Hospitality call permissions



3 The following table describes the fields on the Call permissions screen. Each field can accept a two-digit code.

Table 162 Call permission settings

Field	Values	Description
Vacant filter	<two-digit code>	Enter a code that indicates which calls are allowed when a room is empty. (i.e. 911)
Basic filter	<two-digit code>	Enter a code that indicates which calls are allowed for a basic room phone. (i.e. 911, and internal calls only)
Mid filter	<two-digit code>	Enter a code that indicates which calls are allowed for a phone with mid service. (i.e. 911, internal calls, and 1-800 numbers only)
Full filter	<two-digit code>	Enter a code that indicates which calls are allowed for a phone with full service. (i.e. no restrictions)

Programming Alarm data

The **Alarm data** heading allows you to program how the system provides alarms to the room telephones.

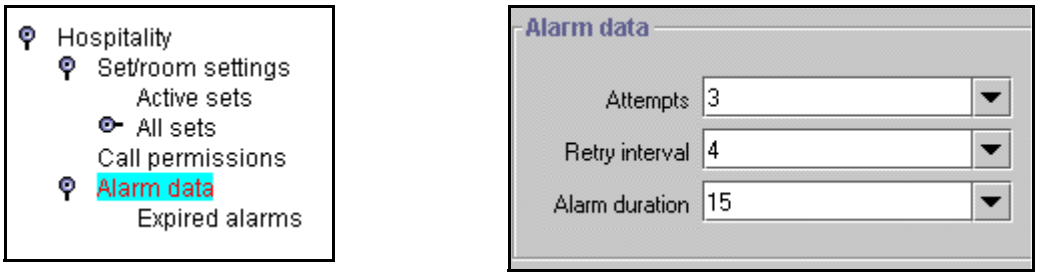
It also allows you to define how to be notified when an alarm expires ("Configuring for expired alarms" on page 595).

Setting alarm parameters

1 Click the keys beside **Services**, **Telephony Services**, and **Hospitality**.

2 Click the **Alarm data** heading.
The Alarm data screen appears in the right frame.

Figure 205 Alarm data fields



3 The following table describes the fields on the Alarm data screen

Table 163 Alarm data settings

Field	Values	Description
Attempts	1, 2, 3, 4, 5	Select the number of times the Alarm time feature attempts to alert the occupant before cancelling.
Retry interval	(in minutes) 2, 3, 4, 5, 6, 7, 8, 9	Select the interval between each attempt to send the alarm.
Alarm duration	(in seconds) 10, 15, 20, 25, 30, 35, 40, 45, 50	Select the period that a telephone alerts for each alarm attempt.

Configuring for expired alarms

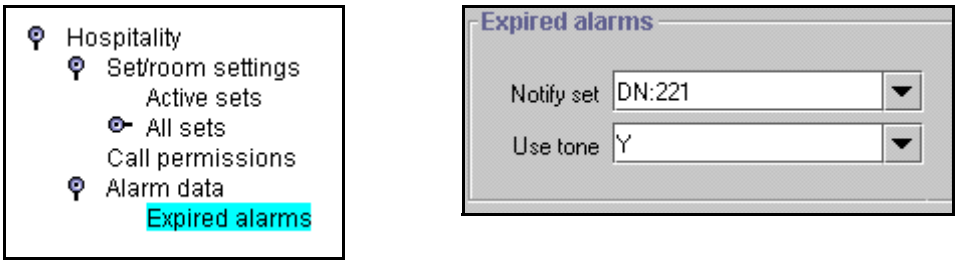
The Expired alarms setting allows you to program the system to notify a specific telephone whenever a Hospitality alarm expires. This occurs when the maximum number of alarm attempts has occurred and the alarm is cancelled without the user responding. You can also choose to allow a caller to hear a tone when an alarm expires.

Follow these steps to set expired alarms.

1 Click the keys beside **Services**, **Telephony Services**, **Hospitality**, and **Alarm data**.

2 Click **Expired alarms**.
The Expired alarms fields appears in the right field.

Figure 206 Expired alarms fields



3 The following table describes the fields on the Alarm data screen.

Table 164 Alarm data settings

Field	Values	Description
Notify set	None/DN: <telephone DN>	Enter a telephone DN if you want to notify a specific telephone when an alarm expires.
Use tone	Y, N	Choose whether you want the user to hear a tone when the alarm expires.

Hospitality matrix

To help you organize your Hospitality information, transfer the following information to a spreadsheet and fill it out as you determine the hospitality features.

Table 165 Hospitality settings matrix

Hospitality	Service change time	Desk password	Room condition password	
Set/Room Settings	Room Number	Requires desk password	N Y	
Call Permissions	Vacant filter: ___ Basic filter: ___ Mid filter: ___ Full filter: ___			
Alarm data	Attempts (1-5)	Retry interval (2-9)	Alarm duration (10-50 seconds)	Time format 12 hour/24 hour
Expired alarms	Notify set:, None, DN:	Use tones: N Y		

Using the Hospitality Services Admin telephone

The front desk personnel can control alarms and from a two-line display administration telephone. The following procedures are available to the users on the Hospitality User Card.

The following sections describe these processes:

Hospitality Services admin alarm feature

Only a Hospitality Services (HS) admin telephone can use the Hospitality Services admin alarm feature. The Hospitality Services admin alarm feature is room-oriented. It does not control the alarms on common telephones.

The Hospitality Services admin feature can:

- determine the current or last alarm time set for a room
- overwrite previous Alarm time programming for a room in the system
  - — assign an Alarm time for any room
  - — change an Alarm time for any room
  - — cancel an Alarm pending for any room

To program the Alarm time for a room with the Hospitality Services admin alarm feature:

1. Press **FEATURE 877** on a two-line display telephone.
2. If configured, the display shows `Password:`.
3. Enter the Desk admin password.
   The display shows `Al of rm#:`.
4. Enter the room number and press **OK**.
5. Press **VIEW**.
   The display shows `Alrm: 07:00am OFF:`.
6. If the alarm time is correct, press the `ON/OFF` display button to activate the alarm.
7. Enter a four-digit alarm time.
   - If the 24-hour format is used (hour: 00 to 23 and minutes: 00 to 59), no confirmation is required. The display shows `Alarm hh:mm ON`.
   - If the 12-hour format is used, the display shows the four-digit time plus `AM or PM?`. Press the **AM** or **PM** display button. The display shows `Alarm hh:mm am ON` or `Alarm hh:mm pm ON`.
8. Press the **RELEASE** button to exit programming.

Setting the state of a room at a telephone

To access the Room Occupancy feature and assign the state of a room set:

1. Press **FEATURE 879** on a two-line display telephone.
   If configured, the display shows `Password:`.
2. Enter the Desk admin password.
   The display shows `Oc of rm#:`.
3. Enter the room number and press **OK**.
   The display shows `rrrrr:Vacant`.
4. Press **CHANGE** and select the required status for the room set: Vacant, Basic, Mid or Full.
   Note: Programming a room to Vacant state cancels any outstanding alarms.
5. To program other rooms, press **FIND** or **NEXT** and return to step 4.
6. When no more rooms require programming, press the **RELEASE** button to exit programming.

Setting room condition

The Room condition (RC) feature allows users to exchange information about the serviced state of a room. Users are front desk attendants and cleaning or maintenance personnel of an establishment. The system maintains a database of the state of each room. This database is accessed from either the room telephone or a Hospitality Services admin telephone.

The front desk attendant can:

- assign any room state to Service done (`Srvc done`)
- assign any room state to Needs service (`Needs srvc`)
- query the state of any room

The system automatically assigns the status of a room to `Needs srvc`, when a room occupancy status changes from occupied to `vacant` or on a daily basis at a time assigned in the initial configuration

To update or query the room condition using a HS admin telephone:

1. Press **FEATURE 878** on a two-line display telephone.
   If configured, the display shows `Password:`.
2. Enter the desk admin password.
   The display shows `Cd of rm#:`.
3. Enter the room number and press **OK**.
   The display shows `rrrrr:Vacant`.
4. Press the **CHANGE** display button and select the required status for the room set:
   - If the room is occupied, select `Srvc done` or `Needs srvc`.
   - If the room is vacant, select `Vacant` or `Needs srvc`. The default setting is Vacant.
5. To update or query other room telephones, press **FIND** or **NEXT** and return to step 4.
6. When there are no more updates or queries, press the **RELEASE** button to exit programming.

Using the Hospitality services room telephone

The room telephones can be used by cleaning staff and guests to set alarms and room states. This section describes these codes and the process for using them.

- "Setting the alarm on a room telephone" on page 598
- "Setting the Room condition" on page 600

Setting the alarm on a room telephone

Guests can set alarms, turn them off and cancel them from their room telephones. The following section describes this process for both digital telephones and analog telephones, or telephones attached to the system using an ATA device.

This section also describes how to:

- "Change or cancel an alarm time" on page 599
- "Turn off an alarm" on page 599

To set the Alarm time feature on a telephone:

1. Press **FEATURE 875**.
   The display shows Alrm: 07:00am OFF.
2. If the alarm time is correct press **ON**.
   The display shows `Alrm:07:00am ON`.
3. Press **DONE** to exit.

To change the alarm time on a telephone:

1. Press **FEATURE 875**.
   The display shows Alrm: 07:00am OFF.
2. To enter a new alarm time press **CHG**.
   The display shows `Enter time:`.
3. Enter a new four-digit alarm time.
4. Press **ON**.
5. Press **DONE** to exit.

   When using the 24-hour clock format (hour: 00 to 23 and minutes: 00 to 59), no confirmation is required. The display shows `Alarm ON hh:mm`.

   When using the 12-hour format, the display shows `hh:mm AM or PM?`. Press the **AM** or **PM** display button. The display shows `Alarm ON hh:mm`.

To program the Alarm time feature on an analog telephone:

1. Press **FEATURE 875**.
   A tone sounds.
2. Enter a four-digit alarm time.

   When using the 24-hour clock format (hour: 00 to 23 and minutes: 00 to 59), a tone sounds.

   When using the 12-hour format, press * to select am, or # to select pm. A tone sounds.

   At the assigned times, the telephone in the room rings to wake up or remind the occupant of the next event or meeting.

Change or cancel an alarm time

When you enter a new Alarm time it overwrites any times previously assigned.

You can also cancel the alarm time feature. If you cancel the Alarm time for any set, it cancels the Alarm time for all the sets in the same room.

- Press **FEATURE #875** to cancel the Alarm time on a telephone with a display.
  The display shows `Alarm OFF`.
- Press **LINK *875** to cancel the Alarm time on an analog or T7000 telephone.

Turn off an alarm

To release a ringing alarm:

- On a telephone with a display, press any button except the **HOLD** button.
- On an analog telephone, lift the handset and then hang up.

Note: If the user presses the **HOLD** button when the set rings, it temporarily deactivates the Alarm. After a number of minutes, the set will ring again.
If the user is on a call when the alarm rings, press any button except **RELEASE** to cancel the alarm and maintain the active call.

Setting the Room condition

The Room condition (RC) feature allows users to exchange information about the serviced state of a room.

Cleaning or maintenance personnel access the system database from a room telephone to:

- assign the associated room state to Service done (`Srvc done`)
- assign the associated room state to Needs service (`Needs srvc`)
- query the state of the associated room on a set with a display

To update the room condition using a room telephone:

1. Press **FEATURE 876** on a two-line display telephone or press **LINK *876** on an analog telephone.
2. At the prompt, enter the status of the room.
   - To set to **Service Done**, press **1** on the dialpad.
   - To set to **Needs Service**, press **2** on the dialpad. You may also be required to enter a room condition password.

     The display shows `Set to srv done or Set to needs srv`.

Chapter 25
Configuring the music source

The Music on Hold and Background Music features provide music to users. For these features to function properly, a music source must be connected to the Business Communications Manager.

There are three ways you can connect the music source to the Business Communications Manager:

- You can connect an external music source to the Media Services Card (MSC) on the Business Communications Manager.
- You can use the IP Music feature to connect to BcmAmp.
  BcmAmp is an audio player application resident on the Business Communications Manager that provides a streaming audio signal to the Business Communications Manager system.
- You can use the IP Music feature to connect to an external music source on the data network. This external music source must be connected to your network and be accessible to the Business Communications Manager. The external music source must also produce a streaming audio signal that is compatible with the Business Communications Manager.

If you are using an external music source connected to the Business Communications Manager, refer to the *Business Communications Manager Installation and Maintenance Guide* for information about how to connect the external music source. If you are using an external IP music source connected on the data network, refer to the documentation that came with the music source for information about how to connect the music source to the data network.

For information about how to turn on Music on Hold and Background Music, refer to "Programming Feature settings" on page 457.

Selecting the music source

After you have connected the music source, you must select the music source you want to use.

1 On the navigation tree, click the **Services** key and click the **IP Music** heading. The Summary screen appears.

2 Configure the IP Music Summary parameters according to the following.

Table 166 IP Music Summary parameters

Setting	Definition
Description	Provides a description of the IP Music Service.
Version	Shows the version number of the IP Music Service.
Music Source	Allows you to select the music source you want to use. Select **Audio Jack** if you are using an external music source that is connected to the MSC card on the Business Communications Manager. Select **BcmAmp** if you are using the IP Music feature to connect to the music source available on the Business Communications Manager. If you select BcmAmp, you must then configure the BcmAmp application before you can use it. For information about how to configure BcmAmp, refer to "Configuring BcmAmp" on page 603. Select **Network Device** if you are using the IP Music feature to connect to a music source on the data network. If you select Network Device, you must configure the Network Device before you can use it. For information about how to configure the Network Device, refer to "Configuring a Network Device to be the IP Music Source" on page 607.

3 Press the **Tab** key to save your changes.

Note: If you choose **Audio Jack** as the Music Source, there is no more configuration required for the Music Source.

Configuring BcmAmp

BcmAmp is an audio player that resides on the Business Communications Manager. If you choose to use BcmAmp, you must configure the play list, which is the music available to BcmAmp. Configuring the play list involves:

Opening the BcmAmp Administration application

To open the BcmAmp Administration application:

1. On the navigation tree, click the **Services** key and click the **IP Music** heading.
   The Summary screen appears.
2. On the **Tools** menu, click **BcmAmp Ctl**.
   A log on screen appears.
3. In the **User Name** box, enter the user name you use to log on to Unified Manager.
4. In the **Password** box, enter the password you use to log on to Unified Manager.
5. Click the OK button.
   The BcmAmp Administration screen appears.

Loading music onto the Business Communications Manager

Before you can add music to the play list, you must the load the music track onto the Business Communications Manager.

1. Start the BcmAmp Administration application.
2. Click the **File Manager** heading.
   A list of audio files already on the Business Communications Manager appears, along with a form for uploading new files.
3. Click the **Browse** button.
4. Navigate to the folder that contains the sound file you want to load.
5. Click on the sound file and then click **Open**.
   The sound file must be a .wav or .au file format.
   The path for the sound file appears in the **Upload** box.

6 If you want to assign a name to this sound file, enter the name in the **As** box.
This name appears on the File List to help identify the sound file.

7 Click the **Go** link.
The file is added to the File List.

8 Repeat steps 3 to 7 for each sound file you want to add to Business Communications Manager.

Restrictions on uploading files

The audio files loaded onto Business Communications Manager are loaded into the same disk space that is used for CallPilot messages. Therefore, every minute of audio file loaded onto the Business Communications Manager reduces the amount of message storage space available to CallPilot by one minute. In order to ensure the proper operation of both BcmAmp and CallPilot, the following restrictions are applied to uploading audio files.

- The maximum size of any single sound file you load onto Business Communications Manager is 5 MB.
- The maximum amount of disk space allowed for BcmAmp audio files is 1 GB.
- If there is less than 1 GB of free disk space on Business Communications Manager, BcmAmp Administration application will no longer allow you to upload audio files. This ensures there is disk space left available for CallPilot.

Note: To minimize the time required to upload audio files, record the audio files as a single channel (mono) using 8-bit samples at a rate of 8 kHz.

Deleting music from Business Communications Manager

If you no longer want to use a sound file, you can delete the file from Business Communications Manager.

1 Start the BcmAmp Administration application.

2 Click the **File Manager** heading.
A list of audio files already on the Business Communications Manager appears.

3 Click the **Remove** link beside the sound file you want to delete.
A confirmation dialog box appears.

4 Click the **OK** button.
The file is permanently removed from the Business Communications Manager.

5 Repeat steps 3 and 4 for each file you want to remove.

Adding music to the Play List

The play list is an ordered list of songs that are heard by users of the Background Music and Music On Hold features. To add a sound file to the Play List:

1. Start the BcmAmp Administration application.
2. Click the **Play List** link.
   The current play list appears.
3. Click the **Add** drop list and click the sound file you want to add.
   The sound files that appear on the Add list are the sound files loaded on the Business Communications Manager.
4. Click the **To** drop list and click on the location on the list where you want to add the sound file (for example, Bottom of List).
5. Click on the **Go** icon.
6. Repeat steps 3 to 5 for each sound file you want to add to the Play List.

Removing music from the Play List

To remove a sound file from the Play List:

1. Start the BcmAmp Administration application.
2. Click the **Play List** link.
   The current play list appears.
3. Click the **Remove** link beside the sound file you want to remove from the Play List.

Note: Clicking the Remove link only removes the sound file from that location in the Play List. If the same sound file appears in another location on the Play List, the other entry is not removed.

Removing a sound file from the Play List does not delete the file from the Business Communications Manager. For information about how to delete a sound file from the Business Communications Manager, refer to "Deleting music from Business Communications Manager" on page 604.

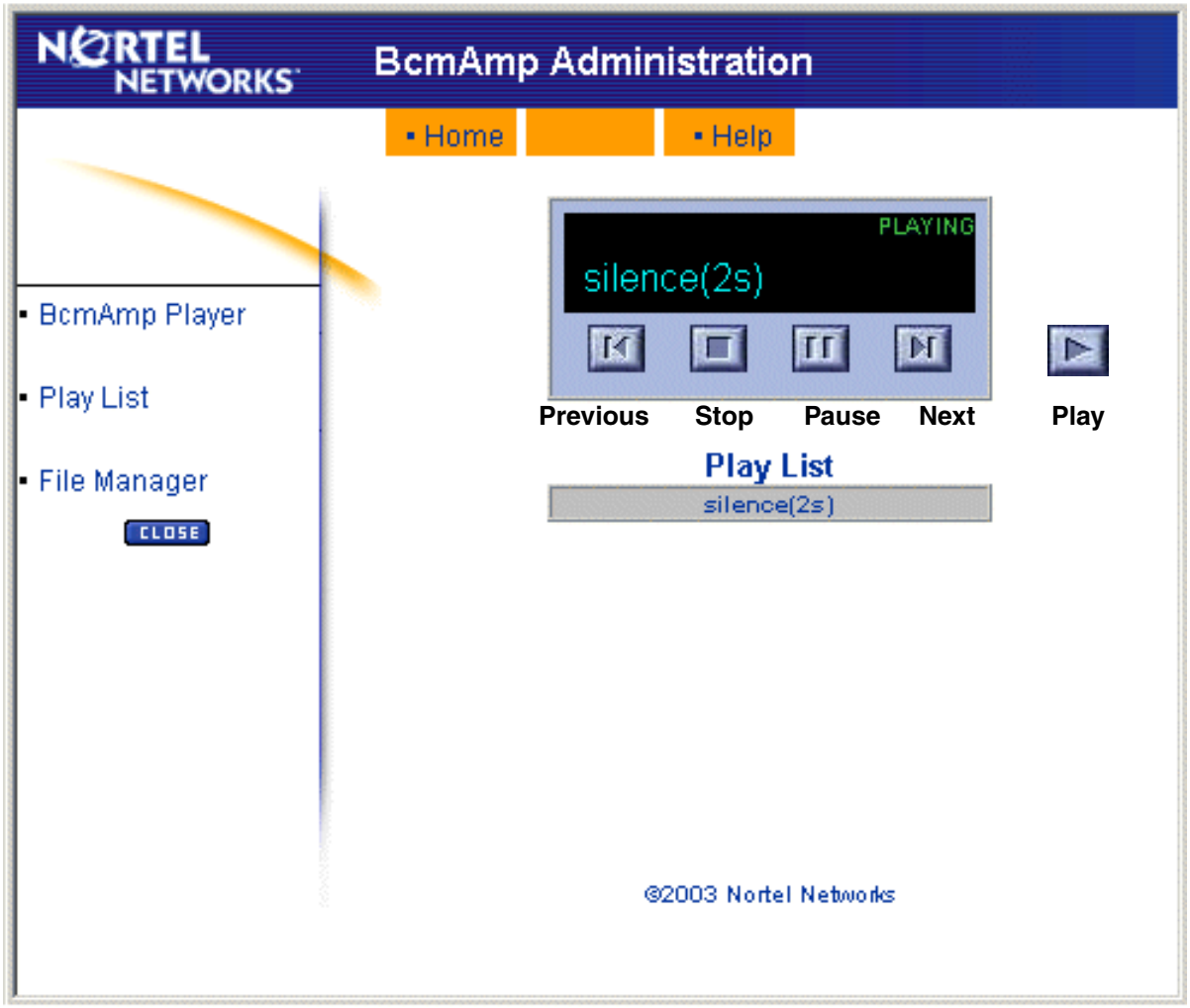
Using the BcmAmp Player

The BcmAmp Player is a web based interface that allows you to select, play, stop, or pause sound files that appear on the Play List. To access the BcmAmp Player:

1 Start the BcmAmp Administration application.

2 Click the **BcmAmp Player** link.
The BcmAmp Player interface appears.

Figure 207 BcmAmp Player



Note: When a song is stopped, the Stop button changes to the Play button.

To select and play a sound file:

- click the **Next** button
- click the **Previous** button
- click the sound file you want

To play a sound file, click the **Play** button.

To stop a sound file, click the **Stop** button.

To pause a sound file, click the **Pause** button.

Configuring a Network Device to be the IP Music Source

To configure a Network Device to be the IP Music source:

1. On the navigation tree, click the **Services** key and click the **IP Music** heading.
   The Summary screen appears.
2. Click the **Network Device** tab.
   The Network Device screen appears.
3. Configure the Network Device parameters according to the following.

Table 167 Networks Device parameters

Setting	Definition
IP Address	Enter the IP address of the music source. You must enter this value in the proper dotted format.
RTP Port	Enter the number of the source port used for the music source. This is the port the Business Communications Manager uses to receive music from the music source. The default value is 2216.
Stream Type	Enter the codec that is used for the incoming music source audio stream. The codec you enter here must match the codec used by the IP Music source. The possible values are **G.711 U-Law**, **G.711 A-Law**, **G.729** or **G.723**. The default value is G.711 U-Law.
Frames per Packets	Number of audio frames per RTP packet. The number of frames you enter must match the number of frames per packet sent from the IP Music source. The possible values are **1**, **2** or **3**. The default value is 3.

4. Press the **Tab** key to save your changes.
5. Press the **Advanced Network** tab.
   The Advanced Network screen appears.
6. Configure the Advanced Network parameters according to the following.

Table 168 Advanced Networks parameters

Setting	Definition
RTP Port	Enter the number of the destination port used for the music source. This is the port Business Communications Manager uses to send music to the users. The default value is 2218.

7 Press the **Tab** key to save your changes.

Note: If you make any changes on the Network Device or Advanced Network screens, you must disable and then re-enable the IP Music service for the change to be recognized by Business Communications Manager. To disable and re-enable the IP Music source, go to the IP Music Summary screen and change the Music Source to **Audio Jack** and then change it back to **Network Device**.

Chapter 26
Configuring the MSC resources

This section describes how to set up the resources controlled by the Media Services Card (MSC), which is the control center for voice and data traffic in the Business Communications Manager.

Warning: Only system administrators should have access to these Unified Manager records. Changing settings can affect other parts of the system. You need to understand the consequences of changes before you make them. Some changes are NOT reversible.

This section includes:

Types of MSC resources

Media Services Card (MSC) resources are required for the following features:

- system functions
- voicemail, call center, and IVR (Interactive Voice Response)
- Fax mail
- IP telephony trunks
- IP clients
- Dial-on-Demand (DoD) WAN and Backup ISDN WAN connections

When you configure the MSC resources, you are configuring how Business Communications Manager shares the MSC resources between these features.

There are several resources that you must check when you are configuring the MSC resources:

- Signaling channels
- Media channels
- DSP resources
- Voice bus paths
- Media gateways

Signaling channels

Signaling channels are the communication channels used to send control signals to and from the MSC. You must have one signaling channel for each device you have connected and feature port you have enabled.

The number of signaling channels you have determines how many devices you can have connected and feature ports you can have enabled on your system. Signaling channels are also known as D channels.

Media channels

Media channels are the communication channels used to send voice and data information between the devices and feature ports. Media channels are required only when a device or feature is sending or receiving voice or data information. For this reason, the devices and feature ports can share media channels.

The number of media channels you have determines how many devices and feature ports can exchange voice and data information at the same time. Media channels are also known as B channels.

DSP resources

Digital Signal Processors (DSP) provide the voice processing functions on Business Communications Manager. Voice processing is required to convert voice information to and from digital format for voicemail, call center and IVR. Voice processing is also required to handle encoding and decoding of IP telephony calls. The DSPs are located on the MS-PEC cards installed in your MSC.

The number of DSP resources you have determines the number of voicemail ports, call center ports, Fax mail ports, IVR ports, IVR Fax ports, WAN connections and IP telephony calls that can be active at the same time.

Voice bus paths

The voice bus paths are the communication channels between the DSPs on the MS-PECs and the master DSP on the MSC. One voice bus path is required for each voice processing task that is operating on the DSPs.

There are 62 voice bus paths available on Business Communications Manager.

Media gateways

Media gateways are logical connections that are a combination of DSP resources, media channels and voice bus paths that provide protocol translation between IP telephones and trunks and analog and digital telephony devices.

For information about settings that affect IP telephony, refer to the *IP Telephony Configuration Guide,* provisioning section.

Rules for managing the MSC resources

The following rules are provided to assist you in configuring your MSC resources.

Signaling channel rules

Signaling channels are the MSC resource that determines how many IP telephones you can connect to your system. If you have a system that does not use IP telephones, the number of signaling channels does not affect your configuration.

- The total number signaling channels available to the MSC depends on the DS30 split you have configured. For information about how to view and change the DS30 split, refer to "Changing the DS30 Split" on page 629.
  If you have a 2/6 DS30 split, the total number of signaling channels is 64.
  If you have a 3/5 DS30 split, the total number of signaling channels is 96.
- Management functions use six signaling channels.
- Dial-on-Demand ISDN WAN uses 27 signaling channels.
  All 27 signaling channels are used, regardless of the number of WAN channels configured.
- Voicemail requires one signaling channel for each voicemail port enabled. You can enable up to 32 voicemail ports.
  Both voicemail and call center use Voicemail ports.
- IP Telephony clients require one signaling channel for each IP telephone connected to the system.
- IP Telephony trunks require one signaling channel.
  Only one signaling channel is required regardless of the number of IP Telephony trunks enabled.
- IVR requires 1 signaling channel for each IVR port enable.
- Up to 24 ports enabled. Maximum of 32 ports between IVR and voicemail.

Media channel rules

The media channels are used to transport voice and data signals between devices.

- Management functions use five media channels. These five channels are reserved for management functions and are always in use.
- Dial-on-Demand ISDN WAN uses 27 media channels.
  All 27 media channels are used, regardless of the number of WAN channels configured. The maximum number of WAN channels is 16.

- Voicemail and call center use one media channel for each active session.
- DECT mobility requires one media channel.
  Note: If your system also has Dial-on-Demand WAN, DECT uses one of the 27 WAN media channels, so an additional channel is not required.
- A call between an IP telephone and a digital or analog telephone or a PSTN line uses a media channel for the duration of the call.
- A call from a digital or analog telephone that uses an IP trunk uses a media channel for the duration of the call.
- A call between two IP telephones on the same Business Communications Manager uses a media channel during call setup. After the call is established, the media channel is released.
- A call on an IP telephone using an IP trunk uses a media channel during call setup. After the call is established, the media channel is released.
- IVR needs 1 media channel for each active session.

Since most of the devices do not use media channels all of the time, your system can have more devices than there are media channels. However, to ensure you have sufficient system resources, make sure the number of media channels you have exceeds your estimate of peak media channel usage. The section below provides an example of how to estimate your peak media channel usage.

Example of how to estimate peak media channel usage

The example below is for a fictional company named CompanyABC. The numbers used are strictly for this example. Actual numbers will vary depending on the company. When you are estimating your peak media channel usage, make sure you use numbers that reflect your business.

- CompanyABC has a Business Communications Manager system with 96 telephones. Of these telephones, 48 are digital telephones and 48 are IP telephones.
  The percentage of IP telephones is 50% (48/96). This percentage is used to estimate how many calls will be made between IP telephones and digital telephones.
- In CompanyABC, the users are typically on the telephone 15 minutes out of each hour, or 25% of the time. During peak hours, the users are on the telephone 30 minutes, or 50% of the time. Therefore, the peak usage of IP telephones is 24 (50% X 48 IP telephones).
- In CompanyABC, half of the calls are made to external destinations and half of the calls are made within the Business Communications Manager system. CompanyABC does not have IP trunks, so the calls from the IP telephones to external destinations must use PSTN lines.
  The peak number of IP telephone calls that use PSTN lines is 12.
  (50% of calls external X 24 IP telephones during peak usage).
- For internal calls, there is a 50% chance the call is made to a digital telephone.
  The peak number of IP telephone calls to digital telephones is 6.
  (50% of calls internal X 24 IP telephones peak usage X 50% number of digital telephones)
- The peak media channel usage for IP telephony is 18.
  (12 media channels for external calls and 6 for calls made to digital telephones.)

DSP resources rules

The number of DSP resources you have depends of the number of type of MS-PEC you have installed. For information about how to determine the MS-PECs you have, refer to "Viewing the MS-PEC configuration" on page 623.

For the purposes of calculating DSP resources, we can estimate the relative power of each configuration as follows:

- 4 MS-PEC I 24 units
- 2 MS-PEC III 64 units
- 4 MS-PEC III 128 units

The number of DSP resources you need depends on the features and type of codec you are using.

- Dial-on-Demand WAN uses 1 unit for each 64Kbit/s channel
- Voicemail, IVR, and call center use 1 unit for each active session
- Fax uses 6 units for each active fax channel
- IP telephone or IP trunk using G.711 codec uses 1 unit
- IP telephone or IP trunk using G.729 codec uses 3 units
- IP telephone or IP trunk using G.723 codec uses 4 units

Note: Some of the DSP resource units listed above are rounded to the nearest whole number. This is done to ease the calculation of the DSP resources you require. To calculate more accurate DSP requirements, use the DSP resource units in shown in the following table.

Table 169 DSP resource requirements

Feature or codec	Resource units on a MS-PEC I	Resource units on a MS-PEC III
G.729	3	2.75
G.723	4	4.2
Fax	5	6
T.38 IP Fax	5	6
IVR Fax	6	6

Voice bus path

There are 62 voice bus paths available on Business Communications Manager.

- Voicemail and IVR use one voice bus path for each active session.
- Dial-on-Demand WAN uses one voice bus path for each 64Kbit/s channel that is active.
- IP telephones and IP trunks require one voice bus path when ever a media channel is required.

Media gateways

One media gateway is required for each call:

- from an IP telephone to an analog or digital telephone
- from an IP telephone using a PSTN line
- from an analog or digital telephone using an IP trunk

Determining the MSC resources you require

The following 20 questions are designed to help determine how many MSC resources you require. Based on the answers to these questions you can calculate the number of signaling channels, media channels, voice bus paths and DSP resource units you need. Use the table in "Evaluation" on page 620 to determine the configurations.

Note: In the following questions, "peak periods" refers to the periods of time when there is the highest overall activity. It is necessary to consider the resource requirements for "peak periods" to determine if available voice bus paths and DSP resources meet your resource requirements at all times.

ISDN WAN (Dial-up/Nailed-up)

As you answer the following questions, record your answers in the table in "Record of required MSC resources" on page 619.

1 What is the maximum required WAN bandwidth?
The range is 0 to 1 Mbit/s (16 x 64 kbit/s) in 64 kbit/s increments.
If the answer is more than zero:

- add 27 to the signaling channel count
- add 27 to the media channel count

2 What is the required WAN bandwidth during peak periods?
The range is 0 to the maximum bandwidth you entered in question 1.
For each 64 kbit/s of bandwidth:

- add 1 to the voice bus time slot count
- add 1 to the DSP resource unit count

DECT mobility

3 How many DECT media bay modules are installed?
The range is 0 to 1 media bay modules.
For each DECT media bay module:

- add 1 to the media channel count

Note: If your system also has Dial-on-Demand WAN, DECT uses one of the 27 WAN media channels, so an additional channel is not required.

Voice Mail and ACD

4 What is the maximum number of Voicemail ports required? Voicemail ports are used for voicemail and call center.
The range is 0 to 32 ports.

For each voicemail port:

- add 1 to the signaling channel count
- add 1 to the media channel count

5 What is the number of Voicemail ports required during peak periods?
The range is 0 to the maximum number of ports selected in question 4.

For each voicemail port

- add 1 to the voice bus path count
- add 1 to the DSP resource unit count

6 How many fax tasks will be used during peak periods?
The range is 0 to 2.

For each fax task:

- add 6 to the DSP resource unit count

Note: The maximum number of voice ports shared between voice mail and IVR is 32. The maximum number of fax ports shared between voice mail, IVR and T.38 IP fax is 8.

Note: The fax DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

IVR and IVR Fax

7 What is the maximum number of IVR ports required? IVR ports are used for interactive voice response applications.
The range is 0 to 24 ports.

For each voicemail port:

- add 1 to the signaling channel count
- add 1 to the media channel count

8 What is the number of IVR ports required during peak periods?
The range is 0 to the maximum number of ports selected in question 7.
For each voicemail port

- add 1 to the voice bus path count
- add 1 to the DSP resource unit count

9 How many fax tasks will be used during peak periods?
The range is 0 to 8.

For each fax task:

- add 6 to the DSP resource unit count

Note: The maximum number of voice ports shared between voice mail and IVR is 32. The maximum number of fax ports shared between voice mail, IVR and T.38 IP Fax is 8.

Note: The fax DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

IP telephones

10 What is the maximum number of IP telephones required?
The range is 0 to 90 IP telephones.

For each IP telephone:

- add 1 to the signaling channel count

11 How many IP telephones will be calling an analog or digital telephone or using a PSTN trunk during peak periods?
The range is 0 to the maximum number of IP telephones selected in question 10.

For each IP telephone:

- add 1 to the media channel count
- add 1 to the voice bus path count

12 How many IP telephones specified in question 10 will be using the G.711 codec?
The range is 0 to the maximum number of IP telephones selected in question 11.

For each IP telephone:

- add 1 to the DSP resource unit count

13 How many IP telephones specified in question 10 will be using the G.729 codec?
The range is 0 to the maximum number of IP telephones selected in question 11.

For each IP telephone:

- add 3 to the DSP resource unit count

Note: The G.729 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

14 How many IP telephones specified in question 10 will be using the G.723 codec?
The range is 0 to the maximum number of IP telephones selected in question 11.

For each IP telephone:

- add 4 to the DSP resource unit count

Note: The G.723 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

IP Trunks

15 What is the maximum number of IP trunks required?
The range is 0 to 60 IP trunks.

If there is more than zero IP trunks:

- add 1 to the signaling channel count

16 How many analog or digital telephones (not IP telephones) will use IP trunks during peak periods?
The range is 0 to the maximum number of IP trunks selected in question 15.

For each IP trunk:

- add 1 to the voice bus path count
- add 1 to the media channel count

17 How many IP trunks specified in question 15 will be using the G.711 codec?
The range is 0 to the maximum number of IP trunks selected in question 16.

For each IP trunk:

- add 1 to the DSP resource unit count

18 How many IP trunks specified in question 15 will be using the G.729 codec?
The range is 0 to the maximum number of IP trunks selected in question 16.

For each IP trunk:

- add 3 to the DSP resource unit count

Note: The G.729 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

19 How many IP trunks specified in question 15 will be using the G.723 codec?
The range is 0 to the maximum number of IP trunks selected in question 16.
For each IP trunk:

- add 4 to the DSP resource unit count

Note: The G.723 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

20 How many T.38 fax tasks will be used during peak periods?
The range is 0 to 8.

For each fax task:

- add 6 to the DSP resource unit count

Note: The maximum number of fax ports shared between voice mail, IVR and T.38 IP Fax is 8.

Note: The fax DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to the table in "DSP resources rules" on page 613.

Note: If the source or destination of the T.38 IP Fax can be fax mail or IVR, the fax message requires two fax tasks (12 units). One fax task handles the IP Fax portion of the transmission and the other task handles the IVR or fax mail portion of the transmission.

Note: To use T.38 Fax, you must have 2 or 4 MS-PEC III installed in your MSC card. For information about how to determine the MS-PECs you have, refer to "Viewing the MS-PEC configuration" on page 623.

Record of required MSC resources

Use the following table to record the MSC resources you require for your Business Communications Manager system. To determine the resources that you require, answer the questions in "Determining the MSC resources you require" on page 614.

Table 170 Required MSC resources

Question	Answer	Signaling channels	Media channels	Voice bus paths	DSP resource units
1. WAN				---	---
2. Peak WAN		---	---		
3. DECT		---		---	---
4. VM/ACD				---	---
5. IVR					
6. Peak VM/ACD		---	---		
7. Peak FAX		---	---	---	
8. Peak IVR					
9. IVR FAX					
10. IP Sets			---	---	---
11. Peak IP Sets		---			---
12. IP Sets G711		---	---	---	
13. IP Sets G729		---	---	---	
14. IP Sets G723		---	---	---	
15. IP Trunks			---	---	---
16. Peak IP Trunks		---			---
17. IP Trunks G.711		---	---	---	
18. IP Trunks G.729		---	---	---	
19. IP Trunks G.723		---	---	---	
20. IP Trunks T.38 Fax		---	---	---	
Totals					

Evaluation

After you have answered the questions and calculated the four totals, use the following rules to determine the required Business Communications Manager configuration.

Table 171 Evaluation of required Business Communications Manager configuration

Resource	Number required	Required configuration
Signaling channel count	58 or less	2/6 DS30 split
	59 to 90	3/5 DS30 split
	91 or more	exceeds Business Communications Manager capacity
Media channel count	58 or less	2/6 DS30 split
	59 to 90	3/5 DS30 split
	91 or more	exceeds Business Communications Manager capacity
Voice bus path count	62 or less	within Business Communications Manager capacity
	63 or more	exceeds Business Communications Manager capacity
DSP resource units	1 to 24	4 MS PEC I
	1 to 64	2 MS PEC III
	65 to 128	4 MS PEC III
	129 or more	exceeds Business Communications Manager capacity

Note: If your system requires more MSC resources than is available on your MS-PEC configuration, you can upgrade your MS-PECs. For information about how to upgrade your MS-PECs, refer to the *Business Communications Manager Installation and Maintenance Guide*.

Example of a Business Communications Manager configuration

The following two tables provide examples of required configurations.

Table 172 Example of required configuration

Question	Answer	Signaling channels	Media channels	Voice bus paths	DSP resource units
1. WAN	512 kbit/s (8)	27	27	---	---
2. Peak WAN	512 kbit/s (8)	---	---	8	8
3. DECT	1	---	0	---	---
4. VM/ACD	8	8	8	---	---
5. IVR					
6. Peak VM/ACD	6	---	---	6	6
7. Peak IVR					
8. Peak FAX	1	---	---	---	6
9. IVR FAX					
10. IP Sets	24	24	---	---	---
11. Peak IP Sets	12	---	12	12	---
12. IP Sets G711	6	---	---	---	6
13. IP Sets G729	4	---	---	---	12
14. IP Sets G723	2	---	---	---	8
15. IP Trunks	32	1	---	---	---
16. Peak IP Trunks	20	---	20	20	---
17. IP Trunks G.711	12	---	---	---	12
18. IP Trunks G.729	6	---	---	---	18
19. IP Trunks G.723	2	---	---	---	8
20. IP Trunks T.38 Fax		---	---	---	
Totals	---	60	67	46	84

Table 173 Evaluation for the example of required configuration

Resource	Number required	Recommended configuration
Signaling channel count	60	3/5 DS30 split
Media channel count	67	3/5 DS30 split
Voice bus path count	46	within Business Communications Manager capacity
DSP resource units	84	4 MS-PEC III

Configuring the MSC resources

After you have determined what MSC resource you need, you can start configuring your MSC resources.

This includes:

Viewing the MSC information

You can view information about the Media Services Card (MSC) that is installed in your Business Communications Manager.

To view the MSC information:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** heading. The Media Services Card screen appears.
2. Click the **MSC Information** tab.
   The MSC Information screen appears. The information on this page is described in the following table.

Table 174 MSC information parameters

Attribute	Description
Description	Shows a description of the MSC
Version	Shows the hardware version of the MSC installed.
ID	Shows the serial number of the Media Services Card.

Viewing the MS-PEC configuration

There are three MS-PEC configurations available for Business Communications Manager:

- four MS-PEC I cards - This configuration provides the fewest number of DSP resources.
- two MS-PEC III cards - This configuration provides more MSC resources than the MS-PEC I configuration.
- four MS-PEC III cards - This configuration provides the maximum number of MSC resources.

To view the MS-PEC information:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** heading. The Media Services Card screen appears.
2. Click the **MS-PEC Information** tab.
   The MS-PEC Information screen appears. The information in the following table appears for each MS-PEC installed in the Media Services Card.

Table 175 MS-PEC information

Attribute	Description
Location	Shows the slot on the Media Services Card where the MS-PEC is installed. The Media Services Card screen shows where these slots are on the Media Services Card.
Type	Shows the type of MS-PEC installed. You can have an MS-PEC I or an MS-PEC III. Empty appears in the Type box, when there is no MS-PEC installed in the slot. **Note**: An MS-PEC III has more DSP resources than an MS-PEC I.
Hardware ID	Shows the hardware ID of the MS-PEC.
DSP 1	Shows the status of the first DSP. The DSP status can be: • **Enabled**: Indicates normal operation. • **User-Disabled**: Indicates that the DSP has been disabled. A DSP is disabled under support conditions only and requires the assistance of a Nortel Networks service representative. • **No Firmware**: Indicates the wrong type of MS-PEC is installed or a data file was deleted from Business Communications Manager. Contact your Nortel Networks service representative. • **Out of Service**: Indicates there is a hardware failure on the MS-PEC. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC. • **Unsupported**: Indicates that the MS-PEC installed is for a different Nortel Networks product and is not compatible with Business Communications Manager. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC. • **Unknown**: Indicates that Business Communications Manager does not recognize the type of MS-PEC installed. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC.
DSP 2	Shows the status of the second DSP. The DSP status can be Enabled, User-Disabled, No Firmware, Out of Service, Unsupported, Unknown or not available (N/A). **Note**: An MS-PEC I does not have a second DSP so its DSP 2 status is N/A.

Understanding the MSC Minimum and Maximum values

The MSC Configuration allows you to determine how the resources are assigned on your Business Communications Manager.

In some Business Communications Manager systems, the total number of features and devices that require resources exceeds the number of resources that are available. To address this issue, Business Communications Manager allows you to share the resources. By changing minimum and maximum values for each component you can fine tune this sharing.

Minimum

The minimum value is the number of resources that are always assigned to a component. You use this number to ensure a base level of service for a specific component. For example, to ensure that at least four people can be using voicemail at all times, you would enter four as a minimum value for the Voice Port component.

The resources that are not assigned using the minimum values are shared by the components. If a component needs additional resources, it can use some of the shared resources to provide service during the busy period. This method of sharing resources allows your Business Communications Manager system to adapt to the changing demands for services.

Maximum

The maximum value is the maximum number of resources that can be used by a component. You use this number to ensure a single component does not consume all of the shared resources.

The MSC Configuration you choose greatly affects the performance of your Business Communications Manager system. Make sure you consider the needs of your users, including peak usage times, when selecting the Minimum and Maximum values. The following table describes the advantages and disadvantages of changing these values.

Table 176 Advantages and Disadvantages of Minimum and Maximum values

Value	Advantage	Disadvantage
Increasing Minimum Value	Increases the guaranteed level of service for a component. The DSP resources you assign as a Minimum are always available to the users of this component.	Decreases the flexibility of DSP resource sharing. DSP resources that are assigned to the Minimum value are not shared with other components. If you set the Minimum level too high, other components may not be available due to a lack of available DSP resources.
Decreasing Minimum Value	More DSP resources are available to share with other components. When there is a large pool of shared DSP resources, Business Communications Manager more readily adapts to changing component use.	Lower guaranteed level of service for this component. If the Minimum value is too low, it is possible that some users will not be able to access this component when other components are in heavy use.
Increasing Maximum Value	Allows this component to use more of the shared DSP resources during times of peak use. This allows more people to use this component at the same time.	During times of peak use, this component may consume all of the shared resources. This may cause other components to be unavailable to users.
Decreasing Maximum Value	Prevents this component from using so many of the shared DSP resources, that other components are unavailable.	Limits the number of people that can use this component even if sufficient DSP resources are available.

Viewing the MSC Configuration

To view the MSC Configuration:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** key.
2. Click the **MSC Configuration** heading.
   The Configurations screen appears.
3. Click the **Current** tab.
   The Current screen appears. This screen show the MSC configuration currently being used on your system.

Changing the MSC configuration

To change the MSC configuration:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** key.
2. Click the **MSC Configuration** heading.
   The Configurations screen appears.
3. Set the Configurations parameters according to the following table.

Table 177 MSC configuration parameters

Attribute	Description
Active Configuration	Select the MSC configuration you want to use. Select **Default** to use the MSC configuration that was programmed at the factory. Select Custom1, Custom2 or Custom3 to use one of the customized MSC configurations you created. For information about how to create a custom MSC configuration, refer to "Creating a custom MSC configuration" on page 626.
Update or Reboot Required	Shows if a system reboot is required before the selected configuration is applied.
Custom 1 Name	Enter the name for the first custom MSC configuration. **Note**: You do not have to change the Custom Name to use a Custom Configuration.
Custom 2 Name	Enter the name for the second custom MSC configuration.
Custom 3 Name	Enter the name for the third custom MSC configuration.

4. Press the **Tab** key to save your changes.

Note: You must reboot the Business Communications Manager for changes to the MSC configuration to take affect.

Creating a custom MSC configuration

You can create up to three custom MSC configurations. You must create a custom MSC configuration before you can apply the configuration to the MSC.

To create a custom MSC configuration:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** key.
2. Click the **MSC Configuration** heading.
   The Configurations screen appears.
3. Click the Custom1 tab to change the first custom configuration.
   The Custom1 screen appears.

   Note: If you want to change the second custom configuration, click the **Custom2** tab. If you want to change the third custom configuration, click the **Custom3** tab.

4. Click the component you want to change (for example, IP Clients). The following table describes each component.

Table 178 MSC custom configuration parameters

Component	Description
IP Clients	IP Clients are IP telephones such as i2004 telephones and i2050 Software Phones. DSP resources are required only when the IP telephone is in use (for example, to make a call, receive a call, listen to voicemail). For information about how to configure IP clients, refer to the *Business Communications Manager IP Telephony Configuration Guide*. **Note**: The codec (G.711, G.723 or G.729) you are using for the IP Client affects how many IP clients you can use on your system.
IP Trunks	IP Trunks are communication channels that Business Communications Manager uses to send and receive IP telephony calls using the Public Data Network. You can use IP trunks to connect your Business Communications Manager system to: • another Business Communications Manager system • a Meridian 1 IPT system • a third-party H.323 end point or gateway For information about how to configure IP trunks, refer to the *Business Communications Manager IP Telephony Configuration Guide*. **Note**: The codec (G.711, G.723 or G.729) you are using for the IP Trunk affects how many IP Trunks you can use on your system.
Media Gateways	Media Gateways provide the connection between IP telephony devices (IP trunks, i2004 telephones, i2050 telephones, and H.323 terminals) and normal telephony devices (PSTN lines; Business Series Terminals (BST) telephones: T7316E, T7316, T7208s, T7100; analog telephones etc.).

Table 178 MSC custom configuration parameters (Continued)

Component	Description
Voice Mail and ACD Ports	Voice Mail and Call Center Ports are communication channels that connect users to the CallPilot Voicemail and Call Center Software. DSP resources are required only when a user connects to voicemail or call center. This includes callers hearing greetings, callers leaving messages, and users accessing their mailboxes. The minimum value for Voice Mail and Call Center Ports must be 2 or higher, unless you want to disable CallPilot VoiceMail and Call Center Software. The maximum value for Voice Mail and Call Center Ports must be 2 or higher, unless you want to disable CallPilot VoiceMail and Call Center Software. To disable CallPilot VoiceMail and Call Center Software, change the minimum and maximum values for Voice Mail and Call Center Ports to zero.
Fax	Fax ports are communication channels that connect a fax machine to the Business Communications Manager. Fax mail ports are communication channels that connect a fax machine to a fax mailbox or a user to a Fax-on-Demand mailbox. IVR fax ports are communication channels that connect a fax machine to IVR functions. T.38 IP Fax ports are communication channels that connect to a fax machine that is using an IP trunk.
WAN	WAN channels are dialup ISDN WAN connections.
IVR Ports	IVR ports are communication channels that connect users to the IVR Software. DSP resources are required only when a user connects to IVR. This includes callers hearing greetings, callers leaving messages, and users accessing their mailboxes. The minimum value for IVR Ports must be 2 or higher, unless you want to disable IVR. The maximum value for IVR Ports must be 2 or higher, unless you want to disable IVR. To disable IVR, change the minimum and maximum values for IVR Ports to zero.
CTE Ports	CTE ports are communication channels that connect CTE applications to the Business Communications Manager. An example of a CTE application is Business Communications Manager Personal Call Manager.

5 On the **Configuration** menu, click **Modify Custom 1**.
Or, right click the component you want to change and click **Modify Custom 1**.
The Custom1 screen appears.

Note: If you are configuring Custom configuration 2, click **Modify Custom 2**.
If you are configuring custom configuration 3, click **Modify Custom 3**.

6 Configure the Component parameters according to the following table.

Table 179 MSC component parameters

Attribute	Description
Component	Shows the name of the component you are modifying.
Minimum	Enter the number of DSP resources you want to reserve for the sole use of this component. The number you choose must be high enough to ensure proper service but low enough that it leaves DSP resources for other components. **Note**: If you set this value to zero, it is possible that this component may become inoperable if other components consume all of the DSP resources.

Table 179 MSC component parameters (Continued)

Attribute	Description
Maximum	Enter the maximum number of resources this component can use. Enter MAX to allow this component to use as many of the available DSP resources as is allowed by the License Limit or the Hardware Limit.
License Limit	Shows the maximum number of resources that are allowed for this component based on the software licenses purchased for this system. You can increase the License limit of a component by entering keycode*s*. For information about how to obtain a keycode, contact your Nortel Networks sales representative.
Hardware Limit	Shows the maximum number of resources that are allowed for this component based on the hardware installed in this system.

7 Click the **Save** button.

8 Repeat steps 6 and 7 for each component you want to change.

After you complete the changes to the custom configuration, you must change the active configuration to apply these changes to the MSC. For information on how to change the active configuration, refer to "Changing the MSC configuration" on page 625.

DTMF Configuration

The DTMF configuration sets the length of the DTMF tones generated by Business Communications Manager.

The system DTMF length may need to be adjusted because of detection errors. For example, some cellular phone tones are closer to the short DTMF millisecond range. If a company is having trouble with cellular phone connections, it may be necessary to change the DTMF length to 30 milliseconds.

To set the DTMF length:

1 On the navigation tree, click the **Resources** key and click the **Media Services Card** key.

2 Click the **DTMF Configuration** heading.
The DTMF Configuration screen appears.

3 In the **DTMF length** box, enter a value between 30 and 60.
This value is the length of the tone in milliseconds.

4 Press the **Tab** key to save your settings.

Changing the DS30 Split

A DS30 bus is a group of 32 signaling channel and 32 media channels. The DS30 split determines how these channels are assigned on Business Communications Manager.

You have a choice of a 2/6 or a 3/5 split. If you choose a 2/6 split, two DS30 buses are assigned to the MSC and six are assigned to the Media Bay Modules. If you choose a 3/5 split, three DS30 buses are assigned to the MSC and five are assigned to the Media Bay Modules.

The split you choose is determined by the number of signaling channels you require for applications such as voice mail, IVR, IP trunks, IP telephones and dialup ISDN WAN connections. If you need 58 signaling channels or less for these applications, use a 2/6 DS30 split. If you need 59 signaling channels or more, use a 3/5 DS30 split.

The DS30 split is set up in the Quick Start Wizard when the system is first configured. If your signaling channel requirements change, for example you want to increase the number of IP telephones, you can change from a 2/6 setting to a 3/5 setting without losing data. All new records added after the update will reflect the new default settings. To determine what the channel requirements are, refer to "Determining the MSC resources you require" on page 614.

Warning: Ensure that the system is idle before you do this procedure. The system needs to be restarted after the setting has been changed.

Note: Ensure you have a current backup before you do this procedure.

Note: You must ensure that your system has adequate DSP resources to support an increase in voice processing traffic. To determine if you have enough DSP resources, refer to "Determining the MSC resources you require" on page 614. If you need to add MS-PEC IIIs, refer to the *Business Communications Manager BCM200/400 Installation and Maintenance Guide* for installation instructions. Refer to the Business Communications Manager sales catalogue for part numbers and ordering instructions.

Warning: If you choose to change the DS30 split of your system after you have configured your system, you could risk losing data for both the core system and optional applications.

Make sure you understand the implications of the changes before you go forward with this procedure.

To change the DS30 split setting:

1. On the navigation tree, click the **Diagnostics** key.
2. Click on **MSC**.
3. On the top menu, click **Configuration**, and select **DS30 split** from the list.
   A dialog box appears. The DS30 Split field displays the current setting for your system.
4. If you want to change the setting, choose the other option from the list.
5. Click **OK** to accept a change or click **Cancel** to leave the option in the original state.
   You will be prompted to restart the Business Communications Manager server.

Note: Changing the DS30 split from 2/6 to 3/5 will preserve the existing telephony data. Any new device records will have default data.

Any change in DS30 split requires a restart of the Business Communications Manager for the change to be applied.

Configuring Double Density

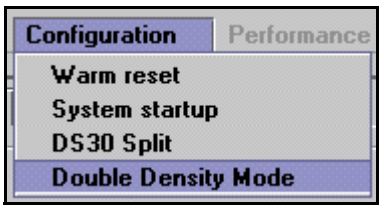
The BCM 3.0 and newer software configures the MSC so that it supports 32 ports for digital telephones on DS30 buses 02 to 05. The default system retains DS30 buses 06 and 07 as single density to allow the deployment of existing Companion system. This system is called a partial double density (PDD) system.

If you do not have a Companion system, and you want to take advantage of the double density ability on all DS30 buses, you can set your system to the full double density (FDD) setting after your system has been set up.

Security note: You cannot regress from a Full Double Density (FDD) system to a Partial Double Density (PDD) system. Ensure that MSC configuration is only available to high-level supervisory personnel ("Managing system and user security access levels" on page 105).

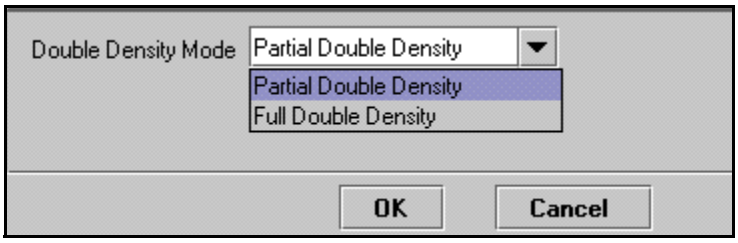
Updating your system to Full Double Density (FDD)

1. Click on the key beside **BCM** and **Diagnostics**.
2. Click on MSC.
3. On the top menu, click **Configuration** and select **Double Density Mode**.



4 On the screen, click the arrow beside the **Double Density Mode** field and select **Full Double Density**.

Figure 208 Double Density Mode choices



5 Click **OK** to update your system to Full Double Density.

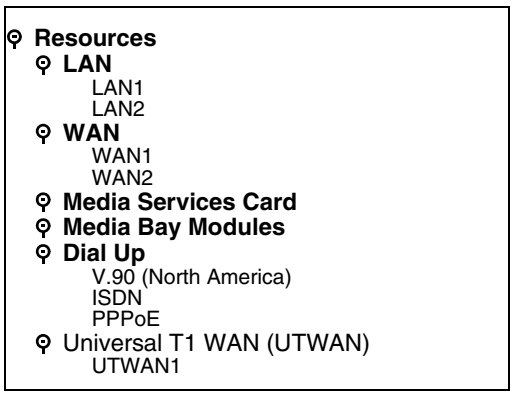
Chapter 27
Using a wizard to change data parameters

This section provides information about viewing and changing Business Communications Manager LAN, WAN, and dialup networking resources settings.

- "Viewing Business Communications Manager resources" on page 633
- "Using the Network Update Wizard" on page 634

The following figure shows the programming map for Business Communications Manager networking resources.

Figure 209 LAN, WAN and Dialup headings



Note: The resources listed on this table may not correspond exactly to the resources available on your Business Communications Manager system.

Viewing Business Communications Manager resources

Unified Manager allows you to view and configure Business Communications Manager networking resources including LAN, WAN, and dial up resources such as ISDN or V.90 modem (North America). To view the networking resources your Business Communications Manager system supports:

1 On the navigation tree, click the **Resources** heading.
The available Business Communications Manager resources appear in a table format. These attributes are described in the table below.

Table 180 Business Communications Manager resources

Attribute	Description
Name	Provides a list of available resources.
Status	Shows the operating status of each resource.
Version	Shows the software version of each resource.
Description	Provides a description of the interface card for each resource.

Using the Network Update Wizard

When your system is first installed, the data resources are set up when the Quick Start Wizard is run. Refer to "Using the Quick Start Wizard" on page 96.

If you need to change any of your system name, LAN, WAN, or dialup settings after your system has been configured, you can use the Network Update Wizard.

Note: Remember to update your Programming Records when you make any type of changes to your system.

To update a LAN, WAN or DNS setting:

1 On the first page of the Unified Manager, click the **Wizards** button.

2 When prompted, enter your system **Login name** and **Password,** then click the **Login** button.

3 Click the **Network Update** icon.

The first page of the Network Update wizard appears. The information on this page reflects the actual hardware installed in your system.

4 Fill out the fields for the data information that you want to change.
Refer to "What you need to know" on page 635.

5 Click **Next**.
The second page of this wizard is a summary page.

6 Check that the settings are correct.

7 Print out the page or save a copy on your computer to add to your programming records

8 Click **Apply**.
The system updates the settings.

What you need to know

Use the following chart to gather the information you need to make the data resource changes that you require. Not all of these fields will appear if your system does not support the specified hardware. Enter only the information that is changing.

