



BCM 4.0 Administration Guide

BCM 4.0 Business Communications Manager

Document Status: **Standard**

Document Version: **03.02**

Part Code: **N0060598**

Date: **October 2006**

Copyright © Nortel Networks Limited 2006

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

*Nortel, Nortel (Logo), the Globemark, and This is the way, This is Nortel (Design mark) are trademarks of Nortel Networks.

*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

*Citrix is a registered trademark of Citrix Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Task List

Getting started with BCM	15
Overview of BCM Administration	23
BCM Management Environment	29
BCM Security Policies and Accounts and Privileges	73
To set system access control policies	79
To set credential complexity	79
To set lockout policy for failed logins	80
To set password expiry policy	81
To set password history	81
To set the authentication method	82
To configure an authentication server in Element Manager	82
To set the idle session timeout	86
To upload a Web Server Certificate	86
To transfer an SSH Key-Pair	87
To add a new user account	88
To modify a user account	89
To add callback for a dial-up user	90
To add Telset access for a user	90
To delete a user account	91
To change a user's password	91
To change the current user's password	91
To create a group	92
To delete a group	92
To modify group privileges	93
To add a user account to a group	93
To delete a user account from a group	93
To release a locked-out user	94
To enable or disable an account immediately	95
To enable or disable an account on a timed basis	95
To enable/disable exclusive access	96
Using the BCM Hardware Inventory	125
To view or update information about the BCM main chassis	127
To view or update expansion unit information	128
To view or update other information about the media bay modules	129
To view or update other information about the BCM main unit	129
To view information about PCI cards	131
To view information about attached devices	132
To view additional information about the BCM hardware inventory	134
Managing BCM with SNMP	135
To configure the BCM SNMP agent	136
To configure BCM SNMP settings	137
To add an SNMP manager to the BCM SNMP manager list	138

To delete an SNMP manager	138
To delete a community string value	140
To configure pass phrases for a service access point	141
To view details associated with a service access point	142
To delete a service access point	142
To modify a service access point	142
To modify a trap destination	144
To delete a trap destination	145
Using the BCM Fault Management System	147
To view an alarm	151
To acknowledge an alarm	151
To clear the alarm log	151
To include or omit acknowledged alarms in the Alarm Banner	153
To specify the alarm set	154
To clear an alarm from the alarm set	154
To reset the Status LED	155
To enable or disable SNMP traps for alarms	156
To enable or disable viewing of selected alarms in the Alarms table	156
To test an alarm	156
Using the BCM Service Management System	241
To view details about services	244
To restart a service	244
Monitoring BCM Status and Metrics	245
To configure monitoring mode	248
To configure logging attributes	249
To view the QoS monitoring information	250
To refresh the QoS monitor data	251
To access UPS Status	251
To access the NTP Metrics	254
To view Interface Metrics	255
To monitor Disk Mirroring	258
To view global QoS metrics	259
To view per interface QoS metrics	260
To view per account QoS metrics	262
To view Trunk Module status	266
To disable or enable a B channel setting	268
To provision a PRI B-channel	269
To enable the internal CSU	270
To check the performance statistics	270
To check the CSU alarms	271
To check carrier failure alarms	271
To check bipolar violations	271
To check short-term alarms	272
To check defects	272
To view CSU Alarm History	272
To access the CbC limit metrics	273
To access the Hunt Group metrics	275
To access PSTN Fallback metrics	276
To configure PVQM threshold settings	278

To access PVQM metrics	281
BCM Utilities	285
To install BCM Monitor separately from BCM Element Manager	286
To remove BCM Monitor	286
To start BCM Monitor without the BCM Element Manager.....	287
To start BCM Monitor from the BCM Element Manager	287
To connect to a different BCM	288
To configure static snapshot settings	289
To save a static snapshot.....	291
To configure dynamic snapshot settings	292
To disable monitoring of UIP messages.....	299
To log UIP data.....	299
To view UIP log files	300
To configure timeout settings	300
To expand a UIP message	301
To clear UIP message details.....	301
To view all lines	302
To view the date and time of minimum and maximum values.....	304
To reset the minimum and maximum values for a statistic.....	305
To ping a device	306
To perform a trace route.....	307
To reboot the BCM	309
To shut down the BCM	309
To perform a warm reset of BCM telephony services	309
To perform a cold reset of BCM telephony services.....	310
To set Release Reasons	311
To use data networking utilities	312
Backing Up and Restoring BCM Data	315
To perform an immediate backup to the BCM.....	320
To perform an immediate backup to your personal computer	321
To perform an immediate backup to a network folder	322
To perform an immediate backup to a USB storage device	323
To perform an immediate backup to an FTP server	324
To perform an immediate backup to an SFTP server.....	325
To view scheduled backups	326
To perform a scheduled backup to the BCM	327
To perform a scheduled backup to a network folder	328
To perform a scheduled backup to a USB storage device	330
To perform a scheduled backup to an FTP server	331
To perform a scheduled backup to an SFTP server.....	332
To modify a scheduled backup.....	334
To delete a backup schedule.....	334
To restore data from the BCM	337
To restore data from your personal computer	338
To restore data from a network folder	339
To restore data from a USB storage device	340
To restore data from an FTP server	341
To restore data from an SFTP server.....	342
To restore the factory configuration.....	343

Managing BCM Logs	345
To perform an immediate log transfer to a USB storage device.....	348
To perform an immediate log transfer to your personal computer.....	350
To perform an immediate log transfer to a network folder.....	351
To perform an immediate log transfer to an FTP server.....	352
To perform an immediate log transfer to an SFTP server.....	353
To perform a scheduled log transfer to a storage location.....	354
To modify a scheduled log transfer.....	356
To delete a scheduled log transfer.....	357
To use the BCM Web Page to transfer log files to other destinations.....	359
To extract log files using the BCM Element Manager.....	361
To specify retrieval criteria.....	365
To filter information in the Retrieval Results table.....	366
To view log details for multiple log records.....	366
Managing BCM Software Updates	369
To obtain updates from the Nortel Technical Support Web page.....	369
To view details about software updates in progress.....	371
To apply an update from your personal computer.....	373
To apply a software update from a USB storage device.....	374
To apply an update from a shared folder.....	375
To apply an update from an FTP server.....	376
To apply an update from an HTTP server.....	377
To create a scheduled software update.....	379
To modify a scheduled software update.....	382
To delete a scheduled software update.....	383
To view the software update history.....	383
To remove a software update.....	385
To view the BCM software inventory.....	386
Accounting Management	387
Management Information Bases	389
To access MIB files from the BCM Web Page.....	391
To access MIB files from the Nortel Customer Service Site.....	391

Contents

Chapter 1	
Getting started with BCM	15
About this guide	15
Purpose	15
Organization	16
Audience	17
Acronyms	17
Symbols and conventions used in this guide	19
Related publications	20
How to get Help	21
Chapter 2	
Overview of BCM Administration	23
About BCM	23
Key components of the BCM system	23
BCM Management Model	25
BCM interfaces	26
LAN	27
WAN	28
Chapter 3	
BCM Management Environment	29
BCM web page	29
BCM Management Environment and Applications	31
Managing BCM with Element Manager	31
Managing BCM with Telset administration	32
Managing BCM Voicemail and ContactCenter: CallPilot Manager	32
Managing IVR for BCM 4.0	32
Managing Digital Mobility for BCM 4.0	32
Programming telephone sets: Desktop Assistant portfolio	33
Performing initialization: Startup Profile	33
Monitoring BCM: BCM Monitor	34
Managing BCM with the serial interface	34
Managing BCM remotely with SNMP	34
BCM Element Manager	34
BCM Element Manager setup	35
Element Manager window attributes	40
Element Manager panels	50
Effective use of BCM Element Manager	50

Element Manager data features	51
BCM Element Manager application logging	61
BCM integrated launch of related applications	61
BCM feature licensing	63
BCM Help system	64
Menu bar Help	64
Field-level Help	66
Context-sensitive Help	66
BCM common file input/output processes	67
Comparison of data repositories	68

Chapter 4

BCM Security Policies and Accounts and Privileges 73

Security Policies panel	73
Configuring system security policies	78
Entry Policy tab	78
Local Authentication Policy tab	78
Authentication Service Policy tab	78
Session Management Policy tab	78
SSL and SSH Policy tab	79
Setting system access control policies	79
Setting credential complexity	79
Setting lockout policy for failed logins	80
Setting password expiry policy	81
Setting password history policy	81
Setting the authentication method	81
Configuring an authentication server	82
Setting the idle session timeout	86
Uploading a Web Server Certificate	86
Transferring an SSH Key-Pair	87
Configuring user accounts, user groups and privileges	87
Adding a new user account	88
Modifying a user account	89
Adding callback for a dial-up user	90
Adding Telset access for a user	90
Deleting a user account	90
Changing a user's password	91
Changing the current user's password	91
Creating a group	92
Deleting a group	92
Modifying group privileges	92
Adding a user account to a group	93

Deleting a user account from a group	93
Re-enable a locked-out user	94
Enabling and disabling an account	95
Enabling and disabling exclusive access	96
User account and user group management fundamentals	96
User accounts	96
Default passwords	98
Default groups	98
Default access privileges excluding set-based privileges	100
Telset access security	108
Telset group access privileges	109
Blocking user accounts	110
Accounts and Privileges panel	110
Current Account	111
View by Accounts	113
View by Account: General	115
View by Account: Remote Access	115
View by Account: History	116
View by Account: Group Membership	116
View by Groups	117
View by Groups: General	117
View by Groups: Members	119
BCM security fundamentals	119
Secure network protocols and encryption	120
Security audits	121
System security considerations	121
Firewalls	122
Security certificate	123
Site authentication	123
Chapter 5	
Using the BCM Hardware Inventory	125
About the BCM Hardware Inventory	125
Viewing and updating information about the BCM system	126
Viewing and updating information about the BCM main unit	126
Viewing and updating BCM expansion unit information	127
Viewing and updating information about media bay modules	128
Viewing and updating other information about the BCM system	129
Viewing information about PCI cards	130
Viewing information about devices	131
Viewing additional information about the BCM hardware inventory	132
.....	134

Chapter 6	
Managing BCM with SNMP	135
Overview of BCM support for SNMP	135
Configuring SNMP settings	136
Configuring general SNMP settings	136
Configuring SNMP community strings	139
Configuring service access points	140
Configuring SNMP trap destinations	143
Viewing and modifying SNMP trap destinations	144
Auto-SNMP dial-out	145
Alarm severity levels	146
Chapter 7	
Using the BCM Fault Management System	147
Overview of BCM fault management	147
About BCM alarms	148
Alarms and log files	149
Alarm severities	149
Administering alarms	150
Using the Alarms Panel	150
Using the Alarm Banner	152
Using the alarm set	153
Alarms and LEDs	154
Using SNMP traps	155
Configuring alarm settings	155
List of BCM alarms	157
Chapter 8	
Using the BCM Service Management System	241
Overview of the BCM service management system	241
BCM services	241
Starting, stopping, and restarting services	244
Chapter 9	
Monitoring BCM Status and Metrics	245
About the system status	245
LED Status	245
QoS Monitor	247
UPS Status	251
NTP Metrics	253
Interface Metrics	255
Disk Mirroring	257
QoS Metrics	258

Telephony Metrics	265
Trunk Module Metrics	266
Viewing Performance History information	268
Viewing D-Channel information	268
Disabling or enabling a B channel setting	268
Provisioning a PRI B-channel	268
Trunk Module CSU statistics	269
Enabling the internal CSU	270
Checking trunk module alarms	271
CbC limit metrics	272
Hunt Group Metrics	274
PSTN Fallback Metrics	276
Proactive Voice Quality Management	277
Chapter 10	
BCM Utilities	285
About BCM Monitor	285
Installing BCM Monitor	286
Connecting to a BCM system	287
Using BCM Monitor to analyze system status	289
Static snapshots	289
Dynamic snapshots	291
BCM Info tab	294
Media Card tab	295
Voice Ports tab	296
IP Devices tab	296
RTP Sessions tab	297
UIP tab	298
Line Monitor tab	301
Usage Indicators tab	302
Using statistical values	304
Ping	305
Trace Route	307
Reset	308
Diagnostic settings	310
Data Networking Utilities	312
Chapter 11	
Backing Up and Restoring BCM Data	315
Overview of backing up and restoring data	315
Backup and restore options	315
Viewing backup and restore activity	316

About backups	316
BCM backup file	317
Backup destinations	318
Performing immediate backups	319
Performing an immediate backup to the BCM	320
Viewing and performing scheduled backups	325
Modifying and deleting scheduled backups	333
Restoring BCM system data	335
Restore options	335
Effects on the system	336
Chapter 12	
Managing BCM Logs	345
Overview of BCM logs	345
Log types	345
Overview of transferring and extracting log files	347
Transferring log files using the BCM Element Manager	347
Performing immediate log archive transfers	348
Performing scheduled log transfers	354
Transferring log files using the BCM Web page	357
Extracting log files	361
Viewing log files using the Log Browser	363
Retrieval Results area	365
Log Details area	366
Viewing log files using other applications	367
Chapter 13	
Managing BCM Software Updates	369
Overview of BCM software updates	369
Obtaining software updates	369
Viewing software updates in progress	370
Applying software updates	371
Creating and modifying scheduled software updates	378
Viewing a history of software updates	383
Removing software updates	384
Viewing the inventory of BCM software	385
Chapter 14	
Accounting Management	387
Overview of accounting management	387
About Call Detail Recording	387
Using Call Detail Recording	388
CDR Toolkit	388

Appendix A	
Management Information Bases	389
About SNMP MIBs	389
MIB file descriptions	389
Accessing, compiling, and installing MIB files	391
Small Site MIB	392
Small Site Event MIB	393

Chapter 1

Getting started with BCM

This section contains information on the following topics:

- [“About this guide” on page 15](#)
- [“Audience” on page 17](#)
- [“Acronyms” on page 17](#)
- [“Symbols and conventions used in this guide” on page 19](#)
- [“Related publications” on page 20](#)
- [“How to get Help” on page 21](#)

About this guide

The *BCM 4.0 Administration Guide* describes how to manage and maintain BCM systems at the Release 4.0 level using BCM Element Manager. In this guide, BCM Release 4.0 refers to BCM 200, BCM 400, and BCM 1000 main units that are running the BCM Release 4.0 software. The BCM product portfolio also includes the BCM50, which is described in a separate guide. For information about managing the BCM50, see the *BCM50 Administration Guide*.

Purpose

The concepts, operations, and tasks described in the guide relate to the FCAPS (fault, configuration, accounting, performance, and security) management features of the BCM system. This guide also describes additional administrative tasks, such as log management, backups, software updates, monitoring, and inventory management. Use the BCM Element Manager to perform these administrative tasks.

In brief, the information in this guide explains:

- Network structure and concepts
- Network management tools
- Fault management & monitoring
- Performance management
- Security administration
- Backup management
- Software updates
- Inventory management

Organization

This guide is organized for easy access to information that explains the administrative concepts, operations and procedures associated with using the BCM management application.

The tasks described in this guide assume that you are using the Element Manager with full administrative privileges. If you do not have full administrative privileges, you may see only a subset of the tasks and panels described in this guide.

Table 1 BCM Management Guide organization

Chapter	Contents
Chapter 2, "Overview of BCM Administration"	This chapter introduces network-level management concepts and techniques.
Chapter 3, "BCM Management Environment"	This chapter contains information on the different tools available to manage your BCM. It also describes the new Element Manager application in detail.
Chapter 4, "BCM Security Policies and Accounts and Privileges"	This chapter describes Security Policies and Accounts and Privileges, which allow you to establish system-wide security policies and maintain system access security using settings on Element Manager.
Chapter 5, "Using the BCM Hardware Inventory"	This chapter describes how to use the Hardware Inventory, which displays information about the BCM system, such as connected expansion units, populated Media Bay Modules (MBMs) and attached telephone devices.
Chapter 6, "Managing BCM with SNMP"	This chapter describes the management of the BCM using SNMP. SNMP is a set of protocols for managing complex networks. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and provide this data to SNMP requesters.
Chapter 7, "Using the BCM Fault Management System"	This chapter contains information about managing alarms generated by the system and administering alarm settings.
Chapter 8, "Using the BCM Service Management System"	This chapter describes how to use Element Manager to view and administer the services that run on the system.
Chapter 9, "Monitoring BCM Status and Metrics"	This chapter describes how to use Element Manager to view detailed information about the performance of the system and of system resources.
Chapter 10, "BCM Utilities"	This chapter contains information about the utilities that are part of the BCM Element Manager. Several utilities are provided to allow partners and customers to monitor and analyze the system.
Chapter 11, "Backing Up and Restoring BCM Data"	This chapter provides information about how to back up and restore data from the system.
Chapter 12, "Managing BCM Logs"	This chapter contains information about viewing and managing log files generated by the BCM.
Chapter 13, "Managing BCM Software Updates"	This chapter contains information about managing software updates.

Table 1 BCM Management Guide organization

Chapter	Contents
Chapter 14, "Accounting Management"	This chapter describes the management of accounts in the BCM. Account management uses the Call Detail Recording (CDR) application to record call activity. Each time a telephone call is made to or from a BCM, detailed information about the call can be captured in a CDR file.
Appendix A, "Management Information Bases"	This appendix contains information about how to install and use Management Information Bases (MIBs) if you use SNMP to manage your system.

Audience

The *BCM 4.0 Administration Guide* is directed to network administrators responsible for maintaining BCM networks. This guide is also useful for network operations center (NOC) personnel supporting a BCM managed services solution. To use this guide, you must:

- be an authorized BCM administrator within your organization
- know basic Nortel BCM terminology
- be knowledgeable about telephony and IP networking technology

Acronyms

The following is a list of acronyms used in this guide.

Table 1 List of acronyms

Acronym	Description
3DES	Triple Data Encryption Standard
AES	Analog Encryption Standard
AIS	Alarm Indication Signal
BCM	Business Communications Manager
BRI	Basic Rate Interface
CbC	Call by Call
CDR	Call Detail Recording
CFA	Carrier Failure Alarms
CLID	Calling Line Identification
CPE	Customer Premises Equipment
CSU	Channel Service Unit
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DN	Directory Number
DNIS	Dialed Number Identification Service

Table 1 List of acronyms

Acronym	Description
DTM	Digital Trunk Module
ES	Errored Seconds
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IVR	Interactive Voice Response
ISDN	Integrated Switched Digital Network
LAN	Local Area Network
MBM	Media Bay Module
MIB	Management Information Base
MGS	Media Gateway Server
MOS	Mean Opinion Score
MPS	Media Path Server
NAT	Network Address Translation
NCM	Network Configuration Manager
NOC	Network Operations Center
NTP	Network Time Protocol
OOF	Out of Frame
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
PVQM	Proactive Voice Quality Monitoring
QoS	Quality of Service
RAI	Remote Alarm Indication
RTP	Real-time Transport Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
UAS	Unavailable Seconds
UPS	Universal Power Supply
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

Symbols and conventions used in this guide

These symbols are used to highlight critical information for the BCM system:



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



Danger: Alerts you to conditions where you can get an electrical shock.



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



Note: A Note alerts you to important information.



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



Security note: 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.



Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.



Warning: Alerts you to remove the BCM main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

These conventions and symbols are used to represent the Business Series Terminal display and dialpad.

Convention	Example	Used for
Word in a special font (shown in the top line of the display)	Pswd:	Command line prompts on display telephones.
Underlined word in capital letters (shown in the bottom line of a two line display telephone)	<u>PLAY</u>	Display option. Available on two line display telephones. Press the button directly below the option on the display to proceed.
Dialpad buttons	#	Buttons you press on the dialpad to select a particular option.

These text conventions are used in this guide to indicate the information described:

Convention	Description
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the info command. Example: Enter show ip {alerts routes} .
<i>italic text</i>	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.

Related publications

Related publications are listed below. To locate specific information, you can refer to the *Master Index of BCM 4.0 Library*.

BCM 4.0 Installation Checklist and Quick Start Guide (N0060602)

BCM1000 BCM 3.7 Installation and Maintenance Guide (N0008587 01)

BCM 4.0 for BCM1000 Installation and Maintenance Guide Addendum (N0060603)

BCM200/400 BCM 4.0 Installation and Maintenance Guide (N0060612)

Keycode Installation Guide (N0060625)

BCM 4.0 Device Configuration Guide (N0060600)

BCM 4.0 Networking Configuration Guide (N0060606)

BCM 4.0 Telset Administration Guide (N0060610)

BCM 4.0 Telephony Device Installation Guide (N0060609)

CallPilot Telephone Administration Guide (N0060618)

CallPilot Contact Center Telephone Administration Guide (N0060615)

IVR Installation and Configuration Guide (N0060624)

BCM 4.0 LAN CTE Configuration Guide (N0060604)

BCM 4.0 Call Detail Recording System Administration Guide (N0060599)

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

<http://www.nortel.com/support>

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

<http://www.nortel.com/callus>

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

<http://www.nortel.com/erc>

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 2

Overview of BCM Administration

The BCM Administration Guide describes the tools available with which to administer, or manage BCM systems. This section is an introduction to the BCM system and its management model.

The administration overview information is divided into three categories:

- About BCM
- BCM Management Model
- BCM Management Interfaces
- BCM Administration Guide overview

About BCM

The BCM system provides private network and telephony management capability to small and medium-sized businesses.

The BCM system:

- integrates voice and data capabilities, IP Telephony gateway functions, and data-routing features into a single telephony system
- enables you to create and provide telephony applications for use in a business environment

BCM Release 4.0 runs on the same hardware platforms as BCM Release 3.x, including BCM 200, BCM 400, and BCM 1000 systems. A major difference between Release 3.x and Release 4.0 is that BCM 3.x software runs on an embedded NT operating system, while BCM 4.0 software runs on the Nortel carrier-grade Linux operating system. An upgrade from a BCM 3.x system to a BCM 4.0 system migrates all of the services and applications of the BCM 3.x systems onto the carrier-grade Linux operating system.

Another important difference between BCM 3.x systems and BCM 4.0 systems is the management environment. Unified Manager was the primary management application for BCM 3.x systems, and BCM Element Manager is the primary management application for BCM 4.0 systems. The BCM Element Manager encompasses not only telephony programming, but also backup management, software update management, and log management, which are all separate utilities in the BCM 3.x management environment. For more information about the BCM Element Manager, see [“BCM Management Environment” on page 29](#).

Key components of the BCM system

The BCM system includes the following key components:

- hardware
- applications

BCM hardware

BCM 4.0 includes the following key elements:

- BCM 200 main unit
- BCM 400 main unit
- BCM 1000 main unit
- BCM expansion unit (compatible with BCM 400 main unit)
- BCM 400 expansion gateway
- BCM media bay modules (MBM):
 - Analog direct inward dialing (ADID)
 - BRIM
 - CTM4/CTM8
 - DTM
 - GATM4/GATM8
 - 4x16
 - 8 x 16
 - ASM8
 - ASM8+, GASM
 - DSM16+/DSM32+
 - DDIM
 - FEM

All of the BCM main units provide call processing and data networking functions. They also provide connections for telephones, as well as LAN and WAN connections. You can install MBMs to provide connections for Public Switched Telephone Network (PSTN) lines. For detailed information about the main units, see the *BCM200/400 BCM 4.0 Installation and Maintenance Guide* (N0060612) and the *BCM 4.0 for BCM1000 Installation and Maintenance Guide Addendum* (N0060603).

BCM applications

BCM 4.0 also supports many of the high-value applications provided on the existing BCM systems.

You enable applications by entering the appropriate keycodes (no additional hardware is required). Some applications are:

- Voice Messaging for standard voicemail and autoattendant features
- Unified Messaging providing integrated voicemail management between voicemail and common email applications
- Fax Suite providing support for attached analog fax devices
- Voice Networking features
- LAN CTE
- IVR

BCM Management Model

Whether BCM is being installed as a standalone element, is part of a network of many BCMs, or is part of a network encompassing both BCMs and other devices, it is necessary to be able to perform a range of administrative tasks to keep the system (or systems) providing the services which they were deployed to provide.

The individual or organization responsible for performing the administration of the system needs to be able to do some or all of the following types of tasks:

- monitor to validate that the system is healthy. For example, power is available, services are running, CPU and memory are within a normal operating envelope
- monitor for fault conditions
- monitor link status and utilization
- system programming is consistent with the requirements of the services
- backups are being kept of the configuration
- review logs of operational information
- retrieve and view logs containing diagnostic information in the event of a system issue
- manage system inventory
- manage software updates
- make changes to the system configuration to change service definitions or add users including adding new features through the application of keycodes

The descriptions and procedures in this guide will assist the administrator in performing these tasks.

The following management model demonstrates how BCM manageability is achieved by breaking the management functions into layers.

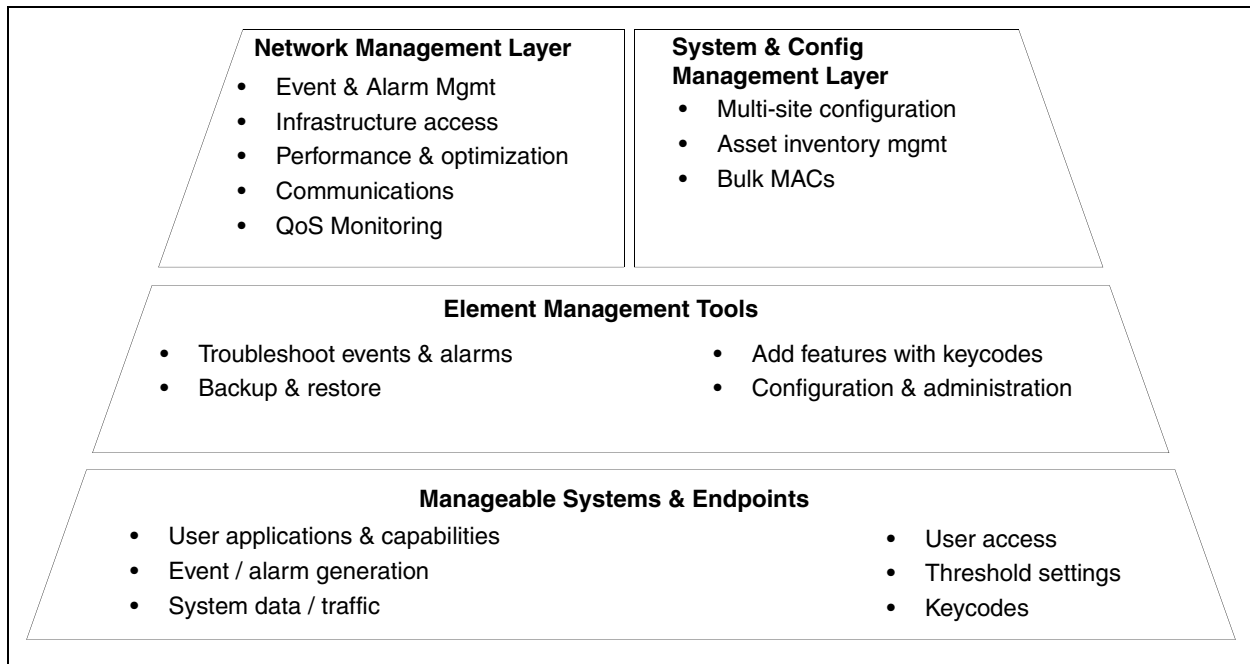
At the base of the model is the element itself. In order to be a manageable system, the element must provide not only the ability to configure services, but must also regulate access to the system by administrative users, generate alarms in the event of issues, support the easy addition of new features through the application of keycodes, provide a means for making a backup of the configured data, and other administrative functions.

The management tools at the next layer provide a user interface to control these functions for a selected BCM device. The primary management application for BCM 4.0 is the BCM Element Manager, complemented by other management applications as explained in [“BCM Management Environment and Applications” on page 31](#). For BCM releases prior to 4.0, the management application is Unified Manager.

If the BCM is one of a number of elements in a network, network management tools at the network management layer facilitate monitoring and management across the network. Nortel provided tools such as Optivity NMS for network monitoring and third party tools supporting multi-vendor networks can only deliver their value if the managed element itself has provided for the right functions at the manageable systems layer.

Also at the network layer, system and configuration management tools can provide support for tasks such as bulk distribution of selected configuration information, network wide inventory management and network wide backup management. The Network Configuration Manager (NCM) server-based management application provides these and other capabilities for managing a network of up to 2000 BCMs. For more information about NCM, please consult the NCM User documentation.

Figure 1 BCM network management model



BCM interfaces

The BCM network can be distributed geographically across different sites. The network administrator must be able to remotely access each BCM in the network. BCM offers alternatives for connecting to the BCM devices (see [Figure 2](#) and [Figure 3](#)) depending on the network configuration and telephony resources available with a given system.

Figure 2 BCM 200 ports and connectors

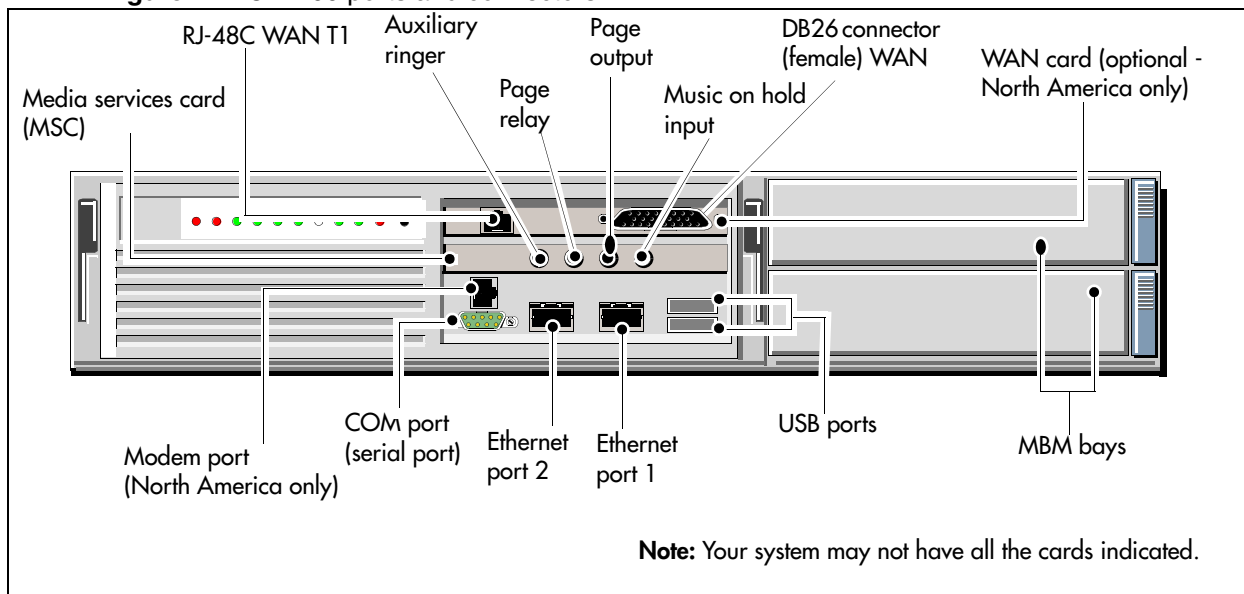
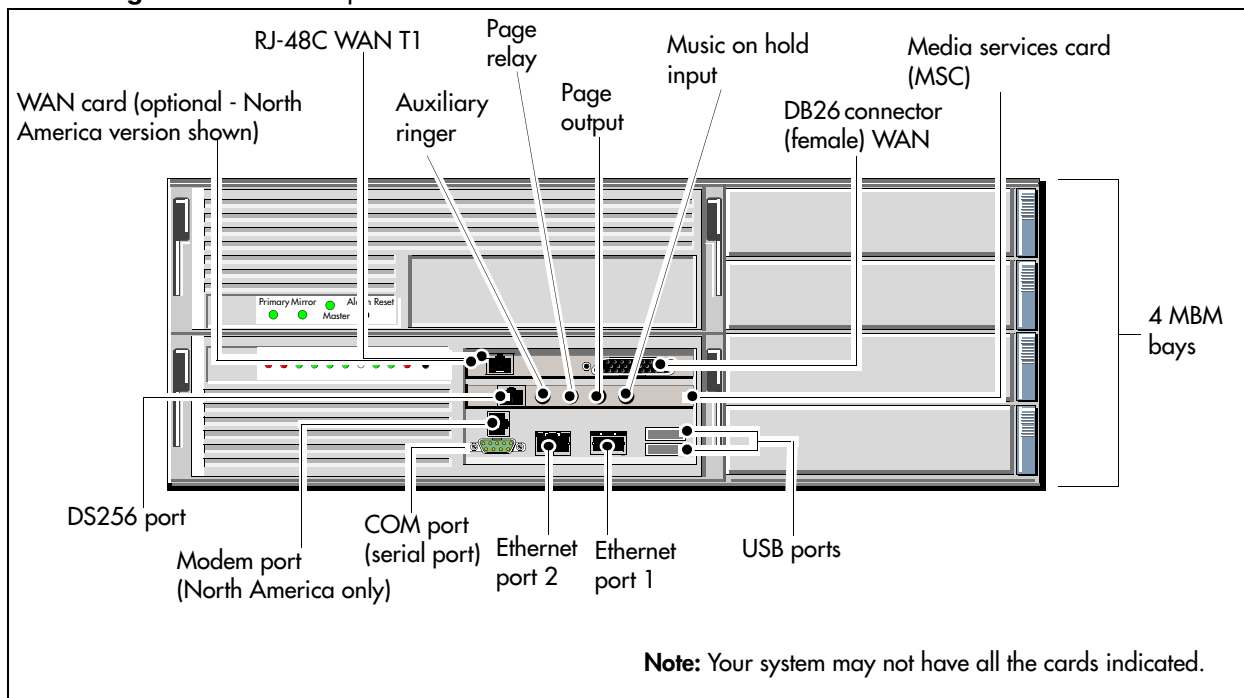


Figure 3 BCM 400 ports and connectors



LAN

A Local Area Network (LAN) is a communications network that connects workstations and computers within a confined geographical area. Often the customer LAN has access to a router, forming a connection to the Internet.