Screen 1, Network settings	
• What is the new name that you want to give your system?	System Name:
LAN 1	
• What is the new IP address for the first LAN card?	IP Address
• What is the new Subnet Mask for the first LAN card?	Subnet Mask
• What is the WINS server address?	WINS Server
LAN 2	
• What is the new IP address for the second LAN card?	IP Address
• What is the new Subnet Mask for the second LAN card?	Subnet Mask
• What is the WINS server address?	WINS Server
WAN 1	
• What is the new IP address for the WAN card?	IP Address
• What is the new Subnet Mask for the WAN card?	Subnet Mask
• Port (read-only)	Port: T1
• What is the new Link Protocol for the WAN card?	Link Protocol
WAN 2	
• What is the new IP address for the WAN card?	IP Address
• What is the new SubNet Mask for the WAN card?	Subnet Mask
• Port (read-only)	Port: V.35
• What is the new Link Protocol for the WAN card?	Link Protocol
Default Next Hop Router	
• What is the new IP address for the next router or link on the network?	(Next Hop on Primary Link)
DNS	
• What is the domain name of the DNS server?	IP Domain
• What is the IP address for the primary server?	Primary Server
• What is the IP address for the secondary server? Note: If you do not enter a primary server, the system will use the secondary server entry as the primary entry.	Secondary Server

Chapter 28
Configuring DHCP

Business Communications Manager provides DHCP (Dynamic Host Configuration Protocol) service to branch office clients. DHCP allows a network administrator to supervise and distribute IP addresses from a central location. This service dynamically assigns IP addresses to branch office computers or IP telephones, so you do not need to manually assign an IP address. It also automatically assigns a new IP address if a device connects to a different place in the network.

This section includes information about:

DHCP configuration overview

To configure Business Communications Manager as your DHCP server, you must create a scope of IP addresses for each LAN interface and then allocate a block of IP addresses to that scope. If you already have a DHCP server then you need to set up Business Communications Manager as a relay agent to that server.

Caution: Check with your network administrator before enabling DHCP. Enabling DHCP on a network that already has a DHCP server can cause problems on the network.

Tip
Because Business Communications Manager retrieves default DHCP parameters from the LAN interface parameters, you must configure a LAN interface before you configure the DHCP server for that interface. For information on configuring a LAN interface, see "Configuring the LAN resources" on page 663.

You must define one DHCP scope for each LAN interface. For DHCP service, there are global attributes that affect all scopes and there are attributes that are specific for each scope.

Tip
Use the Business Communications Manager DHCP default configuration unless your network does not allow it.

If you must modify the DHCP default configuration on Business Communications Manager, make sure configuration settings are consistent throughout the network and take the following into consideration:

- If a change in the DHCP configuration resulted in a change in the IP addresses of a scope, perform one of the following actions to ensure good system operation:
  - Execute *ipconfig/release and ipconfig/renew* on each of the workstations. For Windows 95 and Windows 98, use the *winipcfg*.
  - For clients that do not support *ipconfig* and *winipcfg* (for example, IP telephones), a reboot is necessary to renew their IP addresses.
- If you made a change in the DNS server configuration or DNS name field, repeat the actions stated in the previous step to ensure proper connectivity with the network.
- Always schedule a down time when making changes to the Business Communications Manager DHCP server configuration to minimize impact on your network users.

Configuring the DHCP Mode

You can configure Business Communications Manager as your DHCP Server or as a DHCP Relay Agent by setting the DHCP Mode.

- Choose DHCP server mode if you want Business Communications Manager to supply the IP addresses to the devices on your network.
- Choose DHCP Relay Agent if you have a central DHCP Server on your corporate network and you want Business Communications Manager to pass the DHCP traffic to and from the devices on the LAN.

To set the DHCP Mode:

1. On the navigation tree, click the **Services** key and click the **DHCP** heading.
   The Summary screen appears.
2. Click the **DHCP Mode** tab.
   The DHCP Mode screen appears.
3. Click the DHCP box and click **DHCPRelayAgent** or **DHCPserver**.
   The default is DHCPserver.
4. Press the **Tab** key to save the settings.

Configuring a DHCP Server

If you chose DHCPServer as the DHCP mode, configure the DHCP Server settings in the Global Options and Summary screen.

1 On the navigation tree, click the **Services** key and click the **DHCP** heading.
The Summary screen appears.

2 Configure the DHCP Server Summary attributes according to the following.

Table 181 DHCP Server Summary attributes

Setting	Definition
Description	Displays a description of the DHCP service. This is a read-only field.
Version	Displays the version number of the DHCP service. This is a read-only field.
Status	Allows you to view and change the status of the DHCP Server. To enable DHCP Server, select **Enabled**. To disable DHCP Server, select **Disabled**. When the DHCP Server is running, the status is Up. When the DHCP Server is not running, the status is Disabled.

3 Click the **Global Options** tab.
The Global Options screen appears.

4 Configure the Global Options attributes according to the following.

Table 182 DHCP Global Options

Setting	Definition
IP Domain Name	This setting defaults to the value entered in the **Domain** box of the DNS Summary page (see "Configuring DNS" on page 703) because all the DHCP clients of Business Communications Manager are in the same DNS domain as the Business Communications Manager base unit. Business Communications Manager runs only a DNS cache and does not introduce another DNS zone. The domain name is passed to the client when Business Communications Manager responds to a client's DHCP requests. Use caution if you change this.
WINS Node Type	Allows you to specify a client's WINS node type. Business Communications Manager automatically sets this value to **8** (indicating H-Node) on all DHCP clients of Business Communications Manager. This setting configures the DHCP client PCs to use p-node name resolution before resorting to b-node name resolution. This is efficient when a WINS server is configured for the network. Business Communications Manager also includes a WINS server. Other options available are: **1**: indicates a b-node that uses a broadcast mechanism for NetBIOS name resolution. **2**: indicates a p-node that uses a point-to-point mechanism involving a WINS Server for NetBIOS name resolution. **4**: indicates a m-node that first uses a broadcast and then a point-to-point mechanism for NetBIOS name resolution. Use caution if you change this.
NORTEL IP Terminal Information	Contains vendor specific information for IP telephones. The default value is: Nortel-i2004-A,10.10.10.1:7000,1,1;10.10.10.1:7000,1,1. where: • Nortel-i2004-A — is the identification name for the IP telephone • 10.10.10.1 — is the IP address for the primary Terminal Proxy Server (TPS). This is normally the Published IP address of the Business Communications Manager. • 7000 — is the UDP port number for the TPS (S1) • 1 — is the Initial Action Code for the IP telephone • 1 —is the retry count for attempts to connect to the TPS (S1) • Nortel-i2004-A — is the identification name for the IP telephone • 10.10.10.1 — is the IP address for the backup TPS (S2) • 7000 — is the UDP port number for the TPS (S2) • 1 — is the Initial Action Code for the IP telephone • 1 — is the retry count for attempts to connect to the TPS (S2) **Note**: The S1 and S2 information must be separated by a semi colon (;). The string must be terminated with a period (.).

Table 182 DHCP Global Options (Continued)

Setting	Definition
NORTEL IP Terminal VLAN Id	Allows you to specify the Virtual LAN (VLAN) ID numbers that are given to the IP telephones. 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.** where: • VLAN-A: — is an identifier that tells the IP telephone that this message is a VLAN discovery message. • id1,id2,...idn — are the VLAN ID numbers that DHCP can assign to the IP telephones. You can have up to 10 VLAN ID numbers listed. The VLAN ID numbers must be a number from 0 to 4095. For example, if you wanted to use VLAN IDs 1100, 1200, 1300 and 1400, you would enter the following string in this box: **VLAN-A:1100,1200,1300,1400.** If you do not want DHCP to automatically assign VLAN IDs to the IP telephones, enter **VLAN-A:none.** in this text box. **Note1**: The NORTEL IP Terminal VLAN Id string must be terminated with a period (.). **Note2**: If you do not know the VLAN ID, contact your network administrator. **Note3**: For information about how to setup a VLAN, refer to the user documentation that came with your VLAN compatible switch.

Note: When you change the published IP address of Business Communications Manager, you must reboot the IP telephones.

5 Press the **Tab** key to save the settings.

Note: Event logging is always on for DHCP server. The event information is recorded in the system admin log.

6 Click the **Summary** tab.
The Summary screen appears.

7 Configure the Summary settings according to the following.

Table 183 DHCP Summary settings

Setting	Definition
Description	Shows the a description of the DHCP service operating on Business Communications Manager.
Version	Shows the version number of the DHCP service.
Status	Allows you to enable or disable the DHCP server. When you disable the DHCP server, you need to assign static IP addresses to the clients or configure DHCP as a Relay Agent to use another DHCP server on the network. The default is Disabled.

8 Press the **Tab** key to save the settings.

LAN settings for DHCP Server

This section describes configuring the DHCP server, as well as:

- "Configuring Address ranges for a Local Scope" on page 644
- "Configuring Excluded addresses for a Local Scope" on page 645
- "Configuring Reserved addresses for a Local Scope" on page 647

If you configured the DHCP mode for DHCPServer, then configure the LAN scope attributes as follows. If the DHCP mode is DHCPRelayAgent refer to "LAN settings for DHCP Relay Agent" on page 659.

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

Note: If your Business Communications Manager system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1 and LAN2. This section describes configuring DHCP for LAN1. Follow the same instructions to configure the parameters for LAN2.

3 Configure the scope-specific settings according to the following table.

Table 184 LAN Scope Specific Options

Attribute	Description
Name	Allows you to specify the name of the LAN scope.
Description	Allows you to specify a description for the LAN scope.
DNS Server	Allows you to specify the IP addresses of the primary DNS server and the secondary DNS server in a valid dot format. When you specify a secondary DNS server, separate the two IP addresses by a space. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
WINS Server	Allows you to specify the IP address of the WINS server. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Default Gateway	Allows you to specify the IP address of the default next-hop router. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Lease Time	Allows you to specify the time, in seconds, for an address assignment until the client's lease expires. The default is 259200 seconds (72 hours).
Scope Status	Allows you to enable or disable the scope. The default is enabled.

Note: If the IP address or subnet mask for a LAN interface changes, the system creates or modifies the corresponding DHCP scope for the interface. This operation also involves setting default values for some parameters. By default, Business Communications Manager sets the IP address of the corresponding LAN interface to the DNS Server, WINS Server, Default Gateway options of the scope. It also sets the lease time to three days and creates a range of addresses for the scope. If the IP address of the LAN interface is in the lower half of the subnet, the address range set for the scope includes all the addresses above the LAN interface address. If the IP address of the LAN interface is in the upper half of the subnet, the address range set for the scope includes all the addresses below the LAN interface address. By default, the scope is enabled.

Note: When DNS is disabled in Business Communications Manager, the DNS Server box must be set to the IP address of a remote DNS server.

4 Press the **TAB** key to save the settings.

Configuring Address ranges for a Local Scope

Address ranges allow you to specify the valid IP addresses for the DHCP clients.

Note: You must add at least one Address range to use DHCP server.

Adding an address range

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key and click the **LAN1** heading.
   The LAN Scope Specific Options screen appears.
3. Click the **Address Range** tab.
   The Address Range screen appears.
4. On the **Configuration** menu, click **Add Address Range**.
   The Address Range dialog box appears.
5. Configure the Address Range attributes according to the following table.

Table 185 Address Range attributes

Attribute	Description
Range (R#)	Allows you to specify the Range identifier. The range box uniquely identifies an Address range in the scope. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing range name, it modifies the existing range. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a range, you cannot change the range name. The range name does not have any significance other than identifying an entry.
Start Address	Allows you to specify a the first IP address in the Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Address Range. Make sure the start address and end address are in the same subnet. Enter the IP address in the dotted format.

6. Click the **Save** button to save the address range.

Modifying an address range

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key and click the **LAN1** heading.
   The LAN Scope Specific Options screen appears.
3. Click the **Address Range** tab.
   The Address Range screen appears.
4. Click an address in the Address Range table.

5 On the **Configuration** menu, click **Modify Address Range**.
The Address Range dialog box appears.

6 Modify the Address Range settings.

7 Click the **Save** button.

Deleting an address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Address Range** tab.
The Address Range screen appears.

4 Click an address range in the Address Range table.

5 On the **Configuration** menu, click **Delete Address Range**.
A dialog box appears asking you to confirm the deletion.

6 Click the **Yes** button.

Note: When you delete or modify an IP Address range it removes any excluded addresses that are in the original address range value.

Configuring Excluded addresses for a Local Scope

Excluded addresses allow you to specify the IP addresses that are not available to DHCP clients. The excluded addresses are also used to ensure that Static IP addresses are not re-assigned by DHCP.

Adding an excluded address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Excluded Address** tab.
The Excluded Address screen appears.

4 On the **Configuration** menu, click **Add Excluded Address Range**.
The Excluded Address dialog box appears.

5 Configure the Excluded Address attributes according to the following table.

Table 186 Excluded Addresses

Attribute	Description
Range (E#)	Allows you to specify the Range identifier. The range setting uniquely identifies an excluded range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing excluded range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify an excluded range, you cannot change the range name. The excluded range identifier does not have any significance, other than uniquely identifying an entry.
Start Address	Allows you to specify a the first IP address in the Excluded Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Excluded Address Range. Enter the IP address in the dotted format.

Note: Make sure the start address and end address are in the same subnet. The excluded address range must be completely contained in an IP address range specified for the subnet.

6 Click the **Save** button.

Modifying excluded address ranges

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Excluded Address** tab.
The Excluded Address screen appears.

4 Click an excluded address range in the Excluded Address Range table.

5 On the **Configuration** menu, click **Modify Excluded Address Range**.
The Excluded Address dialog box appears.

6 Modify the Excluded Address settings.

7 Click the **Save** button.

Deleting an excluded address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Excluded Address** tab.
The Excluded Address screen appears.

4 Click an excluded address range in the Excluded Address Range table.

5 On the **Configuration** menu, click **Delete Excluded Address Range**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button.

Configuring Reserved addresses for a Local Scope

Reserved addresses allow you to assign IP addresses to specific DHCP clients.

You can use Reserved Addresses to assign IP addresses to devices that require a static IP address.

Adding a reserved address

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Reserved Address** tab.
The Reserved Address screen appears.

4 On the **Configuration** menu, click **Add Reserve Address**.
The Reserved Address dialog box appears.

5 Configure the Reserved Address settings according to the following table.

Table 187 Reserved Addresses

Setting	Definition
Range (V#)	Allows you to specify the Range identifier. The range setting uniquely identifies a reserved range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'V' followed by a unique number identifying the range in the table. For example, 'V2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing reserved range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify a reserved range, you cannot change the range name. The reserved range name does not have any significance, other than uniquely identifying an entry.
IP Address	Allows you to specify the IP Address that is reserved for this DHCP client. Enter the IP address in the dotted format.
MAC Address	Allows you to specify the MAC address for the DHCP client this IP address is assigned to. The permitted value is 6 bytes in hexadecimal format.
Client Name	Allows you to specify the name of the DHCP client.
Client Description	Allows you to specify the description that will help to identify the DHCP client this IP address is assigned to.

6 Click the **Save** button.

Modifying a reserved address

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Reserved Address** tab.
The Reserved Address screen appears.

4 Click a reserved address in the Reserved Address table.

5 On the **Configuration** menu, click **Modify Reserved Address**.
The Reserved Address screen appears.

6 Modify the Reserved Address settings.

7 Click the **Save** button.

Deleting a reserved address

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Reserved Address** tab.
The Reserved Address screen appears.

4 Click a reserved address in the Reserved Address table.

5 On the **Configuration** menu, click **Delete Reserved Address**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button.

Viewing the Lease Information for a Reserved address

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Lease Info** tab.
The Lease Info screen appears.

4 On the **Configuration** menu, click **Add Reserve Address**.
The Reserved Address dialog box appears.

5 The following table describes the Lease Information that you can view.

Table 188 Reserved Addresses Lease Information

Setting	Definition
Range (L#)	Shows the Range identifier for this Reserved address.
IP Address	Shows the IP Address that is reserved for this DHCP client.
MAC Address	Shows the MAC address for the DHCP client this IP address is assigned to.
Client Name	Shows the name of the DHCP client.

Table 188 Reserved Addresses Lease Information (Continued)

Setting	Definition
Client Description	Shows the description that will help to identify the DHCP client this IP address is assigned to.
Lease Expiration Date	Shows the date when this IP address is no longer reserved for the DHCP client.
Lease Expiration Time	Shows the time when this IP address is no longer reserved for the DHCP client.

Remote Scope

A remote scope is a remote network (not LAN1 or LAN2) that uses the DHCP Server to get IP addresses through a DHCP relay agent.

This section describes:

Adding a Remote Scope

To add a Remote Scope:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** heading and click the **Add** button.
   Or, right click the Remote Scope heading and click **Add**.
3. Configure the remote scope settings according to the following table.

Table 189 Remote Scope settings

Attribute	Description
Subnet name	Allows you to specify the name of the remote scope.
Subnet Comment	Allows you to specify a description of the remote scope.
IP Address	Allows you to specify the IP address of the remote scope. Enter the IP address in the dotted format.
Subnet Mask	Allows you to specify the subnet mask for the remote scope. Enter the subnet mask in the dotted format.

4. Click the **Save** button.

Modifying Remote Scope settings

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Configure the remote scope-specific settings according to the following table.

Table 190 Remote Scope specific settings

Attribute	Description
Name	Allows you to specify the name of the remote scope.
Description	Allows you to specify a description for the remote scope.
DNS Server	Allows you to specify the IP addresses of the primary DNS server and the secondary DNS server in a valid dot format. When you specify a secondary DNS server, separate the two IP addresses by a space.
WINS Server	Allows you to specify the IP address of the WINS server.
Default Gateway	Allows you to specify the IP address of the default next-hop router.
Lease Time	Allows you to specify the time, in seconds, for an address assignment until the client's lease expires.
Scope Status	Allows you to enable or disable the scope.

5. Press the **TAB** key to save the settings.

Configuring Remote Scope Address ranges

Address ranges allow you to specify the valid IP addresses for these DHCP clients.

Adding an address range

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Address Range** tab.
   The Address Range screen appears.
5. On the **Configuration** menu, click **Add Address Range**.
   The Address Range dialog box appears.

6 Configure the Address Range attributes according to the following table.

Table 191 Remote Scope Address Range attributes

Attribute	Description
Range (R#)	Allows you to specify the Range identifier. The range box uniquely identifies an Address range in the scope. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing range name, it modifies the existing range. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a range, you cannot change the range name. The range name does not have any significance other than identifying an entry.
Start Address	Allows you to specify a the first IP address in the Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Address Range. Make sure the start address and end address are in the same subnet. Enter the IP address in the dotted format.

7 Click the **Save** button.

Modifying address ranges

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Address Range** tab.
The Address Range screen appears.

5 Click an address in the Address Range table.

6 On the **Configuration** menu, click **Modify Address Range**.
The Address Range dialog box appears.

7 Modify the Address Range settings.

8 Click the **Save** button.

Deleting an address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Address Range** tab.
The Address Range screen appears.

5 Click an address range in the Address Range table.

6 On the **Configuration** menu, click **Delete Address Range**.
A dialog box appears asking you to confirm the deletion.

7 Click the **Yes** button.

Note: When you delete or modify an IP Address range it removes any excluded addresses that are in the original address range value.

Configuring Remote Scope excluded addresses

Excluded addresses allow you to specify the IP addresses that are not available to DHCP clients. The excluded addresses are also used to ensure that Static IP addresses are not re-assigned by DHCP.

Adding a excluded address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 On the **Configuration** menu, click **Add Excluded Address Range**.
The Excluded Address dialog box appears.

6 Configure the Excluded Address attributes according to the following table.

Table 192 Remote Scope Excluded Addresses

Attribute	Description
Range (E#)	Allows you to specify the Range identifier. The range setting uniquely identifies an excluded range value in the scope. The value for this setting must follow certain conventions. You must type the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing excluded range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify an excluded range, you cannot change the range name. The excluded range name does not have any significance, other than uniquely identifying an entry.
Start Address	Allows you to specify a the first IP address in the Excluded Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Excluded Address Range. Enter the IP address in the dotted format.

Note: Make sure the start address and end address are in the same subnet. The excluded address range must be completely contained in an IP address range specified for the subnet.

7 Click the **Save** button.

Modifying excluded address ranges:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 Click an excluded address range in the Excluded Address Range table.

6 On the **Configuration** menu, click **Modify Excluded Address Range**.
The Excluded Address dialog box appears.

7 Modify the Excluded Address settings.

8 Click the **Save** button.

Deleting an excluded address range

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 Click an excluded address range in the Excluded Address Range table.

6 On the **Configuration** menu, click **Delete Excluded Address Range**.
A message prompts you to confirm the deletion.

7 Click the **Yes** button.

Configuring Remote Scope Reserved Addresses

Reserved addresses allow you to assign IP addresses to specific DHCP clients.

Adding a reserved address

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Reserved Address** tab.
   The Reserved Address screen appears.
5. On the **Configuration** menu, click **Add Reserve Address**.
   The Reserved Address dialog box appears.
6. Configure the Reserved Address settings according to the following table.

Table 193 Remote Scope Reserved Addresses

Setting	Definition
Range (V#)	Allows you to specify the Range identifier. The range setting uniquely identifies a reserved range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'V' followed by a unique number identifying the range in the table. For example, 'V2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing reserved range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify a reserved range, you cannot change the range name. The reserved range name does not have any significance, other than uniquely identifying an entry.
IP Address	Allows you to specify the IP Address that is reserved for this DHCP client. Enter the IP address in the dotted format.
Mac Address	Allows you to specify the MAC address for the DHCP client this IP address is assigned to. The permitted value is 6 bytes in hexadecimal format.
Client Name	Allows you to specify the name of the DHCP client.
Client Description	Allows you to specify the description that will help to identify the DHCP client this IP address is assigned to.
Lease Expiration Date	Shows the date when this IP address is no longer reserved for the DHCP client.
Lease Expiration Time	Shows the time when this IP address is no longer reserved for the DHCP client.

7. Click the **Save** button.

Deleting a reserved address

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Reserved Address** tab.
   The Reserved Address screen appears.
5. Click a reserved address in the Reserved Address table.
6. On the **Configuration** menu, click **Delete Reserved Address**.
   A message prompts you to confirm the deletion.
7. Click the **Yes** button.

Remote Scope Lease Information

To view the Lease information for a reserved address:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Lease Info** tab.
   The Lease Info screen appears.
5. The following table describes the Lease Information you can view for the Reserved Address.

Table 194 Lease Information for a Remote Scope Reserved Addresses

Setting	Definition
Range (L#)	Shows the Range identifier for the Lease Information.
IP Address	Shows the IP Address that is reserved for this DHCP client.
Mac Address	Shows the MAC address for the DHCP client this IP address is assigned to. The permitted value is 6 bytes in hexadecimal format.
Client Name	Shows the name of the DHCP client.
Client Description	Shows the description that will help to identify the DHCP client to which this IP address is assigned.
Lease Expiration Date	Shows the date when this IP address is no longer reserved for the DHCP client.
Lease Expiration Time	Shows the time when this IP address is no longer reserved for the DHCP client.

Deleting a Remote Scope

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to delete.
   The Remote Scope Specific Options screen appears.
4. Click the **Delete** button.
   Or, right click the remote scope you want to delete and click **Delete**.
   A message prompts you to confirm the deletion.
5. Click the **Yes** button.

Configuring a DHCP Relay Agent

If you chose DHCPRelayAgent as the mode, configure the DHCP Relay Agent settings in the Global Options and Server List screens with the following process.

1. On the navigation tree, click the **Services** key and click the **DHCP** heading.
   The DHCP Mode screen appears.
2. Click the **Global Options** tab.
   The Global Options screen appears.
3. Click the **Log Level** box and choose which information is recorded in the system admin log.
   Errors Only - records error messages only
   Warnings Also - records error message and warning messages
   Maximum - records error message, warning messages and event messages
   Disabled - disables recording of DHCP messages
   The default is **Errors Only**.
4. Click the **Server List** tab.
   The Server List screen appears.
5. On the **Configuration** menu, click **Add server**.
   The Server List dialog box appears.
6. Type in the IP address of the DHCP server.

Note: You can specify a number of servers. The routing component searches the list for the server on the same subnet as the interface and forwards the DHCP packet.

7. Click the **Save** button.

Deleting a server from the Server List

1. On the navigation tree, click the **Services** key and click the **DHCP** heading.
   The DHCP Mode screen appears.
2. Click the **Server List** tab.
   The Server List screen appears.
3. Click a server in the Server List.
4. On the **Configuration** menu, click **Delete server**.
   A dialog box appears asking you to confirm the deletion.
5. Click the **Yes** button.

LAN settings for DHCP Relay Agent

If you configured the DHCP mode as DHCPRelayAgent (refer to "Configuring the DHCP Mode" on page 638), then configure the LAN scope attributes as follows. If the mode is DHCPServer refer to "LAN settings for DHCP Server" on page 642.

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The Relay Agent Interface Parameters screen appears.

Note: If your Business Communications Manager system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1 and LAN2. This section describes configuring the DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under the scope for LAN2.

3 Configure the Relay Agent Interface parameters according to the following table.

Table 195 Relay Agent Interface parameters

Attribute	Description
Relay DHCP packets	Allows you to enable or disable the relay of DHCP packets on this interface. The default is disabled.
Hop-count threshold.	Allows you to specify the maximum number of hops. After this number of hops, DHCP requests are discarded. The values are 0 to 16. The default value is 4.
Seconds-since-boot threshold	Allows you to specify the minimum number of seconds since the last boot of Business Communications Manager, before Business Communications Manager forwards DHCP requests. The values are 1 to 3600. The default value is 4.

4 Press the **Tab** key to save the settings.

Importing and Exporting DHCP data

You can export the DHCP data for an interface to a file on the Business Communications Manager system. This saves an image of the current DHCP programming for that interface.

When the IP address of LAN1 or LAN2 changes, the DHCP programming for that interface is lost. To save the DHCP programming, export the DHCP data before you change the IP address of the interface. Then, after you change the IP address, import the DHCP programming for the interface.

Exporting DHCP data

When you export the DHCP data, the following information is saved to the file:

- Address Range
- Excluded Address Range
- Reserved Address Range
- Scope options

The DHCP data is stored on the Business Communications Manager in the directory D:\Data Files\Nortel Networks\Unified Manger. The file is named *ScopeName.dat* where ScopeName is the name of the DHCP scope.

To export the DHCP data:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key to export data for a local scope.
   Click the **Remote Scope** key to export data for a remote scope.
3. Click the scope from which you want to export data.
4. On the **Tools** menu, click **Export**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Note: If you have exported the DHCP data for a scope with this name before, the data from this export will overwrite the previous export.

Importing DHCP data

When you import the DHCP data, the DHCP programming from a previous export replaces the current DHCP programming for the scope.

To import the DHCP data:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key to import data for a local scope.
   Click the **Remote Scope** key to import data for a remote scope.
3. Click the scope for which you want to import data.
4. On the **Tools** menu, click **Import**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Reconciling the DHCP data

To reconcile the DHCP data:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key to reconcile data for a local scope.
   Click the **Remote Scope** key to reconcile data for a remote scope.
3. Click the scope for which you want to reconcile the DHCP data.
4. On the **Tools** menu, click **Reconcile**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Chapter 29
Configuring the LAN resources

Business Communications Manager is equipped with an Ethernet/802.3 network interface card which supports the IEEE 802.3 Ethernet frame format. The Ethernet connection uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage the access to the physical media.

This chapter includes information about:

The Business Communications Manager Ethernet interface card supports the following features:

- 100 BASE T with RJ-45 connector
- 10 / 100 Auto Sense
- full duplex
- fast LAN-to-LAN routing (when using more than one LAN card)
- LAN traffic smoothing
- multiple IP addresses

Viewing the LAN resources

Unified Manager shows all available LAN resources. If your Business Communications Manager base unit is equipped with two LAN interface cards, Unified Manager displays all available LAN resources and names each one (LAN1, LAN2).

To view the available LAN resources:

1. On the navigation tree, click the **Resources** key and click the **LAN** heading.
   The LAN Parameters screen appears.
2. Click the **Resources** tab.
   The Resources screen appears.

Configuring LAN resources

The following section describes how to set up the LAN card on your Business Communications Manager.

The information in this section includes:

Setting LAN global parameters

To set the LAN global parameters:

1 On the navigation tree, click the **Resources** key and click the **LAN** heading.
The Lan Parameters screen appears.

2 Set your global LAN parameters according to the information in the following table.

Table 196 LAN global parameters

Attribute	Description
Fast Routing (Between LANs)	Allows you to enable or disable fast routing to improve LAN-to-LAN routing performance. This feature is for a Business Communications Manager system equipped with two LAN cards. At the same link speed, a smaller packet size means more packets to forward. Use a lower traffic threshold. Permitted values: **Enabled** or **Disabled** Default: **Disabled** **Note**: Do not use Fast Routing on systems that use NAT, IP Firewall Filters, IPSec tunnels, or Quality of Service (QoS). Fast Routing bypasses these features and will cause the packets to be routed incorrectly.
Decrement TTL	When Fast Routing is enabled, Decrement TTL lets you decrement the time-to-live (TTL) value in the IP header of packets as they travel from LAN to LAN. Decrement TTL lets you increase processing time for each fast-routed IP packet, which reduces CPU cycles. This feature is used when other routers or special applications on the network connect to the LAN interfaces. Permitted Values: **Enabled** or **Disabled** Default: **Disabled**
Traffic Smoothing (In Mbps)	Lets you set the rate, in Mbps, at which the LAN driver receives packets from the LAN interface. The main purpose of this feature is to limit the number of host CPU cycles spent on LAN-to-WAN packet forwarding. Normally, LAN drivers operate at link speed, which implies that the driver forwards packets as fast as possible until there is no packet in the receiving buffer. Permitted values: **5**, **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45**, **50, Disabled** Default: **10**

Table 197 Guidelines to configure LAN to LAN traffic smoothing

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1500 bytes
Fast Routing enabled	Not needed	Not needed	Not needed	Not needed	Not needed	Not needed
Fast Routing disabled or LAN-to-WAN routing	20 mbps	30 mbps	50 mbps	50 mbps	Not needed	Not needed

Note:

The settings in the table above ensure data routing uses a maximum of 60 to 70 percent CPU cycles.

If the LAN to WAN link speed is 10 mbps, selecting higher traffic smoothing parameters has no impact on packet forwarding, which the system still performs at a link speed of 10 mbps.

Configuring a LAN interface

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
   The available LAN interfaces appear.
2. Click the LAN interface you want to configure (for example, **LAN1)**.
   The LAN Summary screen appears.
3. Configure the LAN attributes according to the information provided in the following table.

Table 198 LAN Summary attributes

Attribute	Description
IP Address	Enter the IP address of the LAN interface in the following format: 255.255.255.255. If you do not know your LAN interface IP address, contact your network administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask of the LAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your network administrator or your Internet service provider.
Physical Address	Shows the physical address (MAC address) of the LAN interface. This is a read only attribute.
Description	Provides a description of the network interface card supporting the LAN connection. This is a read only attribute.
Version	Shows the version of the LAN interface card. This is a read only attribute.
Speed	Shows the speed of the connection to the LAN interface. This is a read only attribute.
Duplex Type	Shows whether the LAN interface is operating in Full Duplex mode or Half Duplex mode. This is a read only attribute.

Table 198 LAN Summary attributes (Continued)

Attribute	Description
Connection Type	Select a type of connection to the LAN interface. The following values are supported and are interpreted as follows: **Auto Sense**: The LAN interface uses the auto negotiation protocol to choose the maximum possible speed of the connection. Depending on the connected device, the LAN can choose 100 MB or 10MB and full-duplex or half-duplex. **10 MB Half**: The speed is set to 10 Mbit/s and the mode is set to half-duplex. **10 MB Full**: The speed is set to 10 Mbit/s and the mode is set to full-duplex. **100 MB Half**: The speed is set to 100 Mbit/s and the mode is set to half-duplex. **100 MB Full**: The speed is set to 100 Mbit/s and the mode is set to full-duplex. Default value: **Auto Sense** **Important**: If you have an i2004 IP telephone on your network, you must set the Connection Type to **Auto Sense**. **Note**: You may want to limit the incoming traffic to 10 Mbit/s if you notice that the bursty traffic from the connected LAN is degrading the quality of voice calls carried through VoIP over the WAN. Though the LAN traffic gets lower priority in Business Communications Manager, high incoming LAN traffic to the Business Communications Manager base unit can result in service interruptions in the system These interruptions may degrade the quality of voice calls carried as VoIP.
Status	Shows the current status of the LAN connection. The possible states are: **Up**: The LAN card is operational. **Down**: The LAN card is not operational. This is a read only attribute.
Admin Status	Allows you to view and change the Admin Status for this interface. The Admin Status settings determines if the IP address for this interface is included in the routing table. The possible states for Admin Status are: **Up**: The routing table contains entries for this LAN interface. **Down**: The routing table does not contain entries for this LAN interface. The default Admin Status is **Up**. The routing table entries for unused network interfaces can cause routing issues. For this reason, Nortel Networks recommends you disable the Admin Status on any LAN interface that is not connected to the network. To remove the routing table entries for this LAN interface, select **Disable**. If you decide to use a LAN interface that has had the Admin Status disabled, you must enable the Admin Status to add entries for this LAN interface to the routing table. To add routing table entries for this LAN interface, select **Enable**.
Primary Wins Address	Enter the IP address of the Primary WINS server in the following format: 255.255.255.255.
Secondary Wins Address	Enter the IP address of the Secondary WINS server in the following format: 255.255.255.255.

Note: Consult your network administrator for the appropriate configuration information before changing the settings.

When you change these parameters, you must reboot the Business Communications Manager system.

Note: Setting the LAN connection speed to 100 Mbit/s does not reduce performance. However, the CPU is more efficient if you limit your incoming traffic to 10 Mbit/s. To increase your CPU performance, set the connected external LAN hub or switch to **10 Mbit/s** or to **Auto Sense**.

Note: If you enable LAN Traffic Smoothing, the connection type defaults to Auto Sense. Therefore, you do not need to set the connection speed on the external LAN hub or switch.

Configuring multiple IP addresses for the LAN interface

Adding an additional IP address

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
2. Click the heading of the LAN resource you want to modify (for example, LAN1). The LAN Summary screen appears.
3. Click the **Additional IP Address** tab. The Additional IP Address screen appears.
4. On the **Configuration** menu, click **Add Additional IPAddress**. The Additional IP Address screen appears.
5. Configure the Additional IP Address parameters according to the information in the table below.
6. Click the **Save** button.

Table 199 Additional LAN IP address parameters

Attribute	Description
Range (A#)	Enter the Additional IP Address identifier. The Range number uniquely identifies an Additional IP Address. The value for this setting must follow certain conventions. You must type the prefix 'A' followed by a unique number identifying the Additional IP Address. For example, 'A2' is a valid name. If you specify an existing Range number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Range number does not have any significance, other than uniquely identifying an Additional IP Address.
IP Address	Enter the Additional IP address of the LAN interface in the following format: 255.255.255.255.
SubNet Mask	Enter the subnet mask of the LAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your system administrator or your Internet service provider.

Modifying an Additional IP Address

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
2. Click the heading of the LAN resource you want to modify (for example, LAN1).
   The LAN Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. Click the Additional IP Address you want to modify.
5. On the **Configuration** menu, click **Modify Additional IPAddress**.
   The Additional IP Address screen appears.
6. Change the Additional IP Address parameters.
7. Click the **Save** button.

Deleting an Additional IP Address

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
2. Click the heading of the LAN resource you want to modify (for example, LAN1).
   The LAN Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. Click the Additional IP Address you want to delete.
5. On the **Configuration** menu, click **Delete Additional IPAddress**.
   A confirmation dialog box appears.
6. Click the **Yes** button.

Viewing LAN performance

The follow procedure describes how to view your LAN status.

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
2. Click the heading of the LAN resource you want to view (for example, LAN1).
   The LAN Summary screen appears.
3. On the **Performance** menu, click **LAN Graph**.
   The LAN Graph: Statistic Chart screen appears.
4. On the **Performance** menu, click **LAN Table**.
   The LAN Table: Statistic Table screen is appears.

Chapter 30
Configuring the WAN resources

A WAN (wide area network) is a geographically dispersed data communication network. The term WAN distinguishes a broader data communication structure from a local area network (LAN).

This section includes information about:

A WAN can be privately owned or rented, but is usually part of public (shared user) networks.

Business Communications Manager can be equipped with a WAN interface card with two serial synchronous ports (Europe), or a WAN interface card with one T1 port (with integrated CSU) and one serial synchronous port (North America). Both ports on the WAN interface card (WAN1 and WAN2) can be active at the same time. The serial synchronous port supports the following:

- North America: V.35
- Europe: V.35 (Upper Sync Port) and X.21 (Lower Sync Port)
- maximum line speed: 8 Mbit/sec.

Business Communications Manager provides primary and backup WAN links through dial-up connections using a V.90 modem (North America) or ISDN BRI/PRI. For information on V.90 modem or ISDN connections, see "Configuring the Dial Up resources" on page 685. Net Link Manager provides continuous WAN connection status monitoring. For information about Net Link Manager, see "Configuring Net Link Manager" on page 749.

Permanent WAN connection

The permanent WAN connection is normally a dedicated network adapter. The permanent link supports frame relay or Point-to-Point protocol (PPP) at the link layer. The link protocol you use depends on the existing network or on the service you buy from your Internet service provider. The two ports provided by the WAN interface card can be independently configured to run frame relay or PPP.

Frame Relay

Business Communications Manager supports frame relay in group mode and direct mode. In group mode, for each physical port (serial sync or T1 port), there is one IP address for all PVC*s* (permanent virtual circuits).

The available Data Link Control interface numbers are 0-1023. Of the 1023 PVCs, 16 are reserved. The maximum number of PVCs allowed is 1008.

Point-to-Point-Protocol (PPP)

Point-to-Point Protocol (PPP) is a full-duplex transmission protocol for communication between two computers using a serial interface. A typical PPP connection is a personal computer connected by telephone line to a server. For example, your Internet service provider (ISP) provides you with a PPP connection so that the ISP server can respond to your requests, pass them on to the Internet, and return your requested Internet responses to you.

Multi-link Point-to-Point Protocol (MLPPP)

MLPPP is used to connect multiple B-channel*s* together when using PRI or BRI ISDN as the WAN interface. This allows Business Communications Manager to connect B-channels independently of each other so that the ISDN connection can be used for both voice and data.

WAN data compression

Business Communications Manager provides a WAN Data Compression feature. You can use data compression on a permanent WAN connection and on a backup WAN connection. WAN Data Compression is enabled by default. You can enable or disable WAN Data Compression from the "Setting WAN Frame Relay Parameters" screen or from the "WAN PPP Parameters" screen, depending on your system configuration.

On a permanent WAN connection, Business Communications Manager supports the following data compression protocols:

- Frame Relay Forum standard FRF.9 data compression protocol with STAC compression algorithm
- PPP Compression Control Protocol (RFC 1962) with STAC compression algorithm

On dial-up WAN connections, Business Communications Manager supports the following data compression protocol:

- Microsoft Point-to-Point Compression (MPPC), RFC 2118

Viewing WAN resources

To view available WAN resources:

1 On the navigation tree, click the **Resources** key and click the **WAN** heading.
The Resources screen appears.

The Resources screen shows the Name, Status, Version and a Description of the all of the WAN interfaces on the Business Communications Manager.

Note: If you disconnect the WAN cable from the WAN card, the Status does not update immediately. It can take more than two minutes before the Status updates to show the new Status of the WAN card.

Setting global WAN parameters

If PPP is the link protocol for a WAN interface (WAN1 or WAN2), you can restrict access to the network using the PPP Password List. Business Communications Manager uses the information on this list to verify and confirm the identity of the user. Only those users whose names appear on the PPP Password List can access the network. The PPP Password List configuration allows you to add, modify or delete an item on the list.

Configuring the PPP password list

To add an item to the PPP Password List:

1. On the navigation tree, click the **Resources** key and click the **WAN** heading.
   The Resources screen appears.
2. Click the **PPP Password** List tab.
   The PPP Password List screen appears.
3. On the **Configuration** menu, click **Add PPP User&Password**.
   The PPP Password List dialog box appears.
4. Configure the PPP password parameters according to the following table.

Table 200 PPP password parameters

Attribute	Description
(P#)	Enter the PPP Password identifier. The PPP Password number uniquely identifies an PPP User and Password. The value for this setting must follow certain conventions. You must type the prefix 'P' followed by a unique number identifying the PPP User and Password. For example, 'P2' is a valid name. If you specify an existing PPP Password number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The PPP Password number does not have any significance, other than uniquely identifying a PPP User and Password.
PPP User Name	Enter the user name associated with the computer you want Business Communications Manager to identify as a valid network user. You must overwrite the default user name User with the user name you want to add to the list.
PPP Password	Enter the password you want to assign to the user defined in the PPP User Name box. The password can contain a combination of lowercase letters, uppercase letters, numbers and non-alphanumeric characters ($, !, %, ^). **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

5. Click the **Save** button.

Modifying an existing item on the PPP Password List:

1. On the navigation tree, click the **Resources** key and click the **WAN** heading.
   The Resources screen appears.
2. Click the **PPP Password** List tab.
   The PPP Password List screen appears.
3. Click the PPP Password you want to modify.
4. On the **Configuration** menu, click **Modify PPP User&Password**.
   The PPP Password List dialog box appears.
5. Change the PPP password parameters.
6. Click the **Save** button.

Deleting an item from the PPP Password List

1. On the navigation tree, click the **Resources** key and click the **WAN** heading.
   The Resources screen appears.
2. Click the **PPP Password** List tab.
   The PPP Password List screen appears.
3. Click the PPP Password you want to delete.
4. On the **Configuration** menu, click **Delete PPP User&Password**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Configuring the WAN interfaces

The following sections describe how to configure the WAN interfaces on the Business Communications Manager system.

This section includes:

Configuring WAN summary parameters

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Configure the WAN Summary settings according to the information in the following table.

Table 201 WAN summary parameters

Attribute	Description
IP Address	Enter the IP address of the WAN interface. The WAN IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask address of the WAN. The subnet mask IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
Physical Address	Shows the physical address of the WAN interface.
Description	Provides a description of the network interface card that supports the WAN connection.
Port	Shows the port type of the WAN interface.
Version	Shows the version of the WAN interface.
Maximum Link Speed	Shows the operational speed of the WAN interface.
Status	Shows the current resource status of the WAN interface. The possible states are: **Up**: The WAN card is operational. **Down**: The WAN card is not operational.

Table 201 WAN summary parameters (Continued)

Attribute	Description
Link Protocol	Lets you select a WAN link protocol. The options are **Frame Relay** or **PPP** protocol. The default is **Frame Relay**. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**. The link protocol you choose depends on the existing network or the service you buy from your Internet services provider.
Admin Status	Allows you to view and change the Admin Status for this interface. The Admin Status settings determines if the IP address for this interface is included in the routing table. The possible states for Admin Status are: **Up**: The routing table contains entries for this WAN interface. **Down**: The routing table does not contain entries for this WAN interface. The default Admin Status is **Up**. The routing table entries for unused network interfaces can cause routing issues. For this reason, Nortel Networks recommends you disable the Admin Status on any WAN interface that is not connected to the network. To remove the routing table entries for this WAN interface, select **Disable**. If you decide to use a WAN interface that has had the Admin Status disabled, you must enable the Admin Status to add entries for this WAN interface to the routing table. To add routing table entries for this WAN interface, select **Enable**.
Frame Size	Lets you specify the maximum frame size for the layer-2 packet carried on this port. The default is **1500**. **Note**: The Frame Size you enter must be consistent with the maximum frame size that you use use on your network.

4 Press the **TAB** key to save your settings.

Note: Unified Manager refreshes the link protocol screen according to the chosen protocol. Your choice of protocol depends on the existing network or the service you buy from your Internet service provider. Frame relay is the default link protocol. If you change the link protocol the following message appears “Reminder! Previous setting requires rebooting the system to take effect. Please reboot the system...” Click **OK**.

Caution: Reboot the system
You must remember to reboot your system for the changes you made to the link protocol to take effect. You can continue Resources configuration and reboot the system at a convenient time.

Setting WAN Line Parameters

The WAN Line Parameters screen is displayed when configuring a T1 port (North America only). Business Communications Manager supports T1 and fractional T1. Refer to the **Port** box on the WAN Summary Parameters screen to see which type of port your are configuring.

Note: The WAN Line Parameters screen is only available on the WAN1 interface.

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** heading.
   The WAN Summary screen appears.
3. Click the **WAN Line Parameters** tab.
   The WAN Line Parameters screen appears.
4. Configure the WAN Line Parameters according to the information in the following table.

Table 202 WAN line parameters

Attribute	Description
Channel Rate	Lets you set the data transmission rate for each of the DS0 channels in the T1 line. Possible values are **64K** or **56K**. The default value is **64K**.
Clock Source	Lets you set an internal or external T1 clock source. Possible values are **External** or **Internal**. The default value is **External**.
Frame Type	Lets you set the type of framing the T1 line supports. Possible values are **ESF** or **SF(D4)**. The default value is **ESF**. Use the setting your T1 service provider recommends.
Line Coding	Lets you set the type of encoding used in the T1 line. Use the setting your T1 service provider recommends. Possible values are **B8ZS** or **AMI**.
Line Polarity	Lets you set **Normal** or **Inverted** line polarity in the T1 line. Select **Inverted** only if Line Coding is set to **AMI**.
Pulse Density	Lets you control whether the DSU/CSU maintains the minimum level of 1s on the line for AMI encoding. Possible values are **Enabled** or **Disabled**. Default value is **Disabled**.
Channel List	Lets you create a list of T1 channels used when using fractional T1. You can list each channel number or provide a range of numbers separated by a comma or hyphen. The channel list can contain a mix of ranges and individual channel numbers. For example, a valid channel list format is 3,5,6,10-15,18,20-23. To use all the available T1 channels, type **All.** Your T1 service provider can give you this information. Default value is **All**.

Note: Always use the same frame type and line coding method as your service provider.

5 Press the **Tab** key to save the settings.

Setting WAN Sync Parameters

The WAN Sync Parameters screen is only available on the WAN2 interface.

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN2** heading.
The WAN Summary screen appears.

3 Click the **WAN Sync Parameters** tab.
The WAN Sync Parameters screen appears.

4 Configure the WAN Sync Parameters according to the information in the following table.

Table 203 WAN sync parameters

Attribute	Description
Clock Mode	Lets you choose the clock mode. The possible values DTE, DCE or Symmetrical.
DTE Configuration	This setting is only available if you choose DTE as the Clock Mode. This setting lets you select the DTE Configuration. The possible values are Simple/spoke or Hub. The default value is **Simple/spoke**.
Clock Rate	This setting is only available if you choose Symmetrical as the Clock Mode. This setting lets you select the clock rate used. The default value is **1000000**.

5 Press the **Tab** key to save the settings.

Setting WAN Frame Relay Parameters

If you chose frame relay as your link protocol, set the WAN Frame Relay Parameters.

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **WAN Frame Relay Parameters** tab.
The WAN Frame Relay Parameters screen appears.

4 Configure the WAN Frame Relay Parameters by referring to the following table.

Table 204 WAN frame relay parameters

Attribute	Description
LMI Type	Select the type of local management protocol used on this link. The link management type must be the same as the one used by the frame relay service provider. The available options are **Original LMI, ANSI T1.617 Annex D** or **ITU-T Q.933 Annex A**. The default setting is **Original LMI**. **Note**: The most commonly used setting for this parameter is **ANSI T1.617 Annex D**.
Polling Interval	Enter an interval, in seconds, between LMI status inquiry messages. The polling interval must be the same as the one used by the frame relay service provider's switch. Possible values are between **5** and **30** seconds. The default setting is **10**.
Full Enquiry Interval	Enter the maximum number of LMI Status Enquiry messages sent before sending a Full Status Enquiry request. This value must match the corresponding value set in the frame relay service provider's switch. Possible values are between **1** and **255** (in seconds). The default setting is **6**.
Error Threshold	Enter the maximum number of consecutive failures permitted in LMI Status Enquiry before dropping the link. It is also the number of successful consecutive LMI Status Enquiry messages that must be received before marking a link as operational. If you have a backup WAN connection and Net Link Manager configured, the backup connection is started and traffic is routed to the backup when this link is dropped. Also, the backup WAN connection is dropped and traffic is routed to this link when the link is operational. For information about Net Link Manager, refer to "Configuring Net Link Manager" on page 749. Possible values are between **0** and **65000**. The default value is **3**.
Monitored Events	Enter the number of events sampled for making decisions about the error threshold. This value must be set to a higher number than the value set in the **Error Threshold** box. Possible values are a number between **0** and **65000**. The default value is **4**.
DS Code	Enter the Differentiated Services code (DSCode) recognized by the frame relay driver for traffic prioritization. This value is a mask value. When an IP packet is sent, the frame relay driver checks if the packet's DSCode field (in the IP header) has any of the bits defined in the **DS Code** and sets the Discard Eligible (DE) bits to No.
Available PVCs	Shows the PVCs (Permanent Virtual Circuits) available for this WAN interface.
Compression Enabled PVCs	Enter a list of PVCs on which data compression is enabled. The value can be a comma-separated list of DLCI (Data Link Connection Identifier) numbers. You can define a range of DLCIs by inserting a hyphen between the lower and the upper boundaries. A list can contain individual DLCI numbers and DLCI ranges. If data compression is enabled, compression and decompression operations are performed on the data going to and coming from the PVCs on this list.
Access Rate	Enter the maximum access rate on the interface running frame relay in kbps. The frame relay congestion control engine uses this value to limit or shape traffic. The **Access Rate** value is determined using the T1 channels available for data communication on the port attached to this interface and their data rates.

5 Press the **Tab** key to save the settings.

PVC Congestion Control

If frame relay is your link protocol, you must configure PVC Congestion Control. If PPP is your link protocol, there are no PVC Congestion Control settings to configure.

Adding PVC congestion control

Follow these steps to add a PVC congestion control:

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **PVC Congestion Control** tab.
   The PVC Congestion Control screen appears.
4. On the **Configuration** menu, click **Add PVC Congestion Control**.
5. Configure the WAN PVC Congestion Control parameters according to the information in the following table.

Table 205 WAN PVC congestion control parameters

Column	Description
Entry (CC#)	Define each congestion control entry on the interface. A congestion control entry must use the following format: CC#, where the prefix 'CC' is followed by a number. For example, 'CC2' is a valid congestion control entry. Each entry must use a different number. You must use consecutive numbers when entering congestion control entries. If you do not use consecutive numbers, the system adjusts them to be consecutive. If you add an existing entry, the existing entry is modified with new values. When you modify an entry, the name cannot be changed.
DLCI	Enter the data link connection identifier (DLCI) number of the PVC on which to perform congestion control. A DLCI must be configured for congestion control to be performed. Business Communications Manager uses one-second intervals to measure this parameter.
CIR	Enter the committed information rate in kbits. The CIR is the rate the carrier guarantees that the router transmits at over a predetermined time interval when congestion is not present. Contact your service provider for the correct setting. Business Communications Manager uses one-second intervals to measure this parameter.
Committed Burst BC	Lets you define the number of bits, in kbits, the router transmits over a specified time interval if congestion is present. As a rule this value is set for 1/4 the value of the CIR. Business Communications Manager uses one-second intervals to measure this parameter.
Excess Burst BE	Combined with the committed burst rate, lets you set, in kbits, the maximum number of bits the router transmits over a predetermined time interval if there is no congestion. The combined value of committed burst and excess burst must be less than or equal to the line speed.

6. Click the **Save** button.

Modifying PVC congestion controls

Follow these steps to modify a PVC congestion control setting:

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **PVC Congestion Control** tab.
   The PVC Congestion Control screen appears.
4. Click the entry you want to modify in the PVC Congestion Control table
5. On the **Configuration** menu, click **Modify PVC Congestion Control**.
   The PVC Congestion Control dialog box appears.
6. Change the PVC congestion control parameters.
7. Click the **Save** button.

Deleting a PVC congestion control

Follow these steps to delete a PVC congestion control setting.

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **PVC Congestion Control** tab.
   The PVC Congestion Control screen appears.
4. Click the entry you want to delete in the PVC Congestion Control table.
5. On the **Configuration** menu, click **Delete PVC Congestion Control**.
   A message prompts you to confirm the deletion.
6. Click the **Yes** button.

WAN PPP Parameters

If you chose PPP as your link protocol, set the WAN PPP Parameters screen.

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **WAN PPP Parameters** tab.
   The WAN PPP Parameters screen appears.

4 Configure the WAN PPP Parameters according to the information in the following table.

Table 206 WAN PPP parameters

Attribute	Description
LCP Keep Alive Interval	Enter the interval, in seconds, to send a keep alive signal when there is no regular traffic on the PPP link. The default value is **10**.
LQR Interval	Enter the interval, in 1/100 second, to perform link quality monitoring.
Authentication Mode	Specify the Authentication mode a remote user can use. You can select **PAP or CHAP**, **CHAP only**, or **None**. Select CHAP only to restrict the remote user to using CHAP authentication. Select PAP or CHAP to allow the remote user to use PAP or CHAP authentication. Select None to allow the remote user to access the system without using authentication. **Note**: If you select **CHAP only** or **PAP or CHAP**, you must select **UserName-Password** for the **Outgoing Authentication** box.
Outgoing Authentication	Select the type of authentication information that is sent to the far end of the PPP connection. You can select **ComputerName-Password** or **UserName-Password**. Selecting **ComputerName-Password** will send the name of the Business Communications Manager and the password you enter below. Selecting **UserName-Password** will send the user name and password you enter below. **Note**: If you select **ComputerName-Password**, you must select **None** for the **Authentication Mode**.
User Name	Enter the user name that is used for authentication by the far end of the PPP connection.
Password	Enter the password that is used for authentication by the far end of the PPP connection. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.
Compression	Lets you enable or disable data compression over this PPP link. The possible values are: **Enabled**, **Disabled** The default is **Disabled**.

5 Press the **Tab** key to save your settings.

Configuring multiple IP addresses for a WAN interface

You can assign multiple IP addresses to a single WAN interface that is configured to use frame relay. Using this functionality, you can configure the Business Communications Manager as the hub in a hub and spoke configuration. When Business Communications Manager is the hub or central site, Business Communications Manager can provide at least two IP address classes on the primary WAN interface. This allows the system to provide Direct Mode capability.

Examples of uses of multiple IP addresses

- You can use a single WAN physical link to connect to both an intranet and the internet using separate addressing schemes.
- A network service provider can create a separate IP address for management functions over the WAN interface.

In both of these examples, broadcast traffic destined for one IP address would not be transmitted on the links associated with the other IP address.

Restrictions when using multiple IP addresses

- Nortel Networks does not recommend using more than two IP address classes.
- Multiple IP addresses supports RIP routing.
- IPSec does not support the use of these multiple IP addresses for Branch Office Local Endpoint Addresses, Remote Endpoint Addresses or the Destination IP Address for IPSec VPN Clients

Adding an additional IP address

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. On the **Configuration** menu, click **Add Additional IPAddress**.
   The Additional IP Address screen appears.
5. Configure the Additional IP Address parameters with the information in the following table.

Table 207 Additional WAN IP addresses

Attribute	Description
Range (A#)	Enter the Additional IP Address identifier. The Range number uniquely identifies an Additional IP Address. The value for this setting must follow certain conventions. You must type the prefix 'A' followed by a unique number identifying the Additional IP Address. For example, 'A2' is a valid name. If you specify an existing Range number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Range number does not have any significance, other than uniquely identifying an Additional IP Address.

Table 207 Additional WAN IP addresses (Continued)

Attribute	Description
IP Address	Enter the Additional IP address of the WAN interface in the following format: 255.255.255.255.
SubNet Mask	Enter the subnet mask of the WAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your system administrator or your Internet service provider.

6 Click the **Save** button.

Modifying an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **WAN** key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to modify.

5 On the **Configuration** menu, click **Modify Additional IPAddress**.
The Additional IP Address screen appears.

6 Change the Additional IP Address parameters.

7 Click the **Save** button.

Deleting an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **WAN** key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to delete.

5 On the **Configuration** menu, click **Delete Additional IPAddress**.
A confirmation dialog box appears.

6 Click the **Yes** button.

Configuring the DLCI to IP Mapping

When connected to a Frame Relay network, Business Communications Manager uses Frame Relay INARP (Inverse Address Resolution Protocol) messaging to request the next hop protocol address for a given DLCI. If the other end of the connection does not support INARP messaging, there can be a communication failure because the mapping of which DLCI to use to reach a particular IP address is not known.

The DLCI to IP Mapping feature solves this problem by providing static address mapping of the DLCI to remote IP address.

Note: DLCI to IP Mapping feature is available only on the WAN1 and WAN2 interfaces. This feature is not available on the UTWAN interface.

Adding DLCI to IP Mapping

You can add up to 32 DLCI to IP Mapping entries.

To add a DLCI to IP Mapping entry:

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **DLCI to IP Mapping** tab.
   The DLCI to IP Mapping screen appears.
4. On the **Configuration** menu, click **Add DLCI to IP Mapping**.
   The DLCI to IP Mapping dialog box appears.
5. Configure the DLCI to IP Mapping parameters using the information in the following table.

Table 208 DLCI to IP Mapping parameters

Attribute	Description
Index (I#)	This parameter identifies the DLCI to IP Mapping entry. This is a read only parameter.
Local IP	Enter the IP address used for the local end of this connection. The IP address you enter must be one of the IP address assigned to this WAN interface. You must enter the IP address in standard decimal format (for example 10.10.10.1).
DLCI	Enter the Data Link Connection Identifier (DLCI) number for this interface. You can enter a value from 0 to 1024.
Remote IP	Enter the IP address used for remote end of this connection. You must enter the IP address in standard decimal format (for example 10.10.10.1).

6. Click the **Save** button.

Modifying DLCI to IP Mapping

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **DLCI to IP Mapping** tab.
   The DLCI to IP Mapping screen appears.
4. Click the DLCI to IP Mapping entry you want to modify.
5. On the **Configuration** menu, click **Modify DLCI to IP Mapping**.
   The DLCI to IP Mapping dialog box appears.
6. Change the DLCI to IP Mapping parameters.
7. Click the **Save** button.

Deleting DLCI to IP Mapping

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **DLCI to IP Mapping** tab.
   The DLCI to IP Mapping screen appears.
4. Click the DLCI to IP Mapping you want to delete.
5. On the **Configuration** menu, click **Delete DLCI to IP Mapping**.
   A confirmation dialog box appears.
6. Click the **Yes** button.

WAN performance

To access the WAN Primary Link performance graphs and tables for a particular WAN interface:

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. On the **Performance** menu, click **WAN Graph**.
   The WAN Graph: Statistic Chart appears.
4. On the **Performance** menu, click **WAN Table**.
   The WAN Table: Statistic Table appears.

Chapter 31
Configuring the Dial Up resources

Business Communications Manager allows you to create and use dial up connections for Remote Access Service (RAS) or dial-on-demand network access. RAS allows you to access Business Communications Managers remotely by making an IP connection using PPPoE, an ISDN BRI/PRI line, PPTP or the V.90 modem (North America only). After you connect to the Business Communications Manager system, you can access all IP-based system management operations.

Business Communications Manager also supports dial-on-demand for primary and backup WAN connections. Primary and backup WAN connections can use an ISDN BRI/PRI line or a V.90 modem (North America).

This section includes information about:

Configuring the dial up global parameters

1 On the navigation tree, click the **Resources** key and click the **Dial Up** heading.
The RAS Server TCP/IP Configuration screen appears.