A network administrator can connect to and manage a BCM via an IP over LAN interface. If the administrator is accessing the BCM system from an external network, then a connectivity path would need to be provided from the corporate LAN network to the customer's WAN network or to the customer's ISP provider over another device such as a router elsewhere on the customer's premises.

Dialup

The modem supports callback for management user access to the BCM. It can be used to support auto-dialout on SNMP traps, as well as automated sending of Call Detail Records (CDR) to a remote CDR collection point.

Due to modest dialup speeds, the administrator will find that the Element Manager panels take longer to load than if the Element Manager is directly connected.

Configuration backups can be less than 1 Mbyte in size, however if voicemail greetings and messages are included they could grow considerably larger. If the performance being realized over the modem does not meet expectations, the administrator may choose to run backups to the local hard drive or a USB memory device.

For more information on modem configuration see the *BCM 4.0 Device Configuration Guide* (N0060600).

WAN

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as state or country. A WAN usually consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system, or can be connected through private leased lines.

Several protocols are used in the day to day management of a network of BCMs. These include:

- **SNMP** (simple network management protocol): Simple Network Management Protocol is the Internet standard protocol for network management software. It monitors devices on the network, and gathers device performance data for management information (data)bases (“MIB”).
- **HTTPS**: A secure version of HTTP implemented using the secure sockets layer, SSL, transmitting your communications in an encrypted form. HTTPS is used between the BCM Element Manager and the BCM.
- **FTP** (file transfer protocol): FTP is a protocol used to transfer files over a TCP/IP network (Internet, Unix). FTP allows you to log into FTP servers, list directories, and copy files from other workstations.
- **SSH** and other protocols are also used for certain tasks. These are covered in the section “Secure Network Protocols and Encryption” in the BCM Security chapter.

Chapter 3

BCM Management Environment

This chapter contains information on the different tools available for managing your BCM system. It also describes the BCM Element Manager application in detail. It includes the following sections:

- [“BCM web page”](#)
- [“BCM Management Environment and Applications” on page 31](#)
- [“BCM Element Manager”](#)
- [“BCM feature licensing” on page 63](#)
- [“BCM Help system” on page 64](#)
- [“BCM common file input/output processes” on page 67](#)

BCM web page

The BCM web page facilitates the download of applications, documentation, and other information necessary for running the BCM and its services. You connect to the BCM web page by typing the IP address of your BCM device into your browser. A valid user name and password are required in order to access the web page.

There are two default user accounts configured on the BCM at time of shipping: the nnadmin user account and the nnguest user account. See [Chapter 4, “BCM Security Policies and Accounts and Privileges,” on page 73](#) for information on user accounts and security.

You can choose to make the nnguest account available to general users. This account can be configured to provide users with access to download end-user documents and applications that they require from the BCM web page.

The BCM web page contains the following links:

- User Applications - Applications listed in Table 2 that are available to the end users of the BCM.
- User Documentation - Documentation for the BCM end users to explain the end-user applications and BCM-specific tasks.
- Administrator Applications - Applications listed in Table 2 that are available to BCM administrators.

- Administrator Documentation - Documentation for the BCM administrators to explain the BCM management applications and BCM management tasks.
- Nortel's Contact Information - A list of Nortel contact numbers.

Table 2 Applications available on BCM web page

Application	User	Administrator
Administrator Management Tools		
BCM Element Manager	N	Y
Desktop Assistant Pro AE	N	Y
NCM for BCM	N	Y*
BCM Monitor	N	Y
CDR Clients	N	Y
BCM MIBs	N	Y
Radius Dictionary	N	Y
SSH Client (PuTTY)	N	Y
Retrieve Logs	N	Y
Contact Center Applications		
Reporting for Contact Center	N	Y
Multimedia Contact Center	N	Y
IP View Softboard	N	Y
Digital Mobility Tools		
Digital Mobility Controller	N	Y
Digital Mobility Service Tool	N	Y
Templates		
Startup Profile Template	N	Y
Factory Default Programming Record	N	Y
User Applications		
Desktop Assistant	Y	Y
Desktop Assistant Pro	Y	Y
Unified Messaging	Y	Y
Personal Call Manager	Y	Y
LAN CTE Client	Y	Y
IP Software Phone 2050	Y	Y
Mobile Voice Client 2050	Y	Y
Nortel VPN Client	Y	*

* Provides a URL that can be accessed to download the BCM client for NCM.

Administrator documentation is provided in English. User documentation is provided in the following languages:

- English
- French
- Danish
- German
- Spanish
- Dutch
- Italian
- Norwegian
- Swedish
- Portuguese

BCM Management Environment and Applications

A number of tools are available to help manage your BCM. This section describes the following tools:

- [“Managing BCM with Element Manager”](#)
- [“Managing BCM with Terset administration” on page 32](#)
- [“Managing BCM Voicemail and ContactCenter: CallPilot Manager” on page 32](#)
- [“Managing IVR for BCM 4.0” on page 32](#)
- [“Managing Digital Mobility for BCM 4.0” on page 32](#)
- [“Programming telephone sets: Desktop Assistant portfolio” on page 33](#)
- [“Performing initialization: Startup Profile” on page 33](#)
- [“Monitoring BCM: BCM Monitor” on page 34](#)
- [“Managing BCM remotely with SNMP” on page 34](#)

Managing BCM with Element Manager

The primary management application for configuring and administering the BCM 4.0 system is the BCM Element Manager. The BCM Element Manager is a client-based management application that runs on a Windows computer, or on a Citrix server. The Element Manager allows for connection to BCM devices over an IP network. It is used to configure, administer, and monitor BCM devices. See [“BCM Element Manager” on page 34](#) for more information about the BCM Element Manager. Unified Manager cannot be used to manage a BCM 4.0 system.

You can download the BCM Element Manager application from the BCM web page. See [“BCM web page” on page 29](#) for a description of the BCM web page. The procedure [“Installing BCM Element Manager” on page 35](#) provides detailed steps for downloading and installing the BCM Element Manager on a Windows computer.

Managing BCM with Terset administration

While Element Manager is the primary management application, BCM also supports the programming of telephony and applications areas of BCM through set-based administration. This allows installers, already familiar with this interface, to perform programming from the keypad of any telephone connected to the BCM device. This alleviates the need for access to a computer at the customer site. For more information about using Terset programming on the BCM, refer to the following documents:

- *BCM 4.0 Terset Administration Guide* (N0060610)
- *CallPilot Telephone Administration Guide* (N0060618)
- *Contact Center Telephone Administration Guide* (N0060615)

Managing BCM Voicemail and ContactCenter: CallPilot Manager

The integrated voicemail and call center applications are managed using CallPilot Manager, which can be launched from Element Manager. This is the same application used to manage voicemail and contact center applications for the BCM Release 3 software stream. For more information about using CallPilot Manager, refer to the CallPilot documentation on the BCM web page.

CallPilot Manager can be launched only by users with sufficient security privileges. BCM administrators must assign privileges. See [Chapter 4, “BCM Security Policies and Accounts and Privileges,” on page 73](#) for more information on security privileges.

Managing IVR for BCM 4.0

The integrated Interactive Voice Response (IVR) functionality is managed using the IVR application. You can use the BCM Element Manager to specify an IVR server, and download and launch the IVR application.

For more information about the IVR application, see the *IVR Installation and Configuration Guide* (N0060624).

Managing Digital Mobility for BCM 4.0

Digital mobility is managed using applications that you can download from the BCM webpage. Two applications are available:

- Digital Mobility Controller (DMC) OAM program
- Digital Mobility Service Tool

You can use the DMC OAM program to configure, operate, and administer the wireless system through the DMC. Use the Digital Mobility Service Tool to program repeaters and adjust handsets. For more information about these applications, see the *Digital Mobility System Installation and Configuration Guide* (N0000623).

Programming telephone sets: Desktop Assistant portfolio

Element Manager supports the programming of button functions for the digital and IP telephone sets. Some administrators may want to use the Desktop Assistant family of products to complete the customization of button programming and generate labels for the telephone sets. The Desktop Assistant family of applications can be downloaded from the BCM web page. Documentation for these applications is included within the application interface.

The Desktop Assistant family of products consists of:

- Desktop Assistant
- Desktop Assistant Pro
- Desktop Assistant Pro AE



Note: You require a LAN CTE keycode to operate Desktop Assistant Pro and Desktop Assistant Pro AE. See the *BCM LAN CTE Configuration Guide* (N0060604) for more information about installing and using LAN CTE.

Performing initialization: Startup Profile

The Startup Profile is a template that can be edited using Microsoft Excel. It is used to accelerate the initial installation programming of system-level parameters. It helps bring the BCM element to a basic operational and ready-to-customize state without using either BCM Element Manager or Telset administration.

The administrator must fill out the Startup Profile template, save it onto a USB storage device and insert the storage device into the USB port of the BCM before the initial start-up. On start-up the BCM reads the information, and starts up with the correct system parameters and feature licensing already in place.

Some of the parameters included in the Startup Profile are:

- system name
- system profile such as country, telephony template and key voicemail attributes
- system IP parameters
- system level telephony attributes that automatically create default system DNS
- feature licensing (through automated application of the keycode file)
- user accounts
- modem status

For detailed information on the Startup Profile, see the *BCM200/400 BCM 4.0 Installation and Maintenance Guide* (N0060612) and the *BCM 4.0 for BCM1000 Installation and Maintenance Guide Addendum* (N0060603).



Note: You cannot use the Startup Profile with BCM1000 systems because a USB port is not supported.

Monitoring BCM: BCM Monitor

BCM Monitor is a monitoring and diagnostics tool that can monitor BCM systems at Release 3.0 and higher, including BCM50 Release 1.0 and BCM Release 4.0. It is installed as part of the BCM Element Manager installation. See [Chapter 10, “BCM Utilities,” on page 285](#) for information about the BCM Monitor for BCM.

Managing BCM with the serial interface

You may need to perform basic tasks, such as querying or setting the LAN IP address and subnet mask or rebooting the system, when the BCM Element Manager is not available. You can connect to the BCM using the serial port to perform these tasks. The serial port is enabled by default. For information about the serial port interface, see the *BCM200/400 BCM 4.0 Installation and Maintenance Guide* (N0060612) and the *BCM 4.0 for BCM1000 Installation and Maintenance Guide Addendum* (N0060603).

Managing BCM remotely with SNMP

Simple Network Management Protocol is a standard for network management. BCM supports a number of standard MIBs, including:

- MIB II RFC 1213
- Entity MIB RFC 2737
- Host MIB RFC 2790
- IF-MIB (RFC2863)
- SNMP-Framework-MIB (RFC2261)
- OSPFv2 (RFC1850)
- RIPv2 (RFC1724)

SNMPv1, v2c and v3 are supported, as well as SNMP traps.

See [Chapter 6, “Managing BCM with SNMP,” on page 135](#) for more information about using Element Manager with SNMP.

BCM Element Manager

The Element Manager is a client-based management application that runs on a Windows computer or on a Citrix server. The Element Manager allows for connection to BCM devices over an IP network. It is used to configure, administer, and monitor BCM Release 4.0 devices.

The BCM Element Manager has the following system requirements:

- Windows: Windows 98 SE, Windows 2000, Windows XP
- RAM: minimum 256 MB, recommended 512 MB
- free space: 150 MB

The BCM Element Manager allows you to connect to the BCM devices to be managed either through an IP network connection, or through the LAN port on BCM devices that include a LAN port.

This section includes the following information on how to install and use Element Manger:

- [“BCM Element Manager setup” on page 35](#)
- [“Element Manager window attributes” on page 40](#)
- [“Element Manager panels” on page 50](#)
- [“Effective use of BCM Element Manager” on page 50](#)
- [“Element Manager data features” on page 51](#)
- [“BCM Element Manager application logging” on page 61](#)
- [“BCM integrated launch of related applications” on page 61](#)

BCM Element Manager setup

You must perform a series of tasks before you can begin using BCM Element Manager. This section contains the following procedures for preparing Element Manager for use:

- [“Installing BCM Element Manager”](#)
- [“Accessing BCM using Element Manager” on page 37](#)
- [“Adding a BCM to the Network Element tree” on page 38](#)
- [“Finding Network Elements” on page 39](#)
- [“Disconnecting from an element” on page 40](#)
- [“Closing the Element Manager” on page 40](#)

Installing BCM Element Manager

You can download the Element Manager application from the BCM web page and install it on your computer at any time. However, you cannot connect to a BCM with Element Manager until the BCM main unit is installed and running.

To install Element Manager on your computer:

- 1** Connect to the BCM web page:
 - If the BCM is installed on the network use a browser and type in the BCM IP address as the URL in the following format:
`http://xxx.xxx.xxx.xxx`
 - If the BCM is installed but not yet configured, connect directly to the BCM through the LAN port and, using a browser, type the following:
`http://10.10.11.1/`
- 2** Enter the user name and password to be authenticated on the BCM web page. See [Chapter 4, “BCM Security Policies and Accounts and Privileges,” on page 73](#) for information on default user and passwords.
- 3** Select the **Administrator Applications** link.

- 4 Select the **BCM Element Manager** link from the Administrator Applications web page.
- 5 Select the **Download Element Manager** link from Element Manager download page.
- 6 Select the **Open** button on the **File Download** dialog box to download and install the BCM Element Manager on your computer.
- 7 Follow the prompts to install the Element Manager and BCM Monitor on your computer. BCM Monitor replaces any older versions of BCM Monitor already installed on your computer.
- 8 Once the BCM Element Manager is installed, find the BCMEM.exe icon where you installed it. Nortel recommends that you use the default location. The default installation location is C:\Program Files\Nortel\BCM\BCMElementManager\bin\. Double-click on the BCMEM.exe icon to launch the Element Manager.
- 9 When the initial Element Manager window appears, take some time to orient yourself with the various parts of the basic display. Refer to [“Element Manager window attributes” on page 40](#).
- 10 Next steps:
 - If the BCM you want to connect to is installed and has been booted up (both LEDs should be solid green), connect your computer to either the LAN port on the BCM, or to the IP network that connects to the BCM.
 - Set up the BCM as a device in the Network Elements tree. See [“Adding a BCM to the Network Element tree” on page 38](#) for information.



Note: You must install future releases of BCM Element Manager in the same path as the current version to maintain defined network elements; otherwise, you will have to define all network elements again.

Using BCM Element Manager in a Citrix environment

You can run BCM Element Manager in a Citrix environment, using the following software:

- Windows 2000 Server SP4 (fully patched)
- Citrix Metaframe XP Feature Release 3
- Citrix Program Neighborhood Version 7.0

When you run BCM Element Manager in a Citrix environment, the BCM Element Manager is installed on a Citrix server. Users then run Citrix Program Neighborhood to connect to the server and launch the BCM Element Manager.

Element Manager is designed for single-user environments. A single installation of Element Manager will extend the same user preferences to any Citrix user, including the device list and any saved passwords. Citrix administrators can ensure a secure environment by using one of the following approaches:

- install a copy of Element Manager for each user or group of users in different folders, with Windows permissions set for the folder to control access
- in cases where a shared device tree is permitted, ensure that users do not save passwords, but instead enter a password each time they connect

To install Element Manager on a Citrix server:

- 1 From the Citrix server, connect to the BCM web page:
 - If the BCM is installed on the network use a browser and type in the BCM IP address as the URL in the following format:
http://xxx.xxx.xxx.xxx
 - If the BCM is installed but not yet configured, connect directly to the BCM through the LAN port and, using a browser, type the following:
http://10.10.11.1/
- 2 Enter the user name and password to be authenticated on the BCM web page. See [Chapter 4, “BCM Security Policies and Accounts and Privileges,”](#) on page 73 for information on default user and passwords.
- 3 Select the **Administrator Applications** link.
- 4 Select the **BCM Element Manager** link from the Administrator Applications web page.
- 5 Select the **Download Element Manager** link from Element Manager download page.
- 6 Select the **Open** button on the **File Download** dialog box to download and install the BCM Element Manager on your computer.
- 7 Put the Citrix server in install mode by selecting **Add/Remove Programs > Add New Program > CD or Floppy**, or by entering the `change user/install` command from the DOS prompt.
- 8 Follow the prompts to install the Element Manager and BCM Monitor on your computer.

If an older version of Element Manager is already installed on your computer, you can choose to update the existing installation, or perform a new installation. If you choose to perform a new installation, you can copy the existing resources to the new installation, including the device tree, cartridges, and user preferences.

BCM Monitor replaces any older versions of BCM Monitor already installed on your computer.
- 9 Put the Citrix server in execute mode by closing the **After Installation** window, or by entering the `change user/execute` command from the DOS prompt.
- 10 Publish the Element Manager application to make it available to the users using standard Citrix application publishing.

Accessing BCM using Element Manager

The first time Element Manager opens it displays two panels. The Element Navigation Panel located on the left, enables you to create a definition within Element Manager for each BCM to be managing using Element Manager. You can then use the icons for the elements defined within the Element tree to perform various functions associated with that element, such as logging into the element or viewing log files associated with that element.

Creating folders for network elements

Before you add a BCM to the network element tree, you can create folders and subfolders to organize the devices in your network.

- 1 While disconnected from the BCM device, click the **New Folder** icon on the task bar. You can also right-click on **Network Elements** in the Network Element Navigation panel, and select **New Folder**.
- 2 Right-click on the new folder and select **Rename**.
- 3 Enter a name for the folder.

Adding a BCM to the Network Element tree

Before you can connect to a BCM, you must define it in Element Manager as a Network Element.

- 1 Select **Network Elements** from the Network Element Navigation panel, or, if you have defined subfolders, select the subfolder where you want to save the device.

You can define subfolders by right-clicking on **Network Elements** and selecting **New Folder**. If you want to move devices between folders they must be deleted from the old folder and recreated in the new folder.
- 2 Select **Network** from the menu bar or right-click on the folder heading.
- 3 Select **New Network Element > Business Communications Manager**.
- 4 In the **Business Communications Manager Entry** dialog box, enter the IP address for the new network element.
- 5 Enter the **Read-Write Community String**, if it is present.

The **Read-Write Community String** is only present if SNMP is enabled. SNMP is disabled by default. The default SNMP **Read-Write Community String** is `public`. Contact your system administrator to find out the correct SNMP community string to use. See [Chapter 6, “Managing BCM with SNMP,” on page 135](#) for more information about SNMP community strings.

- 6 Click **OK** to exit the dialog box.

An icon representing the newly defined element with its associated IP address appears on the Network Elements tree.



Note: If you want to change the IP address to a name or other type of identification, triple-click the IP address or right-click once on the IP address. Once the field becomes editable, type in the new information.

Refer to [“Element Manager window attributes” on page 40](#) for a detailed description of the common Element Manager window elements.

Next steps: Proceed to [“Connecting to a BCM element” on page 39](#).

Finding Network Elements

You can search for a group of BCMs located on the same subnet by using **Find Network Elements**. This function uses SNMP to search for all of the BCMs in the specified IP address range and add them to the Element Navigation tree. Only BCMs with SNMP enabled will be detected. This tool saves time when trying to quickly populate Element Manager with previously deployed BCMs for the first time.

Use the following procedure to find network elements:

- 1** Right-click the **Network Elements** icon in the Element Navigation Panel.
- 2** Select **Find Network Elements > Business Communications Manager**
The **Network Device Search** dialog box appears.
- 3** Enter the **Start of IP Address range** and press the tab key
- 4** Enter the **End of IP Address range** and press the tab key
- 5** Enter the **Read-Write Community String** and press the tab key
- 6** Click on the **OK** button

The Element Manager searches for the IP addresses specified in the range.

- If the search is successful, the BCMs found within the IP address range are added to Network Elements tree in the Element Navigation Panel.
- If the search is unsuccessful a Network Elements dialog box appears stating **No network elements found**.

Connecting to a BCM element

Use the following steps to connect to your BCM once it is defined in the Element Manager:

- 1** On the Network Elements tree, select the element to which you wish to connect by selecting the IP address or element name as it appears in the Network Element tree.

Login fields appear in the Information panel.

- 2** Enter your log in credentials for the BCM to which you are trying to connect.
- 3** Perform one of the following tasks to connect to the BCM:
 - Click the **Connect** icon on the Icon toolbar
 - Right-click on the IP address or element name and select **Connect**

The Element Manager attempts to connect to the selected element.

- If the connection is successful, Element Manager opens the Configuration and Administration tabs associated to the selected device. See [“Element Manager panels” on page 50](#) for an explanation of the Element Manager screen layout.
- If the Element Manager fails to connect, an error message appears, describing the connection problem. Correct the problem and perform the steps again. If you have a recurring problem, contact Nortel Support for help in resolving the problem.

Disconnecting from an element

You can disconnect Element Manager from a BCM by using one of the following:

- [“Disconnecting in the Element Navigation Panel”](#) on page 40
- [“Disconnecting through the menu bar”](#) on page 40

Disconnecting in the Element Navigation Panel

- 1 Right-click the IP address that you want to disconnect, in the Network Element Navigation Panel.
- 2 Select **Disconnect**.
- 3 Click **Yes** in the Confirmation dialog box to confirm the disconnect request.

Disconnecting through the menu bar

- 1 Click **Session** on the menu bar.
- 2 Select the IP address of the device you want to disconnect.
- 3 Select **Disconnect** from the list of tasks that are displayed.
- 4 Click **Yes** in the Confirmation dialog box to confirm the disconnect request.



Warning: Clicking the X box on the upper right corner causes the Element Manager application to close and all current sessions with BCM devices are terminated. Do not click on the X box to disconnect Element Manager from its current session.

Closing the Element Manager

To close the Element Manager select **File > Exit**, or click on the X box on the upper right corner of the window. Close all active sessions before you close the Element Manager application.

Element Manager window attributes

The initial Element Manager window has several attributes that appear regardless of whether the Element Manager is actively connected to a network element. Although all of the network elements appear, some of the menu options may not be available for the selected device, depending on the device’s state.

The following sections describe the menus and information available on the BCM Element Manager panel:

- [Initial panel details](#) on page 41
- [Information displayed for unconnected elements](#) on page 44
- [Information displayed for connected elements](#) on page 45
- [Configuration task navigation panel details](#) on page 46
- [Administration task navigation panel details](#) on page 48

For information about navigating the panels and tables of the BCM Element Manager, see [Element Manager data features](#) on page 51.

Initial panel details

[Figure 4 on page 41](#) shows the initial panel of a newly-installed Element Manager. At this point, no network elements have been defined, and the Element Manager is not connected to any elements.

Figure 4 Element Manager Window - no defined Elements

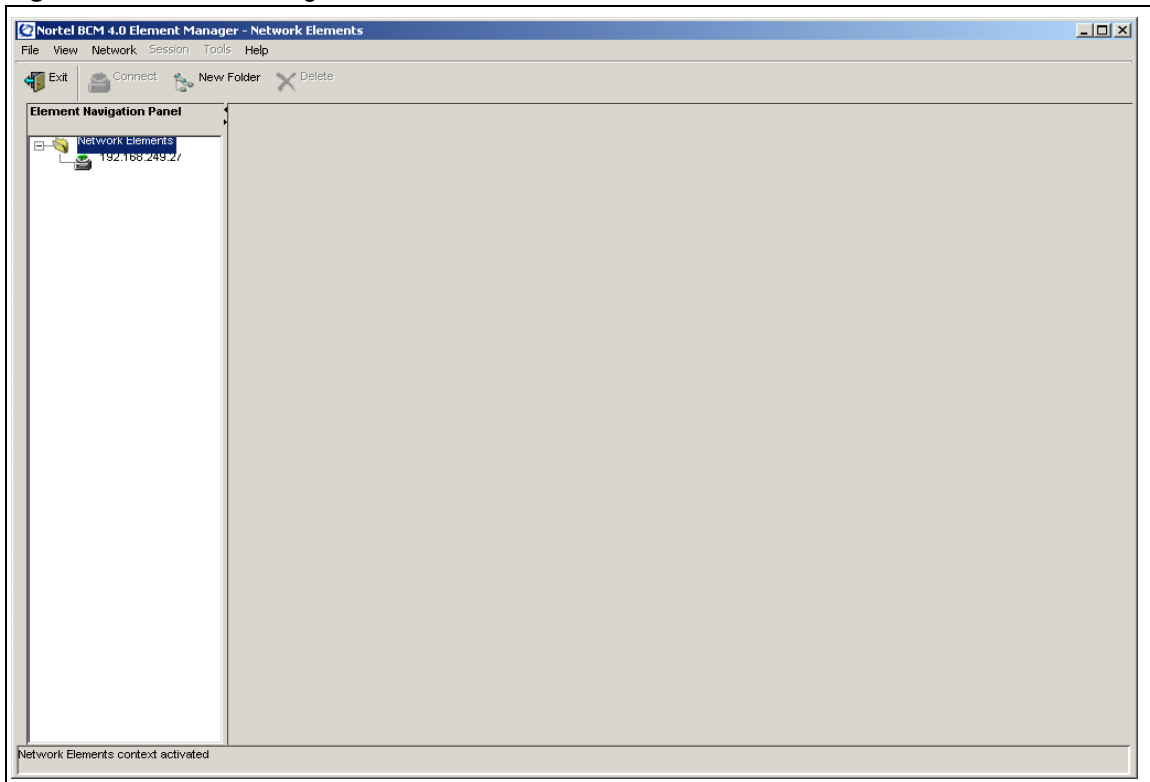


Table 3 lists and describes the initial Element Manager window.

Table 3 Initial Element Manager window attributes

Element	Description
Title bar	When you connect to a device, this area indicates the type of device (Nortel Networks BCM Element Manager - Network Elements) and the IP address for the connected device.
Menu bar	The items on the menu bar are static, however, some items may be greyed out at various stages.
File	This menu provides two selections: <ul style="list-style-type: none"> Exit: a standard exit prompt that closes the Element Manager application. You can also click on the X box on the upper right corner of the window or click Ctrl-X View Network Element Logs: opens a dialog box that allows you to search for and to view logs that are available for the connected element.

Table 3 Initial Element Manager window attributes (Continued)

View	<p>This menu provides three selections:</p> <ul style="list-style-type: none"> • Preferences: Allows you to choose a different appearance for the Element Manager window. • Network Elements: Enabled by default. If you uncheck this setting, the Network Elements panel closes (far left panel). This does not disconnect any connected device. • Refresh (F5): Allows you to refresh the data shown on the window.
Network	<p>This menu is not available when a connected device is selected.</p> <p>When the Network Elements folder icon is selected in the Network Elements tree the following options are available:</p> <ul style="list-style-type: none"> • New Folder: Allows you to create a new folder on the Network Elements tree. Folders allow you to organize your devices. • New Network Element: Allows you to create a new entry under the Network Elements tree. This menu item opens up a dialog box that allows you to enter access parameters for a new Business Communications Manager device to which you want to connect. Once you have connected to the device, this information is saved by Element Manager and the device remains present in the Network Elements tree. Required information is the IP address for the device with which you want to connect. • Find Network Elements: Opens a search dialog box that allows you to do search for devices within a range of IP addresses by using an SNMP query. This function only locates BCMs that have SNMP turned on (by default, SNMP is turned off). <p>When an unconnected device is selected in the network element tree, the following options are available under the Network selection:</p> <ul style="list-style-type: none"> • Delete: Allows you to delete the original entry in the Element Manager network element tree and create a new instance of a network element in the tree with a new IP address. If the IP address of the device changes, you must delete the original entry in the Element Manager network element tree and create a new instance of a network element in the tree with a new IP address. • Connect: When selected, Element Manager attempts to open a connection to the selected element. You can also connect to a network element by right-clicking on the selected element. • View Logs: Opens a View Logs dialog box, which allows you to view any log files for the selected element. See Chapter 12, "Managing BCM Logs," on page 345 for more information on viewing logs.
Session	<p>Allows you to select actions for any of the network elements to which there is a currently active Element Manager session. If there are no active Element Manager sessions, then this selection will be greyed out.</p> <ul style="list-style-type: none"> • Show: If multiple devices are connected, allows you to easily select one of the connected elements from the presented list and switch the active Element Manager view to that element. • Disconnect: Allows you to disconnect from the device. A warning dialog box is presented asking if you really want to disconnect from the device. You can also disconnect from a device by right-clicking on the device in the network element tree and selecting "Disconnect". The Element Manager remains open. • Save Programming Record: Allows you to save programmed information in either Microsoft Excel format or HTML.

Table 3 Initial Element Manager window attributes (Continued)

Tools	<p>This selection provides a point from which tools relevant to the selected element can be launched. This prompt is only active when a connected device is selected on the Network Elements tree.</p> <ul style="list-style-type: none"> • BCM Monitor: This is a separate application, which can be installed at the same time as Element Manager and provides a number of panels that display current system operational information.
Help	<p>Provides information to assist in using the Element Manager.</p> <ul style="list-style-type: none"> • PDF Documents: Provides a link to the documentation interface, on the Business Communications Manager web page, where you can find various PDF books describing the BCM system and programming. • Contents: Provides a link to the help system. Note: A brief function description appears when you mouse over field headings. You can also access help contents by clicking on a heading and pressing F1. Refer to “BCM Help system” on page 64 for more details on Element Manager help available. • Application Log: Collects messages generated by the Element Manager during normal operations. • Customer Support: Provides a link to a Nortel Networks customer support web site. • About: Provides information about the Element Manager, such as the Element Manager Release level.
Icon Toolbar	<p>Four icons are available if the Network Elements folder is at the top of Network Elements tree or if an unconnected device is selected.</p> <ul style="list-style-type: none"> • Connect: Connects the Element Manager to the selected device. • New Folder: Adds a new folder under the Network Elements tree. This icon only works when the Network Elements title is selected. • Delete: Allows you to delete the selected device from the Network Elements tree. • Refresh
Network Elements navigation panel	<p>This panel contains the Network Element Navigation tree which displays devices and groups of devices (folders).</p> <ul style="list-style-type: none"> • The following actions are available in the Network Element navigation panel: Add items: Add Network Elements or folders by right-clicking, or use the selections under the Network menu or the Icon tool bar. Delete items: Select the device or folder and right-click, or use the selections under the Network menu or the Icon toolbar. Connect/Disconnect: Select the device and right-click, or use the selections under the Network menu or the Icon tool bar. • The following actions are available if you right-click on a network element listed in the Network Element Navigation tree. Connected items - Disconnect or view logs Unconnected items - Connect, delete, or view logs • You can rename a folder or a network element by triple-clicking it or by right-clicking the network element and updating the name when the name field opens for editing.

Table 3 Initial Element Manager window attributes (Continued)

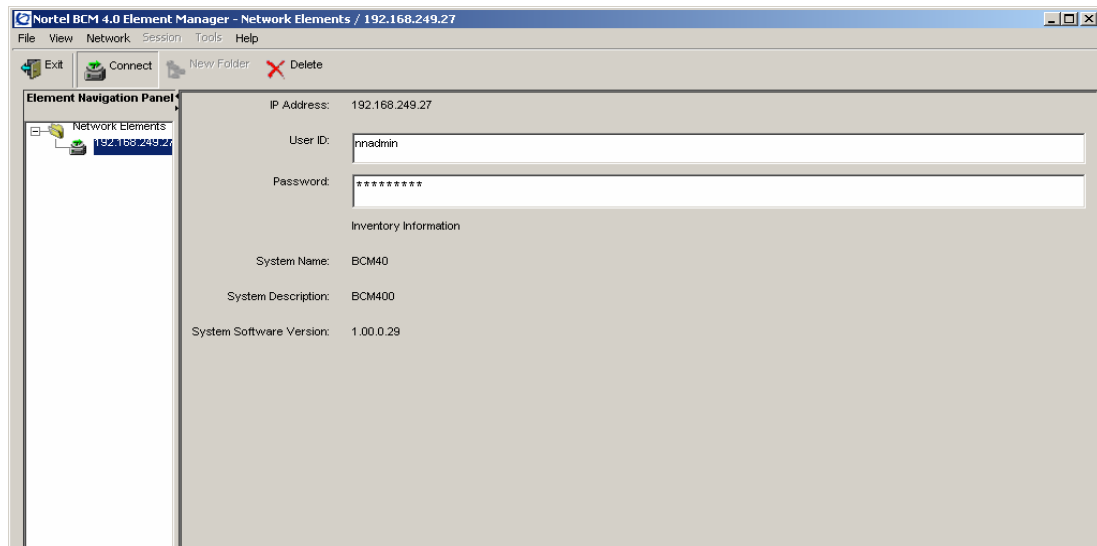
Information panel	The information in the Information panel changes depending on what is selected in the Network Elements tree. <ul style="list-style-type: none">• If a network element is selected that is not connected: The information panel shows the network element connection login information. Refer to Information displayed for unconnected elements on page 44.• If a network element is selected to which there is an Element Manager connection: The task panel opens and shows Configuration and Administration tabs. Refer to Information displayed for connected elements on page 45 for an example of the presentation of the information by Element Manager.
Status bar	The bottom bar of the Element Manager window displays the current status of the selected item.
Expansion Arrows	Clicking on these arrows will either expand or collapse the panels within the Element Manager window. These arrows appear on all panels that have sub-panels that can be expanded or collapsed.