2 Configure the RAS Server TCP/IP settings according to the information in the following table.

Table 209 RAS server TCP/IP parameters

Attribute	Description
Allow Network Access	Select whether to allow dial up access to the entire network (**Yes**) or to restrict access to Business Communications Manager only (**No**). When using dial up for dial-on-demand WAN connection (as a primary or back up WAN connection), set **Allow Network Access** to **Yes**. When using dial up for remote system management purposes only, set **Allow Network Access** to **No**.
Static IP Address Pool	Enter the IP address Business Communications Manager assigns when a remote site dials into the Business Communications Manager system. The default value is **10.10.14.0**
Address Mask	Enter the IP address mask corresponding to the IP address range. The IP addresses from the static address pool then reserved for assignment to remote sites. The default value is **255.255.255.224**.

3 Press the **TAB** key to save your settings.

V.90 modem (North America) dial up

Business Communications Manager is equipped with an internal V.90 modem that connects to your phone line with a RJ-11 connector. The V.90 modem has the following features:

- V.90 56 kbps ITU standard
- V.34 33.6 kbps ITU standard
- V.42/MNP 2-4 error control
- V.42 bis/MNP 5 data compression
- compatible with ITU and Bell Standards from 56 kbps down to 1200 bps

Note: The modem is capable of receiving at a maximum speed of 56 kbps and transmitting at a maximum speed of 31.2 kbps. Because of FCC regulations, receiving speed is limited to 53 kbps. Current line noise can impact the speed of the modem.

The V.90 modem WAN connection always uses PPP as the link layer protocol. For correct operation, the link must be connected to a remote access server (RAS).

Business Communications Manager supports the following authentication features:

- Password Authentication Protocol (PAP)
- Challenge Authentication Protocol (CHAP)

The information in this section includes:

- "Enabling and disabling the V.90 modem interface"
- "Configuring the V.90 modem interface"

Enabling and disabling the V.90 modem interface

If you want to the use the V.90 modem as a backup WAN connection or as interface to send SNMP traps to the SNMP Manager, you must enable the V.90 modem interface.

If you are not using the V.90 modem interface for WAN backup or SNMP traps, Nortel Networks recommends that you disable the modem to help prevent unauthorized access to the Business Communications Manager.

To enable the V.90 modem interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **V.90** heading.
3. Click the **Modem Status** drop list and click **Enabled**.
4. Press the **TAB** key to save the settings.

To disable the V.90 modem interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **V.90** heading.
3. Click the **Modem Status** drop list and click **Disabled**.
4. Press the **TAB** key to save the settings.

Configuring the V.90 modem interface

The V.90 modem is used for WAN backup connection.

Tips

Remember to set Dial Up global parameters before creating modem dial up interfaces. For information about setting Dial Up global parameters, see "Configuring the dial up global parameters" on page 685.

The same modem may be shared between the remote dial-in for system administration and the backup WAN link. The WAN backup function is not available if a break in the WAN permanent connection occurs while a system administrator is connected to Business Communications Manager using the V.90 modem.

To configure the V.90 modem interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **V.90** key to see available modem interfaces.
3. Click the **ModemBackup** heading if you want to configure the interface used for the backup WAN connection.
   Click the **ModemTrapDialOut** heading if you want to configure the interface used for sending SNMP trap messages to the SNMP Manager.
   The V.90 Summary screen appears.
4. Configure the V.90 Summary parameters according to the information in the following table.

Table 210 V.90 modem summary parameters

Attribute	Description
Interface	Shows the name of the modem interface selected.
IP Address	Enter the IP address of the modem interface when it connects. Users can set a fixed IP address for the dial-up interface. If a fixed address is specified, Business Communications Manager uses the address on the receiving end. Users can select **RemoteAssigned** to indicate that Business Communications Manager must obtain an IP address from the remote end and use it. The address obtained depends on the RAS server to which Business Communications Manager connects. The default value is **RemoteAssigned**.
Description	Shows a description of the interface.
Version	Shows the version of the modem subsystem.

Table 210 V.90 modem summary parameters (Continued)

Attribute	Description
Status	View the modem interface resource status and enable or disable the modem interface. The possible states are: **Connect**: The modem is enabled and the dial-up link is currently active. **Disconnect**: The modem interface is enabled and the dial-up link is currently disconnected. **Enabled**: The modem interface is enabled for use. **Disabled**: The modem interface is disabled.

5 Press the **Tab** key to save the settings.

6 Click the **V.90 Link Parameters** tab.
The V.90 Link Parameters screen appears.

7 Configure the Modem Link Parameters according to the information in the following table.

Table 211 Modem link parameters

Attribute	Description
Telephone Number	Lets you type a telephone number to use to connect using the modem interface. If needed, include area codes and all necessary digits to dial an external number.
Alternate Telephone Number	Lets you type an alternate number to use to connect using the modem interface. Include area codes and all necessary digits to dial an external number.
Connect Rate	Lets you specify the initial speed (in bits per second) for the modem to connect. Set to the maximum permissible value for best results. Permitted values: 57600, 38400, 19200, 9600, 4800. **Note**: This is the initial rate; the actual rate is always negotiated.
Dial Retries	Lets you set the number of attempts the system must make when trying to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Lets you set the interval, in seconds, between successive connection attempts. The default value is **60**.
Number Of Rings	Lets you specify the number of rings the Business Communications Manager waits before determining that the far end of the connection is not answering. The default value is **1**.
Speaker Mode	Lets you enable or disable the speaker during initial link establishment.
IP Header Compression	Lets you enable or disable IP header compression. To function, the receiving end must also use this feature.
Software Compression	Lets you enable or disable data compression in the software, instead of the modem. For dial-up connections, Unified Manager uses Microsoft Point-to-Point Compression algorithm (MPPC).
Hardware Compression	Lets you enable or disable data compression in the hardware instead of the software.

Table 211 Modem link parameters (Continued)

Attribute	Description
PPP LCP Extensions	Lets you enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Enter the interval, in seconds, during which the modem interface disconnects when there is no traffic. Select **0** if you want the Business Communications Manager to close the connection when the far end hangs up. Select **PersistentConnection** if this connection is intended to always be connected. **Note**: If you have more than one Trap Community Entry configured with this dial up interface, using a very small number for the Disconnect Time will put you at risk of a racing condition. To reduce the racing condition, enter a larger value for the Disconnect Time.

8 Press the **TAB** key to save the settings.

9 Click the **V.90 Access Parameters** tab.
The V.90 Access Parameters screen appears.

10 Configure the V.90 Modem Access Parameters according to the information in the following table.

Table 212 V.90 modem access parameters

Attribute	Description
Authentication	Lets you select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: The CHAP is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: Only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Lets you enable or disable link authentication in both directions. The default value is **Disabled**.
User Name	Lets you define a user name that the link uses to authenticate itself when dialing out to another router.
User Password	Lets you define a password that the link uses to authenticate itself when dialing out to another router. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

11 Press the **TAB** key to save the settings.

ISDN dial up

Business Communications Manager supports ISDN dial up for dial-on-demand WAN access. You have the choice to use ISDN BRI/PRI as a persistent or dial-on-demand WAN connection or as a backup for your permanent WAN connection.

Tips

To use an ISDN dial-up connection, you must first configure your system for ISDN. For more information, refer to Appendix C, "ISDN overview," on page 869. If your system is already configured to support ISDN, make sure you configure a Data Module for ISDN dial up connection. For more information, see "Configuring a data module" on page 178.

After you have created an ISDN dial up interface, you must use "Configuring Net Link Manager" on page 749 to select which type of network connection the system must use for primary and backup connection.

The information in this section includes:

Creating an ISDN dial up interface

1. On the navigation tree, click the **Resources** key, and click the **Dial Up** key.
2. Click the **ISDN** heading.
3. Click the **Add** button.
   Or, right click the **ISDN** heading and click **Add**.
   The Add ISDN dialog box appears.
4. In the **(Dial In) Name** box, type the name of the interface you are creating.
   This is the name a dial in user must enter to access this interface.

Caution:
If you are creating an ISDN interface to use as a backup for a permanent WAN connection, the **(Dial In) Name** must contain the string "backup". For example, "ISDNbackup" is a valid name if you want to use an ISDN connection as a WAN backup connection.

5. In the **Password** box, type a password.
   This is the password a dial in user must enter to access this interface.

Note: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

6 In the **Confirm Password** box, type the password again.

7 In the **Channel** list, select the channel the connection must use.

8 Click **Save** to save your settings.
The newly created ISDN interface appears under **ISDN**.

Configuring an ISDN interface

To configure an ISDN interface:

1 On the navigation tree, click the **Resources** key and click the **Dial Up** key.

2 Click the **ISDN** key and click on the interface you want to configure.
The ISDN Summary screen appears.

3 Configure the ISDN Summary settings according to the information in the following table.

Table 213 ISDN summary settings

Attribute	Description
Interface	Shows the name of the ISDN interface selected.
IPAddress	Enter the IP address of the ISDN interface when it connects. You can set a fixed IP address for the dial-up interface or you can select **RemoteAssigned** to indicate that Business Communications Manager must obtain an IP address from the remote end. The address obtained depends on the RAS server to which Business Communications Manager connects. The default value is **RemoteAssigned**. **Callback note:** If you want to use secure callback with this interface, enter an IP address. For information about setting up callback, refer to "Managing access passwords" on page 109.
Description	Enter a description of the interface.
Version	Show the version number of the interface.
Status	Lets you view and set the ISDN interface resource status. Possible values are: **Connect**: The ISDN interface is currently connected. Also used to force the interface to initiate a connection. **Disconnect**: The ISDN interface is not currently connected. **Enabled**: The ISDN interface is enabled for use. **Disabled**: The ISDN interface is disabled.

Tip

You cannot select an ISDN interface that is set to "RemoteAssigned" as the Local Gateway IP for the VoIP Gateway.

4 Press the **TAB** key to save the settings.

5 Click the **ISDN Link Parameters** tab.
The ISDN Link Parameters screen appears.

6 Configure the ISDN Link Parameters according to the information in the following table.

Table 214 ISDN link parameters

Attribute	Description
Dial Retries	Enter the number of times the systems attempts to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Enter the interval, in seconds, between connection attempts. The default value is **60**.
IP Header Compression	Enable or disable IP header compression. The feature must be enable at both ends of the connection. The default value is **Enabled**.
Software Compression	Enable or disable software compression. When enabled, all dial-up connections use Microsoft Point-to-Point Compression (MPPC). The default value is **Disabled**.
PPP LCP Extensions	Enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Enter the interval, in seconds, during which the ISDN interface disconnects when there is no traffic. If you select **PersistentConnection**, the ISDN interface will not disconnect. **Note**: If you have more than one Trap Community Entry configured with this dial up interface, using a very small number for the Disconnect Time will put you at risk of a racing condition. To reduce the racing condition, enter a larger value for the Disconnect Time.
DNS Address 1	Enter the IP address of the Primary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server. **Note**: If you select **NoNameServerAddressesUsed**, this setting is automatically set in DNS Address 2 box.
DNS Address 2	Enter the IP address of the Secondary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server.
Protocol	Select the protocol that this ISDN interface uses. You can choose **TCP/IP**, **IPX** or **Both**.

7 Press the **TAB** key to save the settings.

8 Click the **ISDN Access Parameters** tab.
The ISDN Access Parameters screen appears.

9 Configure the ISDN Access Parameters according to the information in the following table.

Table 215 ISDN access parameters

Attribute	Description
Authentication	Select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: When selected, the CHAP is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: When selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Enable or disable link authentication in both directions. The default value is **Disabled**.

10 Press the **TAB** key to save the settings.

11 Click the **ISDN Dial-Out User** tab.
The ISDN Dial-out User screen appears.

12 On the **Configuration** menu, click **Modify ISDN Dial-out User**.

13 Configure the ISDN Dial-out User parameters using the information in the following table.

Table 216 ISDN dial-out user parameters

Attribute	Description
User Name	Enter the user name that the link must use to authenticate itself when dialing out to another router.
Password	Enter the password that the link must use to authenticate itself when dialing out to another router. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

14 Click the **Save** button.

15 Click the **ISDN Channel Characteristics** tab.
The ISDN Channel Characteristics screen appears.

Configuring the ISDN channel characteristics

To add an ISDN channel to the ISDN Channel Characteristics list

1 On the **Configuration** menu, click **Add ISDN Channel.**
The ISDN Channel Characteristics screen appears.

2 Configure the ISDN Channel Characteristic according to the information in the following table.

Table 217 ISDN channel characteristics

Attribute	Description
Row (R#)	Identifies the number of the item in the ISDN channel list.
Port	Select one of the ISDN ports. There are 16 ISDN ports available, named ISDN1 to ISDN16.
Phone1	Enter the primary phone number to use to make an ISDN connection. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain only numerical digits only (no alphabetical or other characters are allowed).
Phone2	Enter an alternate phone number to use to make the ISDN connection. Include all required area codes and all necessary digits to dial an external number. The phone number must contain numerical digits only (no alphabetical or other characters are allowed). If Phone1 dialing fails, and you have specified a number for Phone2, Business Communications Manager will attempt to dial Phone2. **Exception note**: If you have two phone numbers for two different data centers with two distinct IP subnets, you cannot use a local assigned IP address. Instead, use the remote assigned IP option with the correct NetLink Manager setup to route the calls properly.

Table 217 ISDN channel characteristics (Continued)

Attribute	Description
Line Type	Select either a 64K Digital or 56K Digital line. Business Communications Manager ISDN supports two types of Unrestricted Digital Information (UDI) bit streams: UDI, and UDI-56. With UDI, data is transmitted at 64kbps (64K Digital). With UDI-56, a 1 bit is inserted in the eighth bit position of each B-channel time slot while the other 7 bits form the 56kbps channel (56K Digital).
Negotiate Line Type	Choose whether or not the system will select a line with a slower speed if it is unable to connect at the previously set speed. You can choose Yes or No. The default value is Yes

3 Click the Save button.

Assigning an ISDN dial number and IP address

With an ISDN demand-dial interface, you can bundle more than one ISDN channel to increase the throughput. This is referred to as multi-link support.

With each ISDN channel configuration, you can choose to configure a primary dial number (Phone1), and a backup dial number (Phone2). However, you are not allowed to assign different IP addresses for the different phone numbers you are dialing. The main reason behind this restriction is, with multi-link, even if you can reach your destination via different phone numbers, once your ISDN pipe is established, there is only one source and one destination from the IP-layer.

If you assign Phone1 to reach Site A and Phone2 to reach Site B, and Site A and Site B belong to different subnets, the pre-assigned IP address scheme will not work. In this scenario, you must use the Remote Assigned IP address option, and let NetLink Manager take care of the default route for you. For information about setting the IP Address to the RemoteAssigned, refer to "Configuring an ISDN interface" on page 691. For information about configuring Net Link Manager, refer to "Configuring Net Link Manager" on page 749.

Modifying the characteristics of an existing ISDN channel

1 Click the ISDN Channel Characteristic you want to modify.

2 On the **Configuration** menu, click **Modify ISDN Channel.**
The ISDN Channel Characteristics screen appears.

3 Make the necessary changes.

4 Click the **Save** button to save your settings.

Deleting an ISDN channel from the ISDN Channel Characteristics list

1 Click the ISDN Channel Characteristic you want to delete.

2 On the **Configuration** menu, select **Delete ISDN Channel.**
A confirmation dialog box appears.

3 Click the **Yes** button.

Deleting an ISDN interface

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **ISDN** key.
3. Click the heading of the ISDN interface you want to delete.
4. Click the **Delete** button. Or, right click the ISDN interface heading and click **Delete**. A confirmation dialog box appears.
5. Click **Yes**.

Point to Point Protocol on Ethernet (PPPoE)

The information in this section includes:

PPPoE is the protocol Business Communications Manager uses when connecting to a data network using a broadband modem. Digital Subscriber Line (DSL) modems and cable modems are examples of broadband modems.

When the Business Communications Manager uses a PPPoE connection, the Internet Service Provider (ISP) can control access, billing and other types of service on a per-user, rather than a per-site basis.

Settings required for PPPoE

The data packets that pass through the PPPoE connection interact with other routing features in Business Communications Manager. As a result, there are several settings you must make in other features so those features can use the PPPoE connection.

Note: To use PPPoE, you must have a Business Communications Manager system that has two LAN cards.

Table 218 Features that interact with PPPoE

Feature	Description of interaction
LAN interfaces	When you install PPPoE, the LAN1 interface is dedicated to PPPoE. You must not use the LAN1 interface for any other purpose.
IPSec Tunnels	To use IPSec tunnels over the PPPoE interface, Business Communications Manager requires a single known IP address be assigned to the PPPoE interface. If your Internet Service Provider uses DHCP to assign the IP addresses, the DHCP server must assign the same IP address to the PPPoE interface every time Business Communications Manager connects.
Internet Clients	Clients who want to use the Business Communications Manager PPPoE interface to access the internet must set their MTU size to a value less than or equal to 1480 bytes, but not less than 1400 bytes.
Software Keycode	You must purchase and install the PPPoE Software keycode before you can install PPPoE. For information about purchasing the PPPoE Software Keycode, contact your Nortel Networks representative. For information about how to install the PPPoE Software Keycode, refer to the Software Keycode Installation Guide that comes with your Software Keycode.

Installing PPPoE

You must install PPPoE before you can add or configure a PPPoE interface.

Note: To install PPPoE, the computer you are using to access the PPPoE Install Wizard must be connected to the LAN1 interface of Business Communications Manager.

To install PPPoE:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address.
   For example: *HTTPS://10.10.10.1*
   The Business Communications Manager Unified Manager initial page appears.

   Note: You must include **HTTPS://** with the address to access Unified Manager when you are using Internet Explorer as your browser.

3. Click the **Maintenance** button.
   The Network Password screen appears.
4. In the **User Name** box, type the system administrator user name.
5. In the **Password** box, type the system administrator password.
6. Click the **OK** button.
   The Product Maintenance & Support screen appears.
7. Click the **Install Optional Components** link.
   The Install Optional Components screen appears.
8. Click the **PPPoE** link.
   The PPPoE install wizard starts.
9. Follow the prompts on the screen to install PPPoE.
   The PPPoE install wizard consists of three steps. Business Communications Manager reboots after each step.
   It takes 10 to 15 minutes to install PPPoE.

Creating a PPPoE dial up interface

1. On the navigation tree, click the **Resources** key, and click the **Dial Up** key.
2. Click the **PPPoE** heading.
3. Click the **Add** button.
   Or, right click the **PPPoE** heading and click **Add**.
   The Add PPPoE dialog box appears.
4. In the **Name** box, type the name of the interface you are creating.

Note: The Password box and the Confirm Password box are optional fields. You do not need to enter information in these boxes to add a PPPoE interface.

The Interface box is a read only field that shows the interface that connects to the broadband modem.

5. Click **Save** to save your settings.
   The newly created PPPoE interface appears under **PPPoE**.

Configuring a PPPoE interface

To configure a PPPoE interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **PPPoE** key and click on the interface you want to configure.
   The PPPoE Summary screen appears.
3. Configure the PPPoE Summary settings according to the information in the following table.

Table 219 PPPoE summary settings

Attribute	Description
Interface	Shows the name of the PPPoE interface selected.
IPAddress	Shows how Business Communications Manager obtains an IP address. **RemoteAssigned** indicates that Business Communications Manager obtains an IP address from the remote end.
Description	Enter a description of the interface.
Version	Shows the version number of the interface.
Status	Lets you view and set the PPPoE interface status. Possible values are: **Connect**: The PPPoE interface is connected to the ISP **Disconnect**: The PPPoE interface is not connected to the ISP. **Note**: Do not set the PPPoE interface status to Connect until after you have configured the PPPoE interface.

4. Press the **TAB** key to save the settings.
5. Click the **PPPoE Link Parameters** tab.
   The PPPoE Link Parameters screen appears.

6 Configure the PPPoE Link Parameters according to the information in the following table.

Table 220 PPPoE link parameters

Attribute	Description
Dial Retries	Enter the number of times the system attempts to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Enter the interval, in seconds, between connection attempts. The default value is **60**.
IP Header Compression	Enable or disable IP header compression. The feature must be enable at both ends of the connection. The default value is **Enabled**.
Software Compression	Enable or disable software compression. When enabled, all dial-up connections use Microsoft Point-to-Point Compression (MPPC). The default value is **Enabled**.
PPP LCP Extensions	Enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Shows the interval, in seconds, after which the PPPoE interface disconnects when there is no traffic. The Disconnect Time is set to **PersistentConnection** which means the PPPoE interface will not disconnect.
DNS Address 1	Enter the IP address of the Primary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server. **Note**: If you select **NoNameServerAddressesUsed**, this setting is automatically set in DNS Address 2 box.
DNS Address 2	Enter the IP address of the Secondary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server.
Protocol	Select the protocol that this PPPoE interface uses. You can choose **TCP/IP**.

7 Press the **TAB** key to save the settings.

8 Click the **PPPoE Access Parameters** tab.
The PPPoE Access Parameters screen appears.

9 Configure the PPPoE Access Parameters according to information in the following table.

Table 221 PPPoE access parameters

Attribute	Description
Authentication	Select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: When selected, the CHAP is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: When selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Enable or disable link authentication in both directions. The default value is **Disabled**.

10 Press the **TAB** key to save the settings.

11 Click the **PPPoE Dial-Out User** tab.
The PPPoE Dial-out User screen appears.

12 Click the PPPoE Dial-out User you want to modify.

13 On the **Configuration** menu, click **Modify PPPoE Dial-out User**.

14 Configure the PPPoE Dial-out User parameters according to the information in the following table.

Table 222 PPPoE dial-out user parameters

Attribute	Description
User Name	Enter the user name that the link must use to authenticate itself when dialing out to the ISP.
Password	Enter the password that the link must use to authenticate itself when dialing out to the ISP. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

15 Click the **Save** button.

16 Click the **PPPoE Channel Characteristics** tab.
The PPPoE Channel Characteristics screen appears.

17 Configure the PPPoE Channel Characteristic according to the information in the following table.

Table 223 PPPoE channel characteristics

Attribute	Description
Row (R#)	Identifies the number of the item in the PPPoE channel list.
Port	Shows the channel selected for this PPPoE interface. The channel shown here is the channel you selected when you created the PPPoE interface.

After you configure PPPoE, make sure that your broadband modem is powered up and connected to the LAN1 interface.

Connecting to the Internet Service Provider (ISP)

After you have configured the PPPoE interface you need to connect the PPPoE interface to the ISP.

To connect to the ISP:

1 On the navigation tree, click the **Resources** key and click the **Dial Up** key.

2 Click the **PPPoE** key and click on the interface you want to connect to the ISP.
The PPPoE Summary screen appears.

3 Click the **Status** box and then click **Connect**.

Deleting a PPPoE interface

To delete a PPPoE interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **PPPoE** key.
3. Click the heading of the PPPoE interface you want to delete.
4. Click the **Delete** button.
   Or, right click the PPPoE interface heading and click **Delete**.
   A confirmation dialog box appears.
5. Click **Yes**.

Guidelines for using Remote Dial-in

Consider the following guidelines when using remote dial-in:

- The remote dial-in for administration and the backup WAN link share the same modem. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using the back-up interface, Business Communications Manager always calls. Business Communications Manager does not answer an incoming call from a router on the V.90 interface.
- If you are using the remote dial-in for maintenance, Nortel Networks recommends that you use the Preinstall Client Access Home Page to access Business Communications Manager.

Chapter 32
Configuring DNS

Business Communications Manager functions as both a gateway to the Internet and as a DNS proxy.

Note: If your PC is a DHCP client under Business Communications Manager, you do not have to let your workstations know that Business Communications Manager is your Internet gateway.

When Business Communications Manager receives DNS requests from clients, it first checks its local cache for name entries and records. If found locally, Business Communications Manager immediately responds to clients. Otherwise, Business Communications Manager creates a new DNS request to the remote Primary or Secondary DNS servers on behalf of the client. If the remote DNS server responds with the requested records, they are forwarded to clients and cached in Business Communications Manager. By caching the DNS requests, the DNS proxy service on Business Communications Manager reduces the number of external DNS requests and thus reduces the amount of WAN traffic.

The DNS proxy service also provides additional security. When DNS requests are sent to the Primary or Secondary DNS servers, the Business Communications Manager internal IP address is used for the request. By using the Business Communications Manager IP address, the IP addresses of the internal users can remain hidden.

Note: If you use the Quick Install Wizard, DNS proxy is enabled by the wizard.

Using the Business Communications Manager DNS service

Consider the following guidelines when using DNS:

- If you enable the Business Communications Manager DNS service, ensure that you configure each workstation on the network to use Business Communications Manager as DNS server.
- When you disable Business Communications Manager DNS service, set the DNS Server field in DHCP configuration to the remote DNS server IP address. If DHCP service is also disabled in Business Communications Manager, you must configure each workstation on your network to use the remote DNS server.

To configure DNS services settings

1 On the navigation tree, click the **Services** key and click the **DNS** heading.
The DNS Summary screen appears.

2 Configure the DNS Summary attributes according to the following table.

Table 224 DNS Summary attributes

Attribute	Description
Description	Allows you to view the description of the DNS server.
Version	Allows you to view the version of the DNS service.
Status	Allows you to enable or disable the DNS cache proxy in Business Communications Manager.
IP Domain	Allows you to specify the domain name that Business Communications Manager and its DHCP clients uses. When you modify the Domain, the setting automatically copies to **Domain Name** global options under **DHCP** service.
Primary (and Secondary) Server	Allows you to specify the IP addresses of the primary DNS server and the secondary DNS server in a valid dot format. When you specify a secondary DNS server, separate the two IP addresses by a space. The DNS cache uses the servers in the order that you specify, so make sure the IP address of the secondary DNS server appears second.
Forward Timeout	Allows you to specify the time-out, in seconds, to resolve queries using the DNS servers that you specify in DNS server.

3 Press the **Tab** key to save the settings.

Note: The DNS proxy carries security features because it keeps all of the internal IP addresses from external web servers. For information on other security features, see "Configuring NAT (Network Address Translation)" on page 753 and "Configuring IP Firewall Filters" on page 831.

Chapter 33
Configuring IP Routing

The **IP Routing** service setting allows you to select, add or delete routing protocol on specific interfaces, choose routing protocol options, and add or delete static routes.

Note: If you change the IP address or subnet mask of any interface (LAN or WAN), you must reboot Business Communications Manager before you configure IP routing.

Business Communications Manager supports the following IP routing protocols:

- "Routing Information Protocol (RIP)"
- "Open Shortest Path First (OSPF)"

This section also includes information about:

- "Configuring IP Routing global settings" on page 707
- "Configuring IP routing on an interface" on page 709
- "Restarting the router" on page 717

Routing Information Protocol (RIP)

Business Communications Manager supports RIP, a widely-used protocol for managing routing information in a self-contained network, such as a corporate intranet. RIP measures the shortest path between two points on a network in terms of the number of hops between those points.

Business Communications Manager router sends RIP routing information updates that list all the other hosts it knows about, to its nearest neighbor host every 30 seconds. The neighbor host sends the information to its next neighbor, until all the hosts in the network know the routing paths, a state known as network convergence. RIP uses a hop count to determine network distance. Each router in the network uses the routing table information to determine the next host for the packet, until it reaches the destination.

Business Communications Manager supports on demand routing table update and periodic routing table update. On demand routing table update is available only on demand-dial interfaces. Periodic update operates efficiently on persistent links

Business Communications Manager supports IP Subnet Aggregation, or Subnet Summary, in RIP v2. This feature is turned on by default.

When Subnet Aggregation is on and there are two or more subnets with common leading digits in their subnet addresses, RIP v2 will summarize these subnets and advertise a single aggregated entry to its neighboring routers.

For information on how to select RIP as your routing protocol, see "Configuring RIP parameters on a network interface" on page 709.

Open Shortest Path First (OSPF)

Open Shortest Path First protocol bases its path descriptions on “link states” that take into account additional network information. OSPF also lets the user assign cost metrics to a given host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided into areas. For information on how to select OSPF as your routing protocol, see “Configuring OSPF Parameters on a network interface” on page 712.

The implementation of OSPF on Business Communications Manager is designed to operate as an edge router in an OSPF intranet, or as a backup router in a small network. Do not configure Business Communications Manager for multiple OSPF areas.

Note: Business Communications Manager is an edge router and will not act as a router spanning RIP and OSPF routing networks (RIP or OSPF redistribution).

Warning: Because OSPF is a “link-state” based routing protocol, you must not use OSPF on dial-on-demand interfaces. Frequent link status (between “up” and “down”) may cause the protocol to become unstable.

IP routing protocol precedence

The followings table shows the Business Communications Manager IP routing protocols and the precedence order when conflicting or redundant routes occur.

Precedence	IP Routing Protocols	
1.	Static Routing	
2.	OSPF	RIP v1 and v2

Configuring IP Routing global settings

This section describes how to configure global settings for the IP Routing.

It also includes information about:

- "Setting the RIP Global Settings" on page 707
- "Setting the OSPF Global Settings" on page 708

To configure global settings for IP Routing:

1. On the navigation tree, click the **Services** key and click the **IP Routing** heading.
   The IP routing Summary screen appears.
2. Configure the Routing Summary attributes according to the following table.

Table 225 IP Routing Summary attributes

Attribute	Description
Description	Shows a description of the router.
Version	Shows the version of the router.
Status	Shows you the status of the router. The possible values are: **Up**: the IP router is currently functioning. **Enabled**: allows you to enable the router. **Disabled**: allows you to disable the router.

Setting the RIP Global Settings

If your network uses RIP, configure the RIP Global Settings as described below. If your network uses OSPF, refer to "Setting the OSPF Global Settings" on page 708.

1. Click the **RIP Global Settings** tab.
   The RIP Global Settings screen appears.
2. Configure the RIP Global Settings according to the following table.

Table 226 IP RIP Global Settings

Attribute	Description
RIP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Triggered Update Interval	Allows you to specify the minimum interval, in seconds, at which a router must send a routing table update if the metric for a given route changes. If the router detects a change in the routing information, the router sends an update message at the specified interval. Possible values are **1** to **50000**. The default value is **5.**

3 Press the **TAB** key to save your settings.

Setting the OSPF Global Settings

If OSPF is the routing protocol of your choice, configure the OSPF Global Settings as described below.

1 Click the **OSPF Global Settings** tab.
The OSPF Global Settings screen appears.

2 Configure the OSPF Global Settings according to the following table.

Table 227 IP OSPF Global Settings

Attribute	Description
OSPF Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Router ID	Allows you to specify the IP address that uniquely identifies the Business Communications Manager router on your network.
Router Area ID	Allows you to specify the area where your Business Communications Manager router is located on your network. The default value is **0.0.0.0**.
Authentication Type	Allows you to enable or disable password authentication. Values are **None**, **Password**. The default value is **None**. For information on how to set the authentication password, see “Configuring OSPF Parameters on a network interface” on page 712.

3 Press the **TAB** key to save your settings.

Configuring IP routing on an interface

After you configured the IP Routing global settings, you must configure each available network interface to use the routing protocol of your choice or static routes.

Note: You must use the same routing protocol on all interfaces. For example, you can not configure your LAN1 interface to use RIP and your WAN1 interface to use OSPF.

This section provides instructions on how to configure interfaces for IP routing and how to create static routes. The available interfaces appear under the **IP Routing** heading. Follow the same instructions to configure all interfaces. For information on how to create static routes, see "Static routes" on page 715.

This section includes information about:

Configuring RIP parameters on a network interface

Follow these steps to configure RIP parameters on a network interface:

1. On the navigation tree, click the **Services** key and click the **IP Routing** key.
   The available interfaces for IP routing are listed under the **IP Routing** heading.
2. Click the interface you want to configure.
   The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Tips
If you are changing the routing protocol from OSPF to RIP, you must first set the **Routing Protocol** under each available interface to **None** before you can select **RIP**.

Note: The RIP Parameters window does not appear unless you choose RIP as your routing protocol.

3. In the **Routing Protocol** list, click **RIP**.
4. Press the **Tab** key.
   The RIP Parameters tab appears.
5. Click the **RIP Parameters** tab.
   The RIP Parameters window appears.

6 Configure the RIP Parameters according to the following table.

Table 228 IP RIP Parameters

Attribute	Description
Metric	Allows you to assign a cumulative value (in terms of hop count or associated cost [if applicable]) to routes passing through this interface. The routing manager adds the metric value of all routes learned through this interface to the metric value of this interface to make routing decisions. The possible values are **1** to **16**. Because RIP protocol can handle up to 15 hop counts before reaching destination, a value of **16** corresponds to "counting to infinity". The default value is **1**.
Routing Table Update Mode	Allows you to specify the routing table update mode. The possible values are: **On Demand:** The router sends its table when another established router requests it. **Periodic**: The router sends its table to other established router at regular intervals. On dialup interfaces, you must set the Update Mode to **Periodic** to receive updates. The default value is **Periodic**.
Route Announcement Type	Allows you to set the type of routing table update announcements the Business Communications Manager router sends to other routers. The possible values are: **Disabled**: disables sending RIP routing update. If you choose **Disabled**, you must configure the other routers in the subnet to use static routes to access the Business Communications Manager base unit. **RIP 1**: sends only announcements of RIP v1 type in broadcast mode. **RIP 1 Compatible**: sends RIP v1 and RIP v2 packets in broadcast mode. Use this for a network environment that uses RIP v1 and RIP v2. **RIP 2**: sends RIP v2 packets in multicast mode only. Use this type of announcement only if all other routers connected to the Business Communications Manager base unit support RIP v2. The default value is **RIP 1**.
Route Accept Type	Allows you to set the type of routing table update announcements the Business Communications Manager router accepts from other routers. The possible values are: **Disabled**: disables sending RIP routing table update announcements. If you choose **Disabled**, you must create static routes in the Business Communications Manager base unit to access other networks connected to this interface. This method is preferable if you want to keep the routing table small in the Business Communications Manager base unit. **RIP 1**: accepts only announcements of RIP **1** type. **RIP 1 Compatible**: accepts announcements of RIP 1 and RIP 2 types. **RIP 2**: accepts announcements of RIP 2 type only. The default value is **RIP 1**.
Route Expiration Interval	Allows you to define the period of time within which a route in the routing table must be updated to remain a valid route. The possible values are **15** to **259200** seconds**.** The default value is **180** seconds.
Route Removal Interval	Allows you to define the period of time (in seconds) an invalid route remains in the routing table before the routing manager removes it from the routing table. The possible values are **15** to **259200** seconds**.** The default value is **120** seconds
Route Announcement Interval	Allows you to set the time interval (in seconds) between routing table updates when the **Routing Table Update Mode** is set to **Periodic**. The possible values are **5** to **86400** seconds. The default value is **30** seconds.

Table 228 IP RIP Parameters (Continued)

Attribute	Description
Route Tag	Allows you to create a special tag which identifies routes announced over the interface. The route tag helps identify route packets when debugging routing problems using a network sniffer.
Poisoned Reverse	Allows you to enable or disable options designed to avoid routing problems such as loops or metric values exceeding the maximum of 15 hop counts. The following options are available: **Actual**: A routing table update process where a routing table update going out repeats the information sent by the originator. The system tries to solve this state known as a loop involving two routers by sending more routing updates. **Split** (split horizon): A routing table update process designed to avoid sending the same routing information back to the originator. **Poisoned**: A routing table update process designed to advertise unreachable routes as having metric value of 16 regardless of incoming routing update information. The default value is **Split**.
Triggered Updates	Allows you enable immediate route update announcements whenever a metric or other information changes in the routing table entries. When **Triggered Updates** is set to **Enabled**, the system gathers new routing information for the period of time defined in the **Triggered Update Interval** from the RIP Summary window (see "Configuring IP Routing global settings" on page 707). Triggered updates results in more frequent, smaller RIP routing table updates. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Announce Default Route	Allows you to enable or disable the announcement of default routes in incoming route announcements. Use caution when you enable this feature, because improper configuration causes a loss of network connectivity. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Accept Default Route	Allows you to enable or disable the acceptance of incoming default routes announcement. Sets default routes as static routes. If you run Net Link Manager to automatically backup the primary WAN link using a dial-up link, Net Link Manager manages the default routes and the default routes that you add are non-operational as soon as a primary link breaks or comes up again. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.

7 Press **Tab** to save your settings.

Enabling the RIP Subnet summary

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.
The available interfaces for IP routing are listed under the **IP Routing** heading.

2 Click the interface you want to configure.
The Summary window appears.

3 Click the **Configuration** menu and then click **Enable Rip SubnetSumm**.
The message "Please wait..setting data" appears in the message bar at the bottom of the Unified Manager Window. After the Rip Subnet Summary is successfully enabled, the message "Ready" appears in the message bar.

Disabling the RIP Subnet summary

1. On the navigation tree, click the **Services** key and click the **IP Routing** key.
   The available interfaces for IP routing are listed under the **IP Routing** heading.
2. Click the interface you want to configure.
   The Summary window appears.
3. Click the **Configuration** menu and then click **Disable Rip SubnetSumm**.
   The message "Please wait..setting data" appears in the message bar at the bottom of the Unified Manager Window. After the Rip Subnet Summary is successfully disabled, the message "Ready" appears in the message bar.

Configuring OSPF Parameters on a network interface

1. On the navigation tree, click the **Services** key and click the **IP Routing** key.
   The available interfaces for IP routing are listed under the **IP Routing** heading.
2. Click the interface you want to configure.
   The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Warning: Because OSPF is a "link-state" based routing protocol, you must not use OSPF on dial-on-demand interfaces. Frequent link status changes (between "up" and "down") may cause the OSPF protocol to become unstable.

3. In the **Routing Protocol** list, click **OSPF**.

Tips
If you are changing the routing protocol from RIP to OSPF, you must first set the Routing Protocol under each available interface to None before you can select OSPF.

4. Click the **OSPF Parameters** tab.
   The OSPF Parameters screen appears.

Note: The OSPF Parameters tab does not appear unless you choose OSPF as your routing protocol.

5 Configure the OSPF parameters according to the following table.

Table 229 IP OSPF Parameters

Attribute	Description
Metric	This field allows you to assign the link cost for this interface that advertised in the router's link state advertisement for this interface. The Metric is an indication of the cost of the route. If multiple routes exist on a network ID, the Metric is used to decide which route is taken. The route with the lowest Metric is the preferred route. If you enter a high number for the Metric, this interface will not be used as much as an interface with a lower Metric. The possible values are **1** to **32767**. The default value is **1**.
Interface Type	Allows you to select the type of interface that describes your network configuration. The possible values are: **Broadcast**: A broadcast network supports multiple routers and addresses a single physical message to all routers. **P2P**: A point-to-point network joins a single pair of OSPF routers. **NBMA**: A Non-Broadcast-Multi-Access (NBMA) network supports multiple routers and cannot address a single physical message to all routers. The default value is **Broadcast**.
Router Priority	Allows you to assign a priority to the Business Communications Manager router. The possible values are **0** to **255**. A value of 0 indicates that the Business Communications Manager system cannot become the designated router. The default value is **1**.
Transit Delay	Allows you to set (in seconds) the estimated round-trip transit delay in the network connected to the interface. The values are **1** to **3600** seconds. The default value is **1**.
Retransmit Interval	Allows you to set the number of seconds the router waits before retransmitting after a time-out occurs. The values are **1** to **3600** seconds. The default value is **1**.
Hello Interval	Allows you to define how frequently the router must send "hello packets" on an interface. The values are **1** to **32767** seconds. The default value is **10**.
Dead Interval	Allows you to set the maximum number of seconds the router waits to receive the next hello before considering the adjacent router as non operational. The values are **1** to **32767** seconds. The default value is **40**.
Poll Interval	Allows you to define the period of time the router must keep sending hello packets to an adjacent router that is considered non operational. The values are **1** to **32767** seconds. The default value is **120**.
MTU	Allows you to specify the Maximum Transmission Unit for this interface. The values are **1** to **10000**. The default value is **1500**.
Password	Allows you to define an authentication password, if you selected **Password** as the authentication type in the **Authentication Type** box on the OSPF Global Parameters window. There is no default value provided because the **Authentication Type** is set to **None** by default. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

6 Press the **Tab** key to save your settings.

OSPF NBMA Neighbors

Frame Relay on Business Communications Manager is a Non Broadcast Multiple Access (NBMA) network. NBMA is a network that can connect two or more routers, but has no hardware broadcast capability. For OSPF function properly on a NBMA network, you must configure OSPF to unicast to the IP addresses of the routers on the network. The OSPF NBMA Neighbors screen allows you to enter IP addresses of the NBMA Neighbors.

Note: The OSPF NBMA Neighbors is available only for WAN interfaces.

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.

2 Click the WAN interface you want configure.

3 Click the **OSPF NBMA Neighbors** tab.
The OSPF NBMA Neighbors screen appears.

Adding OSPF NBMA Neighbors

1 On the **Configuration** menu, click **Add OSPF Neighbor**.
The OSPF NBMA Neighbors screen appears.

2 Configure the OSPF NBMA Neighbor parameters according to the following table.

Table 230 IP OSPF NBMA Neighbor parameters

Attribute	Description
OSPF Neighbor (ON#)	Allows you to specify the OSPF Neighbor identifier.
Neighbor Address	Allows you to specify the IP address of the neighboring router.
Neighbor Priority	Allows you to specify the priority of the neighboring router. The possible values are **1** to **255**. The default value is **1**.

3 Click the **OK** button.

Modifying OSPF NBMA Neighbors

1 Click the OSPF NBMA Neighbor you want to modify.

2 On the **Configuration** menu, click **Modify OSPF Neighbor**.
The OSPF NBMA Neighbors screen appears.

3 Change the OSPF NBMA Neighbor parameters.

4 Click the **OK** button.

Deleting OSPF NBMA Neighbors

1 Click the OSPF NBMA Neighbor you want to delete.

2 On the **Configuration** menu, click **Delete OSPF Neighbor**.
A confirmation dialog box appears.

3 Click the **Yes** button.

Static routes

You can add static routes to the Business Communications Manager routing table. Static routes added to the routing table take precedence over dynamic routes.

Note: The default route is managed by Net Link Manager. For information about Net Link Manager, refer to "Configuring Net Link Manager" on page 749.

Adding a static route to the routing table

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.

2 Click the interface you want configure.

3 Click the **Static Route** tab.
The Static Route screen appears.

4 On the **Configuration** menu, click **Add Static Route**.
The Static Route dialog box appears.

5 Configure the static route attributes according to the following table.

Table 231 IP Static Route attributes

Attribute	Description
Static Route (SR#)	Assign a number to the static route. For example, the valid static route number for the first static route is SR1. The function of the static route number is to uniquely identify an route. If you add more than one static route, use sequential numbers. If you use the number of an existing static route, the system modifies the existing static route. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a static route, you cannot change the Static Route number.
Destination address	Enter the IP address of the destination network or host.
Destination mask	Enter the subnet mask corresponding to the destination address.
Next Hop Router	Enter the IP address of next hop router.
Metric Value	Enter the metric value associated with the interface. The system adds the metric to the hop count of the routes received through the interface.

6 Click the **Save** button.

Modifying the static route configuration

1. Click a static route you want to modify in the Static Route table.
2. On the **Configuration** menu, click **Modify Static Route**.
   The Static Route dialog box appears.
3. Modify the static route attributes.
4. Click the **Save** button.

Deleting a static route

1. Click the static route you want to delete in the Static Route table.
2. On the **Configuration** menu, click **Delete Static Route**.
   A confirmation message appears.
3. Click the **Yes** button.

Restarting the router

When you make OSPF changes to the router, you need to restart the Routing and Remote Access Service for the changes to take place.

Warning: This procedure will affect any service that requires access across the LAN or WAN, including IP telephone service.

1. On the navigation tree, click the **Services** key.
2. Click the **IP routing** heading.
3. On the **Tools** menu, click **Restart Router**.
   The process takes about a minute.
   When the restart is complete, you will see an information dialog box indicating that the restart was successful.
4. Click the **OK** button, on the dialog box.

Note: If the restart fails, you will receive this message:

```
Generic Error (Failed to restart router. Please reboot the system
for changes to be effective)
```

If you do not need the changes immediately, schedule a cold start of the Business Communications Manager for a low-activity period. The Scheduler is located under the Maintenance button on the first page of the Unified Manager web page.

Otherwise, shut down and then restart the Business Communications Manager. This will disrupt all telephony service.

Chapter 34
Configuring IPX Routing

Business Communications Manager supports RIP and SAP (Service Advertising Protocol) for IPX routing in a NetWare environment. Static routes and static services are also supported.

Business Communications Manager supports IPX basic packet filtering feature.

This section provides instructions about how to configure IPX routing for specific interfaces. All available interfaces appear under the IPX Routing heading. The same configuration procedures apply to all interfaces.

The information in this section includes:

Note: The IPX router manager in your Business Communications Manager system operates separately from the IP routing manager. As a result, RIP configuration under the IP Routing heading has no effect on IPX routing. You must configure IPX RIP parameters under the IPX Routing heading.

Tips
After you create and add a filter for IPX routing on an interface, you must select the Input Filter Action and Output filter Action from the RIP Summary parameters.

Warning: The filter action that indicates either to deny or allow packets that match filter definition applies to all filters. You cannot set a filter action for a specific filter. When you have decided which action the routing manager must perform on packets matching a filter definition, the routing manager performs this action every time it finds a match between packets and filters.

Enabling IPX Routing

IPX Routing does not appear on Unified Manager until you enable it.

To enable IPX Routing:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address.
   For example: *HTTPS://10.10.10.1*.
   The Business Communications Manager Unified Manager initial page appears.

   Note: You must include **HTTPS://** with the address to access Unified Manager when you are using Internet Explorer as your browser.

3. Click the **Maintenance** button.
   The Network Password screen appears.
4. In the **User Name** box, type the system administrator user name.
5. In the **Password** box, type the system administrator password.
6. Click the **OK** button.
   The Product Maintenance & Support screen appears.
7. Click the **Install Optional Components** link.
   The Install Optional Components screen appears.
8. Click the **Install** link beside the **IPX Routing** heading.
   The IPX Routing install wizard starts.
9. Follow the prompts on the screen to enable IPX Routing.

   The IPX Routing install wizard consists of three steps. Business Communications Manager reboots after each step.
   It takes 10 to 15 minutes to enable IPX Routing.

Configuring IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** heading.
   The IPX Routing Summary screen appears.
2. Configure the IPX Routing Summary settings according to the following table.

Table 232 IPX Routing Summary settings

Attribute	Description
Description	Displays the name of the router.
Version	Displays the version number of the router.
Status	Displays the current status of the service.
Internal Network Number	Allows you to specify the internal network number. The internal network number uniquely identifies the computer on the intranet.

3. Click the **IPX Global Settings** tab.
   The IPX Global Settings screen appears.
4. Configure the IPX Global Settings according to the following table.

Table 233 IPX Global settings

Attribute	Description
IPX Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

5. Click the **RIP Global Settings** tab.
   The RIP Global Settings screen appears.
6. Configure the RIP Global Settings according to the following table.

Table 234 IPX RIP Global settings

Attribute	Description
RIP Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

7. Click the **SAP Global Settings** tab.
   The SAP Global Settings screen appears.

8 Configure the SAP Global Settings according to the following table.

Table 235 IPX SAP Global settings

Attribute	Description
SAP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

9 Press the **Tab** key to save the settings.

Configuring IPX routing on an interface

After you configured the IPX Routing global settings, you must configure each available network interface.

This section includes information about:

Configuring Packet Filters for IPX routing

Note: The maximum number of IPX filters you can add is 128.

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to configure for IPX routing.
   The Interface Summary screen appears.
3. Configure the IPX routing packet filter summary settings according to the following table.

Table 236 IPX Packet Filter Summary Settings

Attribute	Description
Interface Name	Displays the name of the interface you are currently configuring for IPX routing.
Input Filter Action	Allows you to specify the action the packet filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for filters. **Permit** all inbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "Adding Packet Input filters" on page 724.
Output Filter Action	Allows you to specify the action the packet filter must perform on outbound traffic. The values possible values are: **Deny** all outbound traffic matching the criterion defined for filters. **Permit** all outbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can choose Permit. To create a filter, refer to "Adding Packet Output filters" on page 725.
Network Number	Allows you to specify the network number (also called external network number) for routing purposes.
Frame Type	Allows you to specify the frame type. The possible values are: Ethernet II, Ethernet 802.2, Ethernet 802.3, Ethernet SNAP**,** Default.

4 Press the **Tab** key to save the settings.

Adding Packet Input filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to configure.
The Interface Summary screen appears.

3 Click the **Packet Input Filters** tab.
The Packet Input Filters screen appears.

4 On the **Configuration** menu, click **Add Packet Input Filter**.
The Packet Input Filters screen appears.

5 Configure the Packet Input Filter parameters according to the following table.

Table 237 IPX Packet Input Filter parameters

Attribute	Description
Packet Input Filter (PIF#)	Allows you to assign a number to the Packet Input Filter. For example, the valid packet input filter number for the first input filter is PIF1. The function of the Packet Input Filter number is to uniquely identify a packet input filter. If you add more than one Packet Input Filter, use sequential numbers. If you use the number of an existing Packet Input Filter, the system modifies the existing Packet Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Packet Input Filter, you cannot change the Packet Input Filter number.
Source Network Number	Allows you to enter the network number that identifies the source IPX network. A valid entry is any 4-byte hexadecimal number.
Source Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.
Source Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Source Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Destination Network Number	Allows you to enter the network number that identifies the destination IPX network. A valid entry is any 4-byte hexadecimal number.
Destination Network Mask	Allows you to enter the network mask to be applied to the destination address. This parameter defines the range of network numbers that you want to filter.
Destination Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Destination Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Packet Type	Allows you to specify the Packet Type. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.

6 Click the **Save** button.

Modifying Packet Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Input Filters** tab.
   The Packet Input Filters screen appears.
4. Click the Packet Input Filter you want to modify.
5. On the **Configuration** menu, click **Modify Packet Input Filter**.
   The Packet Input Filters screen appears.
6. Modify the Packet Input Filter attributes.
7. Click the **Save** button.

Deleting Packet Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Input Filters** tab.
   The Packet Input Filters screen appears.
4. Click the Packet Input Filter you want to delete.
5. On the **Configuration** menu, click **Delete Packet Input Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

Adding Packet Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Output Filters** tab.
   The Packet Output Filters screen appears.
4. On the **Configuration** menu, click **Add Packet Output Filter**.
   The Packet Output Filters screen appears.

5 Configure the Packet Output Filter parameters according to the following table.

Table 238 IPX Packet Output Filter parameters

Attribute	Description
Packet Output Filter (POF#)	Allows you to assign a number to the Packet Output Filter. For example, the valid Packet Output Filter number for the first output filter is POF1. The function of the Packet Output Filter number is to uniquely identify a Packet Output Filter. If you add more than one Packet Output Filter, use sequential numbers. If you use the number of an existing Packet Output Filter, the system modifies the existing Packet Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Packet Output Filter, you cannot change the Packet Output Filter number.
Source Network Number	Allows you to enter the network number that identifies the source IPX network. A valid entry is any 4-byte hexadecimal number.
Source Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.
Source Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Source Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Destination Network Number	Allows you to enter the network number that identifies the destination IPX network. A valid entry is any 4-byte hexadecimal number.
Destination Network Mask	Allows you to enter the network mask to be applied to the destination address. This parameter defines the range of network numbers that you want to filter.
Destination Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Destination Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Packet Type	Allows you to enter the network number that identifies the destination IPX network. A valid entry is any 4-byte hexadecimal number.

6 Click the **Save** button.

Modifying Packet Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **Packet Output Filters** tab.
The Packet Output Filters screen appears.

4 Click the Packet Output Filter you want to modify.

5 On the **Configuration** menu, click **Modify Packet Output Filter**.
The Packet Output Filters screen appears.

6 Modify the Packet Output Filter attributes.

7 Click the **Save** button.

Deleting Packet Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Output Filters** tab.
   The Packet Output Filters screen appears.
4. Click the Packet Output Filter you want to delete.
5. On the **Configuration** menu, click **Delete Packet Output Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

RIP filters for IPX routing

RIP is the routing protocol that routes IPX data packets in an internetwork environment. You can configure IPX packet filters for inbound or outbound traffic on interface handling IPX packets.

Note: The maximum number of IPX filters you can add is 128.

Configuring RIP for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Summary** tab.
   The RIP Summary screen appears.
4. Configure the RIP Summary settings according to the following table.

Table 239 IPX RIP Summary settings

Attribute	Description
Input Filter Action	Allows you to specify the action the packet filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for filters. **Permit** all inbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "Adding RIP Input Filters" on page 729.

Table 239 IPX RIP Summary settings (Continued)

Attribute	Description
Output Filter Action	Allows you to specify the action the packet filter must perform on outbound traffic. The values possible values are: **Deny** all outbound traffic matching the criterion defined for filters. **Permit** all outbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "Adding RIP Output filters" on page 730.

5 Press the **Tab** key to save the settings.

6 Click the **RIP Parameters** tab.
The RIP Parameters screen appears.

7 Configure the RIP Parameters settings according to the following table.

Table 240 IPX RIP Parameters

Attribute	Description
RIP State	Allows you to enable or disable RIP for this interface. The values are **Enabled** or **Disabled**. The default value is **Enabled**
Advertise Routes	Allows you enable or disable the advertisement of routes on the interface you are configuring. The default value is **Enabled**.
Accept Route Advertisements	Allows you to enable or disable the acceptance of route advertisement from remote routers on this interface. The default value is **Enabled**.
Update Mode	Allows you to select an update mode for the routing table. The routing table update modes available are: **Standard** update mode sends out a routing table for a router at regular intervals that you specify in the Update Interval box. New routes are added to the routing table as dynamic routes and are deleted from the routing tables when the router restarts. **Autostatic** update mode sends a routing table on the current interface when other routers connected to this interface request it. New routes to this interface, using RIP, are stored as static routes in the routing table for this interface and remain until you delete them. **No Update** mode never updates the routing tables on the current interface. The default value is **Standard**.
Update Interval	Allows you to set the interval, in seconds, when the routing manager updates the route tables. When you set the Update Mode to **Standard,** the routing manager periodically updates the route tables at the interval you specify in the Update Interval box. The possible values are 5 to 86400 seconds (24 hours). The default value is 60 seconds.
Aging Interval Multiplier	A multiplier used to determine when a route expires and is removed from the route table. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a route remains in the route table for a maximum of 180 seconds (3 X 60) from the last update. The default value is 3.

8 Press the **Tab** key to save the settings.

Adding RIP Input Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Input Filters** tab.
   The RIP Input Filters screen appears.
4. On the **Configuration** menu, click **Add RIP Input Filter**.
   The RIP Input Filters screen appears.
5. Configure the RIP Input Filter parameters according to the following table.

Table 241 IPX RIP Input Filter parameters

Attribute	Description
Input Filter (IF#)	Allows you to assign a number to the RIP Input Filter. For example, the valid RIP input filter number for the first input filter is IF1. The function of the RIP Input Filter number is to uniquely identify a RIP input filter. If you add more than one RIP Input Filter, use sequential numbers. If you use the number of an existing RIP Input Filter, the system modifies the existing RIP Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a RIP Input Filter, you cannot change the RIP Input Filter number.
Network Number	Allows you to enter the network number that identifies the IPX network. A valid entry is any 4-byte hexadecimal number.
Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.

6. Click the **Save** button.

Modifying RIP Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Input Filters** tab.
   The RIP Input Filters screen appears.
4. Click the RIP Input Filter you want to modify.
5. On the **Configuration** menu, click **Modify RIP Input Filter**.
   The RIP Input Filters screen appears.
6. Modify the RIP Input Filter attributes.
7. Click the **Save** button.

Deleting RIP Input filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Input Filters** tab.
The RIP Input Filters screen appears.

4 Click the RIP Input Filter you want to delete.

5 On the **Configuration** menu, click **Delete RIP Input Filter**.
A confirmation message appears.

6 Click the **Yes** button.

Adding RIP Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Output Filters** tab.
The RIP Output Filters screen appears.

4 On the **Configuration** menu, click **Add RIP Output Filter**.
The RIP Output Filters screen appears.

5 Configure the RIP Output Filter parameters according to the following table.

Table 242 IPX RIP Output Filter parameters

Attribute	Description
Output Filter (OF#)	Allows you to assign a number to the RIP Output Filter. For example, the valid RIP Output Filter number for the first output filter is OF1. The function of the RIP Output Filter number is to uniquely identify a RIP Output Filter. If you add more than one RIP Output Filter, use sequential numbers. If you use the number of an existing RIP Output Filter, the system modifies the existing RIP Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a RIP Output Filter, you cannot change the RIP Output Filter number.
Network Number	Allows you to enter the network number that identifies the IPX network. A valid entry is any 4-byte hexadecimal number.
Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.

6 Click the **Save** button.

Modifying RIP Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Output Filters** tab.
   The RIP Output Filters screen appears.
4. Click the RIP Output Filter you want to modify.
5. On the **Configuration** menu, click **Modify RIP Output Filter**.
   The RIP Output Filters screen appears.
6. Modify the RIP Output Filter attributes.
7. Click the **Save** button.

Deleting RIP Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Output Filters** tab.
   The RIP Output Filters screen appears.
4. Click the RIP Output Filter you want to delete.
5. On the **Configuration** menu, click **Delete RIP Output Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

SAP filters for IPX routing

On a Novell network, the Service Advertising Protocol (SAP) provides network control information about available services on a Novell network. You can define and add SAP filters for IPX routing.

Note: The maximum number of IPX filters you can add is 128.

Configuring the SAP for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Summary** tab.
The SAP Summary screen appears.

4 Configure the SAP Summary settings according to the following table.

Table 243 IPX SAP Summary settings

Attribute	Description
Input Filter Action	Allows you to specify the action the filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for SAP filters. **Permit** all inbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "Adding SAP Input Filters" on page 733.
Output Filter Action	Allows you to specify the action the filter must perform on outbound traffic. The possible values are: **Deny** all outbound traffic matching the criterion defined for SAP filters. **Permit** all outbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "Adding SAP Output Filters" on page 735.

5 Press the **Tab** key to save the settings.

6 Click the **SAP Parameters** tab.
The SAP Parameters screen appears.

7 Configure the SAP Parameters according to the following table.

Table 244 IPX SAP Parameters

Attribute	Description
SAP State	Allows you to enable or disable SAP for this interface. The possible values are **Enabled** or **Disabled**. The default value is **Enabled**.

Table 244 IPX SAP Parameters (Continued)

Attribute	Description
Advertise Services	Allows you to enable or disable the advertisement of SAP services on the interface to remote routers. The possible values are **Enabled** or **Disabled**. The default value is **Enabled**.
Accept Service Advertisements	Allows you to enable or disable the acceptance of advertisement of SAP services from remote routers. The possible values are **Enabled** or **Disabled**. The default value is **Enabled.**
Update Mode	Allows you to select an update mode for SAP on the interface. The available options are: **Standard** update mode sends periodic updates at an interval you define in the Update Interval box. **Autostatic** update mode sends a routing table update when other routers connected to this interface request it. New routes to this interface, using SAP, are stored as static routes in the routing table for this interface and remain until you delete them. **No Update** mode never updates the routing tables on the current interface. The default value is **Standard**.
Update Interval	Allows you to set the interval, in seconds at which SAP announcements are updated. If you set the **Update Mode** to **Standard**, the SAP announcements are updated at the interval you specify in the Update Interval box. The possible values **5** to **86400** seconds. The default value is **60** seconds.
Aging Interval Multiplier	A multiplier used to determine when a SAP announcements coming to this interface expires. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a SAP announcement remains valid for a maximum of 180 seconds (3 X 60) from the last announcement. The possible values are **3** to **100**. The default value is **3**.

Adding SAP Input Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Input Filters** tab.
   The SAP Input Filters screen appears.
4. On the **Configuration** menu, click **Add SAP Input Filter**.
   The SAP Input Filters screen appears.
5. Configure the SAP Input Filter parameters according to the following table.

Table 245 IPX SAP Input Filter parameters

Attribute	Description
Input Filter (SapIF#)	Allows you to assign a number to the SAP Input Filter. For example, the valid SAP input filter number for the first input filter is SapIF1. The function of the SAP Input Filter number is to uniquely identify a SAP input filter. If you add more than one SAP Input Filter, use sequential numbers. If you use the number of an existing SAP Input Filter, the system modifies the existing SAP Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a SAP Input Filter, you cannot change the SAP Input Filter number.

Table 245 IPX SAP Input Filter parameters (Continued)

Attribute	Description
Service Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Service Name	Allows you to enter the service name. You can use a wildcard service name such as "*" to indicate all service names.

6 Click the **Save** button.

Modifying SAP Input Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Input Filters** tab.
The SAP Input Filters screen appears.

4 Click the SAP Input Filter you want to modify.

5 On the **Configuration** menu, click **Modify SAP Input Filter**.
The SAP Input Filters screen appears.

6 Modify the SAP Input Filter attributes.

7 Click the **Save** button.

Deleting SAP Input Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Input Filters** tab.
The SAP Input Filters screen appears.

4 Click the SAP Input Filter you want to delete.

5 On the **Configuration** menu, click **Delete SAP Input Filter**.
A confirmation message appears.

6 Click the **Yes** button.

Adding SAP Output Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Output Filters** tab.
The SAP Output Filters screen appears.

4 On the **Configuration** menu, click **Add SAP Output Filter**.

5 Configure the SAP Output Filter parameters according to the following table.

Table 246 IPX SAP Output Filter parameters

Attribute	Description
Output Filter (SapOF#)	Allows you to assign a number to the SAP Output Filter. For example, the valid SAP output filter number for the first output filter is SapOF1. The function of the SAP Output Filter number is to uniquely identify a SAP Output filter. If you add more than one SAP Output Filter, use sequential numbers. If you use the number of an existing SAP Output Filter, the system modifies the existing SAP Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a SAP Output Filter, you cannot change the SAP Output Filter number.
Service Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Service Name	Allows you to enter the service name. You can use a wildcard service name such as "*" to indicate all service names.

6 Click the **Save** button.

Modifying SAP Output Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Output Filters** tab.
The SAP Output Filters screen appears.

4 Click the SAP Output Filter you want to modify.

5 On the **Configuration** menu, click **Modify SAP Output Filter**.

6 Modify the SAP Output filter attributes.

7 Click the **Save** button.

Deleting SAP Output Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Output Filters** tab.
   The SAP Output Filters screen appears.
4. Click the SAP Output Filter you want to delete.
5. On the **Configuration** menu, click **Delete SAP Output Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

Static Routes for IPX Routing

You can add static routes to the IPX routing table. The IPX static routes take precedence over the routes added by routing protocol such as RIP.

Note: The maximum number of IPX routes you can add is 128.

Adding Static Routes for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Routes** tab.
   The Static Routes screen appears.
4. On the **Configuration** menu, choose **Add Static Route**.
   The Static Routes dialog box appears.
5. Configure the static routing attributes according to the following table.

Table 247 IPX Static Routing attributes

Attribute	Description
Static Route (SR#)	Allows you to assign a number to the Static Route. For example, the valid Static Route number for the first static route is SR1. The function of the Static Route number is to uniquely identify a Static Route. If you add more than one Static Route, use sequential numbers. If you use the number of an existing Static Route, the system modifies the existing Static Route. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Static Route, you cannot change the Static Route number.
Net Number	IPX Network Number identifies the destination network for the routing table entry. The permitted value is 4 bytes in hexadecimal format. The default value is **None**.
Next Hop Mac Address	Shows the MAC address of the next hop router to reach the network defined in the **NetNumber** box. The permitted value is 6 bytes in hexadecimal format. The default value is **None**.

Table 247 IPX Static Routing attributes (Continued)

Attribute	Description
Ticks	Time required (in 1/60 seconds) to reach the destination network. The values are **1** to **32,767**. The default value is **None**.
Hops	Shows the number of hops that must be crossed in order to reach the destination network. The permitted values are **0** to **15**. The default value is **0**.

6 Click the **Save** button.

Modifying Static Routes for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface that you want to configure.

3 Click the **Static Routes** tab.
The Static Routes screen appears.

4 Click the Static Route you want to modify.

5 On the **Configuration** menu, choose **Modify Static Route**.
The Static Routes dialog box appears.

6 Modify the static routing table attributes.

7 Click the **Save** button.

Deleting Static Routes for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface that you want to configure.

3 Click the **Static Routes** tab.
The Static Routes screen appears.

4 Click the Static Route you want to delete.

5 On the **Configuration** menu, choose **Delete Static Route**.
A confirmation message appears.

6 Click the **Yes** button.

Static Service for IPX Routing

The following section describes how to manage the static service for IPX routing.

Adding a Static Service for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Services** tab.
   The Static Service screen appears.
4. On the **Configuration** menu, choose **Add Static Service**.
   The Static Routes dialog box appears.
5. Configure the static service attributes according to the following table.

Table 248 IPX Static Service attributes

Attribute	Description
Static Service (SS#)	Allows you to assign a number to the Static Service. For example, the valid Static Service number for the first Static Service is SS1. The function of the Static Service number is to uniquely identify a Static Service. If you add more than one Static Service, use sequential numbers. If you use the number of an existing Static Service, the system modifies the existing Static Service. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Static Service, you cannot change the Static Service number.
Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Name	Shows the static service name. The permitted values can use up to 48 bytes. A wildcard character (*) can also be selected to indicate all service names.
Network	Shows the network part of the service address. The permitted value uses 4 bytes in hexadecimal format. The default value is **None**.
Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Hops	Shows the number of hops to reach the destination network. The permitted values are **0** to **15**. The default value is **0**.

6. Click the **Save** button to save your settings.

Modifying a Static Service for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Services** tab.
   The Static Service screen appears.
4. Click the Static Service you want to modify.
5. On the **Configuration** menu, choose **Modify Static Service**.
   The Static Routes dialog box appears.
6. Modify the static service attributes.
7. Click the **Save** button to save your settings.

Deleting a Static Service for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Services** tab.
   The Static Service screen appears.
4. Click the Static Service you want to delete.
5. On the **Configuration** menu, choose **Delete Static Service**.
   A confirmation message appears.
6. Click the **Yes** button.

Chapter 35
Configuring Web Cache

When you use Business Communications Manager as a web proxy, Business Communications Manager can store, or cache, information downloaded from the Internet. A proxy is a server that acts on behalf of another. Web caching allows LAN workstations to share common information downloaded from the Internet.

With Business Communications Manager configured as a web proxy with web caching:

- LAN workstations have shorter download times.
- The system stores previously downloaded information for future use by all workstations on the LAN.
- Business Communications Manager retrieves information from the Internet only if it is not already cached or if the cached file is out of date compared to the information on the Internet.

To use the Web Cache on the Business Communications Manager, you must configure the client computer to use an Internet Proxy at port 6800, where the internet proxy is the Business Communications Manager.

The web proxy also provides security features similar to the DNS proxy. It hides all of the internal browsers' IP addresses from external web servers. External web servers see only the Business Communications Manager IP address.

Guidelines for using Web caching/Proxy

The Business Communications Manager web proxy uses a web server for running in HTTP-Proxy mode.

Consider the following guidelines when using web caching/proxy:

- You cannot use the web server installed on Business Communications Manager as a general purpose HTTP server. It is only used by the Business Communications Manager web-based management client and Web Cache services.
- If you want to run web sites on your network, you must have a separate HTTP server running on a system other than the Business Communications Manager system. There are two options available for the IP address you publish for your website. You can publish a separate IP address for the HTTP server or you can publish the same IP address as your Business Communications Manager.
  To publish a separate IP address for the HTTP server, publish the IP address of the computer on which you are running the HTTP server.
  To publish the same IP address used for Business Communications Manager, set up a NAT rule to change the public address of the HTTP server to the IP address of Business Communications Manager.
- Some secure web sites are not accessible through the Business Communications Manager Web Cache service. If you are having problems accessing a secure web site, turn off the Web Cache service and try again.

- Web Cache is enabled by default.

To configure the Web Cache settings:

1. On the navigation tree, click the **Services** key and click the **Web Cache** heading. The Web Cache Summary screen appears.
2. Configure the Web Cache attributes according to the following table.

Table 249 Web Cache attributes

Attribute	Description
Description	Shows the description of the Web Cache server.
Version	Shows the version of the Web Cache server.
Status	Shows the status of the Web Cache server. This setting is read-only. The Web Cache server always runs to provide support for Unified Manager.
Server Address	Allows you to specify which IP address to use for interacting with HTTP clients. Since Business Communications Manager typically has more than one IP interface and associated IP Address, users can choose this value. The default for this value is the IP address of the first LAN interface. This value changes when the IP address of the first LAN interface changes. Exercise caution if modifying this value.
Cache Mode	Allows you to enable or disable the cache mode. The default value is **Enabled**.
Cache Size	Allows you to specify the maximum size (1 - 100,000), in KB, of the cache. The default value is **20480** KB.
Garbage Collection Interval	Allows you to specify the interval, in hours, between garbage collection operations on the cache. The values are **1** to **24**. The default value is **4** hours.
Cache Maximum Life	Allows you to specify the maximum life, in hours, on the proxy server for cached HTTP pages. Values are **1** to **24**. The default value is **24** hours.
Maximum Server Threads	Allows you to specify the number of threads ready to serve HTTP requests in the proxy server. Values are **1** to **255**. The default value is **16** threads.

3. Press the **Tab** key to save the settings.

Chapter 36
Configuring QoS monitor

The IP telephony Quality-of-Service (QoS) Monitor periodically monitors the delay and packet-loss of IP networks between two peer gateways. The Business Communications Manager QoS Monitor uses the same method as the Meridian 1 IPT. These monitoring packets are delivered at UDP port 5000.

This section explains how to set the monitor and how to view the mean opinion score:

How QoS monitoring works

There are 25 monitoring packets traveling in each direction every 15 seconds. Each monitoring package has 88 bytes in the IP layer. These monitoring packets are equally spaced out in the 15-second interval. During this 15-second interval, the packets are sent from transmitting Business Communications Manager system to the receiving system and then returned to the transmitting Business Communications Manager system. This results in an *overhead* in the IP layer of 293 bytes/second in one direction [(2x25x88)/15 = 293 bytes/second].

QoS Monitor works on a gateway between two Business Communications Manager systems or between a Business Communications Manager system and a Meridian 1 IPT system. QoS Monitor must be enabled on both ends of the connection.

For information about how to configure remote gateways, refer to the *Business Communications Manager IP Telephony Configuration Guide*.

Note: The remote gateways are identified by their Published IP Addresses. If a remote gateway is accessed through an interface with Network Address Translation (NAT) configured, the Published IP Address must be the same as one of the Public IP Addresses. For information about NAT, refer to "Configuring NAT (Network Address Translation)" on page 753.

The main objective of the QoS Monitor is to allow new IP telephony calls to fall back to the PSTN if the IP network is detected as "bad".

Note: The QoS Monitor on Business Communications Manager running 3.5 or newer software is not compatible with the QoS Monitor on earlier versions of Business Communications Manager.

If you have earlier versions of Business Communications Manager (version 2.0 to 3.0.1) on your network, you must use the QoS Monitor patch to upgrade QoS Monitor on those systems. If you do not upgrade QoS Monitor on these earlier Business Communications Manager systems, IP telephony calls to those systems will not operate correctly.

To obtain the QoS Monitor patch, contact your Nortel Networks support personal.

Setting the QoS monitor

1. On the navigation tree, click the **Services** key and click the **QoS Monitor** heading. The QoS Monitor Summary screen appears.
2. Configure the QoS Monitor Summary attributes according to the following table.

Table 250 QoS Monitor Summary attributes

Attribute	Description
Description	Shows the description of the service.
Status	Allows you to enable or disable the service.
Version	Shows the version of the service.

3. Press the **Tab** key to save the settings.

Viewing the QoS Monitor Mean Opinion Score

To view the QoS Monitor Mean Opinion Score:

1. On the navigation tree, click the **Services** key and click the **Qos Monitor** key.
2. Click the **Mean Opinion Score** heading.

   If you configure or create remote gateways, the mean opinion scores of the connections to these remote gateways are displayed in the screen. The mean opinion scores are a measure of the quality of the voice link, while using an IP trunk, for each codec type. Each configured gateway appears on a separate row.

   Each row consists of the fields for the name of the remote gateway, its IP address, the status of the QoS monitoring for the connection, and the mean opinion scores for each allowed voice codec type and for each direction.

   If the QoS Monitor setting for the remote gateway entry is Disabled, the MOS values for the remote gateway appear as N/A. If the QoS Monitor service is disabled or down for any reason, all MOS values appear as N/A. Also, if no MOS reports are received from a remote gateway, the MOS values in the Received (Recv) direction appear as N/A.

   The MOS values are updated inside the QoS Monitor service every 15 seconds. These updates are a running average of the last five sampled values, which span approximately 75 seconds.

   The MOS values that appear are updated automatically. To display the current MOS values, on the **View** menu, click **Refresh**.

Table 251 Mean Opinion Score descriptions

Attribute	Description
Name	Displays the name of the Remote Gateway.
Destination IP	Displays the IP address of the Remote Gateway.
QoS Monitor	Displays the status of QoS Monitor for this Remote Gateway. If Enabled is displayed, QoS Monitor is currently collecting QoS information for this Remote Gateway. If Disabled is displayed, QoS Monitor is not collecting QoS information.
QoS Indicator	Displays a text description of the current MOS value. The MOS values can be Poor, Fair, Good or Excellent.
G.711-aLaw Trans	Displays the current MOS value calculated when using a G.711 aLaw codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.711-aLaw Recv	Displays the current MOS value calculated when using a G.711 aLaw codec to receive VoIP packets from this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.711-uLaw Trans	Displays the current MOS value calculated when using a G.711 uLaw codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.711-uLaw Recv	Displays the current MOS value calculated when using a G.711 uLaw codec to receive VoIP packets from this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-5.3kbit/s Trans	Displays the current MOS value calculated when using a G.723 5.3 kbit/s codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-5.3kbit/s Recv	Displays the current MOS value calculated when using a G.723 5.3 kbit/s codec to receive VoIP packets from this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-6.3kbit/s Trans	Displays the current MOS value calculated when using a G.723 6.3 kbit/s codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-6.3kbit/s Recv	Displays the current MOS value calculated when using a G.723 6.3 kbit/s codec to receive VoIP packets from this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).

Table 251 Mean Opinion Score descriptions

Attribute	Description
G.729 Trans	Displays the current MOS value calculated when using a G.729 codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.729 Recv	Displays the current MOS value calculated when using a G.729 codec to receive VoIP packets from this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).

Configuring the logging options

1. On the navigation tree, click the **Services** key and click the **Qos Monitor** key.
2. Click the **Mean Opinion Score** heading and click the **Logging** tab.
   The Logging screen appears.
3. Configure the Logging attributes according to the following table.

Table 252 QoS Monitor Logging attributes

Attribute	Description
Status	Allows you to enable or disable the logging of the Mean Opinion Scores. The default value is Disabled.
Max. Log File Size	Allows you to enter the maximum size the Log File can be. Enter a value of 1 to 10240 kbytes. The default value is 10240 kbytes.
Logging Frequency	Allows you to enter the time that Business Communications Manager waits between logging the Mean Opinion scores. Enter a value of 1 to 1440 minutes. The default value is 5 minutes.

4. Press the **Tab** key to save the settings.

Viewing the Mean Opinion Score log

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

Figure 210 Example Mean Opinion Score Log File

```
Mon Sep 08 08:55:44 2003, EastBranch, 10.10.10.2, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 08:55:44 2003, WestBranch, 10.10.10.5, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 08:55:44 2003, MainBranch, 10.10.10.15, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:00:54 2003, EastBranch, 10.10.10.2, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:00:54 2003, WestBranch, 10.10.10.5, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:00:55 2003, MainBranch, 10.10.10.15, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:06:04 2003, EastBranch, 10.10.10.2, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:06:04 2003, WestBranch, 10.10.10.5, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:06:05 2003, MainBranch, 10.10.10.15, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:11:14 2003, EastBranch, 10.10.10.2, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:11:14 2003, WestBranch, 10.10.10.5, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:11:15 2003, MainBranch, 10.10.10.15, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:16:24 2003, EastBranch, 10.10.10.2, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:16:25 2003, WestBranch, 10.10.10.5, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
Mon Sep 08 09:16:25 2003, MainBranch, 10.10.10.15, Enabled, Poor, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00
```

Date and Time
Name
Destination IP
QoS Monitor
QoS Indicator
G.711-aLaw Trans
G.711-aLaw Recv
G.711-uLaw Trans
G.711-uLaw Recv
G.723-5.3kbit/s Trans
G.723-5.3kbit/s Recv
G.723-6.3kbit/s Trans
G.723-6.3kbit/s Recv
G.729 Trans
G.729 Recv

Chapter 37
Configuring Net Link Manager

Net Link Manager is a Business Communications Manager service that provides constant primary link status monitoring. Net Link Manager is also where you select your WAN primary and backup interfaces.

This section contains information about enabling/disabling Net Link Manager, as well as how to select WAN links:

When Net Link Manager detects a primary WAN link failure, Net Link Manager automatically establishes a backup WAN connection, if one is configured. Net Link Manager monitors the WAN primary link by performing multiple tests. When a predetermined number of tests fails, Net Link Manager establishes the backup connection.

The backup connection uses a V.90 modem (North America) or one or more ISDN B-channel*s*. When the backup WAN connection is active, Net Link Manager continues to monitor the status of the primary WAN link connection. When the primary WAN link connection is determined to be available again, Net Link Manager re-establishes the primary WAN link and disconnects/disables the backup connection.

Warning: If dial-up connection is used as the primary WAN connection, no backup link is available.

Note: Net Link Manager manages the default route in Business Communications Manager. If the primary link fails, Net Link Manager removes the default route from the Primary link and adds it to the backup link. This happens during the switch over from primary to backup link. The default route returns to the primary link after the connection to the primary WAN link is re-established.

Enabling or Disabling Net Link Manager

1. On the navigation tree, click the **Services** key and click the **Net Link Mgr** heading.
   The Net Link Manager Summary screen appears.
2. Configure the Net Link Manager attributes according to the following table.

Table 253 Net Link Manager attributes

Attribute	Description
Description	Shows a description of Net Link Manager.
Version	Shows the version number of the subsystem.
Status	Shows the status of Net Link Manager. This box also provides commands to enable or disable Net Link Manager. Possible values: **Up**, **Disabled**, **Enabled** The default value is: **Up**

3. Press the **Tab** key to save the settings.

Selecting a permanent WAN link as the primary WAN connection

1. On the navigation tree, click the **Services** key and click the **Net Link Mgr** heading.
   The Net Link Manager Summary screen appears.
2. Click the **Primary WAN Connection** tab.
   The Primary WAN Connection screen appears
3. Click the **Mode** box and click **Permanent**.
4. Press the **Tab** key to save your choice.
5. Click the **Permanent WAN Connection Setting** tab
   The Permanent WAN Connection Setting screen appears.
6. Configure the Permanent WAN Connections Setting attributes according to the following table.

Table 254 Permanent WAN Connections settings

Attribute	Description
Next Hop on Primary Link	Allows you to enter the IP address (in dot format) of the next hop router. This address is used by Net Link Manager to add a default route in Business Communications Manager. If this address ever becomes unreachable, Net Link Manager dials the backup link and changes the default route. This is usually the remote router of the primary WAN link.
Up Poll Interval	Allows you to set the polling interval on the Primary WAN Link, in seconds. The up poll interval is the interval between successive pings when the next hop on the primary link is available.

Table 254 Permanent WAN Connections settings (Continued)

Attribute	Description
Down Poll Interval	Allows you to set the polling interval on the Primary WAN Link, in seconds, when the primary WAN link is down, and the backup (dial-up) WAN link is operational. A short interval provides faster recovery.
Switch Over Delay	Allows you to define the interval, in seconds, that Net Link Manager waits before switching back to the primary WAN link when it becomes available. This delay is to let the router at the other end of the primary link recognize that the primary link has come up and allows for necessary routing table updates. The default value is **30** seconds.
Backup Dial-up Interface	Allows you to select which dial up interface to use for WAN backup. You must configure a backup interface before you can select it. When you are configuring the backup interface, make sure you include “backup” in the interface name. Only interfaces that contain the word backup in their name appear on this list. For information about how to create an ISDN backup interface, refer to “Creating an ISDN dial up interface” on page 690.
Fast Backup Switch Over	Allows you enable or disable the Fast Backup Switch Over feature. When Fast Backup Switch Over is enabled, Business Communications Manager uses the Link Status of the WAN interface to reduce the amount of time it takes to switch over to the Backup WAN Link, when the Primary WAN Link is down. When Fast Backup Switch Over is **Disabled**, Business Communications Manager retries contacting the next hop router if there is no response from the previous attempt. If there is no response after several retries, Business Communications Manager switches over to the Backup WAN Link. When Fast Backup Switch Over is **Enabled**, Business Communications Manager checks the Link Status of the WAN interface when there is no response from the next hop router. If the Link Status is Down, Business Communications Manager immediately switches over to the Backup WAN link. If the link status is **Up**, Business Communications Manager attempts to contact the next hop router again. If there is no response after several retries, Business Communications Manager switches over to the Backup WAN Link. **Note**: If Business Communications Manager receives a response from the next hop router on any attempt, it does not switch over to the Backup WAN Link. The default setting is **Disabled**. **Note**: The Fast Backup Switch Over feature does not affect how Business Communications Manager switches from the Backup WAN Link to the Primary WAN Link.

7 Press the **Tab** key to save the settings.

Selecting a dial-up link as the primary WAN connection

The dial-up WAN connection supports PPP only. Business Communications Manager supports ISDN dial-up PPPoE dial-up WAN connections.

Setting a dial-up connection as the primary WAN connection means that the Business Communications Manager default route is to the dial-up connection. If the dial-up WAN connection is configured as dial-on-demand, any traffic across the dial-up WAN connection causes the link to be established. Also, if there is no traffic crossing the connection, the link shuts down automatically after a time out.

Note: When you configure your primary WAN connection to use a dial-up WAN connection, no backup WAN connection is available.

1. On the navigation tree, click the **Services** key and click the **Net Link Manager** heading.
   The Net Link Manager Summary screen appears.
2. Click the **Primary WAN Connection** tab.
   The Primary WAN Connection screen appears
3. Click the **Mode** box and click **Dialup**.
4. Press the **Tab** key to save your choice.
5. Click the **Primary WAN Connection Setting** tab.
   The Primary WAN Connection Setting screen appears.
6. From the **Primary Dial-up Interface** box, click the dial-up interface you want to use.

Tips
Before you can select an ISDN or PPPoE dial-up interface to connect to the network, you must first create the dial-up interface under Resources, Dial up. For information on creating an ISDN dial-up interface, see "ISDN dial up" on page 690. For information on creating a PPPoE dial-up interface, see "Point to Point Protocol on Ethernet (PPPoE)" on page 696.

7. Press the **Tab** key to save the settings.

Chapter 38
Configuring NAT (Network Address Translation)

Business Communications Manager provides security and firewall features to protect your private data resources from outsiders.

This section includes information about the different types of NAT, as well as:

- "Enabling and disabling NAT" on page 754
- "Configuring an Interface with NAT" on page 755

The Network Address Translation feature is a network security feature. NAT translates the IP addresses used within your private network to different IP addresses known to Internet users outside your private network. NAT helps ensure network security because each outgoing or incoming request must go through a translation process that also provides the opportunity to qualify or authenticate the request or match it to a previous request. NAT also translates port numbers.

NAT is defined by creating a set of rules and then defining the order in which these rules are evaluated.

Business Communications Manager supports both static and dynamic NAT for a number of packet types and protocols:

NAT Support for:	Type
Packets (static and dynamic)	TCP, UDP, IP
Protocols	H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, TFTP, GOPHER, FINGER, NNTP, RPC, SUNNFS and SNMP

Static NAT

Static NAT is the one-to-one mapping of an IP address on your private network to an IP address from outside your network. Inbound rules must have external IP addresses mapped to specific internal IP addresses.

Dynamic NAT

Dynamic NAT is the mapping between a private network and the outside network, of one address to a pool of addresses, a pool of addresses to one address or a pool of addresses to another. The mappings are made in a translation table and remain there until the table is cleared or until an entry times out.

Note: When using an inbound translation, be sure that all private addresses belong to the existing systems.

NAT and IP Firewall filters

When you use NAT and IP Firewall filters, there are two interactions you need to be aware of.

- On inbound traffic, the NAT rules are applied before the IP Firewall Filter rules.
- On outbound traffic, the IP Firewall Filter rules are applied before the NAT rules.

Managing Business Communications Manager

You cannot manage a Business Communications Manager system through another Business Communications Manager system when it is on the Private side of a NAT enabled interface.

Enabling and disabling NAT

1 On the navigation tree, click the **Services** key and click the **NAT** heading. The NAT Summary screen appears.

2 Configure the NAT Summary attributes according to the following table.

Table 255 NAT Summary attributes

Attribute	Description
Description	Shows a description of NAT.
Version	Shows the version number of the subsystem.
Status	Allows you to enable or disable NAT. Possible values: **Disabled**, **Enabled** The default value is: **Disabled**

3 Press **Tab** to save the setting.

Note: Do not enabled NAT on systems that use Fast Routing between LANs. If you enable NAT and Fast Routing, the packets will not be routed correctly. For information about Fast Routing, refer to "Setting LAN global parameters" on page 664.

Configuring an Interface with NAT

This section describes how to configure an interface with NAT. It also includes information about:

Adding Default rules

1 On the navigation tree, click the **Services** key and click the **NAT** key.

2 Click the interface you want to configure. For example: **LAN1**.
The Rule Order screen appears.

Note: Rules can be configured in several ways, using default rules, setting up individual rules or a combination of the two.

3 Click the **Default Rules** box and click **Disabled**, **Enabled - include IP phones**, or **Enabled - do not include IP phones**.

If you choose **Enabled - include IP phones**, the NAT default rules apply to all data traffic including IP telephony traffic.
There are three default rules set. The first rule is for outbound TCP/UDP traffic. The second rule is for outbound IP traffic. The third rule is for inbound TCP/UDP traffic on port 7000. The IP address for the Public address is the IP address of the interface you configure. The system automatically fills in the rule order. If you choose to add additional rules, the default rules still remain.

If you choose **Enabled - do not include IP phones**, the NAT default rules do not apply to IP telephony traffic, but does apply to all other traffic.
If you choose this option, there are two default rules set. One is for outbound TCP/UDP traffic. The other is for outbound IP traffic. The IP address for the Public address is the IP address of the interface you configure. The system automatically fills in the rule order. If you choose to add additional rules, the default rules still remain.

If you choose **Disabled**, the Default Rules are removed.
The default is Disabled.

Note: The default rules are only for traffic initiated in the outbound direction. You must add rules for inbound traffic or packets will pass in without translation.

Note: Before you can specify the Rule Order you must first add the Rules.

4 Press the **Tab** key to save the settings.

Adding a Rule to an interface

The maximum number of Rules you can add is 32.

1 Click the **Rule Setting** tab.
The Rule Setting screen appears.

2 On the **Configuration** menu, click **Add Rule**.
The Rule Setting dialog box appears.

3 Configure the Rule settings according to the following table.

Table 256 NAT Rule Settings

Attribute	Description
Rule Name (R#)	Allows you to assign a number to the Rule. The Rule Name uniquely identifies a Rule. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the rule. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing rule name, it modifies the existing rule. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a rule, you cannot change the rule name. The rule name does not have any significance other than identifying an entry.
Direction	Allows you to choose the direction of the rule: **In** or **Out**.
Protocol	Allows you to choose the protocol for this interface; **IP**, **TCP**, **UDP**, or **TCP/UDP**.
Private IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Private IP and Private Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Private IP	Allows you to specify the Private IP address. If the Private IP type is fixed, the Rule is invalid without this IP address.
Private Range Mask	Allows you to specify the mask to use with the Private IP. If you want the Rule to apply to a single Private IP address (the Private IP entered), enter 255.255.255.255. If you want the Rule to apply to all Private IP addresses, enter 0.0.0.0.
Private Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **SNMP-TRAP**, **DNS**, **TFTP**, **Gopher**, **Finger**, **H.323**, **HTTP**, **POP3**, **NNTP**, **RPC**, **SUNNFS**, and **UNISTIM**.

Table 256 NAT Rule Settings (Continued)

Attribute	Description
Public IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Public IP and Public Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Public IP	Allows you to specify the Public IP address. This address should be on the outside network.
Public Range Mask	Allows you to specify the mask to use with the Public IP. If you want the Rule to apply to a single Public IP address (the Public IP entered), enter 255.255.255.255. If you want the Rule to apply to all Public IP addresses, enter 0.0.0.0.
Public Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **SNMP-TRAP**, **DNS**, **TFTP**, **Gopher**, **Finger**, **H.323**, **HTTP**, **POP3**, **NNTP**, **RPC**, **SUNNFS**, and **UNISTIM**.

Note: If you do not configure the public and private masks correctly, mappings to non-existent systems can occur. You must specify addresses that exist. For example, if you configure an outbound rule, the Public IP address and Public Mask are the translated addresses. These addresses must be assigned or packets will be sent to a non-existent destination. For inbound rules, the translated address is the Private Address and Mask.

If you want the rule to apply to one IP address only, you must enter a Mask of 255.255.255.255. If you enter any other Mask, the rule will apply to more than one IP address.

4 Click the **Save** button.

Modifying a Rule to an Interface

1 Click the **Rule Setting** tab.
The Rule Setting screen appears.

2 Click the rule you want to modify.

3 On the **Configuration** menu, click **Modify Rule**.
The Rule Setting dialog box appears.

4 Modify the Rule settings.

5 Click the **Save** button.

Deleting a Rule to an Interface

1. Click the **Rule Setting** tab.
   The Rule Setting screen appears.
2. Click the rule you want to delete.
3. On the **Configuration** menu, click **Delete Rule**.
   A message appears that asks you to confirm the deletion.
4. Click the **Yes** button.

Configuring the Rule order

1. When you finish adding rules, click the **Rule Order** tab.
   The Rule Order screen appears.
2. In the **Rule Order** box, configure the order of the rules.

Note: Configure the rule order from most specific to most general. For example, a TCP rule for one port should come before a general rule for all TCP traffic. IP rules should come last.

3. Press **Tab** to update the screen.

Examples of common NAT configurations

A Business Communications Manager has two LANs and a WAN. The WAN connects to the outside and has one public IP address. The LANs are part of a private network. The system maps all outgoing traffic. HTTP traffic is mapped to 10.10.10.4. LAN1 subnet is 10.10.10.0, LAN2 is 10.10.11.0. The WAN address is 48.123.35.41.

The rules would be as follows:

Rule: R4
Direction: In
Private IP Type: Fixed
Protocol: TCP
Private IP Address: 10.10.10.4
Private IP Mask: 255.255.255.255
Private Port Range: HTTP
Public IP type: Fixed
Public IP Address: 48.123.35.41
Public IP mask: 255.255.255.255
Public Port Range: 8080

Default Rules: Enabled Including IP Phones

Rule Order: R1,R2,R3,R4

Note: This setting for Default Rules adds three rules. Additional rules start at R4.
Note: Spaces are not allowed between rule numbers.

A Business Communications Manager has two LANs and a WAN. The WAN connects to an Internet Service Provider that assigns the IP address. The LANs are part of a private network. The system maps all outgoing traffic. HTTP traffic is mapped to 10.10.10.4. LAN1 subnet is 10.10.10.0, LAN2 is 10.10.11.0.

The rules would be as follows:

Rule: R4
Direction: In
Private IP Type: Fixed
Protocol: TCP
Private IP Address: 10.10.10.4
Private IP Mask: 255.255.255.255
Private Port Range: HTTP
Public IP type: Dynamic
Public IP Address: <leave blank>
Public IP mask: <leave blank>
Public Port Range: 8080

Default Rules: Enabled Including IP Phones

Rule Order: R1,R2,R3,R4

Chapter 39
Configuring NTP Client

Network Time Protocol (NTP) is an IP protocol that allows you to synchronize the time on your network devices. The NTP Client allows you to synchronize the time on your Business Communications Manager system with the NTP Server on your network. This ensures that your Business Communications Manager is using the same time as the other Business Communications Manager systems and servers on your network.

There are two clocks operating on the Business Communications Manager system.

- Business Communications Manager system clock: The system clock is used for scheduled tasks and the time stamp on events and alarms. The NTP client synchronizes the system clock with the NTP server time.
- Business Communications Manager telephony clock: The telephony clock provides the time that appears on the Business Communications Manager telephones. The telephony clock gets its time updates from the system clock. Due to delays in the system, there may be a difference between the system time and the time that appears on the telephones.

The information in this section includes:

Configuring the NTP Client settings

Configure the NTP client settings:

1. On the navigation tree, click the **Services** key and click the **NTP Client Settings** heading. The NTP Client Settings screen appears.
2. Configure the NTP Client settings according to the following table.

Table 257 NTP Client settings

Attribute	Description
NTP Server Address	Enter the IP address of the NTP Server to which you are synchronizing the Business Communications Manager time.
Maximum Time Adjustment	Enter the maximum amount of time, in seconds, that the Business Communications Manager system clock can be out of sync with the NTP Server time. Any time difference greater than this value causes the Business Communications Manager time to require manual update. For example, if the Maximum Time Adjustment is set to 60 seconds, but the time difference is 65 seconds, the Business Communications Manager system clock is not updated. **Note**: The next time change update is determined by the **Set Time Every** option. The default value for this option is 0. A value of 0 means there is no Maximum Time Adjustment, so the Business Communications Manager system clock is changed regardless of what the time discrepancy is between the Business Communications Manager and the NTP Server.
Exit After Setting Time Once	Select whether the NTP Client exits after a time adjustment. Choose **Enabled** if you want the NTP Client Service to stop after a time adjustment is made. When you choose Enabled, the time is set only once. Choose **Disabled** if you want the NTP Client Service to continue running after a time adjustment is made.
Set Time Every	Enter the number of seconds between time updates. The default is 86400 seconds (24 hours). **Tip**: An event is entered into the Event Log each time Business Communications Manager accesses the NTP server to check for a time update. If you enter a short time period in this field, the Event Log will quickly fill with VoiceTimeSynch events.
Minimum Time Adjustment	Enter the time difference that must exist between the Business Communications Manager and the NTP Server before a time adjustment is made. If the time difference is less then the number of seconds entered, the time on the Business Communications Manager is not changed.
NTPClient Service Start Type	Select whether the NTP Client Service starts automatically. Choose **Automatic** if you want the NTP Client Service to start now and to start automatically whenever Business Communications Manager is started up or rebooted. Choose **Manual** if you want to start the NTP Client Service manually. For information on how to start the NTP Client Service, refer to "Starting the NTP Client Service" on page 763.

3. Press the **Tab** key to save your settings.

Starting the NTP Client Service

If you set the NTPClient Service Start Type option to Automatic, the NTP Client service starts automatically and will automatically start whenever Business Communications Manager is started up or rebooted.

If you set the NTPClient Service Start Type option to Manual, you must start the NTP Client Service the first time you configure the NTP Client settings. You must also start the NTP Client Service whenever Business Communications Manager is started up or rebooted.

To start the NTP Client Service:

1. On the navigation tree, click the **Diagnostics** key and the **Service Manager** heading. The Service List screen appears.
2. Scroll down the list of until the VoiceTimeSynch service appears.
3. Click the **VoiceTimeSynch** service.
4. On the **Configuration** menu, click **Modify Services**. The Services List dialog box appears.
5. Configure the settings according to the following table.

Table 258 NTP Client Service settings

Attribute	Description
Startup	Select whether the NTP Client Service starts automatically. Choose **Automatic** if you want the NTP Client Service to start automatically when Business Communications Manager is started up or rebooted. Choose **Manual** if you want to start the NTP Client Service manually. Choose **Disabled** to disable the NTP Client Service.
Status	Allows you to view and change the status of the NTP Client Service. Choose **Start** to start the NTP Client Service. When the service successfully starts, the status changes to Running. Choose **Stop** to stop the NTP Client Service. When the service successfully stops, the status changes to Stopped.

6. Click the **Save** button.

Manually updating the Business Communications Manager time

You can force the NTP Client to update the Business Communications Manager time by manually updating the time.

To manually update the time:

1. On the navigation tree, click the **Services** key and click the **NTP Client Settings** heading. The NTP Client Settings screen appears.
2. On the **Tools** menu, click **Update Time**. A confirmation dialog box appears.
3. Click the **Yes** button to update the time.

Note: Do not manually update the Business Communications Manager time until you have configured the NTP Client.

Chapter 40
Virtual Private Networks (VPN)

Business Communications Manager uses the Internet and tunneling protocols to create secure extranets. These secure extranets require a protocol for safe transport from the Business Communications Manager to another device through the Public Data Network (PDN). Business Communications Manager uses the PPTP ("PPTP" on page 766) and IPSec ("IPSec" on page 777) tunneling protocols. Both of these protocols have encryption, but IPSec has a slightly more secure hashing algorithm for negotiating keys.

Extranets can connect:

- mobile users to a fixed private network at their office over the PDN
- private networks in the two branch offices of the same corporation over PDN
- two divisions of the same corporation over the corporate intranet

When connecting two branch offices, the use of a VPN over the public data network is very efficient if the connection is required only intermittently or a dedicated point-to-point link is considered too expensive. Also, with the advent of business-to-business solutions, VPNs can be deployed to provide secure connections between corporations.

PPTP tunnel notes

PPTP tunnels are used when a mobile user wishes to connect securely to a Business Communications Manager or when using the IPX network protocol. PPTP client software is required to use a PPTP tunnel. This client software is available for all personal computer operating systems from Microsoft. This client is included in Windows 98.

PPTP tunnels are created from a client to a server or from a server to a server. To form an extranet using PPTP, a mobile, remote user does the following:

- Establishes a connection with the public data network's point-of-presence (POP), typically through an Internet service provider (ISP) using dial up links.
- After the Internet connection is up, the remote user launches a second connection which is a VPN tunnel to Business Communications Manager. The Business Communications Manager public IP address is used to establish the tunnel.
- On the Business Communications Manager, the user id of the incoming user is enabled for dial-in access.

IPSec tunnel modes

In the IPSec Specification, there are two tunnel modes defined: tunnel mode and transport mode. Business Communications Manager supports only tunnel mode. Tunnel mode describes a method of packetizing TCP/IP traffic to create a virtual tunnel.

Tunnels are created between servers, which are also known as gateways. This is called a Branch Office Connection. The end nodes connect to each other through gateways. These gateways set up the tunnel over the PDN on behalf of the end nodes. The establishment of the tunnel, and the PDN in between, is transparent to the end nodes which behave as if they are interacting through a router. Typically, the edge devices connecting the branches of a corporation to the ISP use VPN in this mode.

Business Communications Manager is compatible with the Contivity Extranet Switch and the Shasta 5000.

The following sections describe configuring the tunnel portion of Business Communications Manager using PPTP or IPSec.

PPTP

PPTP is a tunneling protocol supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 (www.microsoft.com) and is built-in to Windows 98 and later. Third-party vendors have developed PPTP clients for Windows 3.1 and the Macintosh operating system.

The PPTP client and PPTP server software are components on Business Communications Manager.

Note: PPTP uses Remote Access Service (RAS) to establish connections. For this reason, you must do some Dial Up resources configuration when you configure for some of the PPTP configuration parameters.

This section includes information about:

PPTP offers the following features:

- Support for multiple authentication schemes: MS-CHAP, CHAP, or PAP.
- Support for IP address translation via encapsulation.
- Support for IPX tunneling.
- Support for RC4 encryption.
- Support for compression of data packets.

Settings required for PPTP tunnels

The data packets that pass through PPTP tunnels interact with other routing features in Business Communications Manager. As a result, there are several settings you must make in other features for PPTP tunnels to operate.

NAT (Network Address Translation)

You cannot set NAT rules on traffic that goes through the PPTP tunnel. You can set NAT rules for the end points of the PPTP tunnel.

For information about how to change the NAT settings, refer to "Configuring NAT (Network Address Translation)" on page 753.

QoS

You cannot set QoS rules on traffic that goes through the PPTP tunnel. You can set QoS rules for the end points of the PPTP tunnel.

IP Routing and IPX Routing

Do not create a static route to the far end of the tunnel. If you do, packets will not be sent through the tunnel. PPTP sets up the necessary routes when the tunnel is enabled.

Filters

You must set the following parameters in IP Firewall filter programming.

- Allow PPTP protocol under the Protocol field for traffic to and from Business Communications Manager.
- Allow traffic to and from Business Communications Manager on the PPTP port (1723/tcp).

You cannot set IP Firewall filter rules on traffic that goes through the PPTP tunnel. You can set IP Firewall filter rules for the end points of the PPTP tunnel.

For information about how to change Filters, refer to "Configuring IP Firewall Filters" on page 831.

IP Addresses and DHCP Server

Ensure that the IP addresses for the LAN interfaces, WAN interfaces, dial up links, and PPTP tunnels are unique across all sites. This simplifies configuration, eliminates conflicts due to NAT, and prevents the addresses assigned by the DHCP server from conflicting with the IP addresses of subnets in remote sites.

For information about how to change the DHCP Server settings, refer to the DHCP section.

DNS Server

We recommend the following configuration if you are using a DNS Server:

- Choose one of the offices to act as the primary office. The server in primary office must have a dedicated link to the Internet.
- Make the server in the primary office the primary domain server. Ensure the DNS Server in the primary office contains all of the entries for allow the branch offices.
- Configure the DNS Servers in the branch offices to run in cache mode only. Allow a larger time out value on the branch DNS servers to accommodate for on-demand setup of PPTP tunnels to the primary office.
- Configure the branch DNS servers to forward DNS Server requests to the Internet Service Provider first and then to the DNS Server in the primary office.

For information about how to configure the DNS proxy service on Business Communications Manager, refer to the "Configuring DNS" on page 703.

Changing the PPTP settings

The settings of the PPTP Summary screen apply to all of the PPTP tunnels created.

To change the PPTP settings:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading.
   The PPTP Summary screen appears.
3. Configure the PPTP Summary settings according to the following table.

Table 259 PPTP Summary settings

Attribute	Description
Description	Displays the name of the PPTP service. This is a read only attribute.
Version	Displays the version number of the PPTP service. This is a read only attribute.

Table 259 PPTP Summary settings (Continued)

Attribute	Description
Keep Alive Interval	Allows you to specify the amount of time Business Communications Manager waits without any data traffic on the tunnel before it sends an Echo Request message. When the far end of the tunnel receives an Echo Request, the system at the far end must send an Echo Response message. If the far end of the tunnel sends an Echo Response message, Business Communications Manager keeps the tunnel open. If the far end of the tunnel does not send an Echo Response message, the tunnel is closed. You can enter a value from 1 to 65000 seconds. The default value is 60 seconds.
Echo Timeout	Allows you to specify the amount of time Business Communications Manager waits for an Echo Response message. If the Echo Response message is not received before this time limit, Business Communications Manager tears down the PPTP tunnel. You can enter a value from 1 to 65000 seconds. The default value is 60 seconds.
Max TCP Retransmissions	Allows you to specify the maximum number of times TCP retransmits the data packets. Data packets are retransmitted when the far end of a TCP connection does not acknowledge the receipt of a data packet. Business Communications Manager uses a TCP connection to establish a PPTP tunnel. The tunnel establishment packets may get lost while being transported over busy internet, effecting the private network connectivity between sites. Therefore, it is recommended to tune this parameter according to the performance of the internet carrying the PPTP tunnel traffic. You can enter a value from 1 to 65000 packets. The default value is 9 packets. **Note**: If you change this value, you must reboot Business Communications Manager.
Client IP Authentication	Allows to enable or disable Client Authentication. When Client Authentication is enabled, only clients entered on the Client List screen can open a PPTP tunnel. When Client Authentication is disabled, any client with valid credentials can open a PPTP tunnel. Note that valid credentials are required for clients on the Client List as well. You can choose Enabled or Disabled. The default value is Disabled. **Note**: If you change this value, you must reboot Business Communications Manager.

4 Click the **Tab** key to save the settings.

Adding a PPTP client

A PPTP Client is a remote Business Communications Manager or other similar PPTP capable device that you allow to connect to this Business Communications Manager to establish a PPTP tunnel.

The maximum number of PPTP clients is 32.

To add a PPTP client:

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **PPTP** heading.
The PPTP Summary screen appears.

3 Click the **Clients IP List** tab.
The Clients IP List screen appears.

4 On the **Configuration** menu, click **Add to Client IP List**.
The Client IP dialog box appears.

5 Configure the PPTP Client attributes according to the following table.

Table 260 PPTP Client attributes

Attribute	Description
Client	Displays the Client identifier. This is a read only attribute.
Client IP Address	Enter the IP address of the system you are allowing to use a PPTP tunnel to connect to Business Communications Manager. Enter the IP address in the dotted format.

6 Click the **Save** button.

Deleting a PPTP client

To delete a PPTP client:

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **PPTP** heading. The PPTP Summary screen appears.

3 Click the **Clients IP List** tab. The Clients IP List screen appears.

4 Click the PPTP client you want to delete.

5 On the **Configuration** menu, click **Delete From Client IP List**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button to confirm the deletion.

Adding a PPTP tunnel

You can create a PPTP tunnel from a Business Communications Manager system to another Business Communications Manager system or from a Business Communications Manager system to a Contivity Extranet Switch.

Note: When you create a PPTP tunnel, a user profile is created for the tunnel. This user profile is the profile a person uses when they connect to Business Communications Manager using this tunnel. The user name for the profile created is the same as the interface name for the PPTP tunnel.

The maximum number of PPTP tunnels running at one time is 10.

To add a PPTP tunnel:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading.
   The PPTP Summary screen appears.
3. Click the **Add** menu.
   Or, right click the PPTP heading and click **Add**.
   The Add PPTP dialog box appears.
4. Configure the PPTP Tunnel attributes according to the following table.

Table 261 PPTP Tunnel attributes

Attribute	Description
Tunnel Name	Allows you to specify the name that is used to identify this tunnel. This name is the User ID for the remote end of the tunnel. For information about the User ID, refer to "User ID" on page 774.
Incoming Password	Allows you to specify the password used by the other end of the tunnel to connect to this PPTP tunnel on this Business Communications Manager. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.
Confirm Incoming Password	Allows you to re-enter the incoming password to confirm that you have entered the password correctly.
Port Name	Allows you to specify the VPN port that this PPTP tunnel will use. Several PPTP tunnels can be assigned a single VPN port, however only one PPTP tunnel can use the port at a time. To avoid port contention, choose a VPN port that is not frequently used by other PPTP tunnels.

5. Click the **Save** button to add the tunnel.

Configuring a PPTP tunnel

After you have added the PPTP tunnel you need to configure the PPTP settings. To configure a PPTP tunnel:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** key.
3. Click the PPTP tunnel you want to configure.
   The Tunnel Summary screen appears.
4. Configure the Tunnel Summary attributes according to the following table.

Table 262 PPTP Tunnel Summary attributes

Attribute	Description
Interface	Displays the name used to identify this tunnel.
IP Address	You can select **RemoteAssigned** to specify that the IP address for this PPTP tunnel is assigned by the remote device automatically. During tunnel establishment, this end of the tunnel requests an IP address. The PPTP server component on the remote end of the tunnel provides one either from its local pool or from a DHCP server running in that site. If you want Business Communications Manager to provide an IP address from its local pool, you must configure the **Static IP Address Pool** parameter in Dial Up resources. For information about configuring this parameter, refer to "Configuring the dial up global parameters" on page 685. You can also use a static IP address, but this requires coordinating this address on both ends of the the tunnel. Nortel Networks recommends that you use the **RemoteAssigned** option whenever possible.
Description	Allows you to enter a brief description of the PPTP tunnel.
Interface Status	Displays the current status of the interface used by the PPTP tunnel. The status can be Disabled or Enabled. You can change the status of the interface by selecting **Disable** or **Enable**.
Connection Status	Displays the current connection status of the PPTP tunnel. The status can be Connected or Disconnected. You can change the status of the PPTP tunnel by selecting **Connect** or **Disconnect**. When the Interface Status is Enabled, the PPTP tunnel is normally in the Connect state or in the Disconnect state. You can change it to Connect state to connect the tunnel manually and to Disconnect state to disconnect the tunnel manually - irrespective of the Tunnel Link attributes. **Note**: You cannot Disable the tunnel when the status is UP. To Disable the tunnel, you must: 1. Stop all traffic through the tunnel. 2. Change the Connection Status to Disconnect. 3. Change the Interface Status to Disabled.

5 Click the **Tunnel Link Parameters** tab.
The Tunnel Link Parameters screen appears.

6 Configure the Tunnel Link Parameters according to the following table.

Table 263 PPTP Tunnel Link parameters

Attribute	Description
Remote PPTP Server - Primary	Allows you to specify the IP address of the primary PPTP server to which this tunnel connects. Enter the IP address in the dotted format. A DNS name of the PPTP server can be specified for this attribute. However, it takes longer to establish a PPTP tunnel since a DNS resolution must happen first. In branch configurations, the actual DNS server may reside in another location which could cause the DNS resolution to take even more time. Therefore, it is recommended that IP addresses in dotted decimal format be specified for Primary PPTP Server and the Secondary PPTP Server, if it exists.
Remote PPTP Server - Secondary	Allows you to specify the IP address of the PPTP server to which this tunnel connects when the primary server is not available. Enter the IP address in the dotted format.

Table 263 PPTP Tunnel Link parameters (Continued)

Attribute	Description
Connect retries	Allows you to specify the maximum number of times this tunnel attempts to connect to the primary PPTP server. If a connection is not made after the specified number of retries, this tunnel attempts to connect to the secondary PPTP server. If a connection to the secondary PPTP server is not made after the specified number of retries, the tunnel connection fails. Enter a value from 0 to 10. If you enter a value of 0, Business Communications Manager does not try to connect again.
Retry interval	Allows you to specify the number of seconds Business Communications Manager waits between connect retries. Enter a value from 1 to 3600000 seconds.
Connection type	Allows you to specify when the tunnel is established and when it is torn down. A **Persistent** tunnel is brought up as soon as the Business Communications Manager starts. The tunnel remains connected until Business Communications Manager shuts down or an administrator manually disconnects the tunnel by changing the status to Down. An **On Demand** connection is established only when the connectivity provided by it is needed. Administrators specify the destination networks reachable through a tunnel in the Destination Networks tab. When a packet bound for any of those destinations reaches this Business Communications Manager, Business Communications Manager brings up this tunnel. An On Demand tunnel is torn down when an administrator manually changes its status to Down or after the Idle Timeout period as expires.
Idle timeout	Allows you to specify how long Business Communications Manager waits when there is no traffic on the tunnel before the PPTP tunnel is torn down. Idle timeout only applies to tunnels that have a Connection type of on-demand. Persistent PPTP tunnels are not automatically torn down. Enter a value from 0 to 32000 seconds. A value of 0 disables automatic tear down of the tunnel
Data Compression	Allows you to specify if the data sent in this tunnel is compressed. Select Enabled or Disabled.

7 Click the **Tunnel Authentication Parameters** tab.
The Tunnel Authentication Parameters screen appears.

8 Configure the Tunnel Authentication Parameters according to the following table.

Table 264 PPTP Tunnel Authentication parameters

Attribute	Description
Authentication type	Allows you to specify the type of authentication is used for this tunnel. You can select: AllowClearText (PAP authentication), EncryptedOnly (CHAP authentication) or Microsoft Encrypted Only (MS-CHAP). It is recommended that you use MS-CHAP if you are using Data Encryption.
Two Way Authentication	Allows you to enable or disable two way authentication for this tunnel. If you disable two way authentication, the client sends authentication parameters to the server and server verifies the parameters. If you enable two way authentication, the server verifies the client and the client verifies the server.
Data encryption	Allows you to specify the encryption method used for tunneled data. You can choose no encryption (Disabled) or 40-bit encryption (Enabled).

Table 264 PPTP Tunnel Authentication parameters (Continued)

Attribute	Description
User ID	Allows you to specify the User ID that this end of the tunnel sends to the far end of the tunnel for authentication during tunnel establishment. If you are using another Business Communications Manager on the far side of the tunnel, this User ID needs to match the tunnel name or interface name specified on the far side of the tunnel. If you are not using another Business Communications Manager on the far side, then this User ID must satisfy the authentication and other criteria for that device.
Password	Allows you to specify the password used to authenticate with the far side of the tunnel. If PAP is being used, this value is treated as simple password. If CHAP or MS-CHAP is used, this value is used as the CHAP secret and the actual password is not passed over the link. Not sending the actual password provides extra security. This value must match the Incoming Password value specified for the tunnel on the far end. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.

9 Click the **Destination Networks** tab.
The Destination Networks screen appears.

From the Destination Networks screen you can add, modify and delete Destination Networks.

Add a Destination Network

The maximum number of Destination Networks is 128.

1 On the **Configuration** menu, click **Add Destination Network**.
The Destination Networks screen appears.

2 Configure the Destination Networks attributes according to the following table.

Table 265 PPTP Destination Networks attributes

Attribute	Description
Entry (N#)	Displays the Destination Network identifier. This is a read only attribute.
Destination Network	Allows you to enter the IP address of the network or hosts that can be reached through this PPTP tunnel. These IP addresses correspond to the private LAN addresses in the remote sites connected by this tunnel. When this Business Communications Manager receives a data packet from the networks behind it with destination address in these destination networks, Business Communications Manager routes those packets through this tunnel. If this tunnel is not active, it is automatically brought up. Note that Destination Networks are not necessary for persistent connections. Enter the IP Address of the destination network in the remote site in dotted notation.

Table 265 PPTP Destination Networks attributes (Continued)

Attribute	Description
Subnet Mask	Allows you to specify the subnet mask for the destination network. You require Subnet Mask only if you have entered a value in the Destination Network box. Always use a valid subnet address and mask pair. If you are using a mask that contains more than 1 host address, then always specify the subnet number that corresponds to that subnet and not any other address. For example, if you are using a mask of 24 bits, (255.255.255.0) then use a subnet number of 192.168.100.0 and not something like 192.168.100.11 (where the last number should have been 0). Enter the subnet mask in the dotted format.
Preference Level	Allows you to specify the preference level for this tunnel. When there are multiple tunnels assigned to a destination network, the preference level determines which tunnel is used to connect to the destination network. Business Communications Manager attempts to use the tunnel with the lowest preference number first. If the connection fails, Business Communications Manager retries the connection as many time as is specified in the Connect retries box on the Tunnel Link Parameters screen. After the specified number of retries fails, Business Communications Manager attempts to use the tunnel with the next lowest preference level. Business Communications Manager continues to attempt to establish a tunnel until a connection succeeds or all of the tunnels to the destination network have failed. For example, a site may have two connections to the internet to take advantage of varied capacities and costs. You can maintain a PPTP server at each of these connection points. When you are specifying PPTP tunnels to reach private networks in this site, you may want to use the connection that is most cost-effective first and use the other connection only if the most cost effective connection is not in service. To do this, you create two tunnels to reach the site. You specify the corresponding PPTP server addresses for each tunnel, but enter the same destination addresses (unless you want to distinguish between the normal and stand-by operation). However, for the most desired connection to the site, you specify higher precedence level for the tunnel by putting a lower value for Preferred Level than for the other tunnel. When a packet is received by Business Communications Manager with the destination address of this site, Business Communications Manager tries to bring up the most desired tunnel. If the connection succeeds, tunnel is established. If Business Communications Manager cannot connect to this tunnel after the specified number of retries, it attempts to bring up the 'less desired' tunnel using its parameters. This feature is useful for providing redundant links to sites that have multiple connections to the internet. Note that this parameter is only used with On Demand tunnels.

3 Click the **Save** button.

Modifying a Destination Network

1 Click the Destination Network to modify.

2 On the **Configuration** menu, click **Modify Destination Network**.
The Destination Networks screen appears.

3 Change the Destination Networks attributes.

4 Click the **Save** button.

Deleting a Destination Network

1 Click the Destination Network to delete.

2 On the **Configuration** menu, click **Delete Destination Network**.
A message prompts you to confirm the deletion.

3 Click the **Yes** button to confirm the deletion.

Deleting a PPTP tunnel

Note: Before you delete a PPTP tunnel, delete any destination networks assigned to the tunnel.

To delete a PPTP tunnel:

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **PPTP** key.

3 Click the PPTP tunnel you want to delete.
The Tunnel Summary Parameters screen appears.

4 Click the **Delete** menu.
Or, right click the PPTP heading and click **Delete**.
A message prompts you to confirm the deletion.

5 Click the **Yes** button to confirm the deletion.

Note: When you delete a PPTP tunnel, the user profile for the tunnel is not deleted. Since the user profile has dial-in permission, a person at the remote end can still access the Business Communications Manager system using this user profile. To prevent dial-in access from the remote site, you must also delete the user profile that has the same user name as the interface name for the PPTP tunnel. For information about how to delete a user profile, "Deleting a user profile" on page 114.

IPSec

The IPsec tunneling protocol is supported by Nortel Networks and other third-party vendors. IPsec is an emerging standard that offers a strong level of encryption (DES and Triple DES), integrity protection (MD5 and SHA), and the IETF-recommended Internet Security Association & Key Management Protocol (ISAKMP) and Oakley Key Determination Protocols.

This section includes information about:

IPsec offers the following features

- Branch Office support that allows you to configure an IPSec tunnel connection between two private networks.
- Client support via the Contivity VPN client. The Business Communications Manager supports VPN client support from a remote computer with version 4.60 of the Contivity VPN Client installed. No special ISP services are required.
- Support for IP address translation via encapsulation, packet-by-packet authentication.
- Strong encryption and token codes.

Encryption

All of the following encryption methods ensure that the packets have come from the original source at the secure end of the tunnel. Note that some of the encryption types will not appear on some non-US models that are restricted by US Domestic export laws.

The following table shows a comparison of the security provided by the available encryption and authentication methods.

Table 266 Comparing Encryption and Authentication Methods

Method (strongest to weakest)	Encryption of IP Packet Payload	Authentication of IP Packet Payload	Authentication of Entire IP Packet
ESP Triple DES SHA1	Yes	Yes	No
ESP Triple DES MD5	Yes	Yes	No
ESP 56-bit DES SHA1	Yes	Yes	No
ESP 56-bit DES MD5	Yes	Yes	No
ESP 40-bit DES SHA1	Yes	Yes	No
ESP 40-bit DES MD5	Yes	Yes	No
AH HMAC SHA1	No	No	Yes
AH HMAC MD5	No	No	Yes

Note: Using higher-level encryption, such as Triple DES, requires more system resources and increases packet latency. You need to consider this when designing your overall network.

Note: If two devices have different encryption settings, the two devices will negotiate downward until they agree on a compatible encryption capability. For example, if Switch A attempts to negotiate Triple DES encryption with Switch B that is using 56-bit DES, then the Switch B will reject Triple DES encryption in favor of the 56-bit DES.

Each of the systems must have at least one encryption setting in common. If they do not, a tunnel will not be negotiated. In the example above, both systems must have 56-bit DES enabled.

The encryption level you choose is made of three components:

- the protocol
- the encryption method
- the authentication method

Protocol

The protocol can be ESP or AH.