Information displayed for unconnected elements

When you select a device in the Network Element tree to which there is currently no active Element Manager connection, a panel is shown with a number of fields relevant to the selected device. Some of this information does not appear until you have successfully connected to the element with Element Manager.

[Figure 5 on page 45](#) shows the right-hand panel in Element Manager when an unconnected network element is selected.

The fields on this panel are described in [Table 4](#).

Figure 5 Information display for unconnected network element**Table 4** Unconnected network element information

Field	Description
IP Address	The IP address of the selected device.
Read-Write Community String	The current community string for the selected device (shown if SNMP is enabled).
User Name	Name of an authorized BCM user account.
Password	A valid password associated to the User Name.

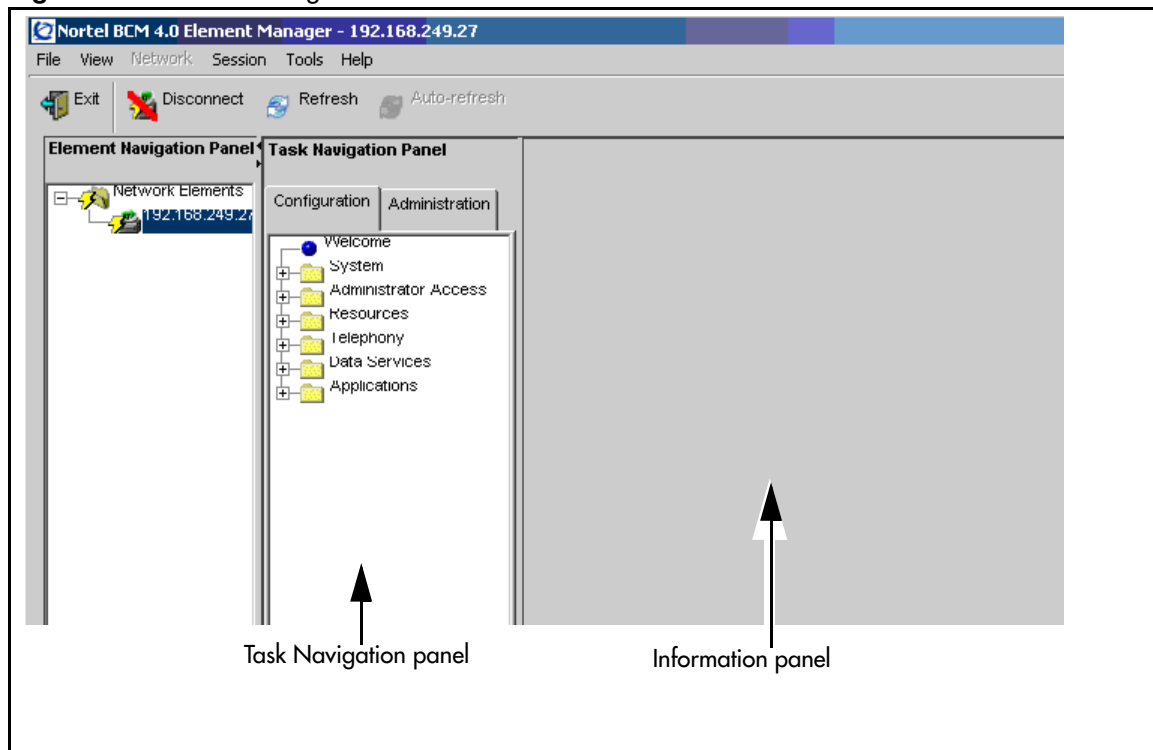
Information displayed for connected elements

Element Manager displays two panels to the right of the Network Elements navigation panel once a BCM element has been connected:

- Task Navigation panel
- Information panel

[Figure 6](#) shows the panels displayed in the Element Manager when it is connected to a BCM.

The Task Navigation panel contains the Configuration tab and the Administration tab. See [“Configuration task navigation panel details” on page 46](#) for information contained in the Configuration navigation tree. See [“Administration task navigation panel details” on page 48](#) for information contained in the Administration navigation tree.

Figure 6 Element Manager window when connected to a BCM

Configuration task navigation panel details

The Configuration task navigation panel contains the Configuration task tree that allows you to set up and configure your BCM and the attached devices.

Table 5 lists the tasks in the Configuration task tree and describes the task functions available within the information panel when the task is selected.

Table 5 Configuration task navigation panel headings

Navigation tree heading	Description
Weclome	View information about the current user session, such as account notifications, user ID, and authentication method.
System	
Identification	View system information
Date and Time	View and set current date and time including selection of time source
Keycodes	Retrieve, view, and manage keycodes
Administrator Access	
Accounts and Privileges	Manage users, groups, and privileges
Security policies	Manage passwords and other security policies, including authentication methods
SNMP	Manage SNMP settings, and trap destinations
Resources	

Table 5 Configuration task navigation panel headings (Continued)

Application Resources	Reserved resources as well as resources in use
Media Gateways	Manage level of Echo cancellation and T.38 UDP redundancy for all media gateways
Port Ranges	Add or delete Ports for IP Telephony
Telephony Resources	Manage location, type and status of both physical and virtual modules including media gateways, IP trunks, and Sets
Network Interfaces	View and modify settings for network interfaces, such as types, protocols, IP addresses, and subnet masks, as well as modem parameters
Telephony	
Global Settings	
Feature Settings	Manage feature settings and timers
Advanced Feature Settings	Manage SWCA, ONN Blocking, Silent Monitor and Call Log Space
IP Terminal Features	Add or delete features and view List of Key Labels
System Speed Dial	Manage speed dial numbers with bypass restrictions
CAP Assignment	View Cap number and set DN
Sets	
Active Sets	Manage line access, capabilities, preferences, and restrictions of set DNs
Active Application DNs	Manage line access, capabilities, preferences, and restrictions of application DNs
Inactive DNs	Manage line access, capabilities, preferences, and restrictions of inactive DNs
All DNs	Manage line access, capabilities, preferences, and restrictions on all system DNs
Lines	
Active Physical Lines	Manage active physical line parameters
Active VoIP Lines	Manage active VoIP line parameters
Target Lines	Manage target line parameters
Inactive Lines	Manage inactive line parameters
All Lines	Manage all lines
Loops	View type, protocol, sampling, ONN blocking for BRI lines
Scheduled Services	Manage scheduled service and list of possible services
Dialing Plan	
General	Manage settings, access codes and direct dial sets
DNs	Manage DNs
Public Network	Manage settings, DN lengths, and carrier codes
Private Network	Manage settings, MCDN, VoIP IDs, ETSI
Line Pools	View pool and access code
Routing	Add or delete routes and destination codes

Table 5 Configuration task navigation panel headings (Continued)

Ring Groups	Manage group membership and line settings
Call Security	
Restriction Filters	Add or delete restrictions and exceptions for restrictions
Remote Access Packages	Add or delete line pool access
Class of Service	Manage passwords for class of service as well as restrictions
Hospitality	Manage general administration, wake-up call settings, call restrictions, and room settings
Hunt Groups	Manage group members and line assignment
Call Detail Recording	Manage report options and data file transfer settings
Data Services	
DHCP Server	Manage general DHCP server settings, IP ranges, and lease info
IP Sec VPN	Manage settings for IP Sec VPN service.
Router	Configure router settings.
NAT and Filters	Manage network address translation and policy filters.
DNS	Enable domain name service and configure DNS addresses.
Web Cache	Manage the web cache.
QoS Queuing	Manage QoS queuing.
Applications	
Voice Messaging/Contact Center	Record remote voice mail system access numbers or connect to local CallPilot applications. Launch CallPilot Manager
LAN CTE	Manage clients, add or delete privileges
IVR	Launch the IVR application.
Music	Manage music settings.

Administration task navigation panel details

The Administration task navigation panel contains the Administration task tree that provides access to the BCM that allows you to monitor and maintain your BCM.

Table 6 lists the tasks in the Administration task tree and describes the task functions available within the information panel when the task is selected.

Table 6 Administration task navigation panel headings

Navigation tree heading	Description
General	
Alarms	View alarm details, clear alarm log or reset LEDs
Alarm Settings	View alarm details and test alarms
SNMP Trap Destinations	Add, delete or modify trap destinations
Service Manager	Start, stop or restart Services (only use this feature when directed by Nortel Networks support, as improper use can affect system operation)

Table 6 Administration task navigation panel headings (Continued)

Hardware Inventory	Manage general information for attached BCM systems and devices
System Status	
LED Status	Monitor the status of the LEDs.
QoS Monitor	Manage Quality of Service monitor modes, logging and mean opinion scores
UPS Status	Manage uninterrupted power supply status, events and metrics
NTP Metrics	Manage network time protocol metrics synchronization details
Interface Metrics	View information about network interfaces, including bandwidth usage and traffic metrics.
Disk Mirroring	View status information about disk mirroring equipment.
QoS Metrics	View QoS metrics, including statistics for total traffic and traffic per queue.
Telephony Metrics	
Trunk Module Metrics	Run loopback test on trunk modules
CbC Limit Metrics	View (Call by Call) logs of denied calls
Hunt Group Metrics	Reset metrics by hunt group
PSTN Fallback Metrics	Reset PSTN fallback metrics
PVQM	View voice quality metrics.
Utilities	
BCM Monitor	Launch BCM Monitor
Ping	Send an ICMP packet to the selected switch to see if it is reachable on the network
Trace Route	Perform a trace route to specified IP address
Ethernet Activity	View Ethernet activity on ports
Reset	Perform a reboot of BCM or either a warm or cold reset of telephony services or router
Diagnostic Settings	Set release reasons for ISDN or VoIP calls
Data Networking Utilities	Display results of debug commands, such as lists of active connections, configuration, and routing information.
Backup and Restore	
Backup	Perform immediate or scheduled backups
Restore	Restore Administration or Configuration settings
Logs	
Log Management	Perform immediate or scheduled log transfers. Types of logs are configuration change, security, alarm, system, and component diagnostic
Software Management	
Software Updates	Scheduled updates, cancel updates in progress or retrieve new updates
Software Update History	View details of software updates and remove updates
Software Inventory	View software details

Element Manager panels

The BCM Element Manager Configuration and Administration trees group the various tasks and functions required to configure the BCM or perform administrative tasks. When either the Configuration tab or the Administration tab is selected, the associated task tree provides access to the information required to complete the tasks. For example, all tasks in the Configuration tab are configuration tasks, organized by workflow. Various types of administrative tasks are presented in the Administration tab, such as monitoring alarms or performing backups.

Some tasks have multiple tabs within the Information panel. Information on the panels may be grouped by related information or tasks.

Repetitive information such as line programming, DN programming, and system speed dial is displayed in table format in the Element Manager. These tables allow you to change the data display, apply filtering, sort data, or copy information between cells. If there is additional information or configuration details available for a selected item in the table, an associated details panel for the selected row appears below the table.

In some cases, further panels can appear beside the main table. This is the case for restriction filters, for example, where there are three side-by-side panels that are programmed in a progressive order from left to right.

Tabs that do not apply to a selected item appear greyed out and behind the active tabs.

You can select fields that are not read-only and enter new data either from your keyboard or by using the drop-down box that appears when a field is selected. Data entered in these fields take immediate effect, unless otherwise noted on the panel or in pop-up confirmation dialog boxes.

Refer to [“Element Manager data features” on page 51](#) for details about navigating and changing information.

Effective use of BCM Element Manager

This section describes how Element Manager interacts with data to help the BCM administrator better understand how to interact with the Element Manager.

The view users see depends on the group to which they belong. They may not be able to see all Element Manager trees or panels. Users assigned to the nadmin group will have administrator privileges and can view all panels and trees available through Element Manager. See the [Chapter 4, “BCM Security Policies and Accounts and Privileges,” on page 73](#) for more information on grouping users and assigning privileges.

The BCM retrieves task bullet data in real time and in sequential order. Once you select a task bullet, Element Manager searches for the data to populate the panels and any associated detail sub-panels or tables for the task. The first search must complete before Element Manager can start the search for the data required for the second selected task. The first task data request is not cancelled by the second task data request. You should only select a second task after the first task request is completed.

Although there is some data caching done, larger tables take longer to load, as do panels with more information in them.

Field data is committed by using add or modify buttons in panels that contain the buttons. For panels without a Commit button use the tab or space keys to leave the field after the data has been filled in to commit the data.

Administrators have the ability to lock out other users for a maximum of 240 minutes from Element Manager by using the **Enable Exclusive Access** function in the **Administrator Access > Accounts and Privileges > Current Account** tab. This ensures that there are no other users creating changes at the same time as the administrator. See [Chapter 4, “BCM Security Policies and Accounts and Privileges,”](#) on page 73 for more information on how to use **Enable Exclusive Access**.

Element Manager data features

The Element Manager arranges repetitive information, such as lines programming, device record (DN record) programming, and system speed dials into tables of information. You can manipulate these tables in terms of data display and filtering, sorting and copying information between cells.

Other information that only requires one or two fields is arranged on composite panels that may have more than one sub-panel. Each sub-panel includes related information.

This section provides the following descriptions:

- [Adding, deleting, and modifying table information](#)
- [Copying table information](#)
- [Rearranging table information](#)
- [Using your keyboard to move around a table](#)

Adding, deleting, and modifying table information

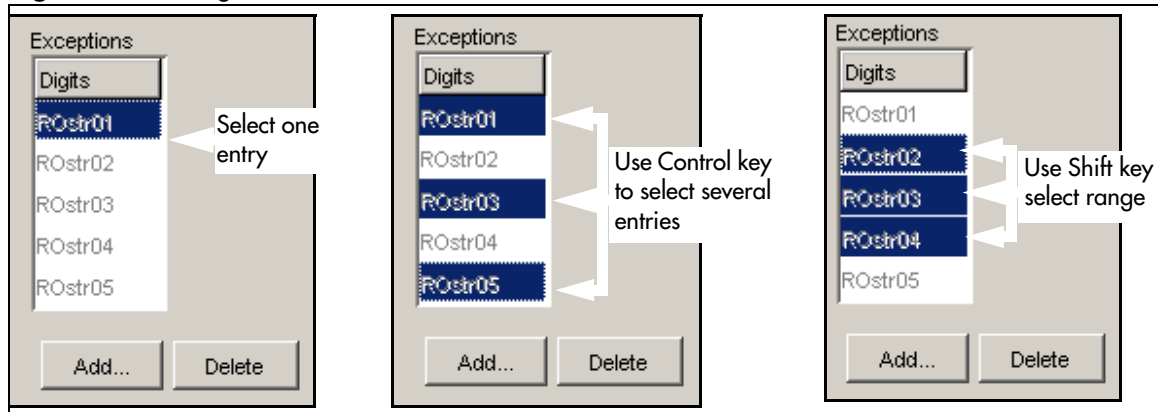
Some tables automatically list all available records, such as the restriction filters. These are tables where the number of entries is restricted by the BCM. Other tables allow you to add or delete entries. These tables have an Add and Delete button under the table.

When you click the **Add** button, an add dialog box appears that allows you to enter basic information, such as a name or DN. When you click OK, the new listing appears on the table, with the default settings.

To modify table settings: click on the fields that you want to change and use the list to choose a new setting, or type in the setting. If information in the table is used by more than one panel, a Modify button may appear. Click on this button to bring up a dialog box where you can change information, as required.

To delete table settings: click on the row you want to delete from the table, then click the Delete button. You can select one line, or you can use the Shift or Ctrl buttons to delete a group of entries.

[Figure 7](#) shows examples of how to select table entries for deletion.

Figure 7 Deleting table entries

Copying table information

You can copy table information using the copy and paste method on tables that require a large amount of propagation of duplicate data. For example, tables within the Sets and Lines task tree items contain the copy and paste functionality.

Use the following steps to copy data within a table:

- 1 Select the row from table that you want to copy by clicking on it.
- 2 Press the **Copy** button
- 3 Select the row or rows to which you want to paste the information.

You can select multiple rows to paste data in by pressing either the Shift or Ctrl key.

- 4 Press the **Paste** button

Either the Paste Set Data or the Paste Line Data dialog box appears depending on whether you are copying data within the **Sets** or **Lines** task tree items. The check boxes within these dialog boxes change depending on the data selected to copy. Table 7 shows the possible check boxes that can appear and what type of data will be copied when they are selected

- 5 **Check** the check boxes for the types of data that you would like to copy to the selected rows.
- 6 Select **OK** to paste the information.

The rows are updated with copied data.