- ESP
  Encapsulating Security Payload (ESP) provides data integrity, source authentication and confidentiality for IP datagrams by encrypting the payload data to be protected. ESP uses the Data Encryption Standard (DES) and Triple DES algorithms.
- AH
  Authentication Header (AH) provides data integrity and source authentication. The AH method does not encrypt data.

Note: The use of a NAT device in the IPSec tunnel path can sometimes cause the AH method to report a security violation. This occurs because the NAT device changes the IP Address of an AH authenticated packet causing the authentication of this packet to fail.

Encryption method

The encryption method can be Triple DES, 56-bit DES or 40-bit DES. Triple DES is the strongest encryption and 40-bit DES is the weakest encryption.

- Triple DES
  Triple DES is an encryption block cipher algorithm that uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits. These three steps triple the complexity of the algorithm.
- 56-bit DES
  56-bit DES is an encryption block cipher algorithm that uses a 56-bit key (with 8 bits of parity) over a 64-bit block. The 56 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.
- 40-bit DES
  40-bit DES is an encryption block cipher algorithm that uses a 40-bit key (with 8 bits of parity) over a 64-bit block. The 40 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps. Both 40- and 56-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.

Authentication method

The authentication method can be SHA1 or MD5.

- SHA1
  Secure Hash Algorithm (SHA1) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. SHA1 does not encrypt data.
- MD5
  Message Digest 5 (MD5) Algorithm produces a 128-bit hash. It is used to confirm the authenticity of a packet. MD5 does not encrypt data. Also, MD5 provides integrity that detects packet modifications.

Both SHA1 and MD5 use Hashed Message Authentication Code (HMAC) to improve authentication. HMAC is a technique that uses a secret key and a message digest function to create a secret message authentication code.

IPSec capacity restrictions

The Business Communications Manager performs all IPSec processing using software. To prevent overloading the Business Communications Manager processor with IPSec traffic processing, the network traffic that requires IPSec processing should not exceed 6Mbps. This is based on using 3DES encryption with SHA authentication.

The maximum number of concurrent tunnels the Business Communications Manager supports is 16. However, this number could be less depending on the configuration. The following are the factors to consider when determining maximum IPSec capacity:

- Tunnel negotiation
  Since tunnel negotiation requires a significant amount of processing time, the number of tunnels that are negotiated at one time should be limited. The tunnels are re-negotiated based on either the Rekey Timeout or the Rekey Data Count. If a number of tunnels will be running concurrently, you should stagger these values.
- Interface throughput
  The maximum throughput of the interfaces of the IPSec endpoints must also be considered. It is much easier to overload the Business Communications Manager if IPSec is being used over a fast LAN interface rather than a slower WAN interface. This is due to the faster speed of the data packets transferred over the LAN interface.

Settings required for IPSec tunnels

The data packets that pass through IPSec tunnels interact with other routing features in Business Communications Manager. As a result, there are several settings you must make in other features for IPSec tunnels to operate.

NAT (Network Address Translation)

Business Communications Manager does not support NAT on the Local Endpoint of an IPSec Tunnel.

Packets can be sent through an IPSec tunnel with or without NAT applied. To send packets through the tunnel with NAT applied, configure the Local Accessible Networks to include only a network for the endpoint itself. For example, if the Local Endpoint is 10.10.13.2, then the Local Accessible Network would be 10.10.13.2 with a mask of 255.255.255.255. To send packets through the tunnel without NAT applied, configure the Local Accessible Networks with the local Private IP network(s) and the Remote Accessible Networks with the networks on the other side of the Remote Endpoint. Using the above example, we know that the other interfaces on the local Business Communications Manager have IP addresses of 10.10.10.1 and 10.10.11.1. The remote Business Communications Manager has a subnet of 12.12.12.1. Therefore, the Local Accessible

Networks would have two networks configured as 10.10.10.0 with a mask 255.255.255.0 and 10.10.11.0 with a mask 255.255.255.0 and the Remote Accessible Networks would be 12.12.12.0 with a mask of 255.255.255.0. All packets that do not match these rules will be NATed and sent out the interface and not through the tunnel. This is a useful configuration if access to both the Internet and the other side of an IPSec tunnel is desired.

Dialup ISDN connections

When you are creating an IPSec tunnel over a Dialup ISDN connection, the endpoint must have a fixed IP address.

Compatibility with Contivity Extranet Switch and Shasta 5000

When connecting to a Contivity Extranet Switch, you must disable Vendor ID and Compression under Base Class on the Contivity Extranet Switch.

Business Communications Manager does not support the IPSec RIP implementation used by the Contivity Extranet Switch. Use Static Routes when connecting to the Contivity Extranet Switch.

When connecting to a Shasta 5000, you must set the PFS to No on the Tunnel configuration of Business Communications Manager.

IPSec and PPTP

The Remote Accessible Networks of an IPSec tunnel cannot be the same as a Destination Network on a PPTP tunnel. The Remote Endpoint of an IPSec tunnel's Remote Endpoint cannot be the same as a Destination Endpoint on a PPTP tunnel.

Multiple IP Address restrictions

Although the Business Communications Manager supports the configuration of additional IP addresses on its network interfaces, IPSec does not currently support the use of these additional IP addresses for Branch Office Local Endpoint Addresses, Remote Endpoint Addresses or the Destination IP Address for IPSec VPN Clients.

For more information about Multiple IP addresses, refer to "Configuring multiple IP addresses for the LAN interface" on page 667.

Firewall rules for IPSec Branch Office and Remote User Tunnels

In order to allow IPSec packets through the firewall interface which blocks all incoming packets, a number of rules must be configured. In addition to allowing the IPSec packets through, you must also remember to create rules to allow the packets that come through the tunnel.

In the Branch office case, up to three rules must be created. One is for the key exchange protocol (IKE), the other two are for the type of protocol used (ESP and/or AH). Table 267, Table 268 and Table 269 show the rules required (these are all inbound rules).

You can create these rules automatically when creating or modifying Branch Office and Remote Tunnels by selecting **Yes** for the **Create Firewall Rules for this tunnel** on the Parameters page for a particular tunnel. The three firewall rules required by the Branch Office tunnels are then created. You can view these rules on the Input Filters' Rule Setting screen for the interface used. If the Branch Office tunnel is enabled and IPSec is enabled globally, then the three rules created are added to the front of the Rule Order that appears on the Input Filters' Rule Order screen for the interface used. If the Branch Office tunnel is later disabled, then the rules are removed from the Rule Order, but still exist on the Input Filters' Rule Setting screen. If the user selects **No** for the **Create Firewall Rules for this tunnel** option, then the three firewall rules created for the Branch Office tunnel are deleted.

You can also create firewall rules for Remote User tunnels. The rule creation process is the same as for Branch Office tunnels except that the user must select which interface they want to create firewall rules for. The six rules in Table 267 to Table 272 are created for Remote User tunnels if you select **Yes** for the **Create Firewall Rules for Interface** option.

Table 267 Firewall rules for IKE

Protocol	UDP
Source IP	Remote Endpoint address for Branch Office; Client PC IP address for Remote User
Source Mask	255.255.255.255
Source Port	500
Destination IP	Local Endpoint address
Destination Mask	255.255.255.255
Destination Port	500

Table 268 Firewall rules for ESP

Protocol	IPSEC_ESP
Source IP	Remote Endpoint address for Branch Office; Client PC IP address for Remote User
Source Mask	255.255.255.255
Destination IP	Local Endpoint address
Destination Mask	255.255.255.255

Table 269 Firewall rules for AH

Protocol	IPSEC_AH
Source IP	Remote Endpoint address for Branch Office; Client PC IP address for Remote User
Source Mask	255.255.255.255
Destination IP	Local Endpoint address
Destination Mask	255.255.255.255

In addition to the above rules, Remote User tunnels need extra rules. These are extra rules are for the QOTD (Quote of the Day) server, Password server and ICMP that the IPSec client issues. Table 270, Table 271 and Table 272 show the rules required.

Table 270 Firewall rules for the QOTD server

Protocol	TCP
Source IP	IP address of the client tunnel (this may be the IP address pool range or the fixed IP address assigned to the tunnel)
Source Mask	255.255.255.255
Destination IP	The IP address of the Private network that the client IP address comes from (for example, if the Client tunnel IP address is 10.10.10.20 and the Private interface IP address is 10.10.10.1, then the destination IP is 10.10.10.1)
Destination Mask	255.255.255.255
Destination Port	17

Table 271 Firewall filter for the Password server

Protocol	TCP
Source IP	IP address of the client tunnel (this may be the IP address pool range or the fixed IP address assigned to the tunnel)
Source Mask	255.255.255.255
Destination IP	The IP address of the Private network that the client IP address comes from (for example, if the Client tunnel IP address is 10.10.10.20 and the Private interface IP address is 10.10.10.1, then the destination IP is 10.10.10.1)
Destination Mask	255.255.255.255
Destination Port	586

Table 272 Firewall filter for the ICMP that the Client sends to the tunnel endpoint

Protocol	ICMP
Source IP	Client PC IP address
Source mask	255.255.255.255
Destination IP	Remote Endpoint address
Destination mask	255.255.255.255

Table 273 Firewall filter for Private Network

Protocol	IP
Source IP	Private Network IP address
Source Mask	Private Network Subnet mask
Source Port	All
Destination IP	Private Network IP address
Destination Mask	Private Network Subnet mask
Destination Port	All

Example

Business Communications Manager 1 has been configured with a WAN1 address of 10.200.40.12 and a LAN 1 address of 10.10.10.1. Your computer at home has the address of 207.44.126.81. You have setup the Business Communications Manager to use the address range 10.10.10.100 - 10.10.10.200 with a mask of 255.255.255.0 for the IPSec Address Pool. You only allow ESP as the IPSec protocol. You will need the following rules:

IR1	
Protocol	UDP
Source IP	207.44.126.81
Source Mask	255.255.255.255
Source Port	500
Destination IP	10.200.40.12
Destination Mask	255.255.255.255
Destination Port	500

IR2	
Protocol	IPSEC_ESP
Source IP	207.44.126.81
Source Mask	255.255.255.255
Destination IP	10.200.40.12
Destination Mask	255.255.255.255

IR3	
Protocol	TCP
Source IP	10.10.10.0
Source Mask	255.255.255.0
Destination IP	10.10.10.1
Destination Mask	255.255.255.255
Destination Port	17

IR4	
Protocol	TCP
Source IP	10.10.10.0
Source Mask	255.255.255.0
Destination IP	10.10.10.1
Destination Mask	255.255.255.255
Destination Port	586

IR5	
Protocol	ICMP
Source IP	207.44.126.81
Source mask	255.255.255.255
Destination IP	10.200.40.12
Destination mask	255.255.255.255

IR6	
Protocol	IP
Source IP	10.10.10.0
Source Mask	255.255.255.0
Source Port	All
Destination IP	10.10.10.0
Destination Mask	255.255.255.0
Destination Port	All

For information about how to add or change Filters, refer to "Configuring IP Firewall Filters" on page 831.

Changing the IPSec global settings

The IPSec global settings apply to all of the IPSec tunnels.

To change the IPSec global settings:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** heading.
   The Global Settings screen appears.

3 Configure the IPSec global settings according to the following table.

Table 274 IPSec Global settings

Attribute	Description
Description	Displays the name of the IPSec service. This is a read only attribute.
Version	Displays the version number of the IPSec service. This is a read only attribute.
Encryption	Allows you to select the encryption levels that you allow your IPSec tunnels to use. The encryption level used for the IPSec tunnel is negotiated when the tunnel is opened. The encryption levels you select are the encryption levels that you allow Business Communications Manager to use for IPSec tunnels. This is a global setting that applies to all of the IPSec tunnels on Business Communications Manager. When you add an IPSec tunnel, you can further restrict the encryption levels for each tunnel. For more information, refer to "Adding a Branch Office IPSec Tunnel" on page 786. For a description of the encryption levels, refer to "Encryption" on page 778.
Status	Allows you to enable or disable the use of IPSec tunnels. You can choose Enabled or Disabled. The default value is Disabled.

4 Click the **Tab** key to save the settings.

IPSec Branch Office configuration

The branch office feature allows you to configure an IPsec tunnel connection between two private networks. Typically, one private network is behind a locally configured switch while the other is behind a remote switch. A branch office configuration allows you to configure the accessible subnetworks behind each switch. The configuration also contains the information that is necessary to set up the connection, such as the switch IP addresses, encryption types and authentication methods.

You can do the following with Branch Office IPSec tunnels:

- "Adding a Branch Office IPSec Tunnel" on page 786
- "Modifying a Branch Office IPSec Tunnel" on page 791
- "Deleting a Branch Office IPSec tunnel" on page 792

Adding a Branch Office IPSec Tunnel

A Branch Office IPSec Tunnel connects two offices together. The IPSec Tunnel connects the local Business Communications Manager system to another Business Communications Manager system, a Contivity Extranet Switch or a Shasta 5000 switch.

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Branch Office Accounts** heading.
The Branch Office Summary screen appears.

3 Click the **Add** button.
Or, right click the **Branch Office Accounts** heading and click **Add**.
The Add Branch Office Accounts dialog box appears.

4 Configure the Branch Office Tunnel Settings according to the following table.

Table 275 IPSec Branch Office Tunnel settings

Attribute	Description
Tunnel Number	Allows you to specify the Tunnel identifier. The Tunnel Number uniquely identifies a IPSec tunnel. The value for this setting must follow certain conventions. You must type the prefix 'T' followed by a unique number identifying the IPSec Tunnel. For example, 'T2' is a valid name. If you specify an existing Tunnel number, you receive an error message. The Tunnel identifier does not have any significance, other than uniquely identifying an entry. The maximum number of tunnels you can add is 20.
IPSec Status	Allows you to view the current status of this IPSec Tunnel. Choose **Enabled** or **Disabled** to change the status of this IPSec Tunnel. The default setting is **Disabled**.
PFS Enabled	Allows you to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys. If you create a tunnel to a Contivity Extranet Switch, you must set PFS Enabled to Yes. You can choose Yes or No. The default setting is Yes. **Note**: Set PFS to No for connections to the Shasta 5000.
Idle Timeout	Allows you to specify the amount of time the tunnel can remain idle before the tunnel is closed. You cannot set the Idle Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 00:15:00. A setting of 00:00:00 disables the Idle Timeout setting.
Highest Encryption	Allows you to select the highest encryption level allowed on this IPSec tunnel. When the encryption level is negotiated for this tunnel, Business Communications Manager will not use any encryption level higher than the encryption level specified in this field. For a description of the encryption levels, refer to “Encryption” on page 778.
Key Type	Select the format for the Preshared Key. The Key Type must be the same on both ends of the IPSec tunnel. The format can be text or hexadecimal. **Note**: If you change the Key Type, the Preshared Key is deleted.
Preshared Key	Allows you to specify the text or hexadecimal string used to authenticate the data sent on this tunnel. The maximum length of the Preshared Key is 32 characters. This key must be used at both ends of the IPSec Tunnel. For best security, use a secure method to share this key.
Confirm Preshared Key	Allows you to re-enter the Preshared Key to confirm that you entered the key correctly.

Table 275 IPSec Branch Office Tunnel settings (Continued)

Attribute	Description
Rekey Timeout	Allows you to specify the amount of time you can use a key before the tunnel is re-negotiated. You should limit the lifetime of a single key used to encrypt data or else you will compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between servers. You cannot set the Rekey Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 08:00:00. A setting of 00:00:00 disables the Rekey Timeout setting.
Rekey Data Count	Allows you to specify the amount of data you can transmit on the tunnel before the tunnel is re-negotiated. Enter a value from 0 to 1000000 Kbytes. A setting of 0 disables the Rekey Data Count. **Note**: If you set the Rekey Data Count too low, the tunnel is re-negotiated too often and will consume extra system resources.
Local Endpoint	Allows you to specify the IP address of the interface on Business Communications Manager that is the entrance or exit of the IPSec tunnel. Enter the IP address in the dotted format.
Remote Endpoint	Allows you to specify the IP address of the remote IPSec gateway that is the entrance or exit of the IPSec tunnel. Enter the IP address in the dotted format. **Note**: Different tunnels cannot have the same Remote Endpoint. This includes PPTP tunnels.
Send All Traffic Through IPSec Tunnel	Select **Yes** if you want all data traffic to be sent through this IPSec tunnel. Select **No** if you do not want all traffic to use this IPSec tunnel. When you select Yes to enable this option, any existing accessible networks for this Branch Office account are saved. If you choose No later, then these saved accessible networks are restored. When a Branch Office account has this option enabled, then all other Branch Office and Remote User tunnels are disabled since all traffic will go through this tunnel. In addition, no other Branch Office or Remote User tunnels can be created while this option is enabled. The default setting is No.
Create Firewall Rules for this Tunnel	Select **Yes** if you want the Business Communications Manager to create Firewall rules that allow traffic for this tunnel to pass through the Firewall. Select **No** if you do not want Business Communications Manager to create Firewall rules for this tunnel. If you are using the Business Communications Manager Firewall, Nortel Networks recommends that you select Yes for this option. The default setting is No.
Keep-Alive Enabled	Allows for quicker detection of lost connectivity. You can select **Yes** or **No**. The default setting is **No**. **Note**: Leave this setting at the default value of **No** for IPSec tunnel connections to systems other than Business Communications Manager or Contivity.

5 Click the **Save** button.

Adding Local Accessible Networks to the Branch Office IPSec tunnel

The maximum number of Local Accessible Networks you can add is 16.

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Branch Office Accounts** key.

3 Click the tunnel you want to modify.
The Tunnel Parameters screen appears.

4 Click the **Local Accessible Networks** tab.
The Local Accessible Networks screen appears.

5 On the **Configuration** menu, click **Add Local Accessible Network**.

6 Configure the Local Accessible Network parameters according to the following table.

Table 276 IPSec Local Accessible Network parameters

Attribute	Description
Network Number (L#)	Allows you to specify the Network identifier. The Network Number uniquely identifies a Local Accessible Network. The value for this setting must follow certain conventions. You must type the prefix 'L' followed by a unique number identifying the Local Accessible Network. For example, 'L2' is a valid name. If you specify an existing Network number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Network identifier does not have any significance, other than uniquely identifying an entry. The maximum number Local Accessible Networks you can add is 16.
IP Address	Allows you to specify the IP addresses of interfaces on Business Communications Manager that can connect to this tunnel. Enter the IP address in the dotted format.
IP Address Mask	Allows you to specify the subnet mask of interfaces on Business Communications Manager that can connect to this tunnel. Enter the Subnet Mask in the dotted format.

7 Click the **Save** button.

Adding Remote Accessible Networks to the Branch Office IPSec tunnel

The maximum number of Remote Accessible Networks you can add is 16.

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Branch Office Accounts** key.

3 Click the tunnel you want to modify.
The Tunnel Parameters screen appears.

4 Click the **Remote Accessible Networks** tab.
The Remote Accessible Networks screen appears.

5 On the **Configuration** menu, click **Add Remote Accessible Network**.

6 Configure the Remote Accessible Network parameters according to the following table.

Table 277 IPSec Remote Accessible Network parameters

Attribute	Description
Network Number (R#)	Allows you to specify the Network identifier. The Network Number uniquely identifies a Remote Accessible Network. The value for this setting must follow certain conventions. You must type the prefix 'R' followed by a unique number identifying the Remote Accessible Network. For example, 'R2' is a valid name. If you specify an existing Network number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Network identifier does not have any significance, other than uniquely identifying an entry. The maximum number of Remote Accessible Networks you can add is 16.
IP Address	Allows you to specify the IP addresses of IPSec gateways that you can connect to using this tunnel. Enter the IP address in the dotted format.
IP Address Mask	Allows you to specify the subnet mask of IPSec gateways that you can connect to using this tunnel. Enter the Subnet Mask in the dotted format.

7 Click the **Save** button.

Note: Different tunnels cannot have the same Remote Accessible Networks.

Sending all traffic from Local Accessible Networks through the IPSec tunnel

If you want to send all traffic from the Local Accessible Networks through the IPSec tunnel, add the eight Remote Accessible Networks in the table below to the tunnel.

You can also generate these local and remote accessible networks by choosing **Yes** for the **Send All Traffic through this tunnel** option when creating or modifying a Branch Office account.

Table 278 Remote Accessible Networks used to route all traffic through the IPSec tunnel

Network Number	IP Address	IP Mask
R1	1.0.0.0	255.0.0.0
R2	2.0.0.0	254.0.0.0
R3	4.0.0.0	252.0.0.0
R4	8.0.0.0	248.0.0.0
R5	16.0.0.0	240.0.0.0
R6	32.0.0.0	224.0.0.0
R7	64.0.0.0	192.0.0.0
R8	128.0.0.0	128.0.0.0

Modifying a Branch Office IPSec Tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
4. Change the required IPSec Tunnel settings.
   For information about the settings refer to "Adding a Branch Office IPSec Tunnel" on page 786.
5. Click the **Tab** key to save your changes.

Modifying Local Accessible Networks to the Branch Office IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
4. Click the **Local Accessible Networks** tab.
   The Local Accessible Networks screen appears.
5. Click the Local Accessible Network you want to modify.
6. On the **Configuration** menu, click **Modify Local Accessible Network**.
7. Modify the Local Accessible Network parameters.
8. Click the **Save** button.

Modifying Remote Accessible Networks to the Branch Office IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
4. Click the **Remote Accessible Networks** tab.
   The Remote Accessible Networks screen appears.
5. Click the Remote Accessible Network you want to modify.
6. On the **Configuration** menu, click **Modify Remote Accessible Network**.
7. Modify the Remote Accessible Network parameters.
8. Click the **Save** button.

Deleting a Branch Office IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to delete.
4. Click the **Delete** button.
   Or, right click the tunnel you want to delete and click **Delete**.
   A message prompts you to confirm the deletion.
5. Click the **Yes** button.

Deleting Local Accessible Networks to the Branch Office IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
4. Click the **Local Accessible Networks** tab.
   The Local Accessible Networks screen appears.
5. Click the Local Accessible Network you want to delete.
6. On the **Configuration** menu, click **Delete Local Accessible Network**.
   A message prompts you to confirm the deletion.
7. Click the **Yes** button.

Deleting Remote Accessible Networks to the Branch Office IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Branch Office Accounts** key.
3. Click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
4. Click the **Remote Accessible Networks** tab.
   The Remote Accessible Networks screen appears.
5. Click the Remote Accessible Network you want to delete.
6. On the **Configuration** menu, click **Delete Remote Accessible Network**.
   A message prompts you to confirm the deletion.
7. Click the **Yes** button.

Creating a tunnel between two Business Communications Managers

The following is an example of a how to connect two Business Communications Manager systems together using an IPSec tunnel.

In this example, the IPSec tunnel connects a Business Communications Manager with a LAN 2 IP address of 10.10.11.1 and another Business Communications Manager with a LAN 2 IP address of 10.10.11.2. LAN 1 on the first Business Communications Manager is on the subnet 12.12.12.0. The LAN 1 of the second Business Communications Manager is on subnet 14.14.14.0.

Configuring the first Business Communications Manager

1. Set the Local Endpoint to **10.10.11.1**.
2. Set the Remote Endpoint to **10.10.11.2**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **12.12.12.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.

Configuring the second Business Communications Manager

1. Set the Local Endpoint to **10.10.11.2**.
2. Set the Remote Endpoint to **10.10.11.1**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **12.12.12.0** with mask **255.255.255.0**.

On the Global settings for both Business Communications Manager systems, set the Status to Enabled.

Creating a tunnel between a Business Communications Manager and a Contivity Extranet Switch v02_61

The following are an examples of a how to connect a Business Communications Manager to a Contivity Extranet Switch using an IPSec tunnel.

In this example, the IPSec tunnel connects a Business Communications Manager with a LAN 2 IP address of 47.81.20.50 and a Contivity Extranet Switch with a Public IP address of 47.82.30.60. LAN 1 on the Business Communications Manager is on the subnet 10.10.11.0. The Contivity Extranet Private LAN is on the subnet 14.14.14.0.

Configuring the Business Communications Manager

1. Set the Local Endpoint to **47.81.20.50**.
2. Set the Remote Endpoint to **47.82.30.60**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **10.10.11.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.

Configuring the Contivity Extranet Switch

1. Go to Profiles->Network and create a Network with the IP address 14.14.14.0 with mask 255.255.255.0. You will use this for the Local Accessible Networks for your Branch Office Connection.
2. Under Profiles->Branch Office, create a Group based on the Base class.
3. In the IPSec section of this new Group, change the Vendor ID to Disabled and change Compression to Disabled. Business Communications Manager does not support Vendor ID or Compression.
4. In the Connectivity section of this new group, change the Nailed Up setting to Disabled. Business Communications Manager does not support the Nailed Up functionality.
5. Select Define Branch Office Connection.
6. Set the routing type to be Static.
7. Set the Local Endpoint to 47.82.30.60 and the Remote Endpoint to 47.82.20.50.
8. Under Local Accessible Networks, select the Network that was created earlier.
9. Set the Remote Accessible Networks to 10.10.11.0 with mask 255.255.255.0.
10. For the Preshared Key, select the Text button and set the key to '123'. This must match the BCM key.
11. Mark the box for Enable Branch Office Connection.

The following example describes how to configure a Business Communications Manager with a Contivity Extranet Switch when NAT is required on the Business Communications Manager and external access is required on the same interface as the tunnel (split tunneling).

Configuring the Business Communications Manager

Using the same systems from the previous example, we will now enable NAT and turn on Default Rules on the Business Communications Manager. The gateway for the LAN 2 interface is 47.82.30.1. For information about how to change NAT parameters, refer to refer to "Configuring NAT (Network Address Translation)" on page 753.

1. Set the Local Endpoint to **47.81.20.50**.
2. Set the Remote Endpoint to **47.82.30.60**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **47.81.20.50** with mask **255.255.255.255** and **10.10.11.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.
7. Under Net Link Manager, set the next hop to **47.82.30.1**.

Configuring the Contivity Extranet Switch

The gateway for the Public LAN interface is 47.81.20.1.

1. Go to Profiles->Network and create a Network with the IP address **14.14.14.0** with mask **255.255.255.0**. You will use this for the Local Accessible Networks for your Branch Office Connection.
2. Under Profiles->Branch Office, create a Group based on the Base class.
3. Under this new Group, change the Vendor ID to Disabled and change Compression to Disabled. Business Communications Manager does not support Vendor ID or Compression.
4. Select Define Branch Office Connection.
5. Set the routing type to be Static.
6. Set the Local Endpoint to **47.82.30.60** and the Remote Endpoint to **47.81.20.50**.
7. Under Local Accessible Networks, select the Network that was created earlier.
8. Set the Remote Accessible Networks to **10.10.11.0** with mask **255.255.255.0** and **47.81.20.50** with mask **255.255.255.255**.
9. For the Preshared Key, select the Text button and set the key to '**123**'. This must match the Business Communications Manager key.
10. Mark the box for Enable Branch Office Connection.
11. Set the Public Default Route to **47.81.20.1**.

IPSec Remote User configuration

The IPSec Remote User feature allows remote users to dial in to an Internet Service Provider (ISP) anywhere in the world and connect to the corporate network in a secure way. All the remote user requires is an IPSec VPN client installed on their computer. This removes the need for the traditional corporate remote access environments where banks of modems were employed to handle incoming service requests.

The IPSec VPN client you require for Business Communications Manager is version 4.60 of the Contivity VPN IPsec remote access user client software. To obtain a copy of this client software, contact your authorized Business Communications Manager distributor. The Contivity VPN IPsec remote access user client software is a Windows application available for the latest releases of Windows 95, Windows 98, Windows NT Workstation, Windows NT Server, Windows 2000 and Windows XP. This client software comes with complete online Help.

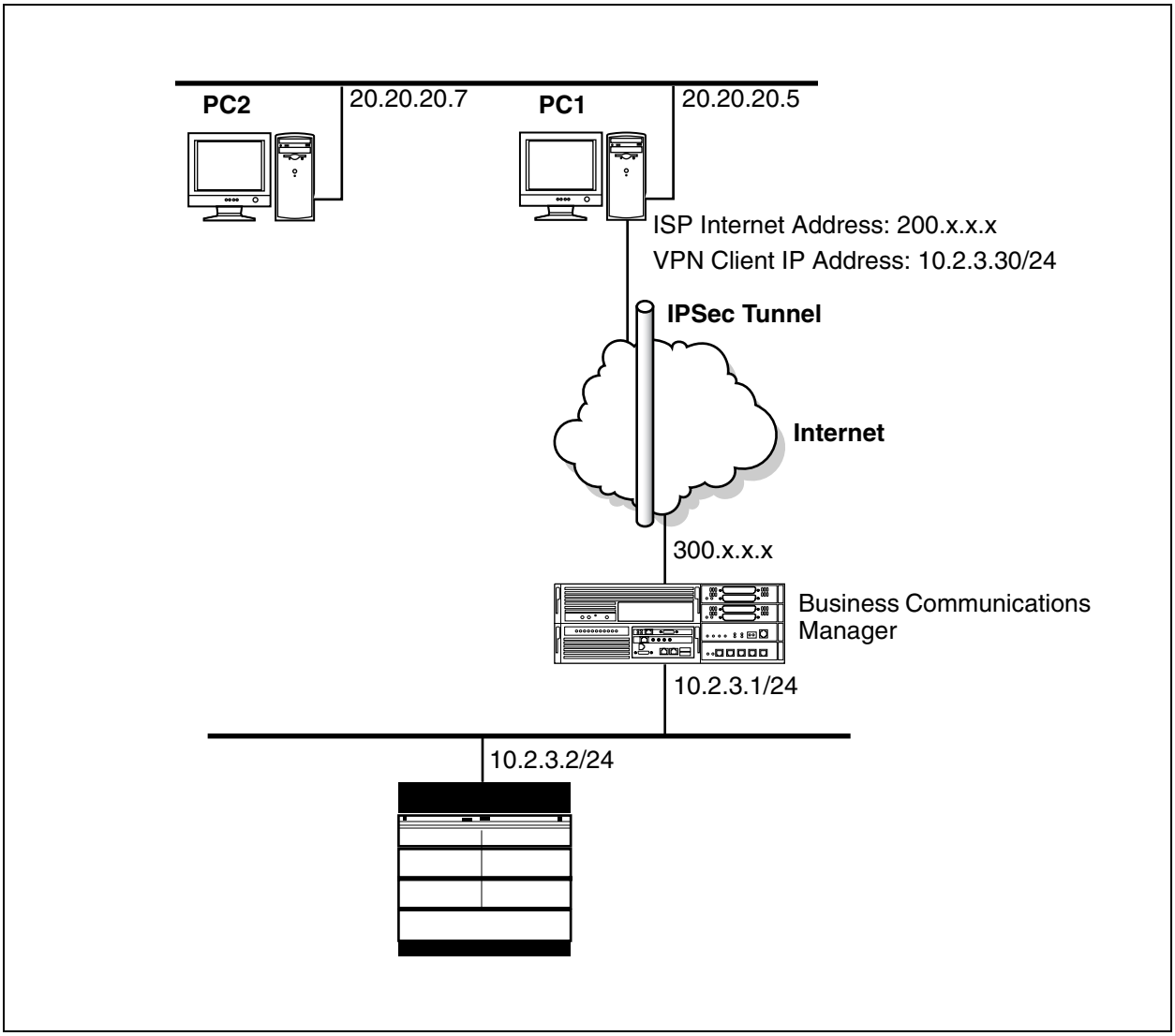
IPSec Remote User Authentication

Business Communications Manager only supports User Name and Password authentication from the VPN Client. The authentication method used is local NT Authentication. No other form of Authentication is supported. Business Communications Manager does not support Contivity Group ID authentication.

Split Tunneling

All client traffic is tunneled through the Business Communications Manager by default. Split Tunneling allows you to configure specific network routes that are downloaded to the client. Only these network routes are then tunneled. Any other traffic goes to the local computer interface. Split tunneling allows you to print locally, for example, even while you are tunneled into the Business Communications Manager.

Figure 211 Example of a Split Tunneling environment



In the example in the figure above, PC1 and PC2 are on a home IP network (20.20.20.0/ 255.255.255.0). PC1 is also connected to the Internet with an ISP granted IP address of 200.x.x.x. PC1 runs an IPSec VPN Client and connects to the Business Communications Manager. Business Communications Manager assigns this VPN Client connection an IP address of 10.2.3.30.

If Split tunneling is disabled, PC1 will NOT be able to access PC2 as ALL traffic will be sent down the IPSec tunnel.

However, if the Remote User Account has Split Tunneling enabled with split tunnel network IP addresses of 10.2.3.0/255.255.255.0, PC1 can establish an IPSec tunnel. When the client establishes an IPSec tunnel, this network address is loaded into the client application. PC1 can then access any system on the 10.2.3.0 network as well as accessing PC2 on IP network 20.20.20.0, while the VPN IPSec Client is still connected.

Split Tunneling security considerations

Business Communications Manager takes precautions against violators potentially hacking tunneled information when the Business Communications Manager is operating in Split Tunnel mode.

The primary precaution is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, if you have a PPP dial-up connection to the Internet with an IP address of 192.168.21.3, and you set up an IPSec client connection to a Business Communications Manager and you are assigned an IPSec client IP address of 192.192.192.192, then any packets that attempt to pass through the IPSec client tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) will be dropped.

To completely eliminate security risks, you should not use the Split Tunneling feature.

Adding a Remote User IPSec Tunnel

A Remote User IPSec Tunnel connects a remote computer to the Business Communications Manager system.

Note: The remote computer must have version 4.60 of the Contivity VPN Client installed.

Note: If the computer running the VPN client is not on the same subnet as the Destination address (i.e. there is at least one router between the computer and the Business Communications Manager), then the default Next Hop Router on the Business Communications Manager must also be through this interface. For instructions on setting up a default Next Hop Router, refer to "Configuring Net Link Manager" on page 749.

Assigning an IP Address to a Remote User Account

The Remote User account requires that an IP address is assigned to the Remote User when they log into the Business Communications Manager. This IP address must be in the private IP network that the Remote User is able to access.

The Business Communications Manager supports two methods of assigning an IP Address to the Remote User Account. You can use a static IP address or a dynamic IP address from an IP Address Pool.

Static IP Address

To assign a static IP address to the Remote User account, you must configure the following two options when you configure the Remote User Account settings:

- Static IP Address
- Static Subnet Mask

Dynamic IP address from an IP Address Pool

To assign a dynamic IP address, you must configure a Remote IP Address Pool and assign the Remote IP Address Pool to the Remote User Account. For information about how to configure a Remote IP Address Pool, refer to "Adding a Remote IP Address Pool" on page 799. To assign the Remote IP Address Pool to the Remote User Account, you must configure the IP Address Pool Name option when you configure the Remote User Account settings.

Note: You must configure either the **IP Address Pool Name** option or the **Static IP Address** and **Static Subnet Mask** options.

Note: When assigning IP addresses for Remote users, make sure that no conflicts can occur with IP Addresses already assigned on the private network. If the private network contains a DHCP server, the range assigned in the IP Address Pool or the Static IP Address must be excluded from the DHCP IP address range.

Adding a Remote User IPSec Tunnel involves the following:

- "Adding a Remote IP Address Pool" on page 799
- "Adding Remote User Accounts" on page 801
- "Configuring Remote User Accounts" on page 803

Adding a Remote IP Address Pool

Remote access users who are using tunneling protocols require two IP addresses to form packets. The addresses are normally referred to as outer and inner addresses. The outer address, or public address, is visible when packets are traveling through the public data networks (PDNs). This address is negotiated between the client and the ISP to which it is connected. Business Communications Manager does not have control of this address.

The inner IP address is the one that eventually appears on the private network when the outer layers of the packet are removed. Therefore, this address must lie within the private network address space. Business Communications Manager provides the remote user with the inner IP address during tunnel setup. This address can come from a defined static IP address for this user account or from an internal address pool.

When assigning IP addresses for remote users, make sure that no conflicts can occur with IP addresses already assigned on the private network.

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** heading.
   The Remote IP Address Pool List screen appears.
3. On the **Configuration** menu, click **Add IP Address Pool**.
   The Remote IP Address Pool List screen appears.

4 Configure the Remote IP Address Pool List settings according to the following table.

Table 279 IPSec Remote IP Address Pool settings

Attribute	Description
Pool Number	Allows you to specify the Remote IP Address Pool List identifier. The Pool Number uniquely identifies a Remote IP Address Pool List. The value for this setting must follow certain conventions. You must type the prefix 'P' followed by a unique number identifying the Remote IP Address Pool List. For example, 'P2' is a valid name. If you specify an existing Pool number, you receive an error message. The Remote IP Address Pool List identifier does not have any significance, other than uniquely identifying an entry.
Start Address	Allows you to specify the first IP address in the Remote IP Address Pool List. Enter the IP address in the dotted format.
End Address	Allows you to specify the last IP address in the Remote IP Address Pool List. Enter the IP address in the dotted format.
Subnet Mask	Allows you to specify the subnet mask for the Remote IP Address Pool List. Enter the Subnet Mask in the dotted format.

5 Click the **Save** button.

Modifying a Remote IP Address Pool

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Remote User Accounts** heading.
The Remote IP Address Pool List screen appears.

3 Click the Remote Address Pool List you want to modify.

4 On the **Configuration** menu, click **Modify IP Address Pool**.
Or, right click the Remote Address Pool List you want to modify and click **Modify IP Address Pool**.
The Remote IP Address Pool List screen appears.

5 Modify the Remote IP Address Pool List parameters.
For information about the settings, refer to the table above.

6 Click the **Save** button.

Deleting a Remote IP Address Pool

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Remote User Accounts** heading.
The Remote IP Address Pool List screen appears.

3 Click the Remote Address Pool List you want to delete.

4 On the **Configuration** menu, click **Delete IP Address Pool**.
Or, right click the Remote Address Pool List you want to modify and click **Delete IP Address Pool**. A message prompts you to confirm the deletion.

5 Click the **Yes** button.

Adding Remote User Accounts

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** heading.
3. Click the **Remote User Summary** tab.
   The Remote User Summary screen appears.
4. Click the **Add** button.
   Or, right click the **Remote User Accounts** heading and click **Add**.
   The Add Remote User Accounts dialog box appears.
5. Configure the Remote User Accounts settings according to the following table.

Table 280 IPSec Remote User Account settings

Attribute	Description
User Number	Allows you to specify the Remote User identifier. The User Number uniquely identifies a Remote User. The value for this setting must follow certain conventions. You must type the prefix 'U' followed by a unique number identifying the Remote User. For example, 'U2' is a valid name. If you specify an existing Remote User number, you receive an error message. The User Number identifier does not have any significance, other than uniquely identifying an entry.
User Name	Allows you to specify the user name that the remote computer uses to access the IPSec tunnel.
Password	Allows you to specify the password that the remote computer uses to access the IPSec tunnel. **Note**: The password you choose must conform to the password policy used for your Business Communications Manager system. For more information about the password policy, refer to "Setting password policy" on page 122.
Confirm Password	Allows you to re-enter the password to confirm that the password was entered correctly.
IP Address Pool Name	Allows you to select the Remote IP Address Pool List you want to use for this Remote User Account. This allows you to assign a Dynamic IP Address (from the IP Address Pool) to the Remote User when they connect. **Note1**: If you select a Remote IP Address Pool List you do not have to specify the Static IP Address or the Static subnet mask. **Note2**: You must add a Remote IP Address Pool List before you can select it from the drop list.
Static IP Address	Allows you to specify the IP address that is used by the remote computer, if the remote computer is using a static IP address. **Note**: You do not need to enter a Static IP address if the Account is using a dynamic IP Address Pool.
Static Subnet Mask	Allows you to specify the Subnet Mask that is used by the remote computer, if the remote computer is using a static IP address. **Note**: You do not need to enter a Static Subnet Mask if the remote computer is using dynamic IP addressing.
IPSec Status	Allows you to view the current status of this IPSec Tunnel. You can also use this field to enable or disable this IPSec tunnel. You can choose Enabled or Disabled. The default setting is Disabled.

Table 280 IPSec Remote User Account settings (Continued)

Attribute	Description
PFS Enabled	Allows you to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys. You can choose Yes or No. The default setting is Yes.
Create Firewall Rules for Interface	Allows you to choose which interface to generate Firewall Filter rules for. These rules are necessary to allow packets for this Remote User tunnel through the firewall. The default value is None which means that no rules are generated.
Idle Timeout	Allows you to specify the amount of time the tunnel can remain idle before the tunnel is closed. You cannot set the Idle Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 00:15:00. A setting of 00:00:00 disables the Idle Timeout setting.
Highest Encryption	Allows you to select the highest encryption level allowed on this IPSec tunnel. When the encryption level is negotiated for this tunnel, Business Communications Manager will not use any encryption level higher than the encryption level specified in this field. For a description of the encryption levels, refer to "Encryption" on page 778.
Rekey Timeout	Allows you to specify the amount of time you can use a key before the tunnel is re-negotiated. You should limit the lifetime of a single key used to encrypt data or else you will compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between servers. You cannot set the Rekey Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 08:00:00. A setting of 00:00:00 disables the Rekey Timeout setting.
Rekey Data Count	Allows you to specify the amount of data you can transmit on the tunnel before the tunnel is re-negotiated. Enter a value from 0 to 1000000 Kbytes. A setting of 0 disables the Rekey Data Count. **Note**: If you set the Rekey Data Count too low, the tunnel is re-negotiated too often and will consume extra system resources.
Split Tunneling Enabled	Allows you to select if the remote computer is allowed to use Split Tunneling. You can choose Yes or No. The default setting is No. **Note**: The Split Tunneling Enabled drop list is not available when you are adding a Remote User account. This drop list appears when you are configuring a Remote User Account.
Domain Name	Allows you to specify the Domain Name of the Domain the remote computer reside in.
Keep-Alive Enabled	Allows for quicker detection of lost connectivity. You can select **Yes** or **No**. The default setting is **No**. **Note**: Leave this setting at the default value of **No** for IPSec tunnel connections to systems other than Business Communications Manager or Contivity.

6 Click the **Save** button.

Configuring Remote User Accounts

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Remote User Accounts** key.

3 Click the Remote User Account you want to modify.
The Remote User Settings screen appears.

4 Change the required Remote User Account settings.
For information about the settings refer to "Adding Remote User Accounts" on page 801.

5 Click the **Tab** key to save your changes.

Configuring the DNS/WINS setting for the Remote User Account

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the **Remote User Accounts** key.

3 Click the Remote User Account you want to modify.
The Remote User Settings screen appears.

4 Click the **DNS/WINS Settings** tab.
The DNS/WINS Settings screen appears.

5 Configure the DNS/WINS Settings according to the following table.

Table 281 DNS/WINS Settings

Attribute	Description
Primary DNS	Allows you to specify the IP address of the Primary DNS server that the remote computer uses. Enter the IP address in the dotted format.
Secondary DNS	Allows you to specify the IP address of the Secondary DNS server the remote computer uses. The remote computer uses the Secondary DNS server if the Primary DNS server is not available or does not have an entry for the domain name specified. Enter the IP address in the dotted format.
Primary WINS	Allows you to specify the IP address of the Primary WINS server that the remote computer uses. Enter the IP address in the dotted format.
Secondary WINS	Allows you to specify the IP address of the Secondary WINS server that the remote computer uses. Enter the IP address in the dotted format.

6 Press the TAB button to save your changes.

Adding a Split Tunnel Network

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** key.
3. Click the Remote User Account you want to modify.
   The Remote User Settings screen appears.
4. Click the **Split Tunnel Networks** tab.
   The Split Tunnel Networks screen appears.
5. On the **Configuration** menu, click **Add Split Tunnel Network**.
   The Split Tunnel Network screen appears.
6. Configure the Split Tunnel Network settings according to the following table.

Table 282 Split Tunnel Network settings

Attribute	Description
Network Number	Allows you to specify the Split Tunnel Network identifier. The Network Number uniquely identifies a Split Tunnel Network. The value for this setting must follow certain conventions. You must type the prefix 'S' followed by a unique number identifying the Split Tunnel Network. For example, 'S2' is a valid name. If you specify an existing Network number, you receive an error message. The Split Tunnel Network identifier does not have any significance, other than uniquely identifying an entry.
IP Address	Allows you to configure the specific IP network addresses that are routed through the IPSec Tunnel. All other IP traffic is routed in the normal fashion. Enter the IP address in the dotted format.
IP Address Mask	Allows you to specify the subnet mask for the other network. Enter the Subnet Mask in the dotted format.

7. Click the **Save** button.

Modifying a Split Tunnel Network

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** key.
3. Click the Remote User Account you want to modify.
   The Remote User Settings screen appears.
4. Click the **Split Tunnel Networks** tab.
   The Split Tunnel Networks screen appears.
5. Click the Split Tunnel Network you want to modify.
6. On the **Configuration** menu, click **Modify Split Tunnel Network**.
   The Split Tunnel Network screen appears.
7. Change the required Split Tunnel Network settings.
   For information about the settings refer to the table above.
8. Click the **Save** button.

Deleting a Split Tunnel Network

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** key.
3. Click the Remote User Account you want to modify.
   The Remote User Settings screen appears.
4. Click the **Split Tunnel Networks** tab.
   The Split Tunnel Networks screen appears.
5. Click the Split Tunnel Network you want to delete.
6. On the **Configuration** menu, click **Delete Split Tunnel Network**.
   A confirmation message appears.
7. Click the **Yes** button.

Deleting a Remote User Account

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** key.
3. Click the Remote User Account you want to delete.
4. Click the **Delete** button.
   Or, right click the Remote User Account you want to delete and click **Delete**.
   A message prompts you to confirm the deletion.
5. Click the **Yes** button.

Creating Banner Text for a remote user

Banner Text is the text that appears when a remote user logs into the Business Communications Manager using the Contivity IPSec VPN Client. You can use this text to display important information (such as security information) to the remote user.

To add Banner Text:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the **Remote User Accounts** heading.
3. Click the **Banner Text** tab.
4. In the **Banner Text** box, enter the text that you want to appear when an Contivity IPSec VPN Client connects to the Business Communications Manager.
   You can enter a maximum 1000 ASCII characters. To start a new line, enter **\n**.
5. Click the **Tab** key to save the settings.

To preview how the Banner Text will appear, on the **View** menu, click **View Banner Text Output**. A new browser window appears showing the Banner Text.

Chapter 41
Policy-enabled networking

This section discusses the Policy services you can configure to enhance your data network.

Included is the following information:

Policy configuration overview

Business Communications Manager enables system administrators to implement classes of service and assign priority levels to different types of traffic. Using Unified Manager, you can configure policies that monitor the characteristics of traffic (for example, its source, destination, and protocol) and perform a controlling action on the traffic when certain user-defined characteristics are matched.

This section includes information about:

Differentiated Services (DiffServ) overview

This section provides information about working with DiffServe, including:

Differentiated services (DiffServ) is a Quality of Service (QoS) network architecture that offers varied levels of service for different types of data traffic. DiffServ allows you to designate a specific level of performance on a packet-by-packet basis instead of using the "best-effort" model for your data delivery. You can give preferential treatment (prioritization) to applications that require high performance and reliable service, such as voice and video over IP.

Business Communications Manager includes the capability to enhance your network traffic management. For each packet, there is an octet in the packet header, the DiffServ (DS) field, that you can designate for specific service. For IP packets, six bits of the DiffServ field is the DiffServ Code Point (*DSCP)*. The DSCP value defines how the packet is to be treated as it travels through the network. You can set traffic criteria to match the DS field, and policy actions to change the DiffServ field to conform to various other mappings.

Business Communications Manager uses DiffServ to manage network traffic and resources. The information that is required to support DiffServ and multi-field classification is transferred using the Common Open Policy Services (COPS) protocol. COPS is a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). All configuration can be performed using SNMP and Unified Manager.

DiffServ IP Quality of Service (QoS) architecture

DiffServ uses a simple mechanism that relies on a special encoding of the first 6 bits of the DiffServ byte in the IP header. This byte is the IPv4 Type of Service (ToS) byte; for IPv6, is the Traffic Class byte. The first 6 bits of this byte are called the DiffServ Code Point (DSCP).

In the packet forwarding path, differentiated services are processed by mapping the packet DSCP to a particular forwarding treatment, or per hop behavior (PHB), at each network node along its path. The code points may be chosen from a set of 32 standard values, a set of 16 recommended values to be used in the future, or a set of 16 values reserved for experimentation and local use. Of the 32 standard values, there are 8 Class Selector code points that are used primarily (but not exclusively) for backward compatibility with existing definitions of the ToS byte.

Business Communications Manager is a DiffServ node that can support DiffServ functions and behavior. DiffServ architecture defines a DiffServ-capable domain as a contiguous set of DiffServ-compliant nodes that operate with a common set of service provisioning policies and PHB definitions. The DiffServ domain is an autonomous system or network such as an internet service provider (ISP) network or campus LAN.

DiffServ assumes the existence of a service level agreement (SLA) between DiffServ domains that share a border. The SLA defines the profile for the aggregate traffic flowing from one network to the other based on policy criteria. In a given traffic direction, the traffic is expected to be shaped at the egress point of the upstream network and policed at the ingress point of the downstream network.

End-to-end QoS is enabled, typically through bilateral agreements (an agreement between two DiffServ domains), between all the domains from the sender to the receiver. These agreements aid in consistent PHB and QoS performance across all domains.

Typically, there are three types of edge devices in a DiffServ domain:

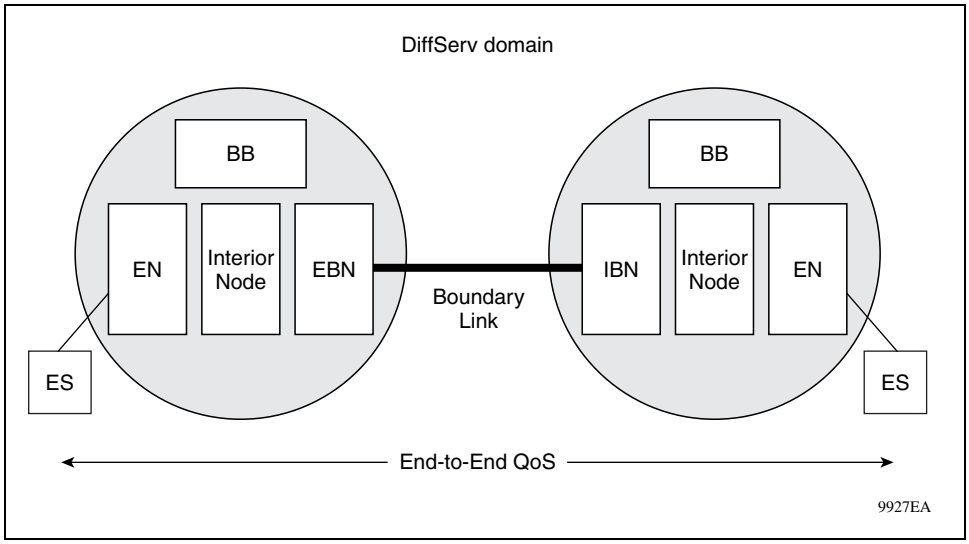
- Edge node (EN) — the switch or router connected directly to the desktop end station (ES) (Business Communications Manager is an edge node in the DiffServ domain)

  Ingress border node (IBN) — the ingress router at the boundary between two DiffServ domains

- Egress border node (EBN) — the egress router at the boundary between two DiffServ domains

The following figure shows the bandwidth broker and various DiffServ nodes in two DiffServ domains.

Figure 212 DiffServ bandwidth brokers and nodes



DiffServ components

The DiffServ architecture is comprised of the following components:

- Traffic conditioners — These components include classifiers, DiffServ-byte markers, shapers, policiers and profilers. Marking is performed at network boundaries, including the edges of the network (first hop router or switch or source host) and administrative boundaries between networks or autonomous systems. Traffic conditions should exist at DiffServ ingress and egress nodes. Business Communications Manager is an edge switch that supports packet classification based on header information in layer 3 and layer 4 of the Open System Interconnection (OSI) layering model. Business Communications Manager can mark and re-mark IP traffic based on the policies you define.
- Packet schedulers and queue managers — PHBs are expected to be implemented by employing a range of queue service and/or queue management disciplines on a network node output interface queue (for example, weighted fair queueing or drop preference queue management). DiffServ does not require a particular discipline for queue management or servicing to realize a particular service. All DiffServ nodes should support the packet scheduling and queue management algorithms that are necessary to implement the required PHB.

  Business Communications Manager supports a queue service discipline that allows packets to be serviced in an absolute priority fashion or using a weighted fair queueing scheduler. This service discipline ensures that packets in the highest-priority queue are serviced quickly without starving lower-priority queues.
- Bandwidth brokers (not supported in Business Communications Manager) — Bandwidth brokering is responsible for bandwidth allocation, QoS policy management, and flow admission control in a given DiffServ domain. Business Communications Manager does not support bandwidth brokering or traffic admission control.

IP service classes

Business Communications Manager supports the following services classes:

- Critical and Network classes have the highest priority over all other traffic.
- Premium class is an end-to-end service functioning similarly to a virtual leased line. Traffic in this service class is guaranteed an agreed upon peak bandwidth. Traffic requiring this service should be shaped at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real time applications like video and voice over IP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.
- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding PHB. These classes are used for real time, delay tolerant traffic and non real time, mission critical traffic.
- Best Effort (standard) class is the standard Internet packet service with an additional, optional use of traffic profiling that is used at the network boundary to request a better effort treatment for packets that are in-profile (packets that do not break the service agreements between the user and the service provider).

The following table describes the service classes and the required treatment. The following table shows how the service classes are mapped to the Business Communications Manager queues.

Table 283 Service classes

Traffic category	Service class	Application type	Required treatment
Critical Network Control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard Network Control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth
Real time, delay intolerant, fixed bandwidth	Premium	Person to person communications requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tolerant, low variable bandwidth	Platinum	Person to person communications requiring interaction with additional minimal delay (such as low cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Real time, delay tolerant, high variable bandwidth	Gold	Single human communication with no interaction (such as Web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, Web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, non-interactive	Bronze	For example, E-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, non-mission critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best effort delivery. Uses remaining available bandwidth.

These Required treatments (or service class behaviors) for these Service classes are implemented using nine queues and a scheduler for these queues. Queue 1 has the highest priority, referred to as Strict Priority. Queues 2 to 9 are scheduled according to a Weighted Fair Queuing (WFQ) scheme. The following table summarizes the mappings between service classes, queues and DSCP codes.

Table 284 Default Queue mapping for Business Communications Manager

NNSC	Default DSCP	Business Communications Manager Queue	Business Communications Manager Scheduler
Premium	40, 46	1	Strict Priority
Network	48, 56	2	Weighted Fair Queuing
Platinum	34, 36, 38	3	Weighted Fair Queuing
Gold	26, 28, 30	4	Weighted Fair Queuing
Silver	18, 20, 22	5	Weighted Fair Queuing
Bronze	10, 12, 14	6	Weighted Fair Queuing
Standard	0	7	Weighted Fair Queuing
Standby	2	8	Weighted Fair Queuing
N/A	N/A	9 (unused)	Weighted Fair Queuing

Packet classifiers

Filters are organized in groups. A filter group is an ordered list of filters. Each group of filters is associated with actions that are executed when the packet matches the first filter in the group. The filter group and the associated actions constitute a *policy*. A *classifier* is an ordered list of policies. Filters can be added or deleted from an existing group.

The order of a filter group in a classifier is called the group precedence. The lower the order of a group in a classifier the higher the precedence. The order in which filters in a given classifier are evaluated depends on the precedence of the filter group in which the filter resides and, on the order of the filter in the group. Filters in the higher-precedence groups are evaluated before filters in the lower-precedence groups.

A classifier is associated with a role combination. Packets received from any port that has the same role combination are classified with the same classifier. The Policy Table in Unified Manager defines the policies of the classifier associated with a given role combination.

IP filters

IP filters are used to classify IP traffic based on the following criteria:

- Layer 3 information, including IP source and subnet addresses, IP destination and subnet addresses, DSCP, and IP protocols such as TCP/UDP
- Layer 4 information, including TCP/UDP port numbers

Business Communications Manager can use 31 IP filters.

COPS

When used with the Optivity Policy Services® (OPS) Version 1.2 or later, a comprehensive network management application combining IP address management with policy-based network traffic control, Business Communications Manager effectively manages network traffic and resources. Information is transferred using the Common Open Policy Services (COPS) protocol, a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). Specifically, COPS for Provisioning (COPS-PR) is used to download information. COPS is used to communicate with edge devices on the network.

OPS provides a centralized management point for DiffServ policies. The policy server distributes policies to edge devices and border routers. These edge devices police traffic flows by marking packets and applying forwarding behaviors to the packets at the network node.

For further information about Optivity products, contact your Nortel Networks sales representative.

Policy overview

Use Unified Manager to configure policies and filters to control the behavior of network traffic. A *policy* is a network traffic controlling mechanism that monitors the characteristics of the traffic (for example, its source, destination, and protocol) and performs a controlling action on the traffic when certain user-defined characteristics are matched. A *policy action* is the effect a policy has on network traffic that matches the traffic profile of the policy. You can assign only one action to a policy. You set up *filters* to establish packet-specific criteria that determine how a packet is to be processed. You can use filters to remark packets by updating the DSCP code points, to change priorities, or to drop packets.

LAN ports on Business Communications Manager are configured according to the policy determining traffic priorities. As packets enter the switch, they are marked according to their priority.

After the packets are marked, they are moved to the proper egress queue based on their marking. When a packet is to be transmitted, the switch looks at the Premium queue first. Then Business Communications Manager examines the other queues and sends packets based on the weighted percentage for the queues. The entire process is repeated. This approach ensures that the Premium packets are serviced quickly and that the other data types (other queues) are not starved and serviced in a round-robin fashion.

A packet is processed as follows:

1. The packet enters Business Communications Manager.
2. Filters are applied.
3. Filter actions are taken and the packet can be modified (DSCP).
4. The packet is assigned a QoS class. A QoS class is designated using the DSCP values.
5. The packet is placed in the appropriate egress queue according to its priority marking as described above.
6. The queues are serviced in a round-robin fashion (strict priority or weighted fair queueing).

Implementing Quality of Service (QoS)

The QoS application delivers a set of tools that, when optimally configured, combat escalating bandwidth costs and optimize application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

To implement QoS, you need to configure the following:

- QoS Summary parameters ("Configuring the QoS Summary parameters" on page 813)
- QoS Devices ("Configuring Devices" on page 814)
- QoS Rules ("Configuring Policy Rules" on page 816)
- QoS Actions ("Configuring Actions" on page 819)
- QoS Policies ("Configuring QoS policies" on page 821)

Configuring the QoS Summary parameters

The QoS Summary parameters are global settings that affect all of the QoS Policies on your system.

To configure the QoS Summary parameters:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** heading.
   The QoS Summary screen appears.
3. Configure the Summary parameters according to the following table.

Table 285 QoS Summary parameters

Setting	Definition
Description	Shows a description of the QoS service.
Version	Shows the version of the QoS service.
Status	Allows you to enable or disable QoS.
Premium Bandwidth (%)	Enter the percentage of bandwidth to reserve for Premium traffic. You can enter a value from 0% to 90%. **Note**: If you set the Premium Bandwidth too high, you can starve out other traffic.
Video Class	Select the traffic category that is used for H.323 Video traffic. You can assign video traffic as **Premium** or **Best Effort**. **Note**: Choose Best Effort if you want to prevent IP Video traffic from competing with IP Telephony traffic.
Premium DS Code	Enter the DiffServ Code used for Premium traffic on your network. The default value is 0xB8.
Number of Phone Ports	Enter the number of phone ports that are available for QoS. After you change this field, you must reboot the Business Communications Manager system before the change will take affect.