Table 7 Paste Data

Check box title	Settings copied	Settings not copied
Control set (Lines, Sets)	<ul style="list-style-type: none"> Control set from the copied source into the selected row 	
Restrictions (Lines, Sets)	<ul style="list-style-type: none"> Set restrictions Set lock Allow Last Number Redial Allow Saved Number Redial Allow Link Line/set restrictions 	<ul style="list-style-type: none"> Direct-dial set designation (which set is the D-Dial set) CAP/TAP assignment ExtraDial set designation Service mode ringing set designation Prime set designation for a line Hunt group appearance
Trunk Data (Lines, Sets)	<ul style="list-style-type: none"> Data in common between the copied and pasted trunks. 	<ul style="list-style-type: none"> Data can be copied between two different trunk cartridge types
Telco data (Lines, Sets)	<ul style="list-style-type: none"> Call Log set (Logging set) 1stDisplay 	<ul style="list-style-type: none"> Log password Log space
Buttons (Sets)	<ul style="list-style-type: none"> All programmable set buttons from the copied set into the selected row's programmable buttons. 	
Line access (Sets)	<ul style="list-style-type: none"> Line assignment Line pool access Prime line designation Number of intercom keys Answer DN's (unless Answer button DN is same as telephone to which is being copied) 	<ul style="list-style-type: none"> Private line appearances

Table 7 Paste Data (Continued)

Check box title	Settings copied	Settings not copied
Capabilities (Sets)	<ul style="list-style-type: none"> • Call Forward No Answer (DN + delay + setting) • Call Forward Busy (DN +setting) • DND on busy • Handsfree setting • Handsfree answerback • Pickup group • Paging zone • Paging • Direct-dial (which set is reached by the D-Dial digit) • Priority calling • Hotline • Auxiliary ringer • Allow redirect • Redirect ring • ATA settings (except Use ringback setting) 	<ul style="list-style-type: none"> • Set name • Use ringback setting under ATA settings • SM Supervisor
User Preferences (Sets)	<ul style="list-style-type: none"> • Language choice • Ring type • Calls log options (<i>Auto logging</i>) • Display contrast • Dialing options (automatic, pre-dial, standard) 	<ul style="list-style-type: none"> • External autodial button assignments • Internal autodial button assignments • Programmable button assignments • Ring volume • User speed dial • CAP/KIM module memory button

Rearranging table information

There are two ways of changing table information layout:

- [“Rearranging columns” on page 55](#)
- [“Rearranging lines” on page 55](#)

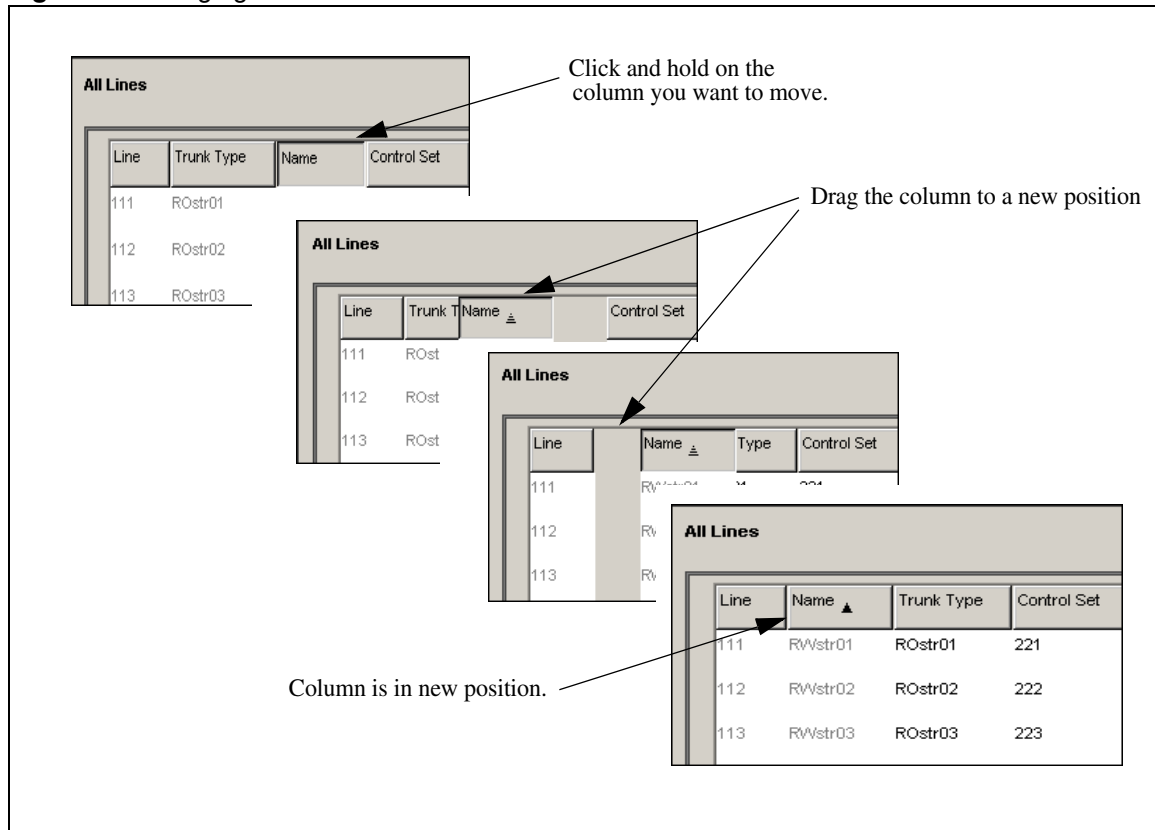
Rearranging columns

You can move columns in a table if you want to temporarily display information in a different way. Changes to the table layouts are not saved. If you leave the panel, the columns return to the default order.

To move a column, click and hold the column heading and drag and drop it to another location on the table.

Figure 8 shows a step-by-step example of how to move a column within a table.

Figure 8 Changing the order of columns in a table



Rearranging lines

If you want to sort table data to make it easier to find information, use the right-click function on table column headings to open a Sort dialog box. The Sort dialog box allows you to choose how a table sorts lines of data.

Figure 9 on page 56 shows the Sort dialog box.

Table 8 lists and describes the fields and buttons in the Sort dialog box.

Figure 9 Sort dialog box

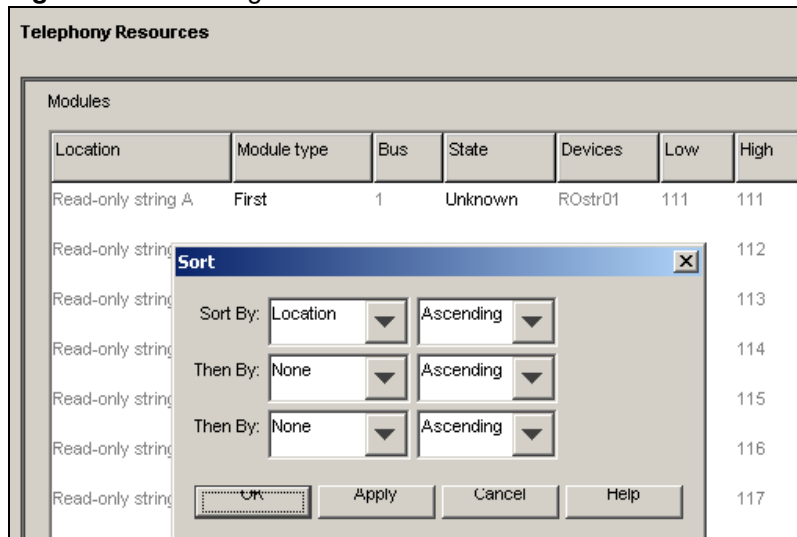


Table 8 Sort dialog box fields

Attribute	Value	Description
Sort By	<column name> Ascending/descending	Choose the column to uses for sorting table data. This is the first column the data set is sorted by.
Then By	None, <column name> Ascending/descending	Choose the column to uses for sorting table data. This is the second column the data set is sorted by.
Then By	None, <column name> Ascending/descending	Choose the column to uses for sorting table data. This is the third column the data set is sorted by.

Table 9 Sort dialog box buttons

Actions	Description
OK	Changes are accepted and the dialog box closes.
Apply	The table rearranges, based on the selections, but the dialog box does not close.
Cancel	No changes are made to the sort order.
Help	Help link to this page.

Using your keyboard to move around a table

Use the <Tab> key or the directional arrow keys on your keyboard to move around a table.

<Tab>	Each press moves the cursor to the field to the right. At the end of a line, the next line is highlighted and the cursor continues moving to the right.
<Shift><Tab>	Each press moves the cursor to the field to the left. At the beginning of a line, the previous line is highlighted and the cursor continues moving to the left from the far-right field.
<Up><Down>	Navigation tree: Moves cursor up/down one heading. Non-table panels: Moves cursor up/down one heading. Selected table: moves up/down one line.
<Left><Right>	Moves cursor to the left/right of the cell. Note that this only works on the currently-selected line.
<Shift><Enter>	Moves forward through the list.
<Carriage Return>	Selected field: brings up the drop-down box icon or the rotary list icon. Check box: selects or clears the check box.

Saving programming records

You can create a programming file that contains the current settings of all or part of your Element Manager data. These files can be saved in either HTML or Excel spreadsheet format. You can access the programming record in the same way you access any other HTML file or by using Excel, version 2002 or later, for the spreadsheet format.

A programming record that contains the factory default settings is available in Excel format from the BCM web page.



Note: Due to the amount of programming data, it may take a long period of time to save all programming records. You may wish to save selected data only.

Figure 10 shows an example of a programming record saved in HTML format and Figure 11 on page 59 shows an example of a programming record saved in Excel spreadsheet format.

Figure 10 Programming record in HTML format

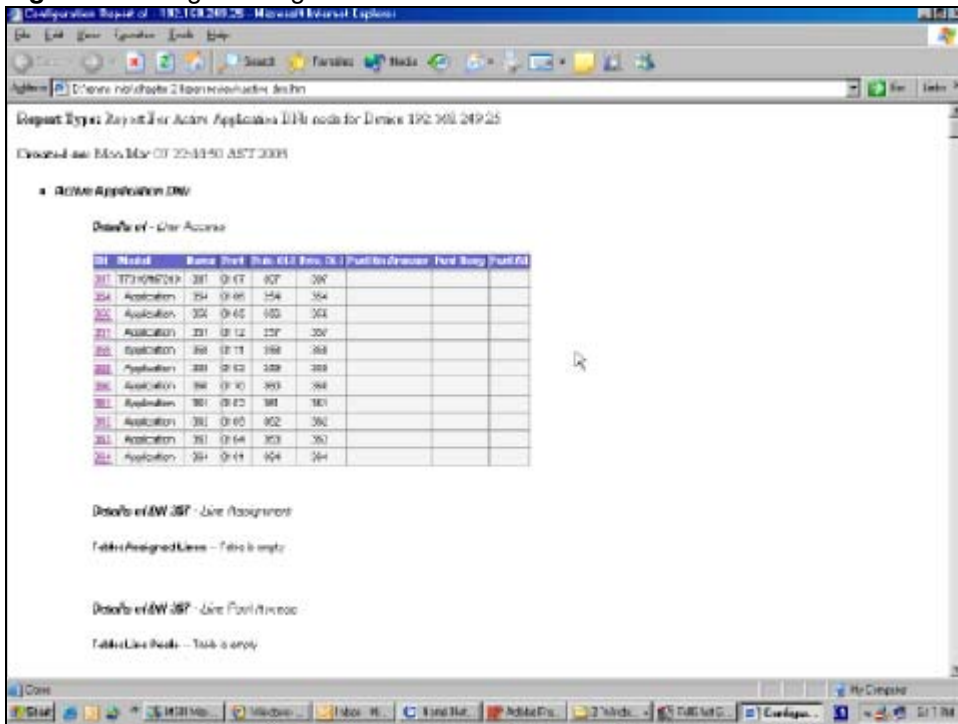


Figure 11 Programming record in an Excel spreadsheet

The screenshot shows a Microsoft Excel spreadsheet titled "active dns.xls". The spreadsheet is organized into several sections:

- Section 1: Active Application DNs** (Rows 7-18)

DN	Model	Name	Part	Pub. OLI	Priv. OLI	Fwd Ho. Ans Fwd Bony	Fwd All
307	17316M7310	307	0107	307	307		
354	Application	354	0106	354	354		
356	Application	356	0105	356	356		
357	Application	357	0112	357	357		
358	Application	358	0111	358	358		
359	Application	359	0103	359	359		
360	Application	360	0110	360	360		
361	Application	361	0102	361	361		
362	Application	362	0109	362	362		
363	Application	363	0104	363	363		
364	Application	364	0101	364	364		
- Section 2: Details of DN 307 - Line Assignment** (Rows 20-21)
- Section 3: Assigned Lines** (Rows 22-24)

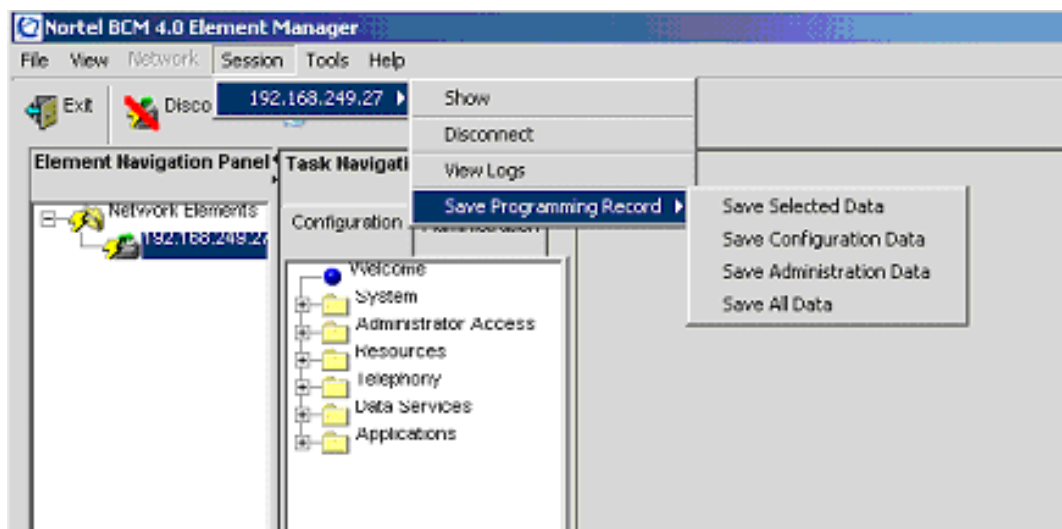
Line	Appearance Type	Appearances	Color ID Set	Usage Set	Priv. Restricted 0	Pub. Restricted
NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE
- Section 4: Details of DN 307 - Line Pool Access** (Rows 25-26)
- Section 5: Line Pools** (Rows 27-31)

Line Pool
A
- Section 6: Details of DN 307 - Answer DNs** (Rows 32-33)
- Section 7: Answer DNs** (Row 34)

To create this file, you use the **Save Programming Record** command on the Session menu. The Save Programming Record provides four menu options.

Figure 12 shows the menu options available.

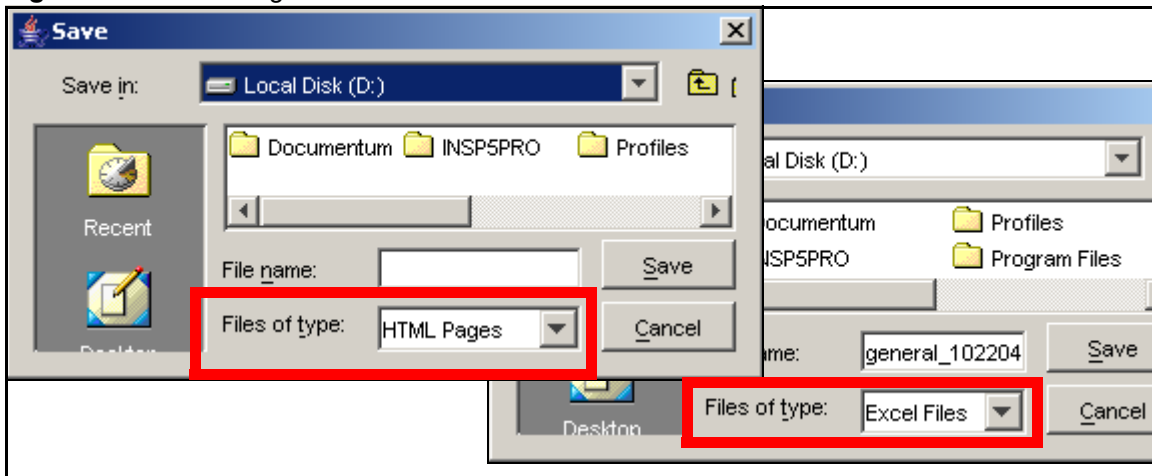
Figure 12 Session selections for saving programming records



Use the following steps to save the data programming:

- 1 Select the item on the task navigation panel for which you want to save the data into an HTML report or Excel workbook. An item can be a task item, task bullet, or a folder.
- 2 Click on **Session > device IP address > Save Programming Record > Save Selected Data**. A **Save** dialog box appears. See Figure 13 for an example of a **Save** dialog box.

Figure 13 Save dialog box



- 3 In the **Save:** field choose the path where you want the file stored.
- 4 In the **Files of type:** field, choose the format in which you want to save the data (HTML or Microsoft Excel spreadsheet).
- 5 Enter a File name. Nortel recommends that you make the current date and system name part of the file name.
- 6 Click on **Save**.



Note: The **Save All Data** selection can take up to 30 - 40 minutes to complete. Your computer must stay connected to the element during this time, as the **Save All Data** function is actively writing into the file specified until the function is complete.

BCM Element Manager application logging

This section describes the logging performed by Element Manager to generate a record of its tasks. There is usually no need to monitor Element Manager log activities. However, the log files are available for troubleshooting should issues arise within the Element Manager operations.

When you select Application Log from the menu bar Help command, the Element Manager Log Browser opens. You can use the Log Browser to sort the events in the Application Log.

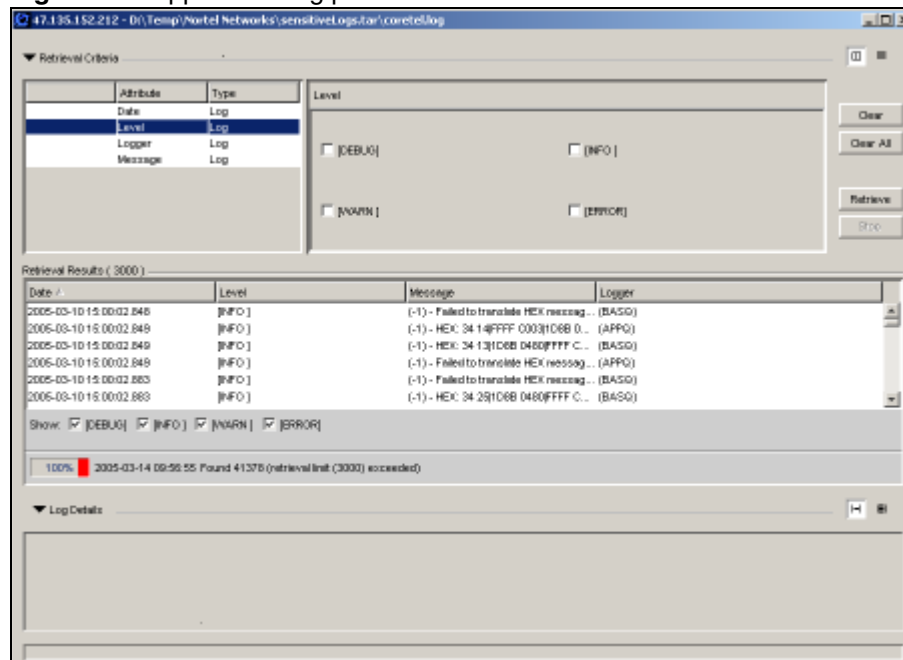
The BCM Element Manager Logs panel has three parts:

- Retrieval Criteria - This panel allows you to specify logging criteria, to clear the defined parameters of a selected criteria, clear all retrieval criteria, retrieve logs based on the specified criteria, or stop logging.
- Retrieval Results - This panel allows you to filter the results shown by retrieving logs based on selected severity level check boxes.
- Log Details - shows the details of the logged message.

You can show or hide the retrieval criteria and log detail panels by clicking on the expansion arrow beside the panel heading.

See [Figure 14 on page 61](#) for the Application log panel.

Figure 14 Application log panel



BCM integrated launch of related applications

BCM Voicemail and CallCenter applications are managed by CallPilot Manager, and real-time system activity is monitored with the BCM Monitor. Other applications are also available from the BCM Web page. All of these applications can be launched through buttons provided at an appropriate location in the BCM Element Manager. You can specify whether you want to pass

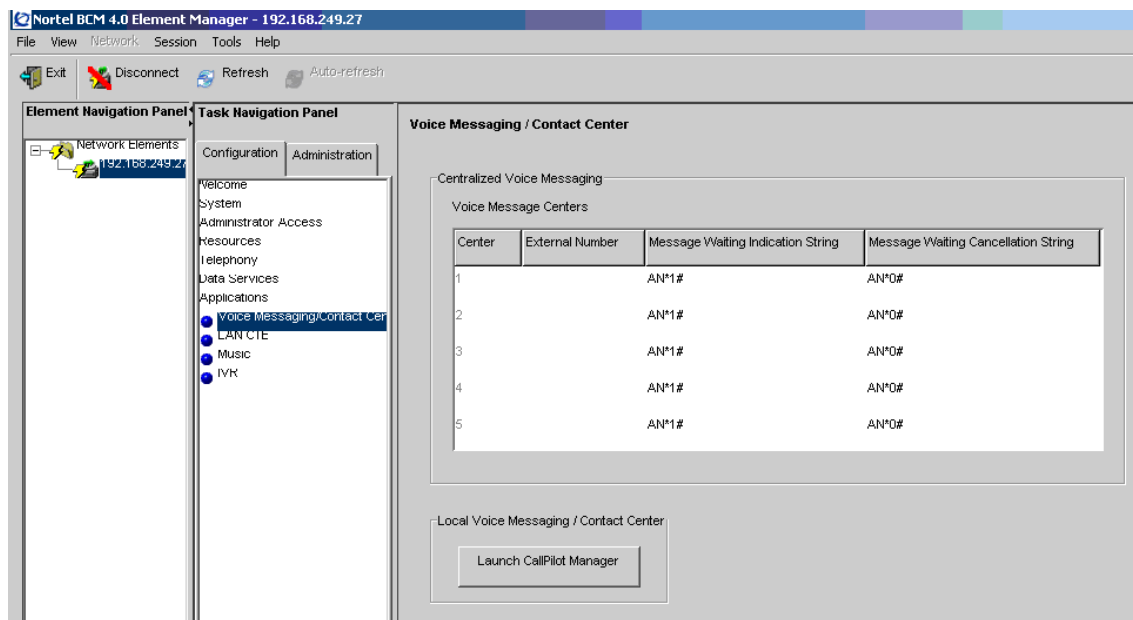
logon credentials to applications launched from the BCM Element Manager under **View > Preferences > Tool Launch**. When you pass logon credentials to these applications, you do not need to re-enter your password when the BCM Element Manager launches them. These applications also have application-based Help systems.

You can launch CallPilot Manager by clicking by the **Launch CallPilot Manager** button under **Configuration Task > Applications > Voice Messaging/Contact Center**.

[Figure 15 on page 62](#) shows the location of the Launch CallPilot Manager button. See the *CallPilot Manager Setup and Operation Guide* for more information on the CallPilot Manager application.

The **Launch CallPilot Manager** button is only visible in Element Manager to groups with the CallCenter privilege assigned to them.

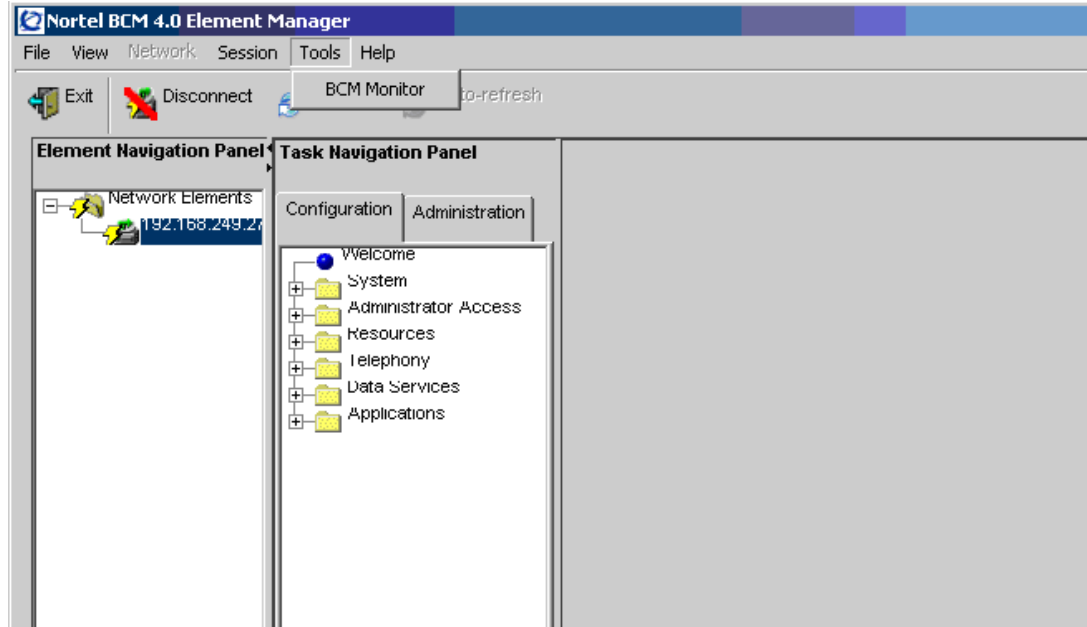
Figure 15 Launch CallPilot Manager button



You can access the BCM Monitor through the **Launch BCM Monitor** button under **Administration Task > Utilities > BCM Monitor**.

[Figure 16 on page 63](#) shows the location of the **Launch BCM Monitor** button.

Figure 16 Launch BCM Monitor button



BCM feature licensing

You require a keycode to enable software features on the BCM200/400. The keycode is a 24-digit code that authenticates the feature or bundle of features you purchased for your BCM.

To obtain and load a keycode you require the following:

- authorization code for the desired feature to demonstrate proof of ownership
- system ID of the system to which you want to apply the new feature

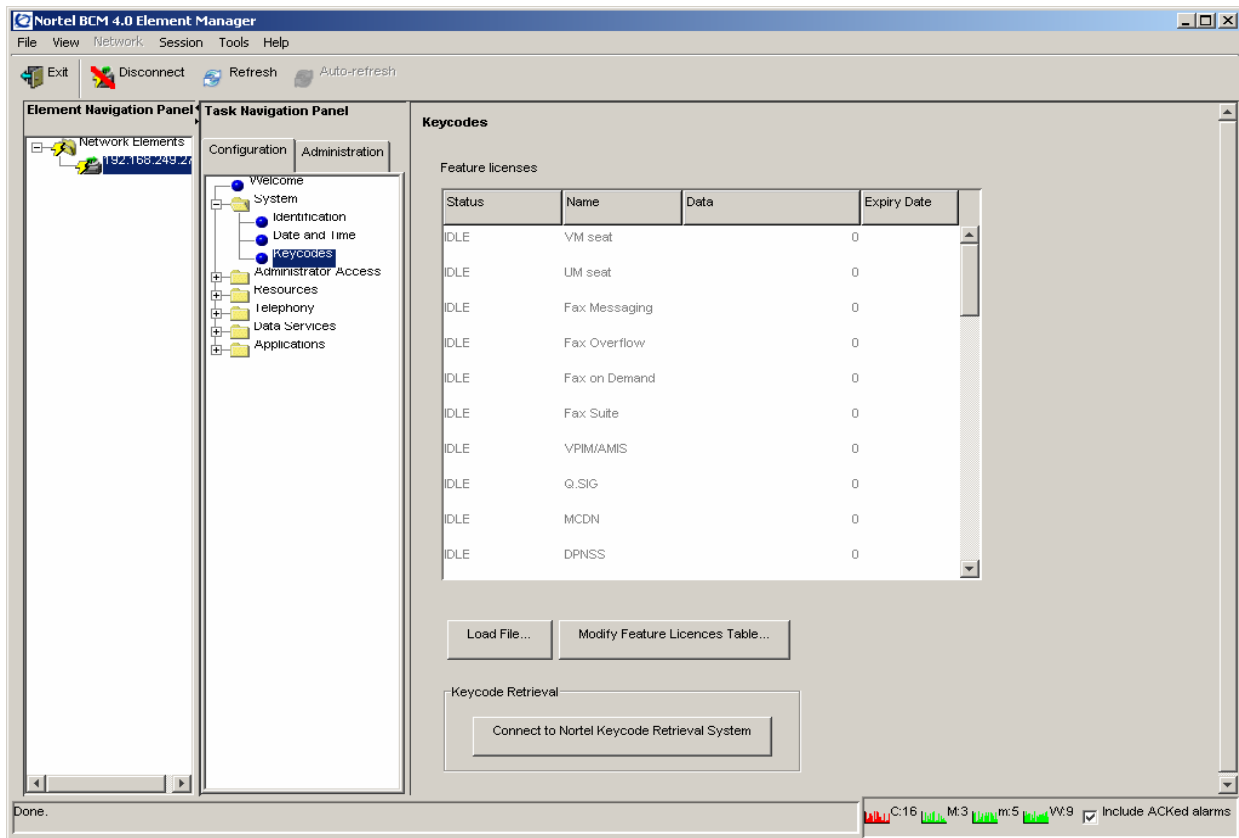
The authorization code is a six-digit code you receive for each of the features you purchase. The authorization code can be found on the label affixed to the “Keycode information sheet” on the last page of the *Keycode Installation Guide* (N0060625).

[Figure 17 on page 64](#) shows the Element Manager keycode panel. See the *Keycode Installation Guide* (N0060625) for details on BCM keycodes.



Note: You receive one keycode whether you purchase one feature or a bundle of features. You receive an authorization code for each feature you purchase. For example, if you have one feature, you receive one authorization code and one keycode. If you purchase four features, you receive four authorization codes and one keycode.

Figure 17 BCM Keycode panel



BCM Help system

The following types of help information are available to you in BCM Element Manager to help you understand how to program your BCM:

- [“Menu bar Help” on page 64](#)
- [“Field-level Help” on page 66](#)
- [“Context-sensitive Help” on page 66](#)

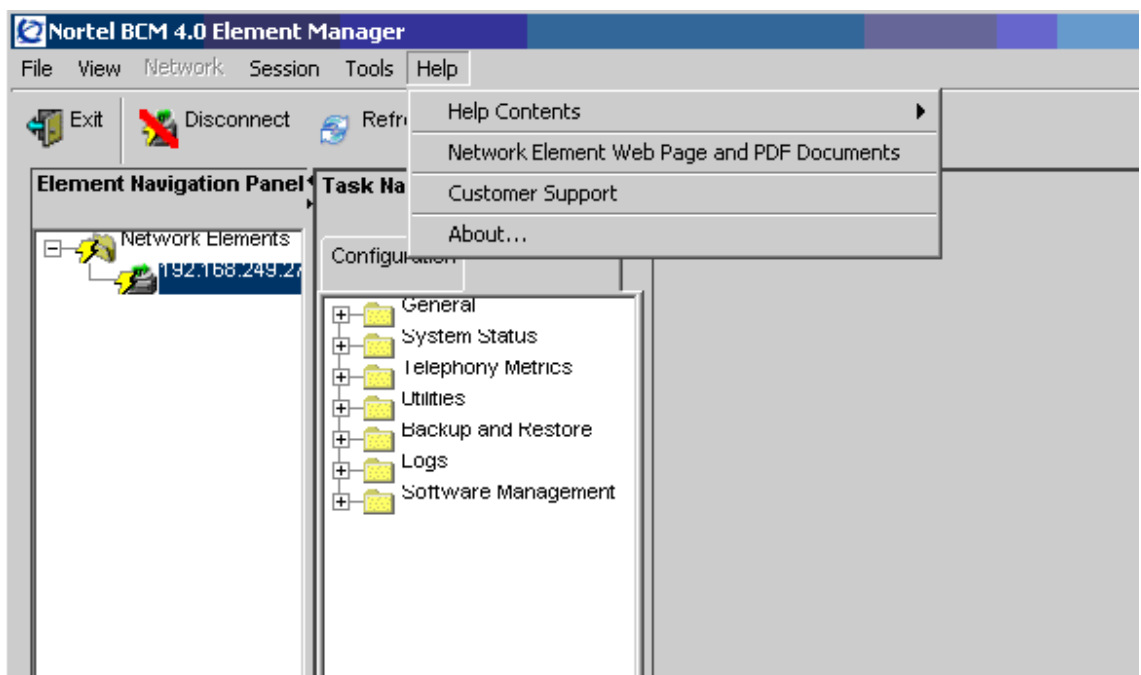
Menu bar Help

The menu bar help provides access to the entire Help system, which includes online help and user manuals in PDF. Table 10 shows the help elements available from menu bar Help.

[Figure 18 on page 65](#) shows the pull-down menu from the Help on the menu bar.