4 Click the **Advanced** tab.
The Advanced screen appears.

5 Click the network adapter you want to modify.

6 On the **Configuration** menu, click **Modify Adapter Water Mark**.
The Advanced property sheet appears.

7 Configure the Advanced parameters according to the following table.

Table 286 QoS Advanced parameters

Setting	Definition
Adapter Name	Shows the name of the network adapter you are modifying.
High Water Mark	Enter the High Water Mark for this network adapter. For LAN adapters, you can enter a value from 1 to 37. For WAN and Dialup adapters, you can enter a value from 1 to 5.
Low Water Mark	Enter the Low Water Mark for this network adapter. For LAN adapters, you can enter a value from 1 to 37. For WAN and Dialup adapters, you can enter a value from 1 to 5. **Note**: The value for the Low Water Mark must be lower than the value for the High Water Mark.

8 Click the **Save** button.

9 Repeat steps 5 to 8 for each network adapter you want to modify.

Configuring Devices

The Devices heading provides access to the Interface Group Table screen, the Interface Queue Table screen, and the DSCP Assignment Table screen. You can configure the Interface Group Table screen. The other two screens provide read-only information.

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) associated with a role combination for the purpose of assigning the same QoS policy to all interfaces in the group.

Creating an interface group configuration

To create an interface group configuration:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Devices** heading.
The Interface Group Table screen appears.

3 On the **Configuration** menu, click **Add Interface Group Entry**.
The Interface Group Table property sheet appears.

4 Configure the Interface Group Table parameters according to the following table.

Table 287 QoS Interface Group Table parameters

Attribute	Description
Group Name	Enter the name for the interface group.
Queue Set Id	This is a read only attribute.
Role Combination	Select the interfaces that you want to include in this interface group.
Capabilities	This is a read only attribute.

5 Click the **Save** button.
The new interface group configuration entry appears in the Interface Group Table.

Modifying an interface group configuration

To modify an Interface group configuration:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QOS** key and click the **Devices** heading.

3 Click the Interface Group Entry you want to change.

4 On the **Configuration** menu, click **Modify Interface Group Entry**.
The Interface Group Table dialog box opens.

5 Change the Role Combination.

6 Click the **Save** button.

Deleting an interface group configuration

To delete an Interface group configuration:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Devices** heading.

3 Click the Interface Group Entry you want to delete.

4 On the **Configuration** menu, click **Delete Interface Group Entry**.
A dialog box opens prompting you to confirm your request.

5 Click the **Yes** button.

Configuring Policy Rules

Policy Rules are IP filters that are defined as part of a QoS Policy.

You can create an IP filter, which enables Business Communications Manager to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

Creating an IP filter configuration

The maximum number of IP filter entries you can add to a QoS Policy is 31.

To create an IP filter configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
   The IP Filter Table screen appears.
3. On the **Configuration** menu, click **Add IP Filter Entry**.
   The IP Filter Table dialog box opens.
4. Configure the IP Filter parameters according to the following table.

Table 288 QoS IP Filter parameters

Attribute	Description
Name	Enter the name of the IP Filter.
Destination Address	Enter a destination IP address in a valid dot format. This address is used to match the destination IP address in the packet's IP header. If you want to ignore the Destination Address setting for this filter, leave this box blank. If you specify an address in this box, you must also specify a subnet mask in the Destination Mask box.
Destination Address Mask	Enter a mask for the destination IP address in a valid dot format. This address is the destination subnet mask. A subnet mask includes or excludes certain values. Subnetworks (or subnets) extend the IP addressing scheme, allowing you to further divide a network into multiple segments. If you specify a Destination Address, you must also specify a Destination Address Mask. Make sure that the mask and address match with each other. For example, a bitwise AND of the mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, an address/mask combination of 10.10.10.32/255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.
Source Address	Enter the source IP address in a valid dot format. This is the IP address to match against the packet's source IP address. If you want to ignore the Source Address setting for this filter, leave this box blank. If you specify an address in this box, you should also specify a subnet mask in the Source Mask box.
Source Address Mask	Enter the source mask of the IP address in a valid dot format. This address is the source subnet mask. A subnet mask includes or excludes certain values. Subnetworks (or subnets) extend the IP addressing scheme, allowing you to further divide a network into multiple segments. If you specify a Source Address, you must also specify a Source Address Mask. Make sure that the mask and address match with each other. For example, a bitwise AND of the mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, an address/mask combination of 10.10.10.32/255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.

Table 288 QoS IP Filter parameters (Continued)

Attribute	Description
DSCP	Enter the DSCP value to match the inbound DSCP. You can enter any decimal value from 0 to 63. If you choose the default (-1), the DSCP value in the packet will be ignored.
Protocol	Select a protocol to match the filter. To select the protocol, choose the protocol from the list or type the numeric value of protocol in the box. You can select TCP, UDP, ICMP, IGMP, RSVP, IP Sec(AH), IPSec(ESP), PPTP/GRE, CBT, EGP, PUP, CHAOS, XNS-IDP, ISO-TP4, IDPR, IPv6, MOBILE, ISO-IP, VINES, MTP, PNNI, PIM, IPX-in-IP, VRRP, L2TP, FC, or None The default is None.
Destination L4 Port	Enter or select a destination port to match the filter. Enter a destination port only if you choose a TCP or a UDP protocol. If you do not want to include the source port in your filter, choose IGNORE. To include a destination port, choose the port from the list services or type the numeric port number of the service. You can choose IGNORE, FTP, TELNET, SMTP, SNMP, DNS, POP, NNTP, or HTTP. You can enter a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can select all of the ports by entering 0-65536. The default is IGNORE.
Source L4 Port	Enter or select a source port to match the filter. Enter a source port only if you choose a TCP or a UDP protocol. If you do not want to include the source port in your filter, choose IGNORE. To include a source port, choose the port from the list services or type the numeric port number of the service. You can choose IGNORE, FTP, TELNET, SMTP, SNMP, DNS, POP, NNTP, or HTTP. You can enter a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can select all of the ports by entering 0-65536. The default is IGNORE.
Permit	Select whether packets that match the filter are permitted to pass.

5 Click the **Save** button.

Modifying an IP filter configuration

To modify an IP filter configuration:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Rules** heading.

3 Click the entry you want to modify.

4 On the **Configuration** menu, click **Modify IP Filter Entry**.
The IP Filter Table dialog box opens.

5 Make the changes to the information about the entry.

6 Click the **Save** button.

Deleting an IP filter configuration

To delete an IP filter configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the entry you want to delete.
4. On the **Configuration** menu, click **Delete IP Filter Entry**.
   A confirmation dialog box opens.
5. Click the **Yes** button to delete the IP Filter Table entry.

Note: You cannot delete a filter if it is referenced in a filter group.

Creating an IP filter group entry

IP filter groups allow you to assign IP filters to a Policy. An IP filter group can consist of one to several IP filters.

When you create an IP filter group, you choose the IP filters to add and you specify the order in which the IP filters are applied.

The maximum number of IP Filter Group entries you can add to a QoS Policy is 31.

To create an IP filter group table entry:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the **IP Filter Group Table** tab.
4. On the **Configuration** menu, click **Add IP Filter Group Entry**.
   The IP Filter Group Table dialog box opens.
5. Configure the IP Filter Group parameters according to the following table.

Table 289 QoS IP Filter Group parameters

Attribute	Description
Filter Group Name	Enter the name of the filter group.
Filter Order	Enter the name of the filter to add to the filter group. If you are adding more than one filter, separate the filter names by a comma. The filters are used in the order you specify.

6. Click the **Save** button.

Modifying an IP filter group configuration

To modify an IP filter group configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the **IP Filter Group Table** tab.
4. Click the IP Filter Group you want to modify.
5. On the **Configuration** menu, click **Modify IP Filter Group Entry**.
   The IP Filter Group Table dialog box opens.
6. Add or delete filters as a member of the Filter Group. You can also change the order in which the filters are applied.
7. Click the **Save** button.

Deleting an IP filter group entry

To delete an IP filter group entry:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the **IP Filter Group Table** tab.
4. Click the IP Filter Group you want to delete.
5. On the **Configuration** menu, click **Delete IP Filter Group Entry**.
   A confirmation dialog box opens.
6. Click the **Yes** button to delete the IP Filter Group Table entry.

Configuring Actions

You configure actions by creating, changing or deleting Actions entries in the Actions screen.

When you assign actions to filters, you specify the type of behavior you want a policy to apply to a flow of IP packets. Actions applied to filters establish packet-specific criteria that determine how a packet is to be processed. You specify the actions associated with specific IP filter groups. When filters match incoming packets, the actions are performed on those packets. Filters can be configured to change the DSCP or to drop packets.

Creating an Action

To create an Action:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Actions** heading.
   The Actions screen appears.

3 On the **Configuration** menu, click **Add Entry**.
The Actions dialog box opens.

4 Configure the Action parameters according to the following table.
Refer to the table "Default Queue mapping for Business Communications Manager" on page 811 for the mapping of DSCP codes, queues and service classes.

Table 290 QoS Action parameters

Attribute	Description
Action Name	Enter the name of this Action.
Packet Drop	Select whether this Action drops the packet (**True**) or keeps the packet (**False**). **Note**: If you choose True to drop the packet, you do not need to choose a value for Update DSCP.
Update DSCP	Enter the new DSCP that this Actions assigns to the packet. You can enter a value from -1 to 63. Enter a value of -1 if you do not want this Action to change the DSCP of the packet.

5 Click the **Save** button.

Modifying an Action entry

To modify an Action entry:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Actions** heading.

3 Click the entry you want to modify.

4 On the **Configuration** menu, click **Modify Entry**.
The Actions dialog box opens.

5 Modify the Action parameters.

6 Click the **Save** button.

Deleting an Action entry

To delete an Action:

1 On the navigation tree, click the **Services** key and the **Policy Management** key.

2 Click the **QoS** key and click the **Actions** heading.

3 Click the Action Entry you want to delete.

4 On the **Configuration** menu, click **Delete Entry**.
A dialog box opens prompting you to confirm your request.

5 Click the **Yes** button.

Configuring QoS policies

A Policy is an association between Devices (interface groups), Rules (IP filter groups), and Actions. When you create a Policy, you define which Devices are affected, which Rules are checked, and what Actions are taken on the specified interface.

Policies are applied according to the precedence order that you assign in the Policies screen.

Adding a policy

To add a policy:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Policies** heading.
3. Click the **Add** button.
   Or, right click the **Policies** heading and click **Add**.
   The Add Policies screen appears.
4. Configure the Policy parameters according to the following table.

Table 291 QoS Policy parameters

Attribute	Description
Name	Enter the name of the Policy.
Filter	Select the filter group that is associated with this policy. You must add a filter group, using the Rules heading, before you can choose it from this box.
Filter Type	Shows the type of filter group that is associated with this policy. This is a read only attribute.
Interface Group	Select the Interface group that is associated with this policy. You must add an interface group, using the Devices heading, before you can choose it from this box.
Interface Direction	Shows the direction of packet flow at the interface to which this policy applies. This is a read only attribute.
Order	Enter the number used to determine the order of precedence for this policy. Nortel Networks recommends that you consider an order numbering strategy (for the values in the Order field) as you configure policies. The policies in the Policy Table are arranged in ascending order according to value in the Order column. By establishing a policy ordering scheme in multiples of, for example, 10 (Order 10, Order 20, Order 30, Order 40, and so on), you are able to insert policies in the appropriate filter precedence location and still retain the precedence of the remaining policies.
Action	Select the action that is performed with policy. You must add an action, using the Actions heading, before you can choose it from this box.

5. Click the **Save** button.

Modifying a policy

To modify a policy:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Policies** key.
3. Click the heading of the policy you want to modify.
4. Click the policy you want to modify.
5. On the **Configuration** menu, click **Modify Entry**.
   The Policy screen appears.
6. Change the Policy attributes.
7. Click the **Save** button.

Deleting a policy

To delete a policy:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Policies** key.
3. Click the heading of the policy you want to delete.
4. Click the **Delete** button.
   Or, right click the heading of the policy you want to delete and click **Delete**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Implementing Common Open Policy Services (COPS)

COPS in your networks allows Business Communications Manager to:

- Gather all relevant Policy information from a policy server (COPS).
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management. For information about COPS, refer to "COPS" on page 812.

The COPS client options available to you in Unified Manager are:

- Viewing COPS statistics and capabilities ("Viewing COPS statistics and capabilities" on page 823)
- Creating COPS client configurations ("Configuring a COPS Client" on page 826)

Note: Configure the role combinations before you configuring dynamic policy management (COPS).

Viewing COPS statistics and capabilities

You can view a list of the capabilities of the COPS client and view the COPS objects provided by all of COPS server connections.

To view COPS capabilities and statistics:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Status and Statistics** heading.
   The COPS Client Capability screen appears.

   The COPS Capabilities box displays a list of the COPS protocols supported by Business Communications Manager. The current supported protocol is copsClientVersion1.
3. Click the **COPS Client Status and Statistics** tab.
   The COPS Client Status and Statistics screen appears. All of the information provided on this screen is read only. The following table describes the items on this screen.

Table 292 Status page items

Item	Descriptions
Address Type	The type of address in copsClientServerAddress.
Address	The IPv4, IPv6, or DNS address of a COPS server.

Table 292 Status page items (Continued)

Item	Descriptions
Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
TCP Port	The TCP port number on the COPS server to which the client is connected.
Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
Last Connection Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
State	The operational state of the connection and COPS protocol with respect to this COPS server.
Server Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
Server Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.
In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
Last Errors	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.
TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 292 Status page items (Continued)

Item	Descriptions
Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
Timeout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocol Keepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Configuring a COPS Client

To configure a COPS client, you enter the information the COPS Client needs to connect to a COPS Server.

Adding a COPS Client Server entry

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Configuration** heading.
   The COPS Client Server screen appears.
3. On the **Configuration** menu, click **Add Cops Client Config Entry**.
   The COPS Client Server screen appears.
4. Configure the COPS Client Server parameters according to the following table.

Table 293 COPS Client Server parameters

Attribute	Description
Address Type	Shows the type of address used for this COPS Client server.
Address	Enter the IP address of the COPS Client server in a valid dot format.
Client Type	Displays the COPS Client type the server is capable of serving.
Authorization Type	Displays the Authorization type used for the server.
TCP Port	Enter the TCP Port used to communicate with the COPS server. You can enter a value from 1 to 65535.
Priority	The Priority determines the order in which the COPS Client attempts to connect to the COPS Server. The COPS Client attempts to connect to the COPS Server with the highest number first. You can enter a value from 0 to 65535. **Note**: If you enter the same Priority for two COPS Servers, the COPS client will randomly select which COPS server to try first.

5. Click the **Save** button.

Modifying a COPS Client Server entry

The TCP Port and Priority are the only parameters you can modify on a COPS Client Server entry.

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Configuration** heading.
   The COPS Client Server screen appears.
3. Click the COPS Client Server entry you want to modify.
4. On the **Configuration** menu, click **Modify Cops Client Config Entry**.
   The COPS Client Server screen appears.
5. Change the TCP Port or Priority of the COPS Client server.
6. Click the **Save** button.

Modifying the COPS Client Server Retry Data

If Business Communications Manager cannot connect to the COPS Client Server on its first attempt, Business Communications Manager will wait and then try to connect again. On the COPS Client Server Retry Data screen, you can enter the number of times that Business Communications Manager attempts to connect again and time it waits between attempts.

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **COPS Client** key and the **Configuration** heading.
The COPS Client Server screen appears.

3 Click the **COPS Client Server Retry Data** tab.
The COPS Client Server Retry Data screen appears.

4 Configure the COPS Client Server Retry Data according to the following table.

Table 294 COPS Client Retry data

Attribute	Description
Server Retry Count	Enter the number of times that Business Communications Manager attempts to connect to the COPS Server if the original connection attempt fails. You can enter a value from 0 to 9999 attempts.
Server Retry Interval	Enter the amount of time that Business Communications Manager waits before attempting to connect to the COPS Client Server again. You can enter a value of 0 to 65535 centiseconds. Note: 100 centiseconds equals one second.

5 Press the **Tab** key to save your changes.

Configuring the Policy Agent characteristics

You can configure the Policy Agent operational parameters. To configure a Policy Agent.

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **Policy Agent** tab.
The Policy Agent screen appears.

3 Configure the Policy Agent settings according to the following table.

Table 295 Policy Agent settings

Attribute	Description
Dynamic Management	Allows you to enable or disable the Policy Server Control. The default value is Disabled. **Note**: If you enable Dynamic Management, local policy control is disabled.
Policy Agent State	Shows the current status of the policy Agent. The possible states are: Running, Initializing or Disabled.
Policy Agent Retry Timer	Enter the time, in seconds, between the receipt of a connections termination/rejection indication and the start of a new connection request. You can enter -1 or a value between 1 and 86400. Note: If you enter a value of -1, a connection retry is not attempted after a failed attempt.

4 Press the **Tab** key to save your settings.

5 Click the **Policy Server** tab.
The Policy Server screen appears.

6 Configure the Policy Server settings according to the following table.

Table 296 Policy Server settings

Attribute	Description
Name	Shows the name of the Policy Server.
ID	Shows the ID of the Policy Server.
Longevity	Allows you to specify when the policy received from the Policy Server expires. The possible values are: **Never Expire**, **Expire Immediately**, **Expire on Timeout** The default value is: **Expire Immediately**.
Time to Live	If you chose Expire on Timeout in the Longevity box, enter the timeout in this box. You can enter a value between 0 and 65535 seconds.

7 Press the **Tab** key to save your settings.

8 Click the **Policy Class Support Table** tab.
The Policy Class Support Table screen appears.

9 This screen displays read only information. This information is described in the following table.

Table 297 Policy Class Support

Attribute	Description
Policy Name	Shows the name of the policy.
Current Instances	Shows the current class entries.
Maximum Installed Instances	Shows the maximum number of allowed class entries.

10 Click the **Policy Device Identification** tab.
The Policy Device Identification screen appears.

11 This screen displays read only information. This information is described in the following table.

Table 298 Policy Device Identification

Attribute	Description
Description	Shows a description of the Business Communications Manager system.
Maximum Message Size	Shows the maximum target message size supported by Business Communications Manager. The maximum COPS message size is 2048.

12 Press the **Tab** key to save your settings.

Chapter 42
Configuring IP Firewall Filters

The Business Communications Manager IP Firewall Filters feature is one of the security features Business Communications Manager offers to protect your network against intruders. The security and firewall features are also used for controlling what outside resources your users will be able to access.

The following features are part of the Business Communications Manager firewall:

- Basic (stateless) Packet Filter ("Basic (stateless) Packet Filter" on page 831)
- Stateful Packet Filters ("Stateful Packet Filters" on page 832)

This section also contains information about:

- "Viewing and changing the status of Firewall Filters" on page 832
- "Configuring IP Firewall Filters for an interface" on page 833
- "Accessing Unified Manager through the Firewall" on page 841

Caution: When blocking incoming packets, make sure you do not block your access to Unified Manager on the system.

Note: For information on using filters for IPX routing, see "Configuring IPX Routing" on page 719.

Packet filtering

A packet filter is a firewall facility that inspects incoming and outgoing packets and uses this information to determine which network packets to allow through the firewall. The traffic may or may not be tracked by keeping the state of the connection.

Basic (stateless) Packet Filter

Business Communications Manager supports basic (or stateless) packet filtering for IP protocols. Stateless packet filtering examines each packet and determines whether or not to pass it through based on the rules entered. No state is maintained for packets evaluated using stateless rules.

Basic Packet Filters are configured by setting the **Stateful** box on the interface screen to No.

Stateful Packet Filters

Business Communications Manager supports stateful packet filtering for IP protocols. Stateful packet filters monitor active sessions and record session information such as IP addresses and port numbers. They maintain state information for each flow (TCP, UDP or ICMP). Stateful filters use the state information to determine if a packet is responding to an earlier request that has been validated by the rule set. If the packet is in response to a previous request, the packet is treated in the same manner. It will either be blocked or allowed though.

Stateful packet filters protect your network against Internet attacks such as source spoofing, where an attacker pretends to be a trusted user by using an IP address that is within the accepted range of IP addresses of your internal network. Business Communications Manager stateful packet filtering validates that addresses coming from outside the network are valid outside addresses. Stateful packet filters also protect your network from a denial-of-service attack, where an attacker tries to block valid users from accessing a resource or a server.

Stateful filtering supports TCP, UDP, IP, and ICMP. Stateful filtering supports the following applications: H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, DHCP, TFTP, GOPHER, FINGER, NNTP, NetBios, POP2, RPC, SNMP and SUNNFS.

IP Firewall filters and NAT

When you use NAT and IP Firewall filters, there are two interactions you need to be aware of.

- On inbound traffic, the NAT rules are applied before the IP Firewall Filter rules.
- On outbound traffic, the IP Firewall Filter rules are applied before the NAT rules.

Viewing and changing the status of Firewall Filters

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **IP Firewall Filters** heading.
   The Firewall Filters Summary screen appears. The Summary screen attributes are:

Table 299 IP Firewall Filters Summary

Attribute	Description
Description	Shows a description of Firewall Filters.
Version	Shows the version number of the subsystem.
Status	Shows the status of Firewall Filters. This box also provides commands to enable or disable Firewall Filters. Possible values: **Disabled**, **Enabled** When the status is Enabled, the state of all of the traffic is monitored. Rules can then be set for each of the interfaces, as necessary. The default value is: **Disabled.**

3. Press the **Tab** key to save your settings.

Configuring IP Firewall Filters for an interface

This section describes configuring IP Firewall Filters for a single interface. Follow the same instructions to configure the parameters for each of the other interfaces.

This section also includes information about:

The following procedures describe how to configure a single interface (LAN1 for example).

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **IP Firewall Filters** key and click the heading of the interface you want to configure. The Logging Settings screen appears.
3. Click the **Logging** box and click **Disabled** or **Enabled**.
4. Click the **Logging Level** box and click one of the following options:
   - Level **1** logs blocked packets
   - Level **2** logs passed packets
   - Level **3** logs both
5. Press the **Tab** key to save your settings.
6. Click the **Log Viewing Options** tab.
   The Log Viewing Options screen appears.
7. Enter the **Start Date** and **End Date** (mm/dd/yyyy).
   This is necessary only if you wish to view existing logging data.

Note: You can configure rules several ways; using default rules, setting up individual rules, or a combination of the two.

Adding Default Rules

Caution: If you turn on the Default Rules, you cannot access Unified Manager on this interface.

1 Click the **Default Rule Status** tab.
The Default Rule Status screen appears.

2 Click the **Status** box and click one of the following options:

- **Enabled - Pass Outgoing and Block Incoming Except IP Phones**
Allows IP telephony registration traffic through, but blocks all other traffic on this interface.

  Note: You must still specify an H.323 rule to allow IP call voice traffic. This setting only allows the IP telephone to contact the system to register.

  Also, Registration must be turned on in the **Services, IP Telephony, Nortel IP Telephone, General** page, before the telephone can access the system to register.

- **Enabled - Pass Outgoing and Block Incoming Including IP Phones**
Blocks all traffic on this interface, including IP telephony traffic.
- **Disabled - Pass All**
The IP Firewall does not check the traffic on this interface. Therefore, all traffic on this interface, both incoming and outgoing, is passed through.

The default is **Disabled**.

Note: Setting an Incoming Rule that blocks all incoming packets and disabling the Default Rules is not the same as enabling the Default Rules.

When block all incoming packets and disable the Default Rules, packets that originate from inside the Firewall are not treated as Stateful. When a response packet is returned, it will not match the Incoming Rule and will be blocked.

When you enable the Default Rules, packets that originate from inside the Firewall are treated as Stateful. When a response packet is returned, it will match the existing state and will be passed.

Adding an Input Filter for a Firewall Filter Interface

Before you can specify a Rule Order, you must add Filter Rules.

The maximum number of Input Filter Rules you can add is 32.

1 Click the **Input Filters' Rule Settings** tab.
The Input Filters' Rule Settings screen appears.

2 On the **Configuration** menu, click **Add Input Filter Rule**.

3 Configure the Input Filter Rule settings according to the following table.

Table 300 Firewall Input Filter Rule settings

Attribute	Description
Rule Name (IR# or OR#)	Allows you to assign a number to the Rule.
Stateful	Allows you to specify if the states of connections that match this rule will be monitored. This permits the creation of one-way rules. For example, you can permit inside traffic to return but block traffic originating from the outside. For more information refer to "Stateful Packet Filters" on page 832. The values are **Yes** and **No**. The default is **Yes**.
Disposition	Allows you to specify if a packet that matches this rule passes through or is blocked. The values are **Block** or **Pass**. The default is **Block**.
Protocol	Allows you to specify the protocol type of the packet to be filtered. The values are; **IP**, **TCP**, **UDP**, **TCP/UDP**, **ICMP**, **OSPF**, **PPTP**, **IPSEC_AH AND IPSEC_ESP**. The default is **IP**.
Source IP Type	Allows you to specify if the Source IP is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Source IP and Source IP Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Source IP	Allows you to specify the source address of the packet to be filtered.
Source Range Mask	Allows you to specify the source address mask of the packet to be filtered. If you enter 255.255.255.255, then the Source IP is a single address. If you enter 0.0.0.0, then the Source IP is all possible addresses.
Source Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **H.323**, **POP**, **NNTP**, **NetBios**, **RPC**, **SUNNFS** and **DCOM**.
Non-standard FTP Port	Select **Yes** if the Source Port Range contains non-standard FTP ports. Select **No** if the Source Port Range does not contain non-standard FTP ports. If your FTP server behind the Business Communications Manager listens on a non-standard port, you must select **Yes** for this option. This is because FTP uses two ports - command(21) and data(20). When a port other than 21 is used for FTP, the IP Firewall needs to be able to deal with the alternate data port as well. The default is **No**.

Table 300 Firewall Input Filter Rule settings (Continued)

Attribute	Description
Destination IP Type	Allows you to specify if the Destination IP Type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Destination IP and Destination IP Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Destination IP	Allows you to specify the Destination IP address.
Destination Range Mask	Allows you to specify the destination address mask of the packet to be filtered. If you enter 255.255.255.255, then the Destination IP is a single address. If you enter 0.0.0.0 then the Destination IP is all possible addresses.
Destination Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **POP**, **NNTP**, **NetBios**, **RPC**, **SUNNFS** and **DCOM**.
Non-standard FTP Port	Select **Yes** if the Destination Port Range contains non-standard FTP ports. Select **No** if the Destination Port Range does not contain non-standard FTP ports. If your FTP server behind the Business Communications Manager listens on a non-standard port, you must select **Yes** for this option. This is because FTP uses two ports - command(21) and data(20). When a port other than 21 is used for FTP, the IP Firewall needs to be able to deal with the alternate data port as well. The default is **No**.
Source Routing	Allows you to specify how the Source Routing is checked. **Present**: Rule matches Only if the packet has the source routing option set. **Absent**: Rule matches Only if the packets does not have the source routing option set. **Ignore**: The source routing option in the packet is not checked and therefore all packets will match. The default is **Ignore**.
IP Options	Allows you to specify how the IP Options are checked. **Present**: Rule matches Only if the packet has the IP options set. **Absent**: Rule matches Only if the packets does not have the IP options set. **Ignore**: The IP Options in the packet are not checked and therefore all packets will match. The default is **Ignore**.
Quick	Allows you to specify the order of rule match. **Yes** means that the first rule match is used. **No** means the last rule match is used. The default is Yes.

Note: When you set filters, make sure you allow the flow of packets going to the RPC port (port 135 TCP or UDP), DCOM ports, and the Unified Manager port (port 443 TCP) for correct Unified Manager operation. For more information about allowing Unified Manager access, refer to "Accessing Unified Manager through the Firewall" on page 841.

To allow access for SSH, you must set the filters to allow the flow of packets to the SSH port (port 22).

To allow access for Telnet, you must set the filters to allow the flow of packets to the Telnet port (port 23). If you block the Telnet port, you can still access Telnet using a direct connection. To make a direct connection, you must be on site and you must connect the LAN port on the Business Communications Manager to the NIC port on your computer using an Ethernet crossover cable.

4 Click the **Save** button.

Modifying an Input Filter for a Firewall Filter Interface

1 Click the **Input Filters' Rule Settings** tab.
The Input Filters' Rule Settings screen appears.

2 Click the Input Filter you want to modify.

3 On the **Configuration** menu, click **Modify Input Filter Rule**.

4 Modify the Input Filter Rule attributes.

5 Click the **Save** button.

Deleting an Input Filter for a Firewall Filter Interface

1 Click the **Input Filters' Rule Settings** tab.
The Input Filters' Rule Settings screen appears.

2 Click the Input Filter you want to delete.

3 On the **Configuration** menu, click **Delete Input Filter Rule**.
A message appears that asks you to confirm the deletion.

4 Click the **Yes** button.

Configuring the order of the Input Filters for an interface

After you enter all of the Input filters, you need to set the order in which the filters are used.

The order of the Input Filter Rules is very important. The more specific rules, such as rules for specific port numbers and addresses, should be placed first. TCP and UDP rules are typically more specific and should be first. Rules for just the IP protocol should be placed last, because they typically ignore port numbers and only match on IP addresses.

The following two examples show how the order of the rules affects what traffic can pass through the IP Firewall.

Example 1: Rule 1 is configured to Pass TCP protocol 25 from any IP address to 10.10.10.20. Rule 2 is configured to Block any TCP protocol from any IP address to any IP address. If Rule 2 is placed before Rule 1, then Rule 1 will never be reached because all TCP protocol 25 packets destined for IP address 10.10.10.20 will be blocked by Rule 2 first.

Example 2: Rule 1 is configured to Pass TCP protocol 6800 from IP address 192.168.10.20 to IP address 10.10.10.20. Rule 2 is configured to Block all IP protocols from any IP address to any IP address. If Rule 2 is placed before Rule 1, all TCP packets will match Rule 2 first and will be blocked.

To configure the order of the input filters:

1. Click the **Input Rules' Filter Order** tab.
   The Input Rules' Filter Settings screen appears.
2. Type in the Input Filter Rule Order for the interface you are configuring.
3. Press the **Tab** key to save your settings.

Adding an Output Filter for a Firewall Filter Interface

Before you can specify a Rule Order, you must add Filters.

The maximum number of Output Filter Rules you can add is 32.

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. On the **Configuration** menu, click **Add Output Filter Rule**.
3. Configure the Output Filter Rule settings. These setting are described in the table in "Adding an Input Filter for a Firewall Filter Interface" on page 835.
4. Click the **Save** button.

Modifying an Output Filter for a Firewall Filter Interface

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. Click the Output Filter you want to modify.
3. On the **Configuration** menu, click **Modify Output Filter Rule**.
4. Modify the Output Filter attributes.
5. Click the **Save** button.

Deleting an Output Filter for a Firewall Filter Interface

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. Click the Output Filter you want to delete.
3. On the **Configuration** menu, click **Delete Output Filter Rule**.
   A message appears that asks you to confirm the deletion.
4. Click the **Yes** button.

Configuring the order of the Output Filters for an interface

After you enter all of the Output filters, you need to set the order in which the filters are used.

The order of the Output Filter Rules is very important. The more specific rules, such as rules for specific port numbers and addresses, should be placed first. TCP and UDP rules are typically more specific and should be first. Rules for just the IP protocol should be placed last, because they typically ignore port numbers and only match on IP addresses.

The following two examples show how the order of the rules affects what traffic can pass through the IP Firewall.

Example 1: Rule 1 is configured to Pass TCP protocol 25 from any IP address to 10.10.10.20. Rule 2 is configured to Block any TCP protocol from any IP address to any IP address. If Rule 2 is placed before Rule 1, then Rule 1 will never be reached because all TCP protocol 25 packets destined for IP address 10.10.10.20 will be blocked by Rule 2 first.

Example 2: Rule 1 is configured to Pass TCP protocol 6800 from IP address 192.168.10.20 to IP address 10.10.10.20. Rule 2 is configured to Block all IP protocols from any IP address to any IP address. If Rule 2 is placed before Rule 1, all TCP packets will match Rule 2 first and will be blocked.

To configure the order of the output filters:

1. Click the **Output Filter Rules' Order** tab.
   The Output Filter Rules' Configuration screen appears.
2. Type in the Output Filters' Rule Order for the interface you are configuring.
3. Press the **Tab** key to save your settings.

Accessing Unified Manager through the Firewall

- Do not set any blocking input rules on the interface that you use to connect to Business Communications Manager using Unified Manager. This includes enabling the default rules.
- Set three Input Rules for Unified Manager traffic, one for RPC, one for DCOM and one for port 443. Configure these three rules as follows:

Table 301 Input Rule Configuration for Unified Manager — RPC

Type of filter	Input Filter
Protocol	TCP
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source Range Mask	255.255.255.255 (or as appropriate)
Source Port Range	ALL
Destination IP Type	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP	IP address for this interface (or blank if IP Type is Dynamic)
Destination Range Mask	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range	RPC (Port 135)

Table 302 Input Rule Configuration for Unified Manager — DCOM

Type of filter	Input Filter
Protocol	TCP
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source Range Mask	255.255.255.255 (or as appropriate)
Source Port Range	ALL
Destination IP Type	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP	IP address for this interface (or blank if IP Type is Dynamic)
Destination Range Mask	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range	DCOM (Ports 54050 – 54100)

Table 303 Input Rule Configuration for Unified Manager — port 443

Type of filter	Input Filter
Protocol	TCP/UDP
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source Range Mask	255.255.255.255 (or as appropriate)
Source Port Range	ALL
Destination IP Type	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP	IP address for this interface (or blank if IP Type is Dynamic)

Table 303 Input Rule Configuration for Unified Manager — port 443 (Continued)

Destination Range Mask	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range	443

Note: The order of these three rules does not matter, as long as these rules come before more general rules.

Firewall rules for Business Communications Manager with Dialup interfaces

For systems with dialup interfaces (ISDN, V.90), we recommend that you add Firewall filters to all interfaces except the dialup interface that blocks NetBIOS traffic. This prevents any NetBIOS packets from getting into the Business Communications Manager and bringing up the dialup interface link.

Table 304 Input Rule Configuration for systems with dialup interfaces

IR1	
Direction:	In
Stateful:	Yes
Disposition:	Block
Protocol:	TCP/UDP
Source IP:	0.0.0.0
Source Mask:	0.0.0.0
Source Port:	NETBIOS
Destination IP:	0.0.0.0
Destination Mask:	0.0.0.0
Destination Port:	NETBIOS

IR2	
Direction:	In
Stateful:	Yes
Disposition:	Block
Protocol:	TCP/UDP
Source IP:	0.0.0.0
Source Mask:	0.0.0.0
Source Port:	NETBIOS
Destination IP:	0.0.0.0
Destination Mask:	0.0.0.0
Destination Port:	DNS

For example, if a Business Communications Manager is configured with two LANs and one ISDN dialout interface, then these Firewall rules should be placed on both of the LANs.

Appendix A
Defining region-based defaults

This section describes some of the differences in the system defaults. These defaults are set based on the region or telephony or CallPilot template that you select in the Quick Start wizard when the system is first configured. Each region is designed using a set of system defaults that provide specific functionality for the geographical area in which the system is deployed.

This section includes information about:

Region-based system settings

The tables in this section provide information about different settings that affected by the region assigned to the system.

Core software and regions

Each Region setting requires a specific core software to perform correctly.

The following table shows the core software available.

Table 305 Core software, defined by region and carrier profile

Core Software (Carrier s/w ID)	T1 CT2 Plus	T1 Etiquette	E1 Euro	E1 Global	E1 CALA
Region	Caribbean Hong Kong North American Taiwan	Caribbean Hong Kong North American Taiwan	Denmark France Germany Holland Italy Norway Spain Sweden Switzerland United Kingdom	Australia Brazil CALA Global PRC	Australia Brazil CALA Global PRC
South American and Central American countries are assigned to regions in the following way: • Caribbean includes Antigua, Bahamas, Barbados, Bermuda, Cayman Islands, Dominican Republic, Jamaica, USVI, Puerto Rico, and Trinidad • CALA refers to all other Caribbean and Latin American countries with European-based standards.					

Languages

The following table lists the languages available for each region and a specific order in which the languages are set as default.

Table 306 Languages

Region	Language
CALA Caribbean Hong Kong North American PRC Taiwan	NA English, NA French, NA Spanish
Australia United Kingdom	UK English
Brazil	Portuguese, NA English
Denmark	Danish, Norwegian, Swedish, NA English
France	Euro French, NA English
Germany	German, NA English
Global	NA English, NA French, NA Spanish, Turkish
Holland	Dutch, Euro French, NA English
Italy	Italian, NA English
Norway	Norwegian, Swedish, Danish, NA English
Spain	Euro Spanish, NA English, Portuguese
Sweden	Swedish, Norwegian, Danish, NA English
Switzerland	German, Euro French, Italian, NA English

The following table shows a breakdown of the language support for South American and Central American countries.

Table 307 South/Central America language breakout

Language	Spanish		English		French	Portuguese
Country	Dominican Republic Jamaica Puerto Rico Argentina Bolivia Chile Columbia Costa Rica Guatemala Mexico Nicaragua	Peru Panama Uruguay Venezuela El Salvador Honduras Ecuador Paraguay	St. Thomas USVI Aruba Bahamas Bermuda Curacao Trinidad Anguilla Antigua Barbados Dominica Grenada	Guyana Montserrat St. Kitts St. Lucia St. Maarten Suriname Turks & Caicos St. Vincent St. Thomas Cayman Islands Belize	Haiti	Brazil

Caller ID displays

The North American region supports the following format: 5554775 (613)

All other regions display the numbers in a continuous string of a maximum of 14 characters: 6135554775

Companding Law by region

The following table shows the companding law used for each region.

DECT systems: You must ensure that DECT systems that require mu-law have the correct region setup before you install the DECT system. Refer to the *DECT Installation and Maintenance Guide* for details.

Table 308 Companding law

Companding Law	
mu-law	A-law
Caribbean Hong Kong North American Taiwan	Australia Brazil CALA Denmark France Germany Global Holland Italy Norway PRC Spain Sweden Switzerland United Kingdom

Mobility services by region

The following table shows the Mobility services that are supported by the Business Communications Manager, and the regions that can use each type.

Table 309 Mobility services, by region

Profile	Available Mobility Service
Caribbean Hong Kong North American PRC	Companion (CT2-Plus, Etiquette)
CALA Brazil	Companion (CT2-Plus)
Taiwan	Companion (CT2-Plus, Etiquette) DECT
Australia Denmark France Germany Global Holland Italy Norway Spain Sweden Switzerland United Kingdom	DECT

Media bay module availability by region

Some of the media bay modules are customized for a specific type of line and are not available to all regions. The following table lists a cross-reference between regions and the type of modules that can be used within the related area.

Table 310 Module availability, by profile

Region	DSM	ASM+	ASM	CTM	4X16	GATM	BRI	DTM	DECT
Australia	✓					✓	✓	✓	✓
Brazil	✓					✓	✓	✓	
Caribbean	✓			✓	✓		✓	✓	
CALA	✓			✓	✓		✓	✓	
Denmark	✓						✓	✓	✓
France	✓						✓	✓	✓
Germany	✓						✓	✓	✓
Global	✓			✓	✓		✓	✓	✓
Holland	✓						✓	✓	✓
Hong Kong	✓			✓	✓		✓	✓	✓
Italy	✓						✓	✓	✓
North American	✓	✓	✓	✓	✓	✓	✓	✓	
Norway	✓						✓	✓	✓
PRC	✓			✓	✓		✓	✓	
Spain	✓						✓	✓	✓
Sweden	✓						✓	✓	✓
Switzerland	✓						✓	✓	✓
Taiwan	✓			✓	✓	✓	✓	✓	✓
United Kingdom	✓	✓				✓	✓	✓	✓

FEM-trunk module combinations by region

Trunk Modules may be connected to the Business Communications Manager system using the Fiber Expansion Module (FEM). The following table provides a cross-reference between regions and the Trunk Modules you can connect to the FEM.

Table 311 Trunk availability, by region

Region	BRI S/T 2/4	BRI U2/4	Analog DID	Analog E&M	Analog CLID	Country- specific analog trunk card
Australia	✓					✓
Brazil	✓					
CALA	✓	✓	✓	✓	✓	
Caribbean	✓	✓	✓	✓	✓	
Denmark	✓					
France	✓					✓
Germany	✓					✓
Global	✓			✓	✓	
Holland	✓					✓
Hong Kong	✓		✓	✓	✓	
Italy	✓					
North American	✓	✓	✓	✓	✓	
Norway	✓					
PRC	✓			✓	✓	
Spain	✓					
Sweden	✓					
Switzerland	✓					
Taiwan	✓		✓	✓	✓	
United Kingdom	✓					✓

PRI line protocol support, by region

Table 312 PRI line protocol supported, by region

Region	BRI T side	BRI S side	PRI	T1
Australia	ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ISDN ETSI 300 403, ETSI QSIG 300 239,	
Brazil CALA	ISDN ETSI 300 403, ETSI QSIG 300 239	ISDN ETSI 300 102	ETSI QSIG 300 239, ISDN ETSI 300 403, MCDN	
Caribbean North American	NI-2	NI-2	NI-2 4ESS DMS100 DMS250 MCDN	Loop E&M DID Ground Fixed trunk types
Hong Kong Taiwan	ITU-T	ITU-T	ITU-T	Loop E&M DID Ground Fixed trunk types
Denmark France Germany Global Holland Norway PRC Spain Sweden Switzerland	ETSI QSIG 300 239, ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 403	
Italy	ISDN ETSI 300 102 ETSI QSIG 300 239	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 102	
United Kingdom	ETSI QSIG 300 239, ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 403	

Supported ISDN line services

The following table shows the ISDN private network services that are supported by the Business Communications Manager.

Table 313 ISDN line services

MCDN over PRI (SL-1)	DPNSS	DASS2	ETSI QSIG
Basic Call	Basic Call	Basic Call	Basic Call
DDI	DDI	DDI	DDI
Name display	Diversion	Originating line identity (OLI)	Name display
Number display	Redirection	Terminating Line Identity (TLI)	Number display
Centralized voice mail	Centralized voice mail	Call Charge Indication (CCI)	
Camp-on	Call Offer	Call Charge Rate Indication (CCRD)	
ISDN Call Connection Limit	Loop avoidance		
Network Call Transfer	Executive Intrusion		
Break-in	Three Party		
Trunk Route Optimization (TRO)	Route Optimization		
Trunk Anti-Tromboning			

The following table shows the network-based ISDN supplementary services and the features available for each.

Table 314 ISDN services, by Protocol

Protocol	Available ISDN services
NI (Caribbean. North America)	Basic Call DID Name display Number display ONN blocking
ETSI Euro (Australia. CALA, Denmark, France, Germany, Global, Holland, Hong Kong, Italy, Norway, PRC, Spain, Sweden, Switzerland, Taiwan, United Kingdom)	Basic Call DDI subaddressing (on S-loop) ETSI Call Diversion (partial rerouting) AOC-E (specific changes for Holland and Italy) MCID CLIP COLP CLIR

Defining time zones by country and language

Time zones are based on the actual time zone where the Business Communications Manager base unit is located. The Time Zone dropdown list on the initialization screen, allows you to be very specific in choosing a compatible time zone. If your exact location is not on the list, choose the one with the time zone closest to you. Note that some time zones are individualized because they do not switch from Standard Time to Daylight Saving Time. For example, this is the case for Saskatchewan.

The format of the time and date changes are based on the prime language of the region. The following table provides a list of formats based on language or country.

Table 315 Time/date formats based on language

Language/Country	Time/Date format
Danish	2001-01-01 13:57
Dutch	1 Jan 01 13:57
EuroFrench	1 jan 13:57
EuroSpanish Brazil	1 Ene 13:57
German	1 Jan 13:57
Italian	1 Gen 13:57

Language/Country	Time/Date format
NA English	Jan 1 1:57 pm
NA French	2001-01-01 13:57
NA Spanish	Ene 1 1:57 pm
Norwegian	1 Jan 13:57
Swedish	2001-01-01 13:57
Turkish	1 Ock 13:57
UK English	1 Jan 1:57 pm

System feature defaults

The following table compares the system defaults for the North American, Global and UK regions. In addition, the following functionality applies:

- Regions for Denmark, Holland and Sweden are the same as the Global region except for the default to local languages and local tones and cadences.
- The Region for the Caribbean is the same as the North American region except that it supports the M7000 telephone.
- The Region for CALA is the same as the Caribbean region, except NI ISDN is replaced by ETSI ISDN (u-law).
- The Region for Europe is the same as the United Kingdom region except there are no default dialing restrictions, and ATA2 parameters are set to European values.

Table 316 Region defaults

Functionality	Attribute	North American	Global	United Kingdom
Direct Dial Access code		0	0	0
DTMF parameters	Tone duration	120 msec	120 msec	120 msec
	Pause time	1.5	1.5	3.5
	Interdigit time	80 msec	80 msec	100 msec
Conference tone		disabled	disabled	enabled

Table 316 Region defaults (Continued)

Functionality	Attribute	North American	Global	United Kingdom
Call Back Kill time		180 sec	180 sec	360 sec
PCM Companding Law		mu-law	a-law EBI	a-law EBI
Race Integration		disabled	disabled	disabled
OLI digits		fixed 10 digits	fixed 10 digits	variable length a maximum of 8
Dial Tone Detection		enabled	enabled	enabled
Hunt Groups	Show in second	disabled	disabled	disabled
	Default delay	4 ring cycles	4 ring cycles	4 ring cycles
	Queue timeout	60 sec	60 sec	60 sec
	If busy	busy tone	busy tone	busy tone
	Mode	broadcast	broadcast	sequential
Target line if busy setting		prime	prime	busy tone
M7000 set		disabled	enabled	enabled
Fax switch		enabled	enabled	enabled
Service Schedule time	Night	start 23:00 end 07:00	start 23:00 end 07:00	start 23:00 end 07:00
	Evening	start 17:00 end 23:00	start 17:00 end 23:00	start 17:00 end 23:00
	Lunch	start 12:00 end 13:00	start 12:00 end 13:00	start 12:00 end 13:00
	Service 4	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
	Service 5	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
	Service 6	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
Call Forward Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	2 ring cycles
	Options	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles
DRT Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles

Table 316 Region defaults (Continued)

Functionality	Attribute	North American	Global	United Kingdom
Handsfree		none	none	none
Pickup Group		none	none	none
Remind Delay		60 secs	60 secs	60 secs
Allow SLR		disabled	disabled	disabled
Transfer Callback	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles
Dialling Plan		market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)
ONN Blocking	VSC for analog tone	n/a	n/a	141
	VSC for analog pulse	n/a	n/a	141
	VSC for BRI	n/a	n/a	141
	VSC for PRI	n/a	n/a	141
	State for BRI/PRI	n/a	n/a	send feature code
Default CO lines		2	2	4
UTAM		enabled	disabled	disabled
	Portable credits	0	defined in the application (max)	n/a
Release reason	Release text	none	none	detail
	Release code	disabled	disabled	disabled
	Display duration	3 sec	3 sec	3 sec
Overlap Receiving		disabled	enabled	disabled
Local Number length for ISDN overlap receiving		8	8	8
Tandem alerting		disabled	disabled	disabled
TON/NPI		national/E.164	national/E.164	unknown/unknown
National number length		10	10	0
national number prepend		n/a	n/a	0
Provide tone on PRI		enabled	n/a	disabled

Dialing plan defaults

Some profiles have default restriction dialing filters. The table below lists the filters for these profiles.

Table 317 Default dialing restrictions, by profile

Profile	Restriction filter #	Restriction/ override	Restriction/ override	Restriction/ override	Restriction/ override	Restriction/ override	Restriction/ override
UK	1	0/0600	1	010			
	5	010	1	00			
	6	*					
North America	1	0	1/1800, 1877, 1888	911/911	9411	976	1976
		1***976	1900	1***900	5551212		
Hong Kong	1	00***	170	172	173	1747	1760
		1761	1766	1770	1771	1772	1775
		1778	1783	1788	900		
Australia	1	0/013	1/13, 1800				
	5	00	1/13, 11, 1800				
	6	*					

BRI and PRI line types

The following table provides a description of the types of lines that BRI and PRI trunks can provide. These are set under **Resources**, **Media Bay Modules**, **Bus XX**, **Module X** on the Unified Manager.

Note that some of these line types are only available when specific regions are chosen.

Table 318 BRI and PRI line types (DTM and BRI modules)

Digital trunk types	Description
T1	digital line that carries data on 24 channels at 1.544 Mbps (North American); 30 channels at 2,048 Mbps (Europe) Loop, E&M, DID and ground start trunks are also versions of T1 lines. You can program auto-answer T1 loop start, T1 E&M trunks, T1 DID, T1 ground start trunk*s*, PRI and IP trunks to map to target lines to provide for attendant bypass (calling directly to a department or individual) and line concentration (one trunk can map onto several target lines).
DID	This is a type of T1 trunk line that allows an outside caller to dial directly into a line on the Business Communications Manager.
Loop	This is a type of T1 line. This type of line is used on systems where the service provider supports disconnect supervision for the digital loop start trunks. These trunks provide remote access to the Business Communications Manager from the public network. This trunk must have disconnect supervision to allow the trunk to be set to auto-answer, which provides the remote access portal.
Ground	T1-groundstart trunk These lines offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for digital loop start trunks. Ground start trunks work with T1 only. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end.
E&M	T1 and E&M. This type of trunk line is used to create simple network connections to other phone systems. This trunk always operates in a disconnected supervised mode.
PRI	ISDN interface with 23 B channels and 1 D channel at 1.544 MBps (in Europe: 30 B channels and 2 D channels at 2.048 Mbps) This is the module that controls system timing. These lines give you incoming and outgoing access to an ISDN network and are auto-answer trunks, by default. These lines provide a fast, accurate and reliable means of sending and receiving data, images, text and voice information. using PRI lines allows for faster transmission speeds and the addition of a variety of powerful business applications, including remote LAN access, video conferencing, file transfer and internet access.
BRI	ISDN loop that provides both T, S and U2 and U4 (region-specific) reference point loops. These loops can support both network (T and S loops) and terminal equipment (S loop) connections. This type of line provides incoming and outgoing access to an ISDN network. ETSI ISDN BRI is the European Telecommunications Standards Institute specification for BRI ISDN service. BRI provides two bearer B-channels operating at 64 kbits/s and a data D-channel which operates at 16 kbits/s. The D-channel is used primarily to carry call information. Like loop start trunks, BRI lines can be configured as manual-answer or auto-answer.
DASS2	(British) Trunk provides multi-line IDA interconnection to the British Telecom network.

Table 318 BRI and PRI line types (DTM and BRI modules) (Continued)

Digital trunk types	Description
DPNSS	(international term: Q.Sig or Q.931) a digital private network signaling system which allows phone systems from different manufacturers to be tied together over E1 lines, offering significant enhancements to Business Communications Manager networking capabilities. DPNSS makes it easier to support centralized network functionality within private networks, for operators and attendants dealing with large numbers of calls. Its routing capabilities provide more of the larger-network capabilities without the expense of installing a new system, re-configuring all the nodes and worrying about a lot of downtime. Most functionality over DPNSS lines is transparent once the DPNSS is programmed into the system. DPNSS allows a local node, acting as a terminating node, to communicate with other PBXs over the network using E1 lines. For example, corporate offices separated geographically can be linked over DPNSS lines to other Business Communications Manager systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Business Communications Manager systems to function like a private network.
Analog trunk types	
Public	Provides potential access for any set on the system.
Private	Provides potential access for a specific set.

CallPilot regions

The CallPilot portion of the Business Communications Manager application also has a region setting that defines some call-management-related system defaults.

The CallPilot region is specified at system initialization and start up when you run the Quick Start Wizard. You can also change this setting under **System, Identification**.

The following table lists the default prime language for the countries (regions) where the voice mail application is supported.

Table 319 CallPilot region default languages by country

Country	Default voice mail language
North America	NA English
UK	UK English
Australia	NA English
Denmark	Danish
Holland	Dutch
Sweden	Swedish
France	Euro French
CALA	LA Spanish
Caribbean	NA English
Europe	UK English

Country	Default voice mail language
Germany	German
Global	NA English
Italy	Italian
Norway	Norwegian
Spain	Spanish
Switzerland	German
Hong Kong	NA English
PRC	Mandarin (Taiwan)
Taiwan	Mandarin (Taiwan)
Brazil	Portuguese

The following list are the default settings that are the same for all CallPilot regions:

- Application name string VM
- Group list lead digit 9
- Country log header Access version: %s VM version:
- SC maximum lines 10_20 334
- TA Admin Name Voice Mail
- AMIS enabled
- Bilingualism enabled
- digital network access enabled
- Fax feature available enabled
- AMIS address start key #
- Operator Revert key 0
- Touch Tone Gateway disabled
- Maximum CLID entry 16
- Maximum network length 16

The following table lists the feature default settings that differ among the CallPilot regions.

Table 320 CallPilot feature default anomalies

	Mail box login		Alternate QZ mapping		Max local number length			National Number Length				Maximum CLID display			
Regions	**	88	False	True	7	8	11	8	9	10	11	7	8	9	16
Australia		✓		✓		✓			✓				✓		
CALA	✓			✓		✓		✓					✓		
Caribbean	✓		✓		✓					✓		✓			
Denmark		✓		✓		✓					✓		✓		
Europe		✓		✓	✓						✓				✓
France		✓		✓	✓						✓	✓			
Germany		✓		✓	✓						✓	✓			
Global		✓		✓	✓						✓				✓
Holland		✓		✓	✓						✓	✓			
Hong Kong	✓		✓				✓			✓				✓	
Italy		✓		✓	✓						✓	✓			
North America	✓		✓		✓					✓		✓			
Norway		✓		✓	✓						✓	✓			
PRC	✓		✓				✓			✓				✓	
Spain		✓		✓	✓						✓	✓			
Sweden		✓		✓		✓					✓		✓		
Switzerland		✓		✓	✓						✓	✓			
Taiwan	✓		✓				✓			✓				✓	
UK		✓		✓			✓				✓			✓	

Appendix B
System Features

This section contains two lists:

- "Business Communications Manager feature codes" on page 861 which contains a complete list of the feature codes that can be accessed from digital and IP telephones.
- "Button programming features" on page 865 contains a list of the features that are programmable under the DN record **Button Programming** heading.

Business Communications Manager feature codes

This appendix provides a quick reference for Business Communications Manager features available by pressing the FEATURE button on M-series telephones, Business Series Terminals (BST T-series), and IP telephones. The following provides feature names sorted in alphabetical order and numerically, by feature code.

The portable handsets, such as Companion, DECT, and NetVision telephones, do not support all call features, or they may have alternate ways of using the feature codes. Refer to the *Telephony Features Handbook* for lists of supported features for these handsets, and to the user documentation for the specific product to find out how to use the codes on each type of telephone.

Table 321 Features sorted by feature name and by activation code

Sorted by feature name	
Feature name	**FEATURE** <code>
Alarm time (room set)	875
Alarm time - Cancel	#875
Alarm time (HS admin set)	877
Autodial - External	*1
Autodial - Internal	*2
Auto Hold	73
Auto Hold - Cancel	#73
Background Music	86
Background Music - Cancel	#86
Button inquiry	*0
Call Center agent login/log out	904
Call Center agent make busy/ready	908
Call Center queue status	909
Call Charge Indication	818
Call Duration Timer	77
Call Forward	4

Sorted by activation code	
FEATURE <code>	**Description**
0	Speed Dial - Activate
*0	Button inquiry
1	Messages - Send
#1	Messages - Cancel Send
*1	Autodial - External
2	Ring Again
#2	Ring Again - Cancel
*2	Autodial - Internal
3	Conference Call
*3	Memory buttons - Program
4	Call Forward
#4	Call Forward - Cancel
*4	Speed Dial - Add, change
5	Last Number Redial
*501	Language - Primary[1]
*502	Language - Alternate[1]

Table 321 Features sorted by feature name and by activation code (Continued)

Sorted by feature name	
Feature name	**FEATURE** <code>
Call Forward - Cancel	#4
Call Forward to Voice Mail	984
Call Information	811
Call Log - Delete items (Auto bumping)	815
Call Log - Manual	813
Call Log - View information	812
Call Log options	*84
Call Log password	*85
Call Park	74
Call Queuing	801
Camp-on	82
Call Log password	*85
Class of Service	68
Conference Call	3
Contrast adjustment	*7
Dialing Mode	*82
Call Log options	*84
Directed Pickup	76
Display Voice Mail DN, skillset or IVR DN	985
Do not Disturb	85
Do not Disturb - Cancel	#85
Exclusive Hold	79
Express Messaging	980
Group Listening	802
Group Listening - Cancel	#802
Group Pickup	75
IP Services list	*900
IP Hot desking	*999
Language - Primary[1]	*501
Language - Alternate[1]	*502
Language - Alternate 2[1]	*503
Language - Alternate 3[1]	*504
Last Number Redial	5
Line buttons - Move	*81
Line Pool	64
Line Redirection	84

Sorted by activation code	
FEATURE <code>	**Description**
*503	Language - Alternate 2[1]
*504	Language - Alternate 3[1]
*510	Time zone readjust (IP telephones)
*503	Language - Alternate 2[1]
*520	Find available SWCA
*521 to *536	System Wide Call Appearance (SWCA)
*537	Find oldest SWCA
*538	Find newest SWCA
*550	Silent Monitor
*6	Ring Type
60	Page
61	Page - Internal (telephone speakers)
62	Page - External (external speakers)
63	Page - Combined (internal & external)
64	Line Pool
65	Messages - View
66	Voice Call
67	Saved Number Redial
68	Class of Service
69	Priority Call
*7	Contrast adjustment
70	Transfer
#70	Transfer - Cancel
71	Link
73	Auto Hold
#73	Auto Hold - Cancel
74	Call Park
75	Group Pickup
76	Directed Pickup
77	Call Duration Timer
78	Pause
79	Exclusive Hold
*80	Ring Volume
*81	Line buttons - Move
82	Camp-on

Table 321 Features sorted by feature name and by activation code (Continued)

Sorted by feature name	
Feature name	**FEATURE** <code>
Line Redirection - Cancel	#84
Link	71
Long tones	808
Malicious call identification (MCID)	897
Memory buttons - Program	*3
Messages - Send	1
Messages - Cancel Send	#1
Messages - View	65
Name and number blocking	819
Name and number blocking - Cancel	#819
Page	60
Page - Combined (internal & external)	63
Page - External (external speakers)	62
Page - Internal (telephone speakers)	61
Pause	78
Priority Call	69
Privacy (on/off)	83
Record call	989
Ring Again	2
Ring Again - Cancel	#2
Ring Type	*6
Ring Volume	*80
Ringing (Signal) Call	807
Room condition (Room set)	876
Room condition (HS admin set)	878
Room occupancy	879
Run/Stop	*9
Saved Number Redial	67
Silent Monitoring	*550
Speed Dial - Add, change	*4
Speed Dial - Activate	0
Static Time	806
Static Time - Cancel	#806
System Wide Call Appearance (SWCA)	*521 to *536

Sorted by activation code	
FEATURE <code>	**Description**
83	Privacy (on/off)
84	Line Redirection
#84	Line Redirection - Cancel
*84	Call Log options
85	Do not Disturb
#85	Do not Disturb - Cancel
*85	Call Log password
86	Background Music
#86	Background Music - Cancel
88	Voice Call Deny
#88	Cancel Voice Call Deny
800	Trunk Answer
801	Call Queuing
802	Group Listening
#802	Group Listening - Cancel
803	Time
804	Wait for dial tone
805	Test telephone display
806	Static Time
#806	Static Time - Cancel
807	Ringing (Signal) Call
808	Long tones
#809	Name and number blocking - Cancel
811	Call Information
812	Call Log - View information
813	Call Log - Manual
815	Call Log - Delete items (autobumping)
818	Call Charge Indication
819	Name and number blocking
870	Viewing active services
#871	Turning Ringing service off
871	Turning Ringing service on
#872	Turning Restriction service off
872	Turning Restriction service on
873	Turning Routing service on[2]

Table 321 Features sorted by feature name and by activation code (Continued)

Sorted by feature name	
Feature name	**FEATURE** <code>
Find available SWCA	*520
Find oldest SWCA	*537
Find newest SWCA	*538
Test telephone display	805
Time	803
Time zone adjust (IP telephones)	*510
Transfer	70
Transfer - Cancel	#70
Transfer to mailbox	986
Trunk Answer	800
Turning Restriction service off	#872
Turning Restriction service on	872
Turning Ringing service off	#871
Turning Ringing service on	871
Turning Routing service off	#873
Turning Routing service on[2]	873
View active services	870
Voice Call	66
Voice Call Deny	88
Voice Call Deny - Cancel	#88
Voice Mail direct	988
Voice Mail Interrupt	987
Voice Mail login	981
Voice Mail Operator settings	982
Wait for dial tone	804

Sorted by activation code	
FEATURE <code>	**Description**
#873	Turning Routing service off
875	Alarm time
#875	Alarm time - Cancel
876	Room condition (Room set)
877	Alarm time (HS admin)
878	Room condition (HS admin)
879	Room occupancy
897	Malicious call identification (MCID)
*9	Run/Stop
*900	IP Services list
904	Call Center agent login/log out
908	Call Center agent make busy/ready
909	Call Center queue status
980	Express Messaging
981	Voice Mail login
982	Voice Mail Operator settings
984	Call Forward to Voice Mail
985	Display Voice Mail DN, skillset, or IVR DN
986	Transfer to mailbox
987	Voice Mail Interrupt
988	Voice mail direct
989	Record call
*999	IP Hot desking

Notes

[1] For the Companion C3050 Etiquette, C3060 Portable, and C3050 CT2Plus portable telephones, enter ** followed by the numeric code to activate this feature.

[2]Contact your System Administrator for the service control password.

Button programming features

This section describes the features available for Button Programming. (**Services, Telephony Services, System DNs, Available DNs, DN<number>, User Preferences, Button Programming, Button** ##). Refer to the *Telephony Feature Handbook* for information about using these features.

Note that some of these features need other system settings in order to work.

- Some of the buttons are controlled by features located under **Services, Telephony Services, System DNs, Available DNs, DNxx, Capabilities**). Paging is an example of a feature that requires other settings.
- Some features also require that the service be available on the line from your telephone service provider. The types of lines provided are also determined by what region is chosen for your system. MCID (malicious call identification) is an example of this type of feature.

Table 322 Button Programming Feature settings

Set command (**FEATURE** <code>)	Feature	Description
	None	Button is configured for button programming, but nothing has been entered.
0	Speed dial	This button activates the speed dial feature. The telephone prompts the user for a speed dial code.
1	Send Message	Send a message to another set within the network
#1	Cancel Send Message	Cancel a message you sent to another set within the network
2	Ring again	Sets Ring again feature.
3	Conference/Transfer	Initiates call between three parties.
4	Call Forward	Allows the user to enter a number to call forward current telephone.
5	Last number redial	Causes set to redial the last number it received.
60	Page - General	Allows the user to page all sets.
61	Page - Zone	Allows the user to page a specific zone which is identified within the Button programming.
62	Page - Speaker	Allows the user to page through the speaker on a specific telephone.
63	Page - Speaker and zone	Allows the user to page through the speaker on telephones in a specific zone, which is identified within Button programming.
64	Line Pool	Allows the user to access a line pool. Either specific pools assigned to the telephone, or other general pools. The pool this button accesses is specified during Button Programming for this feature.
65	Reply message	Allows the user to access messages and send a reply to the message sender.
#65	Cancel Message Waiting	Allows the user to cancel the message waiting indicator.
66	Voice call	Allows the user to make an announcement or begin a call through the speaker of another telephone.
67	Saved Number Redial	Allows the user to redial a number that they saved while on the call.

Table 322 Button Programming Feature settings (Continued)

Set command (**FEATURE** <code>)	Feature	Description
68	Restriction override	Allows the user to override any restrictions for the call they are trying to dial.
69	Priority Call	Allows the user to access a telephone that is currently busy.
70	Transfer	Allows the user to transfer an existing call to another telephone.
71	Link	Activates the Link command, which allows the user to access special features on a remote PBX system.
72	Timed Release	(NOT ACTIVE)
74	Call Park	Allows the user to park a call on another telephone in the system.
*520	Find available SWCA key	System will search for a free SWCA key among the SWCA keys that are assigned to the current telephone.
*521 to *536	System Wide Call Appearance (1 to 16)	Non-intercom calls are associated with an available SWCA key when the call is answered or originated, or put on Hold. Features that interact with this feature: Hold, telephone keys, outgoing and incoming calls.
*537	Find oldest SWCA call	System will search among the SWCA keys assigned to the telephone, and unpark the call that has been parked the longest.
*538	Find newest SWCA call	System will search among the SWCA keys assigned to the telephone, and unpark the call that has been most recently parked.
*550	Silent Monitor	Monitor hunt group calls. (Telephone must be assigned with SM supervisor)
75	Group Pickup	Allows the user to answer a call made to another set within the Pickup group.
76	Directed Pickup	Allows the user to answer any telephone that rings within the system.
77	Call Timer	Allows the user to see how long a call lasted.
78	Pause	Allows the user to insert a pause during a dialing sequence.
79	Exclusive Hold	Allows the user to put a call on hold at the current telephone. All appearances of the call on other telephones indicate the line is busy.
800	Trunk Answer	Allows the user to answer a ringing call placed in a service mode.
801	Call Queuing	Allows the user to answer calls in order when several calls occur at once. Calls are presented in this order: incoming calls, timed-out forwarded calls, then camped calls
802	Group Listening	This feature opens the microphone on the set to allow a group of people to hear a call through the telephone speaker, but the user must talk to the caller through the handset.
803	Time	Displays the current time.
804	Wait for Dialtone	Places a pause in a dialing string that holds the following digits until a dialtone is perceived on the line.
807	Ringing (Signal) Call	Enter **FEATURE** 807 and an extension to directly ring another telephone inside the system. This is the same process as pressing an intercom button and dialing an extension.
808	Long tones	Allows the user to specify the type of tones dialed out.

Table 322 Button Programming Feature settings (Continued)

Set command (**FEATURE** <code>)	Feature	Description
811	Call Information	Allows the user to view information about a current call.
812	Call Log - View Information	Allows the user to view call log information.
813	Call Log - Manual	Allows the user to manually active call logging.
815	Call Logs autobumping	Allows the user to manually remove the oldest log item.
818	Call Charge Indication	Allows the user to view the charges for a call. (available on DASS2 and ETSI Euro trunks only)
819	ONN blocking	Allows the user to block the call information from the telephone for an outgoing call.
82	Camp-on	Allows the user to transfer and park an external call to another telephone in the system.
83	Privacy Control	Allows the user to make a shared line private, or release a shared line from private control.
84	Line Redirection	Allows the user to redirect a line within the system.
85	Do Not Disturb	Allows the user to block incoming calls from ringing on the telephone.
86	Background music	Allows the user to play music provided by a background music source through the speaker on the telephone.
870	Service Mode Status	Allows the user to view the current service mode being used.
871	Ringing Service	Allows the user to change the ringing service schedule.
872	Restriction Service	Allows the user to change the restriction service schedule.
873	Routing Service	Allows the user to change the routing service schedule.
88	Voice Call Deny	Allows the user to turn off the voice call feature at their set.
897	MCID	(Malicious Call Identification) Allows the user to query the system for information about a call within 25 seconds after the user hangs up, but before the caller hangs up.
*501	Language Choice	Access a menu to choose what language you want a telephone to use for display prompts.
7	Contrast	Digital telephones: Set the level of contrast for the telephone display
904	ACD agent login/log out	Allows the user to log in or out of ACD (Attendant Console Directory).
908	ACD agent make busy/ ready	Allows the user to indicate ready or busy status on ACD.
909	ACD queue status	Allows the user to view the status of queued calls on ACD.
980	Express Messaging	Allows the user to log directly into voice mail to leave a message.
981	Voice Mail Login	Opens your mailbox to play your messages and to access mailbox options.
982	Voice Mail Operator settings	Allows the user to set the parameters for the voice mail operator.
984	Call forward to voice mail	Forwards incoming calls to your mailbox. (Available for the Norstar Voice Mail interface only.)

Table 322 Button Programming Feature settings (Continued)

Set command (**FEATURE** <code>)	Feature	Description
985	Display voice mail DN	Displays the voice mail, skill set, or IVR extension number.
986	Transfer to mailbox	Transfers calls to a mailbox on the CallPilot system.
987	Voice mail interrupt	Intercepts a caller who is listening to your mailbox greeting or leaving a message.
988	Voice mail direct	
989	Record call	
*900	IP Services List	IP telephones only. Allows the user to access a feature menu. This is the same menu that is accessed by pressing the Services key.
*999	IP Hot Desking	IP telephones only. Allows the user to access the hot desking feature. This feature allows calls to be diverted from one IP telephone to another.

Appendix C
ISDN overview

This section provides some general information about using ISDN lines on your Business Communications Manager system. Detailed information about ISDN is widely available through the internet. Your service provider can also provide you with specific information to help you understand what suits your requirements.

Information in this section includes:

Welcome to ISDN

Integrated Services Digital Network (ISDN) technology provides a fast, accurate and reliable means of sending and receiving voice, data, images, text, and other information through the telecom network.

ISDN uses existing analog telephone wires and divides it into separate digital channels which increases bandwidth.

ISDN uses a single transport to carry multiple information types. What once required separate networks for voice, data, images, or video conferencing is now combined onto one common high-speed transport.

Nortel Networks endeavours to test all variations of ISDN PRI on Business Communications Manager; however, due to the number of variations, this is not always possible.

This section includes information about:

Analog versus ISDN

ISDN offers significantly higher bandwidth and speed than analog transmission because of its end-to-end digital connectivity on all transmission circuits. Being digital allows ISDN lines to provide better quality signaling than analog POTS lines, and ISDN out-of band data channel signaling offers faster call set up and tear down.

While an analog line carries only a single transmission at a time, an ISDN line can carry one or more voice, data, fax, and video transmissions simultaneously.

An analog modem operating at 14.4 K takes about 4.5 minutes to transfer a 1MB data file and a 28.8K modem takes about half that time. Using one channel of an ISDN line, the transfer time is reduced to only 1 minute and if two ISDN channels are used, transfer time is just 30 seconds.

When transmitting data, the connect time for an average ISDN call is about three seconds per call, compared to about 21 seconds for the average analog modem call.

Types of ISDN service

Two types of ISDN services (lines) are available: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Each line is made up of separate channels known as B and D channels which transmit information simultaneously.

- BRI is known as 2B+D because it consists of two B-channels and one D-channel.
- PRI is known as 23B+D(in North America) or as 30B+D (in Europe). In North America, 23B+D consists of 23 B-channels and one D-channel (T1 carrier). In Europe, 30B+D consists of 30 B-channels and one D-channel (E1 carrier).

B channels: B channels are the bearer channel and are used to carry voice or data information and have speeds of 64 kbps. Since each ISDN link (BRI or PRI) has more than one B-channel, a user can perform more than one transmission at the same time, using a single ISDN link.

D channels: The standard signaling protocol is transmitted over a dedicated data channel called the D-channel. The D-channel carries call setup and feature activation information to the destination and has speeds of 16 kbps (BRI) and 64 kbps PRI. Data information consists of control and signal information and for BRI only, packet-switched data such as credit card verification.

ISDN Layers

ISDN layers refer to the standards established to guide the manufacturers of ISDN equipment and are based on the OSI (Open Systems Interconnection) model. The layers include both physical connections, such as wiring, and logical connections, which are programmed in computer software.

When equipment is designed to the ISDN standard for one of the layers, it works with equipment for the layers above and below it. There are three layers at work in ISDN for Business Communications Manager. To support ISDN service, all three layers must be working properly.

- Layer 1: A physical connection that supports fundamental signaling passed between the ISDN network (your service provider) and the Business Communications Manager system. When the LED on a BRI S/T Media Bay Module configured as BRI is lit, your layer 1 is functioning.
- Layer 2: A logical connection between the central office or the far end and the Business Communications Manager system. Business Communications Manager has one or two of these connections for each BRI link, and one for each PRI link. Without Layer 2, call processing is not possible and there is no dial tone.
- Layer 3: Also a logical connection between the ISDN network (your service provider) and the Business Communications Manager system. For BRI lines, layer 3 is where call processing and service profile identifier (SPID) information is exchanged. This controls which central office services are available to the connection. For example, a network connection can be programmed to carry data calls.

  Note: Throughout this chapter, references are made to Service profile identifiers (SPIDs). SPIDs are a part of the BRI National ISDN standard. SPIDs are not used in the ETSI BRI standard or on PRI.

The system of layers is important when you are installing, maintaining, and troubleshooting an ISDN system. For information about troubleshooting ISDN, see the *System Management User Guide*.

ISDN bearer capability

Bearer capability describes the transmission standard used by the BRI or PRI line so that it can work within a larger ISDN hardware and software network.

The bearer capability for BRI and PRI is voice/speech, 3.1 kHz audio, and data (unrestricted 64 kbps, restricted 64 kbps, or 56 kbps).

Services and features for ISDN BRI and PRI

As part of an ISDN digital network, your system supports enhanced capabilities and features, including:

- faster call set up and tear down
- high quality voice transmission
- dial-up Internet and local area network (LAN) access
- video transmission
- network name display
- name and number blocking (PRI, BRI and analog)
- access to public protocols

This section discusses features and services in the following sections:

- "Network name display" on page 873
- "Name and number blocking (ONN)" on page 874
- "Call by Call Service Selection for PRI" on page 874
- "Emergency 911 dialing" on page 875
- "2-way DID" on page 875
- "Dialing plan and PRI" on page 875

PRI services and features

These are the services and features provided over PRI lines:

- Call-by-call service selection (NI protocol)
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking (SL-1 protocol)

BRI services and features

These are the services and features provided over BRI lines:

- data transmission at speeds up to 128 kbps per loop (depending on the bandwidth supported by your service provider)
- shared digital lines for voice and data ISDN terminal equipment

Business Communications Manager Basic Rate Interface (BRI) also support D-channel packet service between a network and terminal connection. This allows you to add applications such as point-of-sale terminals without additional network connections.

Any analog or digital network connections can be shared by all Business Communications Manager telephones, peripherals and applications, and ISDN terminal equipment (TE).

Business Communications Manager supports the following ISDN services and features offered by ISDN service providers:

- D-channel packet service (BRI only) to support devices such as transaction terminals. Transaction terminals are used to swipe credit or debit cards and transmit the information to a financial institution in data packets.
- Calling number identification (appears on both Business Communications Manager sets and ISDN terminal equipment with the capability to show the information)
- Multi-Line hunt or DN hunting which switches a call to another ISDN line if the line usually used by the Network DN is busy. (*BRI only*)
- Subaddressing of terminal equipment (TE) on the same BRI loop. However, terminal equipment which supports sub-addressing is not commonly available in North America. (*BRI only*)

Transmission of B-channel packet data using nailed up trunks is not supported by Business Communications Manager.

Contact your ISDN service provider for more information about these services and features. For more information about ordering ISDN service in North America, see "Ordering ISDN PRI" on page 880 and "Ordering ISDN BRI" on page 880.

The terminal equipment (TE) connected to the Business Communications Manager system can use some feature codes supported by the ISDN service provider.

Network name display

This feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network. For information about programming this feature, see "Network name display" on page 453.

Your Business Communications Manager system displays the name of an incoming call when it is available from the service provider. If the Calling Party Name has the status of *private* it may be displayed as `Private name` if that is how the service provider has indicated that it should be displayed. If the Calling Party Name is unavailable it may be displayed as `Unknown name`.

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

The available features include:

- Receiving Connected Name
- Receiving Calling Name
- Receiving Redirected Name
- Sending Connected Name
- Sending Calling Party Name

For more information, see "Network name display" on page 453. Consult your customer service representative to determine which of these features is compatible with your service provider.

Name and number blocking (ONN)

(North America only)

When activated **FEATURE 819** allows you to block the outgoing name and/or number on a per-call basis. Name and number blocking can be used with a Business Communications Manager set. For information about programming this feature, see "Setting outgoing name and number blocking" on page 479.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

ETSI note: Refer to "Supported ISDN line services" on page 852 for information about protocols supported by E1 lines.

Call by Call Service Selection for PRI

(North America only)

PRI lines can be dynamically allocated to different service types with the Call by Call feature. PRI lines do not have to be pre-allocated to a given service type. Outgoing calls are routed through a dedicated PRI Pool and the calls can be routed based on various schedules.

The service types that may be available, depending on your service provider are described below.

- Public: Public service calls connect your Business Communications Manager set with a Central Office (CO). DID and DOD calls are supported.
- Private: Private service calls connect your Business Communications Manager set with a Virtual Private Network. DID and DOD calls are supported. A private dialing plan may be used.
- Tie: Tie services are private incoming and outgoing services that connect Private Branch Exchanges (PBX) such as Business Communications Manager.
- FX (Foreign Exchange): FX service calls logically connect your Business Communications Manager telephone to a remote CO. It provides the equivalent of local service at the distant exchange.
- Outwats: Outwats is for outgoing calls. This allows you to originate calls to telephones in a specific geographical area called a zone or band. Typically a flat monthly fee is charged for this service.
- Inwats: Inwats is a type of long distance service which allows you to receive calls originating within specified areas without a charge to the caller. A toll-free number is assigned to allow for reversed billing.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Emergency 911 dialing

(North America only)

The ISDN PRI feature is capable of transmitting the telephone number and internal extension number of a calling station dialing 911 to the Public Switched Telephone Network (PSTN). State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations. For most installations the following configuration rules should be followed, unless local regulations require a modification.

- All PSTN connections must be over PRI.
- In order for all sets to be reached from a Public Safety Answering Position (PSAP), the system must be configured for DID access to all sets. In order to reduce confusion, the dial digits for each set should be configured to correspond to the set extension number.
- The OLI digits for each set should be identical to the DID dialed digits for the set.
- The routing table should route 911 to a PRI line pool.
- If attendant notification is required, the routing table must be set up for all 911 calls to use a dedicated line which has an appearance on the attendant console.
- The actual digit string 911 is not hard-coded into the system. More than one emergency number can be supported.

If transmission of internal extension numbers is not required or desired, then it is recommended that the person in charge of the system maintain a site map or location directory that allows emergency personnel to rapidly locate a Business Communications Manager set given its DID number. This list should be kept up to date and readily available.

IP telephony note: Ensure that you **do not** apply a 911 route to an IP telephone that is off the premises where the PSAP is connected to the system.

2-way DID

With PRI the same lines can be used for receiving direct inward dialing (DID) and for making direct outward dialing (DOD) calls.

The dialing plan configured by your customer service representative determines how calls are routed. Consult your customer service representative to determine whether or not this feature is compatible with your service provider.

Dialing plan and PRI

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing incoming and outgoing calls. All PRI calls must go through a dialing plan.

Notes about the dialing plan:

- allows incoming calls to be routed to sets based on service type and digits received
- provides the ability to map user-dialed digits to a service type on a Call by Call basis

- allows long distance carrier selection through user-dialed Carrier Access Codes

Consult your customer service representative to determine how your dialing plan is configured.

ISDN hardware

To support connections to an ISDN network and ISDN terminal equipment, your Business Communications Manager must be equipped with a BRI S/T Media Bay Module (BRIM) or a Digital Trunk Media Bay Module (DTM) card configured for PRI.

This section describes the hardware:

- "PRI hardware"
- "BRI hardware" on page 876

PRI hardware

The Digital Trunk Media Bay Module (DTM) is configured for PRI. In most PRI network configurations, you need one DTM configured as PRI to act as the primary clock reference. The only time when you may not have a DTM designated as the PRI primary clock reference is in a network where your Business Communications Manager system is connected back-to-back with another switch using a PRI link. If the other switch is loop-timed to your Business Communications Manager system, your DTM (PRI) can be designated as a timing master.

If your Business Communications Manager has more than one DTM configured as PRI, you must assign the first DTM as the primary reference, the second DTM as the secondary reference, and the third DTM as the timing master.

If the system has a BRI module, it should be set as the timing master when a DTM in the same network is defined as the primary reference.

BRI hardware

The loops on the BRI module can be programmed to support either network or terminal connections. This allows you to customize your arrangement of lines, voice terminals, data terminals and other ISDN equipment. This section describes some basic hardware configurations for network and terminal connections for each loop type.

A BRI module provides four loops. Each loop can be individually programmed as:

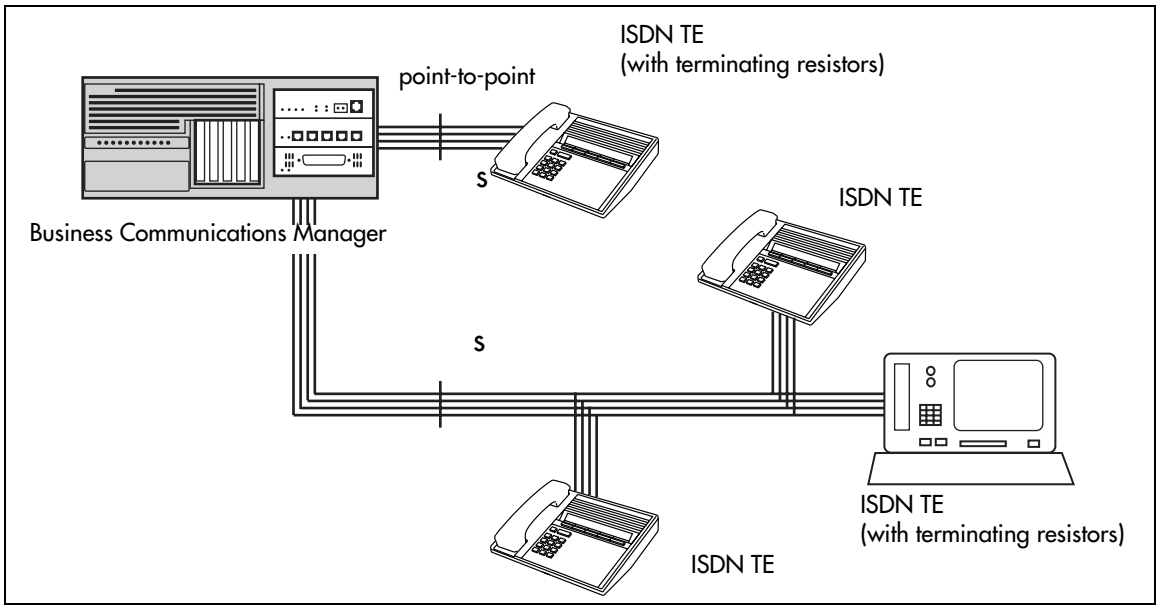
- an S reference point connection (S loop) to ISDN terminal equipment (TE), or
- a T or S reference point connection (T loop or S loop) to an ISDN network using an external NT1

S Reference Point

The S reference point connection provides either a point-to-point or point-to-multipoint digital connection between Business Communications Manager and ISDN terminal equipment (TE) that uses an S interface. Refer to the figure below.

S loops support up to seven ISDN DNs, which identify TE to the Business Communications Manager system.

Figure 213 S reference point

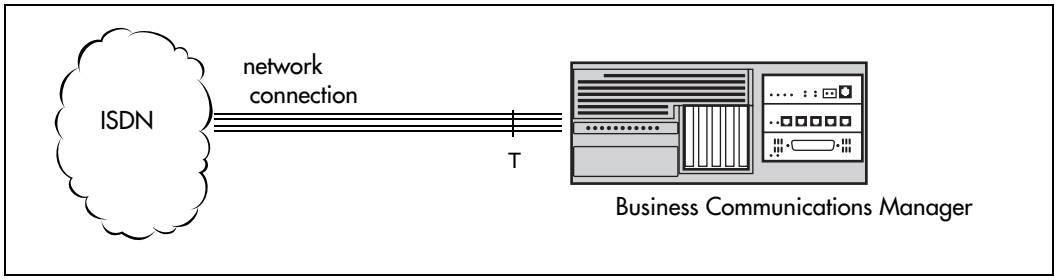


T Reference Points

The T reference point connections provide a point-to-point digital connection between the ISDN network and Business Communications Manager. Refer to the figure below.

A T loop provides lines that can be shared by all Business Communications Manager telephones, peripherals and applications, and ISDN TE.

Figure 214 T reference point



A T loop can be used in combination with an S loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. D-packet service is a 16 kbps data transmission service that uses the D-channel of an ISDN line. The T and S loops must be on the same physical module.

Clock Source for ISDN

Systems with ISDN interfaces need to synchronize clocking with the ISDN network and any ISDN terminal equipment connected to the network. Systems synchronize clocking to the first functionally available network connection. If there are excessive errors on the reference network connection, the next available network connection is used for clock synchronization. The clock synchronization process generates alarm codes and event messages. Clock synchronization is supported by the DTM, BRI module, and FEM.

The Business Communications Manager derives timing from the network using T reference points (loops). Terminal equipment on S reference points (loops) derive timing from the Business Communications Manager system.

When you configure the network connections to the Business Communications Manager, you should take into account the system preferences for selecting loops for synchronization:

- lower numbered loops have preference over higher numbered loops
- the loop preference order is: 201, 202, 203, 204 etc.
- the system skips S and analog loops on Mod2 Card 1, when selecting a network connection for synchronization

Systems with only S loops act as timing masters for the attached terminal equipment (TE), and are not synchronized to the network. ISDN TE without access to a network connection (BRI lines) has limited or no functionality.

If your system has both a BRI S/T configured as BRI, and a DTM configured as PRI, it is recommended that you use PRI as the primary clock source. See “PRI hardware” on page 876.

ISDN BRI NT1 equipment

The NT1 (network termination type 1) connects an S interface (four-wire) to a U interface (two-wire). In most cases, it connects loops from a BRI module to the network connection, which uses the U interface.

The NT1 converts and reformats data so it can be transmitted to and from the S or T connection. In addition, it manages the maintenance messages travelling between the network and the NT1, and between the NT1 and the Business Communications Manager system.

The NT1 from Nortel Networks is packaged two ways:

- a stand alone package which contains one NT1 card (NTBX80XX) and a power supply (NTBX81XX)
- a modular package which contains up to 12 NT1 cards (NTBX83XX) and a power supply (NTBX86AA)

ISDN standards compatibility

In North America, Business Communications Manager ISDN equipment supports National ISDN standards for basic call and calling line identification services. Business Communications Manager BRI is compliant with National ISDN-1 and PRI is compliant with National ISDN-2.

Business Communications Manager does not support EKTS (Electronic Key Telephone System) or CACH (Call Appearance Call Handling).

In Europe, Business Communications Manager supports ETSI Euro and ETSI QSIG standards, and PRI SL-1 protocol.

Planning your ISDN network

Consult the *Installation and Maintenance Gui*de to determine a configuration of ISDN trunks and terminal equipment (TE) for the Business Communications Manager system, then order the appropriate ISDN capability package from your ISDN service provider.

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs), network directory numbers (Network DNs), terminal endpoint identifiers (TEIs), and other information as required to program your Business Communications Manager, TE and other ISDN equipment.

Business Communications Manager does not support any package with EKTS or CACH. EKTS is a package of features provided by the service provider and may include features such as Call Forwarding, Link, Three-Way Calling, and Calling Party Identification.

Ordering ISDN PRI

This section provides information about how to order ISDN PRI service for your Business Communications Manager.

Ordering ISDN PRI Service in Canada

In Canada, order Megalink™ service, the trade name for standard PRI service and set the Business Communications Manager equipment to the supported protocol that is identified by your service provider, either DMS-100 or NI-2.

Ordering ISDN PRI Service in United States

In the United States order PRI service from your service provider. Set the Business Communications Manager equipment to the PRI protocol indicated by your service provider.

Ordering ISDN PRI Service Outside of Canada and the United States

Outside of Canada and the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Business Communications Manager equipment to the Euro ISDN protocol.

Ordering ISDN BRI

This section provides information about how to order ISDN BRI service for your Business Communications Manager.

Ordering ISDN BRI Service in Canada

In Canada, order Microlink™ service, the trade name for standard BRI service. You can order either regular Microlink™ service, which includes the CLID feature, or Centrex Microlink™, which includes access to additional ISDN network features, including Call Forwarding).

When ordering Microlink™ service, it must be ordered with EKTS turned off. If you will be using a point-of-sale terminal adapter (POSTA), ask for D-packet service to be enabled.

Ordering ISDN BRI Service in the United States

In the U.S., regardless of the CO (Central Office) type, order National ISDN BRI-NI-1 with EKTS (Electronic Key Telephone System) turned off. Use the following packages as a guideline for ordering your National ISDN BRI-NI-1. However, we recommend using packages M or P with the Business Communications Manager system. Contact your service provider for more information about the capability packages it offers. Bellcore/National ISDN Users Forum (NIUF ISDN packages supported by Business Communications Manager (for ordering in U.S.).

	Capability	Feature set	Optional features	Point-of-sale	Voice	Data
M	Alternate voice/circuit-switched data on both B-channels	--	CLID	--	X	X
P	Alternate voice/circuit-switched data on both B-channels D-channel packet	flexible calling for voice (not supported by Business Communications Manager) Basic D-Channel Packet	additional call offering (not supported by Business Communications Manager) calling line identification	X	X	X

If you want to transmit both voice and data, and support D-channel packet service, order package P. However, Business Communications Manager does not support the flexible calling for voice and additional call offering features that are included in package P.

Multi-Line Hunt may be ordered with your package. When a telephone number (the Network DN) in the group of numbers assigned by your service providers is busy, the Multi-Line Hunt feature connects the call to another telephone number in the group. Business Communications Manager supports the feature only on point-to-point, network connections (T loop). Check with your service provider for more information about Multi-Line Hunt.

Any of the ISDN packages will allow you to use sub-addressing, but your ISDN TE must be equipped to use sub-addressing for the feature to work.

Ordering ISDN BRI Service Outside Canada or the United States

Outside of Canada or the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Business Communications Manager equipment to the Euro ISDN protocol.

Supported ISDN Protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI and BRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

For more information on the supported protocols and services, refer to “Provisioning for Call by Call limits with PRI” on page 340.

ISDN Programming

Most of the programming for PRI and BRI lines, and ISDN terminals is performed under the **Resources, Media Bay Modules** heading in the Unified Manager. This section gives you an overview of programming for PRI and BRI lines, ISDN terminals and devices, and D-packet services.

PRI or BRI programming activity	Programming heading
View or change the Digital Trunk Module (DTM) Configure DTM for PRI	Resources, Media Bay Modules, Bus 0#
Provision or pre-provision lines	Resources, Media Bay Modules, Bus 0#, Modules on Bus, Module 1, Provision lines
Enable or disable BRIM-S/T and DTM	Resources, Media Bay Modules, Bus 0#, Modules on Bus Module 1
View status of line, loop or port	Resources, Media Bay Modules, Bus #, Ports on Bus

Program PRI Resources

Some steps may not be necessary depending on the service you are using. For more detailed programming information, see "Configuring resources — media bay modules" on page 123 and "Configuring lines" on page 227. For complete module installation instructions and safety precautions, see the *Business Communications Manager Installation and Maintenance Guides*.

1. Collect the information supplied by your service provider to support your ISDN package.
2. Install the DTM. (For information, refer to the *Installation and Maintenance Guides*.)
3. Configure the DTM for PRI. For information on how to configure a module, see "Explaining the Media Bay Modules headings" on page 124.
4. Configure the lines on the modules. For more information, see "Understanding how the system identifies lines" on page 229.

Programming ISDN BRI Resources

Some steps may not be necessary depending on the service you are providing. For more detailed programming information, see "Configuring resources — media bay modules" on page 123 and "Configuring lines" on page 227. For complete module installation instructions and safety precautions, see the *Business Communications Manager Installation and Maintenance Guide*.

1. Collect the information supplied by your service provider to support your ISDN package. This includes network service profile identifiers (SPIDs) and Network DNs. If you are supporting a point-of-sale terminal adapter, you also need one or more static terminal endpoint identifiers (TEIs).
2. Install the BRIM S/T module in the Business Communications Manager system. (For information, refer to the *Installation and Maintenance Guides*).
3. Select the module type (BRI-ST). For information on selecting a module type, see "Explaining the Media Bay Modules headings" on page 124.
4. Select the type (T or S) for each loop. For information on how to select a loop type, see "Identifying BRI T-loops (T1 profiles)" on page 267, "Identifying BRI T-loops (ETSI, QSIG)" on page 271, and "Setting BRI for ISDN device connections" on page 278.
5. Configure the loop type settings:
   a. If the module uses a T loop, enter the following configuration information (for North America only) as supplied by your service provider:
      - the SPID assigned to the loop
      - the number of B-channels associated with each SPID
      - the Network DNs used with the network SPID
      - the call type of the Network DN.

   Repeat the programming for the second network SPID, if any.

   If the T loop is used for D-packet service: turn on the service, assign the appropriate S-loop mapping and assign the static TEIs (provided by the telco to support a point-of-sale terminal adapter or other D-packet service device) to the loop.

   b. If the loop type is S, select the sampling used on the loop. Assign ISDN DNs to the loop and designate one of the assigned ISDN DNs to be the DN for the loop (Loop DN).

      Note: You can have a maximum of 58 ISDN DNs on your system. However, there are only 28 default DNs provided. The default ISDN DN range is 597 to 694. To add to the defaults, you need to use DNs from the Companion DN range: 565 to 597 (change DN type to **ISDN and DECT**)

   Companion/DECT: If you have either a Companion wireless system, which uses the **Companion** range, or a DECT portable system, which uses the ISDN and DECT range, ensure you do not overwrite any DNs assigned to the handsets for these systems.
6. Provision the loops and lines. For more information, see "Provisioning lines (PRI, T1, DASS2)" on page 140.

7 If you are configuring auto-answer BRI trunks to map to target lines, program the received number for the target line (see "Assigning target lines" on page 287) to be the same as the Network DN supplied by your service provider (Loops, Loop XXX, SPIDs, SPID 1, Network DN).

Program the ISDN terminals and devices with the appropriate ISDN DNs and terminal SPIDs by following the instructions that come with the devices. For more information see "Program ISDN Equipment" on page 886. If you are setting up a D-packet service, program the point-of-sale terminal adapter or other D-packet service device with the appropriate TEI from your service provider, terminal SPID, and DN by following the instructions that come with the device.

Program PRI Lines

When the hardware configuration is complete, your PRI lines are ready to be programmed. For information on programming your PRI lines, see "Provisioning for Call by Call limits with PRI" on page 340.

Program ISDN BRI Lines

When the hardware configuration is complete, your BRI lines are ready to be programmed in the same way as analog lines. You can, for example, place them in pools and assign them to Business Communications Manager telephones and ISDN terminal equipment. However, there are some differences in the way BRI lines work that will influence how you configure them to handle incoming and outgoing calls.

For BRI lines, in most cases, your service provider supplies two SPIDs – one for each B channel. Each SPID and one or more Network DNs are associated with a single line. Calls to a Network DN come in on a specific line, and pressing a line button selects the same line every time.

If your service provider supplies you with a single SPID for both B channels, incoming and outgoing calls are handled according to the loop. The two lines provided by the BRI loop are "pooled" for both incoming and outgoing calls.

For example, if Loop 201 is programmed with a single SPID, which supports lines 061 and 062, incoming calls made to a Network DN associated with the SPID appear on either line 061 or line 062. If you press the line button for line 061, either line 061 or line 062 is selected. For loops which use a single SPID, assign both lines on a loop to a set to guarantee that all calls appear at the set.

Program Direct Inward System Access (DISA) on PRI Lines

(North America)

When a DTM is configured for PRI, all lines on that module are set to Auto Answer without DISA. DISA, however, can be accessed by one of two methods.

Method 1:

Define the DISA DN to match the trailing digits of the Called Party Number (CDN).

With Public, Private, and Tie service types, the CDN is simply truncated to the Target Line Receive Digit Length and is parsed to match the Target Line Receive Digits. DISA can be accessed by having the DISA DN match the trailing digits of the CDN. For example, with a Receive Digit Length = 4, and DISA DN = 1234, a call made to Public DN 763-1234 will be handled as follows:

- the ISDN setup message will contain a CDN of 763-1234
- the CDN will be truncated to the 4 digits, 1234
- 1234 matches the DISA DN
- the call will be answered with DISA

Method 2: (North America only)

Use incoming Call by Call (CbC) Service routing to map the call type to the DISA DN. Refer to "Configuring call routing" on page 320 for more information.

With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. This is programmed under "Configuring Call by Call services" on page 339. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4, DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234).

A call presented to the Business Communications Manager system with service type FX and SID 2 will be handled as follows:

- The ISDN setup message will specify FX with SID = 2
- The FX SID = 2 will be mapped to DISA DN digits 1234

The call will be answered with DISA.

Program ISDN Equipment

PRI modules support various applications that are enabled by PRI.

Terminal equipment for BRI Cards

ISDN devices and terminals connected to the Business Communications Manager system must be configured under Services, Telephony Services, Loops. You choose directory numbers for ISDN equipment from a predetermined range of DNs (597 to 694). Any of the ISDN DNs can be assigned to an S loop, but each can only be assigned to one loop and a single device. If you require more than the default 32 devices, you can use the Companion range of DNs (565 to 596). If you need these extra DNs, change the DN type from **Companion** to **ISDN and DECT**.

Devices on an S loop (BRI cards only)

Terminal equipment using an S loop must be assigned an ISDN directory number (ISDN DN). This allows the TE to be assigned lines and to communicate with other devices connected to the Business Communications Manager system. Each DN can be assigned to only one TE and one loop.

You assign ISDN DNs to S loops from the **Telephony Services** subheading, under **Loops**, **DNs on Loop**, **Assign DNs**. Each S loop can be programmed with eight ISDN DNs, but you cannot exceed a total of 58 ISDN DNs for the Business Communications Manager system.

S or LT Loop DN

Once you have assigned ISDN DNs to a loop, designate one of the DNs as a Loop DN. The Loop DN acts as a main ISDN DN and completes the configuration of the loop.

The ISDN terminal equipment (TE) on the loop is also programmed with its ISDN DN. See the instructions that come with the ISDN device for information about how to program it to recognize its assigned DN. Most devices will require both a terminal service profile identifier (terminal SPID) and a DN, and some will require two terminal SPIDs and two ISDN DNs. The SPID used with the device should not be confused with a SPID used for network connections using a T loop.

To create a terminal SPID for a device, add at least two zeros to the end of the ISDN DN. Add more zeros to the beginning or end of the ISDN DN until you have the length of SPID required by the TE. For example, if an ISDN telephone requires a six-digit SPID and has a DN of 667, its SPID is 066700. If the same TE requires a minimum of ten digits, the SPID is 0000066700.

Most ISDN terminals require a five-digit SPID. An ISDN PC card usually requires a ten-digit SPID. Follow the directions that come with the ISDN device to program it with a SPID and ISDN DN.

D-packet Service (BRI only)

The D-packet service supplied by the Business Communications Manager system supports a point-of-sale terminal adapter (POSTA). Connecting a POSTA allows transaction terminals (devices where you swipe credit or debit cards) to transmit information using the D channel of the BRI line, while the B channels of the BRI line remain available for voice and data calls. A special adapter links transaction equipment, such as cash registers, credit card verification rigs, and point-of-sale terminals, to the X.25 network, which is a data communications network designed to transmit information in the form of small data packets.

To support the D-packet service, your ISDN network and financial institution must be equipped with a D-packet handler. To convert the protocol used by the transaction equipment to the X.25 protocol, your ISDN network must also be equipped with an integrated X.25 PAD which works with the following versions of X.25: Datapac 32011, CCITT, T3POS, ITT and API. The ISDN service package you order must include D-packet service (for example, Package P in the United States; Microlink™ with D-channel in Canada).

Your service provider supplies a Terminal Endpoint Identifier (TEI) and DN to support D-packet service. The TEI is a number between 00 and 63 (in Canada, the default range is 21-63). Your service provider may also supply you with a DN to program your D-packet device. The DN for D-packet service becomes part of the dialing string used by the D-packet to call the packet handler.

Glossary

The following sections provide brief explanations of the terms used in this documentation.

ABCDEFGHIKLMNOPQRSTUVW

A

absorb length

This setting determines how many of the digits in a destination code the system does not dial. You assign the Absorb Length under **Destination codes**. (Services, Telephony Services, Call Routing). Refer to "Grouping destination codes using a wild card" on page 329.

access codes

A digit or group of digits that provide direction to the system as to how to route a call or access a feature, such as call park. The Access Codes heading also provides access to the line pool codes and carrier codes. (Services, Telephony Services, General Settings, Access Codes). Destination codes are a form of access codes for routing services (Services, Telephony Services, Call Routing). Refer to "Determining line access dialing" on page 308.

Address Resolution Protocol (ARP)

ARP is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. The physical machine address is also known as a Media Access Control or MAC address. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

As an example, this protocol is used when the Business Communications Manager maps an IP address to an IP telephone.

alarm code

A number that appears on an alarm telephone display when the system detects a fault.

ANSI

American National Standards Institute. This is the ISDN protocol define by the institute for telecommunications standards within North America. See also ETSI.

answer DNs

This telephone button allows you to monitor activity that occurs on another telephone in the system by indicating incoming calls to the other telephone. For instance, an attendant with a telephone with answer buttons can see which telephones on the system are ringing, and can answer the incoming call, if necessary.

One telephone can have up to eight Answer DNs. When you assign an Answer DN to a telephone, the system connects that DN to a button with an indicator on that telephone.

There are three answer key levels, which determine which calls appear on the answer button. This is a system setting. Some features, such as overflow routing, require specific levels before they can occur.

In BCM 3.5 and newer software, an Answer DN for a internal telephone can also act as a autodial button to that telephone. The Answer DN telephone must be idle for this type of call.

Application Program Interface (API)

An API is an interface used by an application to make requests of the operating system or another application. Unlike the graphical user interface or command interface, which are direct user interfaces, the API is an interface to an operating system or a program.

asynchronous

A method of transmission where the time intervals between characters are not required to be equal. Signals are sourced from independent clocks with different frequencies and phase relationships. Start and stop bits may be added to coordinate character transfer.

ATA2

The Analog Terminal Adapter (ATA2) connects analog telecommunication devices, such as fax machines, answering machines, and single line telephones, to a digital media bay module on the Business Communications Manager system. Refer to "Determining analog settings" on page 412.

autobumping

A feature that determines how the system handles new Call Log items when your Call Log is full. When Autobumping is on, the system deletes the oldest entry when there is a new log entry. If Autobumping is off, your system does not log calls when your log is full. This feature is set by the user at the telephone.

auto dial

A memory button that provides one-touch dialing of external or internal numbers or accesses features. Internal autodial buttons with indicators, display a solid indicator when that telephone is busy. In BCM 3.5 and newer software, Answer DNs can act as auto dial buttons for internal telephones.

Auto DN

This is a system directory number that is assigned to auto-answer trunks that are used to allow remote users to call into the system. On these trunks, the callers do not enter a password, but directly access the system. From a security perspective, ensure that these trunks have adequate restrictions (Remote Access Packages) to prevent unauthorized system usage. See also DISA DN.

auto hold

A feature that automatically places an active call on hold when you select another line to answer or make a call. This feature can also be activated by the user with **FEATURE** 73, if the feature has not been allowed on the telephone record (Capabilities). See also full autohold (on idle line).

auto log options

A feature that allows you to select the type of calls stored in your Call Log. You can log calls not answered, calls not answered at this telephone but answered in the system, all calls answered and not answered at this telephone, or no calls. This option is set under **User Preferences**. (Services, Telephony Services, System DNs)

Automatic Daylight Savings Time

A feature that switches the system to standard or daylight savings time at programmed times. This feature is set when you run the Quick Install Wizard and specify a time zone setting. An IP telephone that is in a different time zone than the system to which it is registered, must be configured manually to the local time, and then manually changed when Daylight Savings Time occurs.

automatic dialing

A feature that allows a device, such as a fax machine, to send a dialing sequence without receiving external ques.This feature is activated under **User Preferences**. (Services, Telephony Services, System DNs)

automatic handsfree (HF answerback)

This feature automatically puts the telephone in handsfree mode when you make or answer a call. This feature is assigned under Capabilities. (Services, Telephony Services, System DNs). Note: Not all models of telephones can use this feature.

automatic privacy

See Privacy.

auxiliary ringer

An external telephone ringer or bell which rings when a line or a telephone rings. You can program an auxiliary ringer to ring when the system is in a selected schedule. Enable the auxiliary ringer under **Capabilities**. (Services, Telephony Services, System DNs). Note: Not all models of telephones can access an external ringer.

B

B-channel

This is an ISDN line bearer channel which is used for voice or data transmission.

background music

A feature that plays music through the speaker of a telephone. This feature can use either an external music source attached to the MSC on the Business Communications Manager or the IP music feature, if appropriate music files are available. The feature is enabled under **Feature settings**. (Services, Telephony Services, General Settings)

backup

This is a process, enabled through the BRU button on the front page of the Unified Manager. This application allows you to copy all or specific data files from your Business Communications Manager system to a file that can be transferred to a secure place in case of system problems that would require the Business Communications Manager to be re-initialized. This same application allows to your recover the information from a backup to your Business Communications Manager.

base station

This device is part of the wireless/portable handset systems that can be used with the Business Communications Manager. It contains radio equipment that receives and sends signals to a cordless handset used within a specific radius of the base station. The base station connects to a media bay module installed in your Business Communications Manager System.

Basic Input Output System (BIOS)

A program contained in Read Only Memory (ROM) that acts as the interface between software programs and the computer hardware.

baud rate

A unit of measurement of data transmission speed through a media channel, such as a modem. Baud rate is approximately equivalent to Bits Per Second (BPS).

BCM400/BCM200

The BCM400 base unit was developed to replace the BCM1000 base unit. The BCM400 can support four media bay modules as well as the remote cabinet. It can be ordered as a standard system, or with redundant power supply, fans, and a mirrored (RAID) disk system. The BCM200 supports two media bay modules, and is a stand-alone unit. These hardware platforms were introduced in conjunction with Business Communications Manager release 3.0. Only the BCM1000 supports earlier versions of the Business Communications Software.

bearer channel

See B-channel.

bit

An abbreviation for Binary Digit. A bit is the smallest unit of information identified by the computer. A bit has one of two values, 0 or 1, to indicate off or on.

bit error rate test

A test that checks the transmission of data across the voice and data channels between the system and any telephone.

BLF

The Busy Lamp Field (BLF) is the display field beside the buttons on the telephones that display an arrow indicator when the button is in use.

BPS (Bits Per Second)

The speed of data transmission between two computers.

break-in

If you attempt to forward a call to another telephone, and that telephone is busy, you can use this feature to attempt to interrupt the call. Intrusion levels are assigned to each telephone, which means this feature will not work if the telephone receiving the transferred call was assigned a higher intrusion level. Also, the user at the other end has the option of refusing the call by entering the Do Not Disturb feature code.

BRI

The Basic Rate Interface (BRI) ISDN interface uses two B-channels and a D-channel (2B+D). ETSI BRI is the European Telecommunications Standards Institute specification for BRI ISDN service. BRI is supplied to the Business Communications Manager through a BRI media bay module. For details about BRI service, refer to “ISDN overview” on page 869.

BST

Business Series Terminals (BST) are a group of telephones created to replace the M-series telephones. The T7000 is equivalent to the M7000; the T7100 is equivalent to the M7100(N); the T7208 is equivalent to the M7208(N); the T7316 is roughly equivalent to the M7310(N), but without the second level of memory buttons, and it has a separate Mute key. There is no equivalent to the M7324(N), however, the T7316E has the capacity to connect to Key Indicator Modules (KIMs), which can replace the M7324(N) with attached Central Answering Position (CAP) modules. Refer to “Setting up CAP stations” on page 434). The T7316E can also function alone and differs from the T7316 by providing both a separate Mute and separate Handsfree button below the dial pad. The default numbering is also different on systems running BCM 3.5 and newer software. On systems running software previous to BCM 3.5, the T7316E acts identically to the T7316 and displays call icons instead of arrows beside buttons with indicators. Refer to “T7316E Business Series Terminal button defaults” on page 422.

Upgrade note: The T7316 and T7316E are viewed as completely different sets by the system. Therefore, when systems are upgraded from software previous to BCM 3.5, T7316E telephones will drop the T7316 programming and acquire the T7316E default programming.

BST doorphone

This piece of hardware acts as an alerter and intercom at an outside entrance to your office. The device uses the paging feature to provide an alerter chime or voice connections to internal telephones. The doorphone is based on the M7324 firmware.

bus

A collection of communication lines that carry electronic signals between components in the system. Besides internal communications, the Business Communications Manager MSC uses buses to support media bay modules and IP telephony components.

byte

The amount of space required to store a single character. One byte is equal to eight bits.

C

callback

Modem security: If this feature is enabled, a user dialing into the Unified Manager can be confirmed by having the Business Communications Manager terminate the dial-in and then dial back to the number provided for the user. This ensures that the user is dialing from a known source.

Call return: If you park, camp, or transfer a call to another telephone and no one answers the call, the call rings again at your telephone. Set the timing for this in Timers, Transfer callback timeout. (Services, Telephony Services, General Settings). See also call queuing.

Call-by-Call services

This is a PRI (North American) line feature that provides a system of remapping specific incoming lines for specific destinations. These services include INWATs (800), foreign exchange (FX), international 800, switched digital (SDS), and nine hundred (900). The type of service is based on the type of central office switch from which the line originates.

call duration timer

A feature that allows you to check how long you were on your last call or how long you have been on your present call. (**FEATURE 77**)

- no active call: set displays the duration of the last active call
- active call: set displays elapsed time of call (not dynamic)

call forward

A feature that forwards all the calls arriving at your telephone to another telephone in your system, or, if you are using ISDN lines to forward the call, to external systems. To have calls forwarded outside the system on other types of lines, use the line redirection feature. Call forward is configured under **Capabilities**. (Services, Telephony Services, System DNs)

- Call Forward No Answer: forwards all calls if the original target telephone is not answered. The system transfers the calls after a specific number of rings.
- Call Forward On Busy: forwards all calls if the target telephone rings busy.
- Call Forward All Calls: This setting is only used when the system has been converted to a Survivable Remote Gateway (SRG) and is acting as a Branch Office to a central IP server.
- Call Forward Override: The system allows you to call a telephone that has calls forwarded to your telephone.

Analog telephone note: To call forward to telephones outside your system, you must enter LINK 2 after you dial the external number.

call information

This feature allows you to display information about incoming calls. For external calls, you can display the name of the caller, telephone number, and line name. For an internal call, you can display the name of the caller and the internal number of their telephone. You can receive information about ringing, answered, or held calls. (**FEATURE 813**)

call log

If call log is active on a telephone, the use can view a record of incoming calls. (**FEATURE 812**)
The log can contain the following information for every call:

- sequence number in the call log
- name and number of caller
- long distance indication
- call answered indication
- time and date of the call
- number of repeated calls from the same source
- name of the line that the call came in on.

See autobumping and auto log options for more information.

call park

This feature allows you to place a call on hold so that another user can retrieve it from another telephone in the system. The user retrieves the call by selecting an internal line and entering a retrieval code.

The retrieval code appears on the display of your telephone when you park the call. You can park up to 25 calls on the system at one time. (**FEATURE 74**)

You can also specify a prefix to the retrieval under **Access codes**. (Services, Telephony Services, General Settings) You also need to specify a timeout for parked calls (Services, Telephony Services, General settings, **Timers**)

call park callback

This feature returns an unanswered parked call to the telephone where it originated after a set number of rings.

call park prefix

The first digit of the retrieval code of a parked call.
This digit cannot conflict with:

- the first digit of any existing extension number
- line pool access codes
- the direct-dial digit
- the external line access or destination code

The default Call Park prefix digit is 1. To disable Call Park, set the Call Park prefix to None. Assign the Call Park prefix under **Access codes**. (Services, Telephony Services, General Settings)

call pickup directed

This feature allows you to answer a call ringing at any telephone by entering the internal number of that telephone. (**FEATURE 76** <DN>)

call pickup group

See Pickup Group.

call queuing

If you have several calls waiting at your telephone, you can activate the Call Queuing feature to answer the calls in order of priority.

The order of priority is: incoming calls, callback calls (calls that were parked or forward but were not answered before the timers ran out), and camped calls. (**FEATURE 801**)

Camp-on

A feature that allows you to reroute a call and park it on a telephone when all the lines on that telephone are busy. To answer a camped call, use call queuing or select a line if the camped call appears on your telephone. Queued calls get priority over camped calls.

MCDN: On a private network using the MCDN protocol, the central attendant can camp calls on any telephone in the network.

camp timeout

The length of a delay before a camped call returns to the telephone that camped the call. Set the length of delay under Timers. (Services, Telephony Services, General Settings)

CAP

A central answering position (CAP) consists of a T7316E BST connected to one or more key indicators modules (KIM), or an M7324 telephone connected to one or two central answering position (CAP) modules.
Without system configuration, the modules support extra memory buttons (CAP module, 48; KIM, 24). The system can support as many of these CAPs as the telephony resources support T7316E telephone or M7324 telephone.
If the telephone is configured in system programming under CAP/KIM assignment this enhanced CAP (eCAP) supports line appearances; the eKIM also supports multiple appearances of a target line and hunt group designators. The system supports a maximum of 12 eCAPs.
Programming note: The KIM does not support hunt group DNs as auto dial buttons. Individual hunt group members, however, can be assigned to auto dial buttons.

carrier access codes

Telephony service provides have unique codes that can be used in front of a dialing string to direct a call through a specific carrier. When you use destination codes, add these codes to the destination code or to the dial-out string for the route.

CDP

The Coordinated Dialing Plan (CDP) is used on networked sites each site is viewed as an independent node in that each site has a range of extension numbers (i.e. 2221-2267), with a unique (to the private network) prefix number. Example: Site one = prefix 10, therefore you would dial numbers from 102221 to 1022267 to reach that network. Site two = prefix 20, therefore, you would dial numbers from 202221 to 2022267 to reach that network. See also, Universal Dialing Plan. Set the specifications for CDP under Dialing plan, Private network. (Services, Telephony Services, General Settings)

central answering position

See CAP.

centralized auto attendant

You can use the Business Communications Manager auto attendant and voice mail applications on one Business Communications Manager system within a private MCDN network to support all the systems connected on the private network. The Business Communications Manager can also be set up to access voice mail and auto attendant systems attached to other systems, such as a Meridian 1 (M1) connected to Octet voice mail or CallPilot voice mail systems, a DSM100/SL100 switch, or a Succession 1000/1000M.

centralized voice mail

You can use the Business Communications Manager auto attendant and voice mail applications on one Business Communications Manager system within a private MCDN network to support all the systems connected on the private network. The Business Communications Manager can also be set up to access voice mail systems attached to other systems, such as a Meridian 1. If the M1 is supporting the voice mail system, and the private network is MCDN, the Business Communications Manager systems on the network can also support the attendant call features from the M1. The Business Communications Manager also supports centralized voice mail connected to a DSM100/ SL100, or a Succession 1000/1000M.

CHAP

Challenge-Handshake Authentication Protocol (CHAP) is a method of establishing security on PPP links where the peers must share a plain text identifier. The caller sends a challenge message to its receiving peer and the receiver responds with a value it calculates based on the identifier. The first peer then matches the response with its own calculation. If the values match, the link is established.

CHAP is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).

cipher

Cryptographic algorithms used as part of security authentication between the system and servers and clients. A cipher suite contains a number of these algorithms:

- DES: Data Encryption Standard
- DSA: Digital Signature Algorithm
- KEA: Key Exchange Algorithm
- MD5: Message Digest algorithm
- RC2 and RC4: Rivest encryption ciphers
- RSA: A public-key algorithm for both encryption and authentication
- RSA key exchange: A key-exchange algorithm for SSL-based
- SHA-1: Secure Hash Algorithm
- SKIPJACK: a classified symmetric-key algorithm
- Triple-DES: DES applied three times

(Information obtained from Netscape Navigator Corporation; http://developer.netscape.com/docs/manuals/security/sslin/index.html)

client

A client is a computer system or process that requests a service of another computer system or process. For example, a workstation requesting the contents of a file from a file server is a client of the file server.

clock sources

This is a feature of DTM and BRI modules that allows you to determine where these modules receive their synchronization timing for the network.

coldstart

A coldstart occurs when you lose all system programming. You can lose system programming after a major event such as an extended power failure. If this occurs, you will need to restore the data to your system from your backup files.

conference

A feature that allows you to establish a three-person call at your telephone. (**FEATURE 3)** or the programmed conference/transfer button on the telephone)

configuration

See programming.

control telephone

The control telephone allows you to access the services menus and add or change when the services run. Manually-activated services take precdence over automatic services. The control telephone for each DN is configured under the General tab on the DN record.

Coordinated Dialing Plan (CDP)

Refer to CDP.

COS password

The Class of Service password (COS) defines the set of features and lines available to the user for a call into the Business Communications Manager system. The COS password determines which restriction filters and remote access packages are active when the caller uses a specific password. Callers accessing the system from outside the system can change the Class of Service for a call by entering a six-digit Class of Service password. However, internal users cannot change their access to features with a COS password, only their restriction filters. Assign this feature under COS Passwords. (Services, Telephony Services, General Settings) See also, DISA DN and Auto DN.

CSU

A Channel Service Unit (CSU) device on the digit trunk interface (DTI) that is the termination point of the T1 lines from the T1 service provider. The CSU collects statistics on the quality of the T1 signal. The CSU ensures network compliance with FCC rules and protects the network from harmful signals or voltages.

D

D-channel

A data channel transmission channel which is packet-switched is referred to as a D-channel. It is used for call setup, signaling and data transmission.

DASS2

Digital Access Signaling System Number 2 (DASS2) is a UK proprietary standard for signaling on ISDN connections between customer premises and the public network. DASS2 is used between the customer equipment and ISDN local exchange and is suitable for multiple access.

Data link connection identifier

See DLCI.

DDI Mux

The Digital Drop and Insert Mux media bay module is a specialized two-level module allows you to choose which channels on a T1 line you want to dedicate to data transmissions and which channels you want to dedicate to telephony operations. Both lines are programmed under **Services, Telephony Services, Lines**.

DECT

The Digital Enhanced Cordless Telecommunications (DECT) cordless protocol provides localized mobility services to the Business Communication Manager through a DECT media bay module connected to DECT base stations. This service is region-specific. Refer to the *DECT Installation and Configuration Guide* for details.

default

Default settings are the settings automatically programmed into the programming when you first install the system. You change the settings from their defaults using the Unified Manager. Defaults are determined by which region and which telephony template you choose when you first install your system. (Quick Start Wizard)

Delayed ring transfer

See DRT.

destination code

A destination code is an assigned number with up to 12-digits that the user dials before the outgoing call string. The system reads and translates the code into routing and dial-out information. This code must not conflict with any other access code on the system. Assign destination codes in Destination Codes. (Services, Telephony Services, Call Routing)

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows network administrators to centrally manage and automate the assignment of IP addresses in an network. When an organization sets up its computer users with a connection to the internet, internet protocols (TCP/IP) demands that an IP address must be assigned to each machine as well as to any device connected to the network.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP allows the network administrator to supervise and distribute IP addresses from a central point. It also automatically sends a new IP address when a computer is plugged into a different place in the network.

dial-up connection

A dial-up connection is a temporary connection between computers that is established over an analog or digital telephone line.

dialing plan

This is the overall numbering plan for your system that determines what numbers need to be dialed to reach specific destinations, and what numbers need to be received to be directed into the system, or through the system, in the case where the Business Communications Manager is acting as a node on a tandem network. This plan consists of a number of components, including the Public DN, the DN length, the received number and the received number length, line pool and destination codes, network codes, access codes, as well as the DNs for each telephones and piece of system equipment.

dialing restriction

See restriction filters.

DID

A Direct Inward Dial office setup provides each telephone with a dedicated number. The incoming DID line has a range of numbers, and these are mapped to each telephone in the system using target lines. Lines are set to auto answer so that you can forward unanswered calls to a receptionist or to a voice mail system.

DiffServ

Differentiated Services (DiffServ) is a method of implementing QoS service for IP networks. DiffServ is intended to improve network performance. Instead of applying faster, more advanced technology, networks are managed by appropriate network policies. With DiffServ there is a cost associated with higher quality services, and a risk with lower quality services.

Digital Private Network Signaling System

See DPNSS.

direct-dial

This feature allows you to dial an assigned telephone in your system, or external to your system, with a single digit. You can assign as many as five direct dial telephones in a system. These telephones are configured under the Direct Dial heading (Services, Telephony Services, General Settings).

Each telephone in the system has one direct-dial telephone. Each telephone can be assigned a direct-dial set under Capabilities. (Services, Telephony Services, System DNs). If Ringing service schedules are active on the system, an additional direct dial telephone can be identified, for example, a night security desk.

direct-dial digit

This is a single, system-wide digit for calling the assigned direct-dial telephone of any telephone. This digit is defined under Access codes. (Services, Telephony Services, General settings)

directed pickup

See call pickup directed.

directory number

See DNs.

DISA

Directed Inward System Access (DISA) is a feature that is assigned to lines to allow the system to answer calls from users from outside the system, who want to access the system and use system features. When this feature is active, the external user hears a stuttered dial tone and must enter a valid class of service (COS) password to proceed.

DISA DN

This is a system directory number that is assigned to auto-answer trunks that require a remote users to enter a COS password to gain access to the system. See also COS password and Auto DN.

disconnect supervision

This line setting enables the system to detect if an external caller hangs up. After an external caller hangs up, the system disconnects the line. Disconnect supervision is defined under the module settings for the lines. (Resources, Media Bay Modules). You can also assign disconnect supervision to devices connected to an ASM8+ media bay module (BCM 3.6 and newer software) to provide disconnect supervision on a per-device basis.

disk drive

A mass storage device that searches, reads and writes data on a disk.

display

A one or two line screen on a Business Communications Manager telephone that shows commands and options for that telephone.

display buttons

The three buttons that appear below the display on a Business Communications Manager telephone.

display options

The options available to a user. These options appear on the telephone display. Select the options on the display using the display buttons. Enter information from the dialpad.

distinctive ring

In system programming, this feature allows you to define a distinct ring for different types of calls, to provide a priority system for incoming calls. You can determine distinctive ring patterns for lines, telephones and hunt groups. A hierarchy of ring patterns determines which distinctive ring source predominates.

As a feature, the user can choose a specific ring type for incoming calls (**FEATURE** *6).

DLCI

The Data Link Connection Identifier (DLCI) is used to identify a permanent virtual circuit (PVC) in frame relay networks.

DND

The Do Not Disturb (DND) feature stops calls from ringing at your telephone. Only Priority Calls will override this feature and ring at your telephone. A line button flashes when you receive a call, but the call does not ring. (**FEATURE 86**) You can set the telephone to send this signal automatically through a setting in Capabilities. (Services, Telephony Services, System DNs)

DNs

A unique number that the Business Communications Manager system assigns to every telephone or data terminal. You use the DN to identify a device for the Business Communications Manager configurations that require telephone-specific features. The system also assigns DNs to other applications such as Call Center and Hunt groups. Companion and ISDN and DECT equipment have separate sets of DNs that are exclusive that that type of device.

Directory numbers are the digit string that the system uses to identify telephones and system devices and applications. The DN record provides access to configuring telephone functionality, including defining the features the user can access, the features the telephone supports, and the lines that can be used by the telephone to send and receive calls. See also, DN.

DNS

The domain name system or domain name server (DNS) is the system in the Internet that maps names of objects, most usually host names, into IP numbers or other resource record values. The name space of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.

DNS proxy

A Domain Name Service (DNS) proxy translates alphabetic domain names into computer-readable IP addresses. For example, the domain name www.nortelnetworks.com for the Nortel Networks web site can translate to the IP address 192.177.5.18. After a domain name is translated into an IP address, the workstations on your network can communicate with the web site. Depending on the configuration of your system, you can let your workstations know that Business Communications Manager is the DNS proxy.

domain name

The domain name is used to organize Internet names into manageable groups, such as nortelnetworks.com, where nortelnetworks is the domain name.

Domain Name Server (DNS)

See DNS.

Do Not Disturb

See DND.

double density

Double density for station modules is a function of Business Communications Manager 3.0 and later software. This functionality uses the B2 portions of the line to provide an additional 16 possible telephone connections on each MSC bus. Only station modules that support this feature provide this access, including the ASM8, DSM16+ and the DSM32+ media bay modules. The Business Communications Manager has two double density system settings. Partial Double Density (PDD) is the default system setup. This configuration leaves Bus 06 and 07 with B1/B2 capability to support the Companion system. Full Double Density (FDD) provides 32 lines on all six module buses.

D-packet

A BRI T loop can be used in combination with a BRI S loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. D-packet service is a 16 kbps data transmission service that uses the D-channel of an ISDN line. The T and S loops must be on the same physical module.

DPNSS

Digital Private Network Signaling System (DPNSS) is a networking protocol that provides access to Business Communications Manager features over multiple combined networks. Corporate offices, separated geographically, can be linked over DPNSS to other Business Communications Manager systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Business Communications Manager systems to function like a private network. DPNSS is available in International systems only.

driver (device)

A program that allows a hardware peripheral, such as a network interface card, to communicate with the Business Communications Manager base unit.

DRT

Delayed Ring Transfer to Prime (DRT) allows the system to transfer an unanswered call on an external line to the prime telephone related to that line if the targeted telephone is not answered within the configured number of rings. Configure this setting under Feature settings, Delayed Ringer Transfer. (Services, Telephony Services, General Settings)

DTMF

Dual tone multifrequency (DTMF) provides two distinct telephone signaling tones used for dialing.

Dynamic Host Configuration Protocol

See DHCP.

dynamic IP address

Dynamic IP addresses are assigned to computers by an IP address server, as the computer needs it. Usually there is a particular range or scope of IP addresses that your network uses. With dynamic IP addressing, a computer can have a different IP address every time it connects to the network. Other devices must know the IP address of the computer so they can communicate with it. The IP address server manages the assignment of IP addresses to the client workstations. See also static IP address.

E

EDO

Extended Data-Out (EDO) is a type of Dynamic Random Access Memory (RAM) where storing data to and reading data from the memory is faster.

eKIM

An enhanced Key Indicator Module (eKIM) is a KIM attached to a T7316E BST that has been configured under CAP/KIM assignment. When programmed as an eKIM, the module supports line appearances, multiple appearances of a target line, and hunt group appearances. Neither an eKIM or an OKIM support Hunt Group DNs as autodial keys.

Emergency 911 dialing

The ability to access a public emergency response system by dialing 911. State and local requirements for support of Emergency 911 Dialing service by Customer Premises Equipment vary. Ask your local telecommunications service provider about compliance with applicable laws and regulations. Note, there are special restrictions about setting up this service on IP telephones that are connected to the Business Communications Manager.

emergency telephone

A single-line telephone, also referred to as a 500/2500 telephone, that becomes active when there is no power to the Business Communications Manager base unit.

enbloc dialing

A system feature where the system does not dial out a number until all the call numbers have been entered. This allows the system to determine where the call needs to be routed outside the system.

ethernet

A Local Area Network (LAN) protocol that is the original Carrier Sense Multiple Access/ Collision Detect (CSMA/CD) LAN that allows computers, and Business Communications Manager base units to listen for pauses before they communicate. Ethernet LANs use coaxial cable or twisted pair wiring to connect network equipment.

ETSI

European Telecommunications Standards Institute. ETSI defines the protocol defined by the institute that provides telecommunications standards in Europe. See also ANSI and QSIG.

event message

The system stores event messages in the system log and displays these messages during a maintenance session. They record many different events and activities in the system.

exceptions

See overrides.

Extended Data-Out

See EDO.

external code

The number you dial to access a line outside of your Business Communications Manager system. For instance, the external code to access the public network is set to a default of 9.

These codes are defined under Access codes (Services, Telephony Services, General Settings) and Destination codes (Services, Telephony Services, Call Routing). You also use an external code to support the T7100 telephone and single-line telephones connected to an Analog Terminal Adapter (ATA2).

external paging

Use this feature to make voice announcements over an externally-installed loudspeaker connected to the Business Communications Manager base unit through the MSC.

F

FAX

FAX works with Business Communications Manager Voice Messaging and IVR (Interactive Voice Response). FAX allows a caller to send a fax document to a voice mailbox. BCM 3.5 and newer software supports fax over IP trunks using the T.38 protocol. IP trunks and IP fax are described in the *IP Telephony Configuration Guide*.

Feature button

This is a code that is entered at a telephone to activate a feature. Each code is entered after you press the FEATURE button on a system telephone. The keycap icon for FEATURE varies, depending on telephone model. If you have a feature loaded into a memory button, when you press the memory button, the feature is initiated and you follow the display messages. On remote telephones and telephones that do not have a Feature button, such as analog telephones, the * button is used. On analog telephones, this is referred to as a LINK button.

filtering

Filtering is the process of examining a data packet on the network to determine the destination of the data and whether the packet should be passed along on the local LAN, copied to another LAN, or dropped.

FQDN

A Fully Qualified Domain Name (FQDN) consists of a combination of host name and domain name. For example, mycomputer.nortelnetworks.com is a Fully Qualified Domain Name.

frame

A frame is a unit of data transmission in a local area network.

frame relay

A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.

FTP

The file transfer protocol (FTP) allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.

full autohold (on idle line)

When this feature is on, Full Autohold automatically puts the current line on hold when you select another line. Enable Full Autohold under Line XXX, Trunk Line Data. (Services, Telephony Services, Lines)

You can also define auto hold for each telephone. See auto hold.

full double density (FDD)

See double density.

Fully Qualified Domain Name

See FQDN.

G

gateway

A system that links two different types of networks and enables them to communicate with each other. Business Communications Manager is the gateway that links your network to the intranet or internet. Depending on your configuration, you can let your workstations know that Business Communications Manager is the internet gateway. When you configure voice over IP (VoIP) trunking, you need to configure the parameters for the local system (local gateway) and remote system (remote gateway) so the system can correctly receive and send information over the trunk. If the network has a Gatekeeper application, this application determines where data packets go, and it is not necessary to configure the remote gateway in this case. However, you do need to send the local system parameters to the Gatekeeper administrator.

ground start trunk

Ground start trunks provide the same features as loop start trunks. Use this type of trunk when the local service provider does not support disconnect supervision for the digital loop start trunks. By configuring lines as ground start, the system can identify when a caller hangs up the telephone at the far end. Ground start trunks are available only on a Digital Trunk Interface module (DTM).

group listening

This feature allows you to have other people in your office hear a caller through your telephone speaker. The caller hears you when you speak into the receiver and cannot hear other people in the office. (**FEATURE 802**)

You can cancel Group Listen for the current call. Group Listen cancels automatically when you hang up the Group Listen call.

H

H.323

H.323 is the standard for using IP to send voice and video within intranets and on the public Internet.

handsfree

A feature you can use to make calls through your telephone without lifting the telephone receiver. Activate Handsfree under Capabilities (Services, Telephony Services, System DNs). When you activate handsfree, Business Communications Manager assigns a handsfree/mute button on the lower right button of the telephone (M-series telephones). The T7208 and T7316 have separate mute buttons, so only handsfree is assigned to the lower right button. The T7316E has both a separate mute button and a separate handsfree button located under the dialpad. 7000s, 7100s, the i2001, and portable handsets do not have this feature as they do not have the necessary speakers and microphones. IP i2002, i2004 telephones do allow handsfree. They, too, have a separate handsfree button (beside the handset) and mute button (under the volume bar).

Handsfree volume note: The telephone volume level returns to the default volume level set on the telephone after each handsfree call. This is not configurable in system programming.

handsfree (HF) answerback

This feature automatically turns on the microphone at a telephone that receives a Voice Call so that the person receiving the call can respond without lifting the receiver. Activate HF Answerback under Capabilities (Services, Telephony Services, System DNs).

hard disk

A data storage device that uses rigid magnetic disks permanently installed inside the computer CPU or a portable unit.

HDLC

High-level Data Link Control (HDLC) is a group of protocols or rules for transmitting data between network points or nodes. Data is organized into a unit, called a frame, and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in Layer 2 of the industry communication reference model, Open Systems Interconnection (OSI).

held line reminder

A telephone rings and displays the message `On hold: LINENAM` when you place an external call on hold for programmed period of time. Set the Held Line Reminder under Feature settings. (Services, Telephony Services, General Settings).

High-level Data Link Control

See HDLC.

HLC

The Home Location Code (HLC), also known as a Location code (LOC) is used as part of a UDP dialing plan to identify each node on a private network.

Hold button

Use this button to interrupt calls so that you can perform another task without disconnecting the caller.

Home Location Code

See HLC and location code.

hookswitch Flash

See Link.

hospitality services

These features allow a hostelry to use room and desk telephones to communicate housekeeping and alarm information between each room and the front desk (admin telephone), including setting call restrictions at different levels for each room. The telephones also have all configured system call capabilities.

host name

In networking, this is the name of a computer that provides services, such as database access, to other computers or Business Communications Manager base units in the domain. Computers with a host name also have a unique IP address. Because the Business Communications Manager base unit has a unique IP address, the Business Communications Manager base unit qualifies as a host.

host system signaling

Also referred to as end-to-end signaling. Telephones can access a remote system or dial a number on an different carrier by using host feature activation codes, such as Link, Pause and Run/Stop.

hot desking

This is an IP telephone feature that allows a user to forward complete IP functionality from one IP telephone to another one, even at a remote location until the feature is deactivated. The feature is activated at the receiving telephone, but can be deactivated with either IP telephone. Refer to the *Telephony Feature Handbook* for a description of the feature and how to use it. The *IP Telephony Configuration Guide* describes how to set up the feature. Note: Headset functionality is not forwarded by hot desking. Once the hot desking is enabled, you need to press the Headset button on the target telephone to re-enable the headset mode.

Hotline

This feature automatically calls a pre-assigned number when you lift the telephone receiver or press the handsfree button. A Hotline number can be an internal or external number. Assign Hotline under Capabilities, Hotline. (Services, Telephony Services, System DNs)

HTTP proxy

See web proxy.

Hunt group

Hunt groups are groups of telephones that have been configured to answer all calls to a Hunt DN. Call appearance on each telephone depends on programming. This feature allows you to direct specific lines to specific groups of people, such as a sales group, or technical group for a specific product.

I

ICCL

This MCDN networking feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.

ICMP

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, however, the messages are processed by the TCP/IP software and are not directly apparent to the application user.

IETF

The Internet Engineering Task Force (IETF) is the committee that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society's Internet Architecture Board (IAB).

in-band

In-band is a method of device access that utilizes a network interface component within the device.

Install Client button

This button, located on the Unified Manager front page, provides access to Business Communications Manager supplementary management programs, such as the Java class files. Some of the applications located under this button require keycodes before they can be used.

Integrated Services Digital Network

See ISDN.

Interactive Voice Response

See IVR.

intercom button

A button that provides access to telephones within a Business Communications Manager system. These buttons can also provides access to external lines by adding an access or destination code to the dialed number. You can assign a telephone a maximum of eight intercom buttons, although not all buttons will display, depending on the style of telephone. Configure intercom (I/C) buttons under DN XXX, Line Access. (Services, Telephony Services, System DNs)

intercom keys

See intercom button.

internal channel

These are the media processing channels that support voice and data processing from sources other than the media bay modules. This support includes traffic from the LAN and WAN networks VoIP trunks, dial-up modem, voice mail applications and IVR. On the Unified Manager, these are DS30 bus 01 and 08 on a default system. If you change your system to a DS30 3/5 split, DS30 bus 07 also changes to internal channels and no longer supports a media bay module.

internal line

A line on your telephone dedicated to making calls to destinations inside your Business Communications Manager, also called Target lines. An internal line can connect you with an external caller if you use it to access a line or line pool. You can direct internal lines to specific telephones or groups of telephones using target lines.

internal number

A number, referred to in Unified Manager as a Directory Number (DN), which identifies a telephone or device assigned to the Business Communications Manager. See also DN.

internal user

A person using a telephone connected to the Business Communications Manager telephone.

Internet

A global TCP/IP network linking millions of computers for communications purposes.

Internet Engineering Task Force

See IETF.

Internet-standard Network Management Framework

Device configuration and monitoring via SNMP.

Interrupt Request

See IRQ.

IP

The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into units called packets. Each of these packets contains the Internet address of the sender and the receiver.

IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

IP address

The Internet Protocol address is a unique identifier that allows communication over the Internet to be directed to the appropriate destination. Every computer on the Internet must have a unique IP address. IP addresses are allocated by an Internet service provider (ISP) in the following format: nnn.nnn.nnn.nnn, where nnn is a numeric value from 0 to 255. IP addressing might be referred to as being a static IP address or a dynamic IP address.

IP music

With this feature you can provide background music to the system from the IP network instead of installing music source hardware.

IP telephones

Business Communications Manager IP telephones and the Symbol NetVision wireless IP telephone, can make calls out of the system over land lines as well as VoIP trunks. The telephones are IP telephones because they connect to the Business Communications Manager through an IP connection, rather than a hard-wired connection. Once they connect to the system, the Business Communications Manager converts the information as required for the trunk on which the call is going out.

IPX

IPX (Internetwork Packet Exchange) is a networking protocol from Novell that interconnects networks that use Novell NetWare clients and servers. IPX is a datagram or packet protocol. IPX works at the network layer of communication protocols and is connectionless (that is, it does not require a sustained connection during an exchange of packets as, for example, a regular voice phone call does).

IRQ

IRQ is a signal that is sent by a hardware device to the microprocessor, requesting its immediate attention. For example, every communications port has an interrupt request line for telling the microprocessor when data is received or transmitted.

IRQ conflict

An IRQ conflict occurs when two hardware devices have the same IRQ. When an IRQ conflict occurs, the user must configure the IRQ settings to solve the conflict.

ISDN

A digital telephone service that allows for a combination voice and data connection over a single, high-speed connection. ISDN service can operate over the same copper twisted-pair telephone line as analog telephone service. The Business Communications Manager uses two versions of ISDN, BRI and PRI.

ISDN call connection limitation

See ICCL.

IVR

Interactive Voice Response is an automated telephony application that prompts callers with a combination of recorded menus and prompts, and real-time data from databases. Users enter digits from their touch tone key pad that directs the IVR application to access databases and play information back to the caller

J

Java class files

These files are loaded onto your computer when you open the Unified Manager. You require the JVM or Sun JRE application on your computer to run them.

Java Runtime Environment

See JRE.

Java Virtual Machine

See JVM.

JRE

Sun Java JRE is the Java protocol produced by Sun Microsystems. Use this application for Browsers that do not support or do not come with JVM. Supported on BCM 3.5 and newer software.

JVM

This Windows application runs as part of the Browser on your computer. It is a required application for running the Unified Manager.

K

Kbyte

The abbreviation for kilobyte. A kilobyte is equal to 1024 bytes.

keycode

This code is used to enable application options on the Business Communications Manager. These codes are entered by the installer or system administrator. Keycodes are a combination of access codes that are encrypted to open a single application on a specific Business Communications Manager. Refer to the *Software Keycode Installation Guide* for details.

KIM

The Key Indicator Module (KIM) is an add-on module for the BST T7316E telephone. Depending on how the T7316E is configured in system programming, the module supports only memory button programming (OKIM), or it can support memory button programming, line appearances (including multiples of the same target line), and hunt group appearances (eKIM). The KIM is supported only on BCM 3.5 and newer software. The T7316E/KIM combination is called a Central Answer Position (CAP) and replaces the M7324/CAP module hardware.

L

LAN

A Local Area Network is a group of computers or Business Communications Manager base units connected so they can communicate and work together.

LAN Manager

See LM

Last Number Redial

This feature allows you to redial the last external number you dialed. (**FEATURE 5**)

Least cost routing

See routing service.

line

The complete path of a voice or data connection between one telephone, or other device, and another. Note that this line does not need to be a physical line. The Business Communications Manager considers voice over IP (VoIP) trunks and target lines to be the same as physical lines, in terms of programming.

line number

A number that identifies an external line connected to the Business Communications Manager. The total number of lines depends on the number and type of trunk media bay modules installed. Voice over IP (VoIP) trunks and target lines are also defined as line numbers, although they do not connect to the system through physical lines.

line pool

A group of lines used for making external calls. Line pools provide an efficient way of giving a group of users access to a group external lines using one line button. This also provides cost saving because you can assign a greater number of telephones to fewer lines, depending on your system traffic rates. Assign a line to be part of a line pool under Trunk, Line data. (Services, Telephony Services, Lines, Physical lines or VoIP lines).

Note that PRI lines have a separate line pool collection (PRI A to PRI 0). PRI line pools cannot be directly accessed. They must be put configured into routes, which are then assigned a destination code.

line redirection

This feature allows you to redirect all calls from an incoming line, usually to a destination outside the system. After you redirect a line, you cannot answer the line within the system. (**FEATURE 84**)

You enable the service and set up redirect ring under Capabilities. (Services, Telephony Services, System DNs)

This feature differs from Call Forward in that Call Forward redirects calls coming in on all lines to another destination, such as voice mail, while Line Redirection redirects only the specific line.

Link

If you connect the Business Communications Manager system to a Private Branch Exchange (PBX), you can use a Link signal to access special features. You can include the Link signal as part of a longer stored sequence on an external auto dial button or in a Speed Dial code. The Link symbol uses two of the 24 spaces in a dialing sequence.

LM

The LAN Manager is a challenge/response authentication protocol.

Local Area Network

See LAN.

location code

A location code (LOC) is used as part of a UDP dialing plan to identify each node on a private network. It is also referred to as a Home Location Code (HML).

Long Tones

This feature allows you to control the length of a tone so that you can signal devices such as fax or answering machines. These devices require tones longer than the standard 120 milliseconds. (**FEATURE 808**)

M

MAC address

The Media Access Control is a physical address that is the portion of the data-link layer in 802.x networks.It controls addressing information of the packet and enables data to be sent and received across a local area network. IP telephones, for instance, have a MAC address that allows the Business Communications Manager to keep track of individual telephones even if dynamic IP addresses are used.

mailbox

A storage place for voice messages on Business Communications Manager Voice Messaging.

Maintenance button

This button, located on the front page of the Unified Manager, provides access to a number of troubleshooting and diagnostic tools for your system. It also includes the tools for controlling the DECT modem. Documentation, or your service technician will direct you when you need to use these tools.

MCDN

Although defined as a Meridian Customer-Defined Network, this network protocol provides Meridian system attendant features (break-in and camp-on) to Business Communications Manager systems that are network to the Meridian over PRI SL-1 lines, providing the MCDN keycode has been entered at the Business Communication Manager. There are setup requirements from both ends of this network link to properly enable the features. The MCDN protocol also provides network trunking features such as Trunk Anti-Tromboning (TAT) and Trunk Route Optimization (TRO). Business Communications Managers can also be networked without a Meridian system, but in this case, the Meridian attendant features are not supported. VoIP trunks can also provide MCDN networking features if the MCDN keycode is applied to the system.

Media Access Control

See MAC address.

media channel

Media channels are the communication channels used to send voice and data information between the devices and feature ports. Media channels are also known as B channels. The Business Communications Manager uses the MSC to manage these channels on the system.

Media Services card

See MSC.

Meridian 1 ISDN Primary Rate Interface

A protocol used between members of the Nortel Networks Meridian family of Private Telecommunication Network Exchanges. The signaling information is carried via time slot 16 of a 2.048 Mbit/s digital transmission system.

Meridian IPT

This Meridian software is required if you want to establish VoIP trunks between your Business Communications Manager and a Meridian system.

MHz

The abbreviation for megahertz, which is a unit of measure indicating frequency in millions of cycles per second.

microprocessor

An electronic component that is the center of all activity inside the Business Communications Manager base unit. The microprocessor controls the operation of the computer and is responsible for executing program commands. A microprocessor is also referred to as the Central Processing Unit (CPU).

modem

A communications device that allows computers to exchange data over telephone lines. A modem uses electronic processes called modulation and demodulation. The modem changes (modulates) the data into tones to send to another modem and converts (demodulates) tones when receiving from another modem.

move line

This feature allows you to move external lines assigned to your telephone to different buttons on your telephone.

MSC

The Media Services Card (MSC) is an internal card that controls the call processing for the Business Communications Manager system. This card carries the identity of the system. If the card is replaced, all keycodes need to be regenerated using the new card identification number. Refer to "Configuring the MSC resources" on page 609.

Multilink PPP

Multilink PPP is an extension to the PPP protocol that enables you to group a set of links into a bundle for more bandwidth. The links in the bundle can operate at different speeds. Typical links can be ISDN B-channels, dial-up connections, and leased-lines.

music source

You can connect a radio or other source of music to the system to provide music for the Music on Hold and Background Music features. A music source is customer-supplied. The source is connected through a jack on the MSC on the Business Communications Manager. You can also set up the IP music feature, which uses sound files from the internet or downloaded to the Unified Manager.

MWI

If the the network line supports message waiting indicators, an external message activates an indicator on the telephone or provides a tone indicating a message is waiting. If the telephone has line indicators, and the message comes in over an assigned line, an indicator appears beside the line, and a call waiting message appears on the telephone display. For telephones without displays, a tone can be configured, or, if the telephone has one, a MWI lamp may light.

N

NI

National ISDN is an ISDN protocol that is used by profiles outside of North America. See also ANSI.

navigation key

This is the small icon beside many of the headers in the Unified Manager navigation tree. Clicking on the icon reveals any subheadings beneath the main heading.

navigation tree

This is the menu of Unified Manager topics that appears in the left frame of the Unified Manager screens accessed through the Configure button.

NCRI

Network Call Redirection Information (NCRI) redirects calls across an MCDN network using Call Forward (all calls, no answer, busy) and Call Transfer features. The call destination also receives the necessary redirection information. This feature allows the system to automatically redirect calls from within a Business Communications Manager system to the mail system, such as Meridian Mail, which resides outside the Business Communications Manager system on the Meridian 1.

NetBIOS

The Network Basic Input/Output System (NetBIOS) is an interface and upper-level protocol developed by IBM for use with a proprietary adapter for its PC network product. NetBIOS provides a standard interface to the lower networking layers. The protocol provides higher-level programs with access to the network. Windows NT systems use NetBIOS.

NetVision

The NetVision handsets are wireless IP telephones produced by Symbol that are supported by the Business Communications Manager IP telephony structure.

network

Two or more computers linked electronically to share programs and exchange data. This process requires both hardware devices and software to coordinate the connection and data exchange.

Network Call Redirection Information

See NCRI.

network device

A network device is a hardware device used as a communications component within a network.

network DN

A number supplied by the ISDN network service provider for ISDN terminal equipment. Refer to “Adding SPID network DNs” on page 269.

Network Interface Card

See NIC.

NIC

A Network Interface Card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network. Personal computers and workstations on local area networks (LANs) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.

NT LAN Manager

A challenge/response authentication protocol.

O

On Hold

A setting that controls what external callers hear: music, tones, or silence, when you place the call on hold. Configure this setting under Feature settings. (Services, Telephony Services, General settings)

Open Shortest Path First

See OSPF.

OSPF

Open Shortest Path First (OSPF) is a routing protocol used within larger autonomous and complex networks in preference to the Routing Information Protocol (RIP) which suits a small network. Like RIP, OSPF is designated by the Internet Engineering Task Force as one of several Interior Gateway Protocols.

out-of-band

Out-of-band is a method of device access which circumvents the network interface components within the device.

overflow

For digital and IP telephones, turn this setting on to allow the system to choose a fallback path for an outgoing call.

The feature is turned on under Routing Service, <schedule>. (Services, Telephony Services, Scheduled Services). You also need to set up routes and schedules that provide the correct routing for the normal and fallback lines.

overrides

One component of a restriction filter. Overrides are numbers you can dial when they are not allowed by a more general restriction. Enter these numbers under Overrides for each restriction within specific filters. (Services, Telephony Services, Restrictions filters, Filter XX, Restrictions)

P

packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file, such as an e-mail message, HTML file, GIF file, URL request, and so forth, is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file.

A packet switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit switching, is used for networks allocated for voice connections. In circuit switching, lines in the network are shared among many users as with packet switching, but each connection requires the dedication of a particular path for the duration of the connection.

Packet and *datagram* are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.

Page

Use this feature to make announcements over the Business Communications Manager system. You can make page announcements over the telephone speakers and/or external speakers. The 7000, 7100, i2001, and portable handsets cannot receive pages.

- Page tone is defined under Feature settings. (Services, Telephony Services, General Settings)
- Page Time out is defined under Timers (Services, Telephony Services, General Settings). This setting controls how long a Page Announcement can last.
- Page zone defines An area in the office that receives internal page announcements that other areas of the office do not hear. This feature is defined for each telephone under Capabilities. (Services, Telephony Services, System DNs)
- Auto hold for incoming page: When enabled, this feature puts current calls on hold for the duration of the page announcement. Note: If a call was muted before it was put on hold, it will not necessarily remain muted when it is released after the page announcement.

PAP

Password Authentication Protocol (PAP) is a procedure used by PPP servers to validate a connection request. PAP works as follows:

1. After the link is established, the requestor sends a password and an ID to the server.
2. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP.

Park prefix

See call park prefix.

Park timeout

The time before an unanswered parked call returns to the telephone that parked it. Set this feature in Timers. (Services, Telephony Services, General settings)

partial double density (PDD)

See double density.

Password Authentication Protocol

See PAP.

PBX system

A PBX is a small telephone system connected to a central office (CO), but which is owned and operated privately. An example of a PBX system is the Meridian 1 system. The PBX can connect directly to telephones or pass lines on to another private telephone system, such as a Business Communications Manager.

This is a telephone configuration used by larger offices which have more telephones than incoming lines. The incoming lines are assigned to a pool, and each telephone is given access to the pool. On the receptionist telephone, the lines are assigned individually to indicator buttons.

PCI

Peripheral Component Interconnect (PCI) slots are hardware sockets on a circuit board. For instance, the Business Communications Manager has four PCI slots on the MSC board. Each slot contains one PEC III card, which handles call processing for the system.

Peripheral Component Interconnect Slot

See PCI.

Permanent virtual circuit

See PVC.

Personal speed dial

These are two-digit codes between 71 and 94 that are assigned to specific telephones to dial external numbers with just one button press. Configure speed dials under User Preferences, User speed dials, Speed dial #XX. (Services, Telephony Services, System DNs)

Phantom DNs

A Phantom DN is a DN record for a telephone that does not physically exist. You can assign lines to the telephone that can be programmed to Appear and Ring. This allows you to assign an Answer key from the non-existent telephone to an existing telephone. This might be used in the case where a customer number has been changed, but the number still gets used. Rather than assign a telephone to the line, you can create a phantom DN and assign an Answer key to an active telephone.

pickup group

You can place a telephone into one of nine call pickup groups. You can pick up a call ringing at a telephone within a pickup group from any telephone within the same pickup group. Assign a telephone to a pickup group under Capabilities. (Services, Telephony Services, System DNs)

pin-1

An indicator on the first pin on an electronic component. You use this indicator to help you correctly align the component when attaching or installing it.

Point-to-point protocol

See PPP.

pool

See line pool.

port

A connector on the Business Communications Manager base unit that allows data exchange with external devices, such as external page or music equipment or a serial cable connection to a computer.

power cable

A cable that connects the Business Communications Manager base unit to a power source.

PPP

Point-to-point protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected to a server by a telephone line. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

pre-dial

A feature that allows you to enter a number and check it on your telephone display before you lift the handset or select a line. The Business Communications Manager system dials the number when you lift the receiver or select a line.

PRI

Primary Interface (PRI) ISDN lines use 23 B-channels (North America) and a D-channel (23B+D). E1 PRI provides 30 B-channels and a D-channel (30B+D).

prime line

The line the system selects for your telephone when you lift the receiver, press the handsfree button or use an external dialing feature. Assign a Prime Line to a telephone under Line access. The default is the intercom button (I/C). (Services, Telephony Services, System DNs)

prime set

A telephone designated as a Prime set provides backup answering for incoming calls on external lines. The prime telephone for a line will ring for any unanswered calls on that line. Assign a prime telephone to a line under Line XXX, Trunk Line data. (Services, Telephony Services, Lines).

priority call

If you get a busy signal when you call a person in your office, you can interrupt that person for an urgent call. Enable this feature for a telephone under Capabilities. Set the intrusion level, which defines who can interrupt calls and whom you can interrupt under Capabilities, Intrusion. (Services, Telephony Services, System DNs). (**FEATURE 69**)

Privacy

This feature determines if a system user can select a line in use at another telephone and join an established call. Auto Privacy can be enabled under Line XX, Trunk Line data. Users can turn this feature on and off during separate calls. (**FEATURE 83**)

private access code

A one-digit number that identifies the systems on a private network that is using the a Universal Dialing Plan (UDP). This number is assigned in front of the Home Local Code (HLC) that is unique to each node. **Dial string:** (<priv.access.code>+<HLC>+<DN>)

Private branch exchange

See PBX system.

private line

See Private to.

private network

A telephone network including PBXes, such as Meridian 1, and/or Business Communications Managers connected through dedicated land trunks (E&M, T1/E1, PRI Sl-1, PRI CbC, BRI) or voice over IP (VoIP) trunks.

Private to

This feature allows you to select the telephone that exclusively uses a line. The line cannot appear on another telephone, except the prime telephone for that line. You cannot place private lines into line pools. Private lines are assigned under Line XXX, Trunk Line data, Line Type. (Services, Telephony Services, Lines)

programming

Setting the way the Business Communications Manager system works. Programming includes system-wide settings and separate telephone and line settings.

protocol

A set of rules and procedures for exchanging data between computers or Business Communications Manager base units on a network or through the Internet.

proxy

A proxy is a server that acts on behalf of another.

PSTN

The Public Switched Network (PSTN) provides central office lines that connect the system to the public network. Configure lines under Telephony Services, Lines.
Note: Private network lines are PSTN lines that have been designated by the central office as exclusive lines that directly connect two private telephony systems. In a private network, toll charges are not charged on a per-call basis, but are figured into the cost of the line services.

public network

The central office telephone network that provides trunks and lines to individual telephone users and private systems.

pulse/tone dialing

An external line setting for pulse or tone dialing. Pulse is the traditional method of dialing used by rotary-dial or push-button single-line telephones. Tone dialing allows telephones to communicate with other devices such as answering machines. You require tone dialing to access the features that PBX systems can provide or to use another system remotely.

PVC

The Permanent Virtual Circuit (PVC) is an end-to-end virtual connection in frame relay networks.

Q

QoS

On the Internet and in other networks, Quality of Service (QoS) refers to guaranteed throughput level. QoS allows a server to measure, improve and, to some level, guarantee the transmission rates, error rates, and other data transmission characteristics. QoS is critical for the continuous and real-time transmission of video and multimedia information which use high bandwidth.

QSIG

Q reference point signaling. QSIG is an ETSI (International) standard signaling for multi-vendor peer-to-peer communications between PBXs and/or central offices.

Quality of Service

See QoS.

R

RAM (Random Access Memory)

Computer memory that stores data temporarily. RAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased when you restart or turn off the Business Communications Manager base unit.

RAS

The Remote Access Server (RAS) is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporate network. Home users get access to the Internet through remote access to an Internet service provider (ISP).

A remote access server is the computer and associated software that is set up to handle users seeking access to the network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

recall

See Link.

receiver

In this document, this term can refer to the handset of a telephone.

regression code

This feature restores the previous system security number so that previously applied UTAM Activation Codes and Portable Credit Codes can be re-entered to restore full system operation for Companion components. Also required in cases of system recovery. You cannot use this code again.

relaying

Relaying is the process of moving data along a path determined by a routing process. The data is relayed between a source and a destination.

remind delay

A feature, referred to as held line reminder, causes a telephone to beep and display the message `On hold: LINENAM` when a call has been on hold for a programmable period of time. Turn the feature on and set the timing under Feature settings. (Services, Telephony Services, General settings)

remote access

The ability to dial into a Business Communications Manager system from outside the system and use selected features. The Class of Service determines which lines, features, and dialing capabilities are available.

In private networking, this term refers to one system accessing another system over a private trunk, for instance, for centralized voice mail. In this case, even though the number is dialed over a private trunk, and the dialing plan may be set up so that the user dials the same number of digits as for an internal call, routing is set up to dial out of the current system and into or through the connected system.

remote access dial restriction

See restriction filters.

remote access packages

A restriction filter that is applied to an incoming line to control which digits are dialed during an incoming remote access call. Remote access packages are defined under Remote Access packages (Services, Telephony Services, General Settings), and assigned under COS Passwords (Services, Telephony Services, General Settings)

remote access service

See RAS.

remote device

A remote device is any network device that is accessible only by means of communication over a digital or analog (dial-up) network.

remote monitoring

A feature that allows an off-site technician with a computer to call in and troubleshoot your system through the built-in modem.

remote paging

This feature allows remote users to use the system paging feature. Access to this feature is governed by the Class of Service for the call.

remote user

Someone who calls into a Business Communications Manager system from a telephone outside that system and uses system features or lines. See Remote Access.

restriction filters

Restriction filters are configured to prevent some telephone numbers or feature codes from being dialed. Restriction filters can be applied to lines, sets, specific lines on a set, and to Class of Service passwords. Under restriction filters, you can enter override numbers that you want to circumvent the general restrictions. Configure filters under Restriction filters. (Services, Telephony Services)

restrictions

Restrictions are numbers you cannot dial when that dialing filter is in effect. You can use **FEATURE 68** to override restrictions for a line to make a call.

restriction service

You can assign alternative dialing filters to lines, telephones, lines on a particular telephone, and alternative remote filters to lines at specified times of the day and on specified days. Set up restriction schedules under Restriction service. (Services, Telephony Services, Scheduled Services)

ring again

The ring again feature instructs the system to tell you when a currently busy telephony hangs up or when an unanswered telephone is being used. (**FEATURE 2**)

ring group

Ring groups allow you to program a specific group of telephones to ring during a scheduled time, for specific lines. You can program a maximum of 20 ring groups.

Configure ring groups under Ringing service. (Services, Telephony Services, Scheduled Services)

ringing service

A Services section that allows you to make additional telephones ring at specified times of the day and on specified days. Refer to ring group.

ring type

A feature that allows you to select one of four distinctive rings for your telephone. See also distinctive ring. This feature is set under User Preferences, but can be changed at a telephone. (Services, Telephony Services, System DNs)

ring volume

A feature that allows you to set the volume at which your telephone rings. This is a telephone feature and has no system setting.

RIP

Routing Information Protocol (RIP) enables routers in the same autonomous system to exchange routing information by means of periodic updates. RIP is a widely-used protocol for managing routing information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs.

Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts is has on record) to its closest neighbor host every 30 seconds. The neighbor host passes the information to its next neighbor and so on until all hosts within the network have the same routing path information, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network.

The major alternative to RIP is the Open Shortest Path First Protocol (OSPF).

Release button

Ends a call in the same way that hanging up the receiver does.

ROM (Read Only Memory)

Memory that stores data permanently. ROM contains instructions that the Business Communications Manager base unit needs to operate. The instructions stored in ROM cannot be changed and are used by the Business Communications Manager base unit each time it is turned on or restarted.

router

A router is a device that forwards traffic between networks, based on network layer information and routing tables. A router decides which path network traffic follows using routing protocols to gain information about the network and algorithms to choose the best route based on a routing matrix.

routing

The path a message takes from its origin to its destination on a network or the Internet. Configure telephony routing under Call Routing. (Services, Telephony Services). Configure intranet/internet routing under the Data headings).

Routing Information Protocol

See RIP.

routing service

Routing services defines schedules that allow you to change the route of a call without changing the destination code. This provides a way of shifting from one service provider to another at different times of the day if the rates are better. The system determines the routing; the user continues to dial the same number. Use Routing services to configure these schedules. (Services, Telephony Services, Scheduled Services)

Run/Stop

A feature that creates a break point in a programmed external dialing sequence. When you press a programmed key, the system dials the number up to the run/stop. When you press the programmed key again, the system dials the digits following the run/stop.

S

SAPS

A Station Auxiliary Power Supply (SAPS) provides power to a telephone that is more than 300 m (975 ft.) and less than 1200 m (3900 ft.) from the Business Communications Manager, or to a CAP configuration. M7324/CAP module CAP configurations require a SAPS for all modules. T7316E/KIM CAP configurations only require a SAPS if more than four KIMs are connected to the T7316E.

saved number redial

A feature that allows you to save the number of the external call you are on, providing you dialed the call, so that you can call it again later.

schedules

Any of six sets of services you can apply to your system. Schedules allow you to control ringing, routing and restrictions services based on day of the week and time of day. You also need schedules if the system VoIP trunks are set to allow fallback to PSTN lines. See "Configuring schedules" on page 483 and the *IP Telephony Configuration Guide*.

Secure Sockets Layer

See SSL.

selective line redirection

See line redirection.

serial port

A port that sends and receives data one bit at a time. You can use this port to connect the Business Communications Manager base unit to a printer, external modem or mouse. The serial port connector has nine pins and is identified by software with the letters COM and a single digit, such as COM1.

Server Message Block

See SMB.

service control password

This is the password that you enter when you want to start or change routing and restriction service settings.

Service modes

See services.

Service Profile Identifiers

See SPIDs.

services

You can define service schedules for ringing services, restriction services and routing services. This allows you to control call access a different times of the day and for different days of the week.

set

This book often uses this term in reference to telephones or telephony devices.

Set lock

This feature allows you to limit the number of features that are available at a telephone. Full set lock allows very few changes or features, Partial set lock allows more changes and features, and No set lock allows any change or any feature. Assign the Set lock under DNXX, Restrictions, Set Restrictions. (Services, Telephony Services, System DNs)

set relocation

This feature maintains the personal and system programming on digital telephones that get moved to a different jack on the same system, providing no other telephone is plugged into the original jack first. This feature is set under Feature Settings. (Services, Telephony Services, General Settings)

signaling channel

Signaling channels are the communication channels used to send control signals to and from the MSC. Signaling channels are also known as D-channels.

silent monitoring

This is the term used to define the monitoring feature that allows supervisors to monitor Hunt group or Call Center calls. This guide describes the Hunt group monitor features ("Monitoring Hunt groups" on page 585). Call Center monitoring is described in the Call Center documentation.

Simple Network Management Protocol

See SNMP.

SL-1

This is a type of PRI line that can be used to create a private network between two systems. It also supports the MCDN protocol. **VoIP programming note:** Prior to BCM 3.5, the SL-1 protocol was used as the gateway protocol for VoIP trunking. For BCM 3.5 and newer software, the CSE protocol is recommended for most VoIP trunking, unless otherwise specified by the network administrator. VoIP trunking information is contained in the *IP Telephony Configuration Guide*.

SMB

The Server Message Block (SMB) is a message format used by Windows to share files, directories and devices.

SNMP

Simple Network Management (SNMP) is the protocol governing network management and the monitoring of network devices and their functions.

SPIDs

Service Profile Identifiers (SPIDs) are a number that identifies a specific ISDN line. When you obtain ISDN service, your telephone company assigns a SPID to your line. Part of the initialization procedure is to configure your ISDN terminal adapter to use this SPID.

Most telephone companies in North America use the Generic SPID Format, which is a 14-digit number. The first 10 digits identify the telephone number, called the Directory Number (DN). The remaining four digits identify a particular ISDN device, in the case where multiple devices share the same Directory Number.

Each ISDN BRI line has two telephone numbers. Each of these telephone numbers has a SPID. Refer to "Adding SPIDs" on page 268.

square system

This is a basic office system where all telephones have all the lines assigned to individual indicator buttons. If the system has a receptionist, the receptionist answers the call, then calls or pages the person.

SSL

Secure Sockets Layer (SSL) is a security protocol that the Business Communications Manager uses to provide secure access to the system, including the Unified Manager. The access application recommended by Nortel is PuTTY SSH (by SSH inc.). This application replaces the Telnet access used on BCM 3.0 and previous versions of the Business Communications Manager. SSH is accessed through the **Install Clients** button on the first page of the Unified Manager. Refer to the *Management User Guide* for instructions about installing it and using it to access the system.

Start DN

This is the first directory number (DN) in the DN range on the system. This number is specified during system setup (Quick Start Wizard). Changing this number causes the system to perform a cold boot and all telephony programming would be lost. This number is assigned by default to DS30 02 first port. The Start DN defaults for a number of settings, such as Prime line, Control telephone, and Auxiliary ringer (ringing groups).

startup programming

When a Business Communications Manager system is first installed and powered up, you must perform Startup programming before you program other features. Startup initializes the system programming to defaults. Use the Quick Start Wizard to perform this process.

static IP address

A static IP address, or fixed IP address, is an IP address that is permanently assigned to a device on a network. The device retains the same IP address every time it connects to the network and is known to other devices on the network by that IP address.

station auxiliary power supply

See SAPS.

station media bay module

A computer module which provides access to telephone lines within the Business Communications Manager system. The 16-port digital station media bay module (DSM 16+) connects a maximum of 16 digital telephone telephones to the system. The 32-port digital station media bay module (DSM32+) connects a maximum of 32 digital telephone sets to the system. The Analog Station Media Bay Module (ASM8/ASM8+) connects a maximum of eight analog telephony devices to the system. The Unified Manager displays these lines as DN numbers. On systems running BCM 3.0 and newer software, DS30 bus 02 to 05 default to double density, which means that each of these DS30 buses can support up to 32 telephones. Legacy station modules can only support the first 16 DNs on each bus. The DSM16+ (two per bus), the DSM32+ (one per bus) can support the full 32 DNs. As well, the ASM8/ASM8+ can be configured on all four offsets, instead of just two. DS30 bus 06 and 07 default to single density, allowing them to support legacy Companion equipment. However, the system can be configured to Full Double Density (FDD), which means that these two bus blocks would also support 32 DNs, but would not longer support Companion.

station set test

A series of diagnostic tests for these components of a telephone: display, buttons, handset, speaker, and power.

subnet mask

A value used to route packets on TCP/IP networks. When the IP layer has to deliver a packet through an interface, it uses the destination address contained in the packet, together with the subnet mask of the interface to select an interface, and the next hop in that subnet.

Symbol

See NetVision.

synchronous

A synchronous signal is sourced from the same timing reference. A synchronous signal causes the interval between successive bits, characters, or events to remain constant or locked in to a specific clock frequency.

Synchronous Dynamic Random Access Memory (SDRAM)

Computer memory that stores data temporarily. SDRAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased when you restart or turn off the Business Communications Manager base unit.

system data

An option in the Set Copy function which refers to the programmable system settings that apply to all telephones and lines.

system speed dial code

This two or three-digit code (01 to 70 or 001 to 255) allows you to program speed dial codes for the entire system. Configure system speed dial codes under System speed dial. (Services, Telephony Services). These codes can be assigned to memory keys. Alpha-tagging: You can also use your speed dial list to provide name display for number-only analog CLID lines and target lines. When you configure an external number into a system speed dial, including a name, the system will display the name defined in the system speed dial list if an incoming call number matches a specified number of digits on the speed dial list. To take advantage of this feature, each telephone assigned with these lines must have CLID display allowed for the specific line in the DN record of that telephone.

system startup

See startup programming.

SWCA

The System-wide Call Appearance (SWCA) feature allows incoming calls to be parked on indicator buttons. Groups of telephones with the same programmed buttons can answer any call that gets parked on the SWCA buttons. When the call is parked on the button (the button is blinking), anyone in the group can answer the call. When the call has been answered, the indicator becomes solid. If the call is reparked, the call can be picked up by any other user in the group.

T

T1

Digital carrier system or line that carries data at 1.544 Mb/s. These lines can be used to connect systems on a private network. See also universal T1 Wide Area Network (UTWAN).

T700 telephone

This telephone has four programmable buttons, but no display, and is not available in all markets.

T7100 telephone

This telephone has a single line display and one programmable button without an indicator.

T7208 telephone

This telephone has a single-line display and eight programmable buttons with indicators.

T7316 telephone

The telephone has a two-line display with three display buttons, 16 programmable buttons with indicators, and eight programmable buttons without indicators. This telephone has a separate Mute button. It also has a headset button that allows the user to switch from handset to headset without unplugging the headset.

T7316E telephone

This telephone is based on the T7316 except that the T7316E has separate Mute and Handsfree keys under the dialpad and can support Key Indicator Modules (KIMs) to provide extra memory, line and hunt group appearance support (eKIM). The default button programming for this telephone is also different from the T7316. However, on systems running software earlier than BCM 3.5, this telephone acts like a T7316.

tandem calling

On a private network, a node can pass a call to one or more nodes on the private network, and then out to the PSTN of the appropriate remote node. This allows a business to reduce long-distance call charges by having the number appear as if it came from the local system. Each system must ensure that the appropriate remote access package is assigned to the lines used for the private network, as the system sees calls from outside the system, even if they come over private lines, as remote-access calls, and treats them accordingly.

tandem network

The private networking chapter describes how a tandem network is configured. A tandem network is a group of systems that are linked, each to one or two other systems. For instance if you have systems A, B, C, D, E and F, A is connected to B, B is connected to A and C, C is connected to B and D, and so on. In this case, for a call to move from A to F, which are not connected, the call routes through all the systems between the two.

TAPI

The Telephony Application Program Interface (TAPI) is a standard program interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources elsewhere in the world.

target line

These are internal system lines used only to answer incoming calls. These lines route calls to specific telephones. A target line routes a call according to digits it receives from an incoming trunk. Program target lines under Target lines (Services, Telephony Services, Lines). Assign target lines to telephones under DN XXX, Line access, Line assignment. (Services, Telephony Services, System DNs). The DID telephony profile automatically assigns target lines to all telephone DNs. This profile is picked when your system is first set up, when you program the Quick Start Wizard. You can configure target lines on more than one telephone, or multiple times on one telephone. As soon as one call is answered, the line becomes clear and can be picked up by a second telephone or a second line.

TAT

The Trunk Anti-tromboning (TAT) MCDN call-reroute feature works to find better routes during a transfer of an active call. This feature acts to prevent unnecessary tandeming and tromboning of trunks.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a language controlling communication between computers on the Internet.

TCP checks packets of information for errors, sends requests for re-transmission in the event of errors and returns multiple packets of a message into the original sequence when the message reaches its destination.

IP controls how packets are sent out over networks and has a packet addressing method that lets any computer on the Internet forward a packet to another computer that is a step or more nearer to the packet target.

TEI

A Terminal Endpoint Identifier (TEI) is a digit used to identify devices using an ISDN connection for D-channel packet service.

Telephony Application Program Interface

See TAPI.

Telnet

Telnet is a service that provides terminal-emulation capabilities for logging into the Business Communications Manager unit from a remote location. See also, SSL.

Terminal Endpoint Identifiers

See TEI.

token-ring

A token-ring is a network topology and data signaling scheme where a special data packet (called a token) is passed from one station to another along an electrical ring. A transmitting station takes possession of the token, transmits the data, then frees the token after the data has made a complete circuit of the electrical ring.

tone dial telephone

A push button telephone that emits DTMF tones.

TOS

The type of service field is located in the IP packet header and is used in DiffServ processing.

transfer

A feature that allows you to redirect a call to another telephone in your Business Communications Manager system, over a network or outside your system. (FEATURE 3)

transfer callback

If a transferred call is not answered after a specific number of rings, the call returns to the telephone that made the transfer. Transfer Callback does not apply to calls transferred externally. The number of rings is assigned under Timers, Transfer callback timeout. (Services, Telephony Services, General Settings)

Transmission Control Protocol/Internet Protocol

See TCP/IP

TRO

The trunk route optimization MCDN feature allows the call to find the most direct route through the private network to send a call between nodes. This function occurs during the initial alerting phase of a call.

tromboning

Tromboning refers to the way a transferred call uses lines on a network. If TAT is not present (no MCDN protocol is applied), a call made from a telephone on another system, and then transferred from the telephone to a third telephone on the first system can consume two network lines. By using TAT, the transferred call becomes an internal call once it is transferred, freeing up the network lines.

trunk

The physical connection between the Business Communications Manager system and the outside world using the public telephone system or another network system.

trunk answer

Use this feature to answer a call on any line that has an active Ringing service Service Mode, when that line does not appear on your telephone. Enable Trunk Answer under Ringing Service, Schedules, <schedule name>. (Services, Telephony Services, Scheduled Services)

trunk anti-tromboning

See TAT.

trunk media bay modules

A computer module which provides access to telecommunications trunks.

- The digital trunk media bay module (DTM) provides the connection between a standard digital PSTN T1 or PRI line and the Business Communications Manager system.
- The Caller ID trunk media bay module (CTM)/Global analog trunk module (GATM) provides the ability to access four (CTM/GATM4) or eight (CTM8/GATM8) analog Caller ID PSTN lines. The 4X16 module combines a CTM and a DSM to support four lines and 16 telephone connections on one module.
  The GATM, connects to the lines through an amphenol connector rather than an RJ connector like the CTM. The GATM also supports downloadable firmware (BCM 3.5 and newer software), depending on how the country DIP switches are set. Currently the GATM is only supported in North America, Australia, United Kingdom and Taiwan markets.
- The Basic Rate Interface media bay module (BRI) provides access to a maximum of eight BRI ISDN telephone lines, two per loop. Each loop on the BRI can be configured for either ISDN trunks or ISDN station devices.

trunk route optimization

See TRO.

Type of Service

See TOS.

U

UDP

Telephony dialing plan: Networked systems that connects using a Universal Dialing Plan (UDP) have system identification numbers and a location code that are unique to each system. Also, the Private DN length is the same on all systems. The system identification numbers and location codes are entered as a unique destination code that gets dialed out with whatever extension is being dialed. See also CDP.

Data protocol: User Datagram Protocol (UDP) is a protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.
Like the Transmission Control Protocol, UDP uses IP to actually transfer a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.
Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

Universal Dialing Plan

See UDP.

universal power supply

See UPS.

universal T1 Wide Area Network

See UTWAN.

unsupervised line

A line for which disconnect supervision is disabled. If an external caller hangs up, the system does not detect the disconnection and does not hang up its line. See disconnect supervision.

UPS

The Universal Power Supply is a third-party piece of hardware that attaches through the Business Communications Manager serial port to provide power backup in case of a power failure.

user data

User Data is an option in the Set Copy feature. User Data refers to the personal settings which are unique to a telephone, and which are not programmed for the system. You program User Data for each telephone.

These settings, for example, include Personal Speed Dial and the assignment of programmable memory buttons.

User Datagram Protocol

See UDP.

user filter

See restriction filters.

user preferences

These are settings that define a specific telephone and how the buttons on that telephone are programmed.

User Speed Dial

Two-digit codes (71-94) you program to dial external telephone numbers. You program User Speed Dial numbers for each telephone, and these numbers are available only at the telephone on which they are programmed.

UTWAN

The Universal T1 Wide Area Network (UTWAN) feature allows a Business Communications Manager system to use a Universal T1 digital line. A Universal T1 line is a digital line that allows some of the 24 lines to be used for standard telephony traffic and some of the lines to be used as a WAN connection. When you use a the UTWAN feature, a single DTM and a Universal T1 line can provide both your WAN connections and your telephone lines.

V

V.90

A data transmission standard used by the modem installed in the Business Communications Manager base unit. This standard allows data to be transmitted to the modem at 56 kbit/s and transmitted from the modem at 33 kbit/s.

voice call

Use this feature to make an announcement or begin a conversation through the speaker of another telephone in the system. The telephone you call does not ring. Instead, the person you call hears a beep and then your voice. Their telephone will beep periodically to remind the person that their microphone is open. (**FEATURE 66**) Some telephones cannot receive voice calls (7000, 7100, i2001, and portable handsets that do not have speakers). For these telephones, set all calls to ring on the telephone, so the user can be alerted that a voice call is occurring.

voice call deny

Use this feature to prevent your telephone from receiving voice call.

voice message center

A maximum of five external voice message centers can be programmed onto a Business Communications Manager. However, each telephone can only access one system. If the Business Communciations Manager is hosting voice messaging for other systems, remote call-in must be set up to accommodate external callers, even over a private MCDN network. Refer also to centralized voice mail and centralized auto attendant.

VoIP trunking

Voice over IP (VoIP) is the capability to deliver voice traffic using the IP network. VoIP is a set of facilities for managing the delivery of voice information using the IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

In addition to IP, VoIP also uses the real-time protocol (RTP) to help ensure that packets get delivered in a timely way.

The Business Communications Manager provides VoIP trunks that access a gateway on the system. The gateway receives packetized voice transmissions from users within the company and then routes them to a specific destination in another part of its intranet (local area or wide area network). VoIP trunks can be used by both digital and IP telephones. These trunks can also supply the MCDN trunking features such as TAT, TRO and ICCL. IP telephone and trunk programming is dealt with in the *IP Telephony Configuration Guide*.

W

wait for dial tone

A feature that causes a sequence of numbers to pause until dial tone is present on the line before continuing to dial. The Wait for dial tone symbol uses two of the 24 spaces in a dialing sequence.

WAN

The Wide Area Network is a collection of computers or Business Communications Manager base units connected or networked to each other over long distances, normally using common carrier facilities.

web cache

A web cache is a server or collection of servers that store copies of Internet content. The web cache server can be either located on the LAN where the clients it serves are also located, or it can be embedded within the enterprise WAN or at the client's Internet Service Provider (ISP).

web proxy

A web proxy, or HTTP proxy, is a server that acts on behalf of the requester of pages from an HTTP server and the Internet. You must bypass this server to correctly use the Business Communications Manager.

WFQ

Weighted Fair Queuing (WFQ) is a queuing method that allows low volume traffic such as Telnet to be given priority and interactive traffic receives higher priority than batch transfers. Also, high bandwidth usage traffic such as batch file transfer traffic gets equal priority with other high bandwidth use traffic.

Wide Area Network

See WAN.

wild card

In the Unified Manager dialing rules, the character A is used to represent any digit from 0 to 9 instead of an asterisk (*). For instance, you may define a destination code of 062A to represent a range of destination codes that all use the same route and absorb length, with different dial-out digits.

wizards

Wizards are applications that provide a quick way of performing a task. The Unified Manager has wizards for system setup, configuring telephones and telephone numbering, changing the network settings, and for configuring the DECT system.

Index

Symbols

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z