Table 10 Element Manager help elements

Help menu option	Description
BCM Web Page and PDF Documents	Link to PDF documents located on the BCM web page.
Contents	Opens a browser window that shows the help information by contents or index and allows a search.
Customer Support	Opens a browser to a Nortel Networks customer support web site
About	Provides information about the BCM Element Manager software.

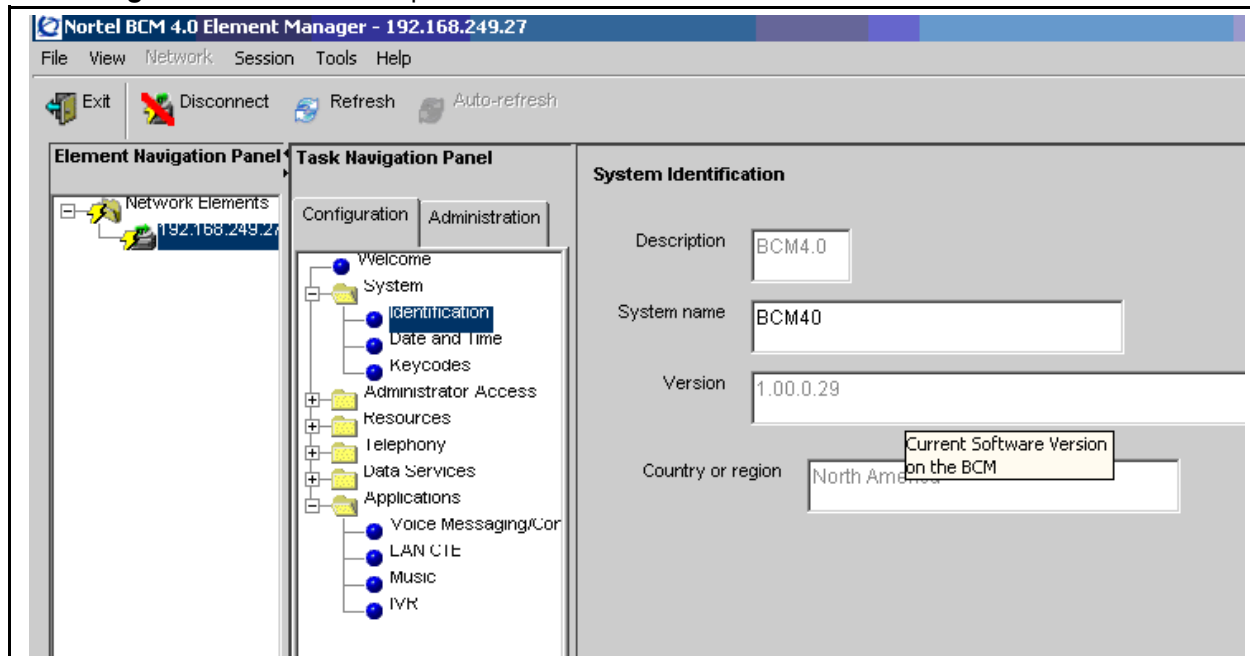
Figure 18 BCM Element Manager menu bar help

Field-level Help

When you position the cursor over a field, a pop-up box provides a brief description of the information required in the field.

Figure 19 shows an example of a field-level help pop-up box.

Figure 19 Field-level Help

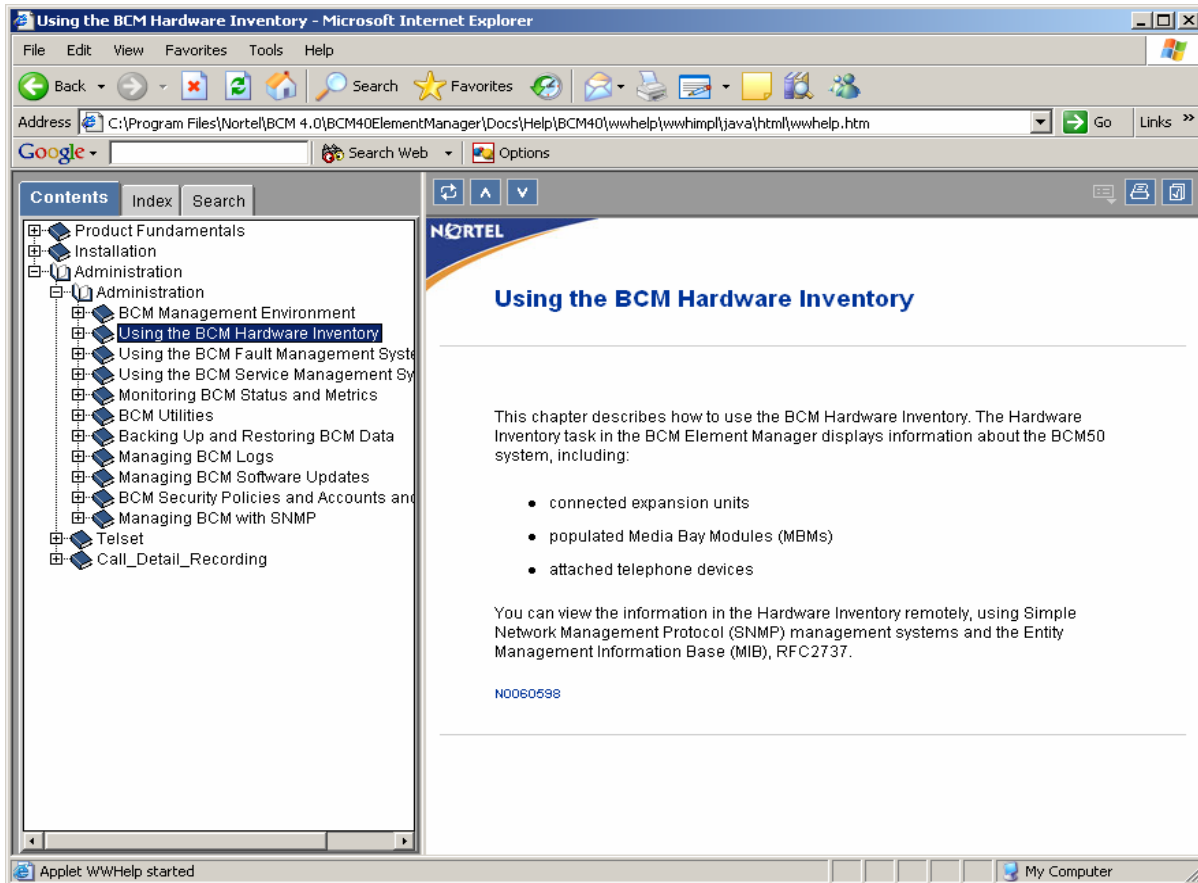


Context-sensitive Help

You can view context-sensitive Help by clicking on a navigation tree heading, tab heading, or field heading of a connected BCM device and pressing the F1 function key. This help opens an HTML page containing overview information or panel descriptions specific to the selected heading. Once the HTML help module opens, it also provides links to tasks and other features related to the panel function.

Figure 20 on page 67 shows the HTML page opened when context-sensitive help is selected. Context-sensitive help does not contain Element Manager program-specific information, for example the title bar, menu bar, or status bar.

Figure 20 Context-sensitive HTML page



BCM common file input/output processes

Many BCM tasks require task data to be transferred, to or retrieved from, different destinations or sources. BCM can use the following data repositories when transferring or retrieving task data:

- BCM
- personal computer
- network folder
- FTP server
- SFTP server
- USB storage device
- HTTP/HTTPS server

Table 11 shows the data repositories that can be used for transferring task data to or from your BCM device during a task that requires data input or output.

Table 11 Task data source and destination repositories

Task Data Repository	Backup and Restore	Logs	Software Updates	Keycodes
The BCM	Y	N	N	N
Personal computer	Y*	Y*	Y	Y
Network folder	Y	Y	Y	Y
FTP	Y	Y	Y	N
SFTP	Y	Y	N	N
USB storage device	Y	Y	Y	N
HTTP/HTTPS Server	N	N	Y	N

* Available only for **On Demand** request of a task; not available for tasks to be run at a later time.

Comparison of data repositories

Each data repository has its advantages and disadvantages. Use this table to determine which data repository solution matches your priorities. For example, if security is a primary concern for you, consider setting up an SFTP or HTTPS server. If you are looking for a data repository solution that is easy to implement, the BCM, a personal computer, and a USB drive are all relatively easy to set up.

Table 12 Comparison of data repository solutions

Task Data Repository	Ease of Use	Speed	Security
BCM	H	H	M
Personal computer	H	L/M/H	M
Network folder	M	L/M/H	M
USB	H	H	L
FTP	M	M	L
SFTP	L	L	H
HTTP/HTTPS	L	M	L/H

The following sections contain information to help you choose the best data repository solution for your environment and provide tips for implementation.

The BCM

Transferring information on the BCM is quick and easy, but does not protect your data in the event of damage to the BCM. It makes an ideal solution in small environments where the BCM is the only computer on site, and where no network resources are available.

Personal computer

Storing information on a personal computer is a safe option either for short-term storage, or for environments where only one computer is used to access Element Manager. If you are using a personal computer to store BCM information, ensure that you do not have multiple administrators storing backup information on multiple computers, as this can lead to version control issues. The speed of transferring information to or from a personal computer is based on the speed of the network. Similarly, the security of the transfer is based on the security of the network. While this is a good solution for on-demand transfers, it is not an option for scheduled tasks.

Network folder

A network folder is the only solution that covers backups, logs, software updates, and keycodes. You must make sure that the folder is set up as a shared Windows resource and the BCM is properly configured to have write access to the network folder. For information on setting up a network folder, contact your network administrator. Saving information to a network folder can take a significant amount of time. The speed and security of the transfer are based on the speed and security of the network. See Table 13 for the information required to use a network folder.

Table 13 Configure Network Folder attributes

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder.
User Name	Enter the user name associated with the network folder.
Password	Enter the password associated with the network folder.
Directory	Enter the path to the subdirectory, as applicable.

FTP servers

Storing information on an FTP server is similar to storing information in a network folder. It offers a centrally accessible way to store BCM data. The speed of transferring to an FTP server is based on the speed of your network. Transfers to an FTP server generally have a low level of security, unless the transfer is set up to run through a VPN.

See Table 14 for the information required to use an FTP server.

Table 14 Configure FTP server attributes

Attribute	Action
FTP or server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.

Table 14 Configure FTP server attributes

Attribute	Action
Password	Enter the password associated with the FTP server.
Directory	Enter the path to the subdirectory, as applicable.

SFTP servers

The process of using an SFTP server is similar to the process for using an FTP server. However, an SFTP server has a greater level of security than an FTP server, and more credentials are required to use an SFTP server. You must set up and manage security keys and certificates, including generating a SSH key, which you must then install on the SFTP server. For information on using SFTP servers and generating SSH keys, see [Chapter 4, “BCM Security Policies and Accounts and Privileges,”](#) on page 73.

See Table 15 for the information required to use an SFTP folder.

Table 15 Configure FTP or SFTP Server attributes

Attribute	Action
FTP or SFTP Server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Password	Enter the password associated with the SFTP server.
Directory	Enter the path to the subdirectory, as applicable.

USB storage device

Storing information to a USB storage device is a very quick way of saving information, as the transfers occur much more quickly than network or FTP transfers, depending on the speed of the USB drive. The USB storage device must be connected to the BCM. The backup and log information can be saved only to the top level of the USB storage drive file hierarchy. Transfers from the BCM to a USB storage device are relatively secure, but a USB storage device is small and can be stolen easily if it is not in a secure location. The USB storage device must be formatted as a FAT32 drive. The following USB storage devices are supported:

- SanDisk 512 MB Cruzer Mini USB 2.0 Flash Drive
- SanDisk 256 MB Cruzer Mini USB 2.0 Flash Drive
- Lexar 512 MB Jumpdrive Sport 2.0/Rubber C
- Kingston 256 MB 2.0 DataTraveler Memory (DataTraveler PLUS)
- Kingston DataTraveler USB FlashDrive 256 (DataTraveler ELITE)
- Apacer 256 MB USB 2.0 HT202 Handy Drive



Note: A USB port is not supported on BCM 1000 platforms.

HTTP/HTTPS server

HTTP and HTTPS servers are available as an option only for software updates. It can be a good solution if you have many BCMs that require software updates from a centralized location. See Table 16 for the information required to use an HTTP or HTTPS server.

Table 16 Configure HTTP or HTTPS server attributes

Attribute	Action
HTTP Server	Enter the hostname or IP address of the HTTP server.
User Name	Enter the user name associated with the HTTP server.
Password	Enter the password associated with the HTTP server.
Directory	Enter the path to the subdirectory, as applicable.
Use HTTPS	Specify whether the server requires SSL

Chapter 4

BCM Security Policies and Accounts and Privileges

BCM Security Policies and Accounts and Privileges allows you to establish system-wide security policies and maintain access security on your system using settings on the Element Manager. This chapter describes the security policies that you can configure through the BCM Element Manager. The BCM provides security capabilities such as NAT, VPN, DoS alert, data communication, DHCP, VLAN, and PPP.



Security Note: This symbol is 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.

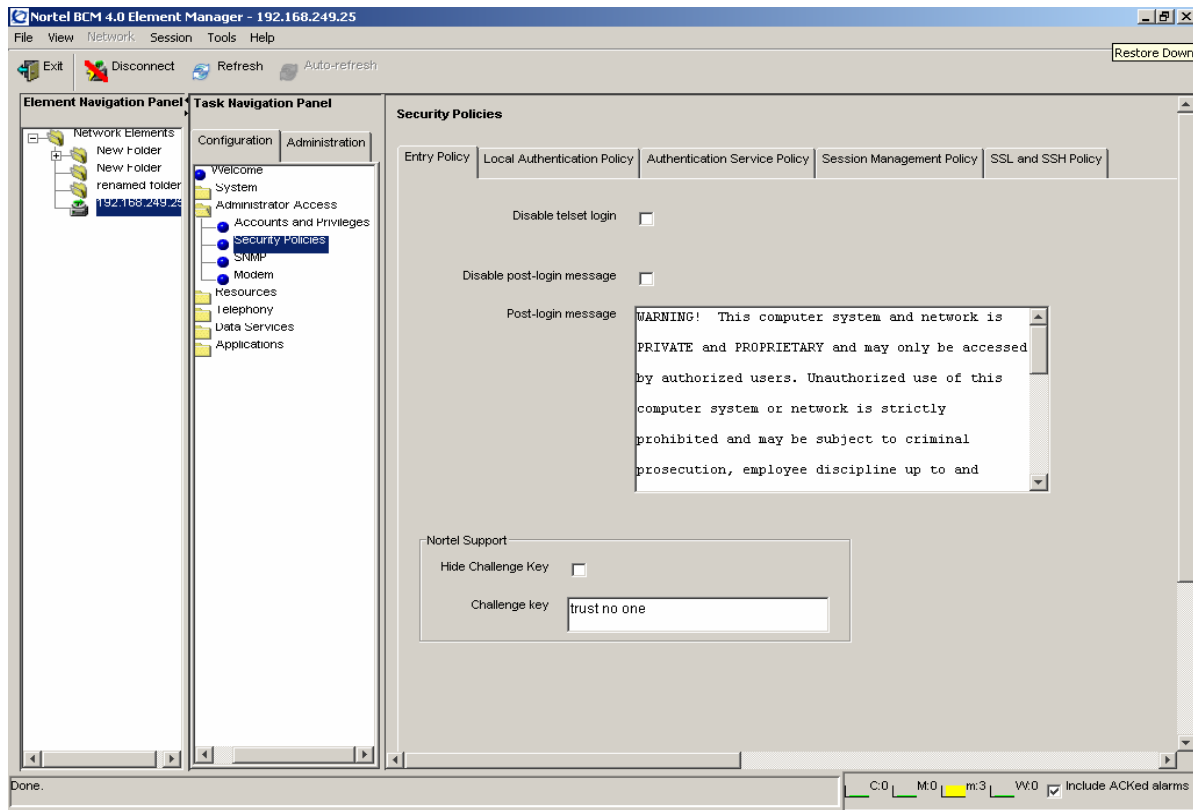
The information in this chapter is organized as follows:

- [Security Policies panel](#) on page 73 describes the fields on the Security Policies panel
- [Configuring system security policies](#) on page 78 provides procedures for setting system-level security that applies to all configured users, for installing the web server certificate, and for downloading the SSH key-pair
- [Configuring user accounts, user groups and privileges](#) on page 87 provides procedures for managing access to both the Element Manager and to the telset configuration menus.
- [User account and user group management fundamentals](#) on page 96 provides information about user accounts, passwords, and privileges.
- [Accounts and Privileges panel](#) on page 110 describes the fields on the Accounts and Privileges panel.
- [BCM security fundamentals](#) on page 119 provides an overview of the BCM security policies such as firewalls, protocols, encryption, audits, certificates, and site authentication.

Security Policies panel

The fields that make up the Security Policies panel are described in this section. When you set security policies, they apply to the entire BCM system rather than to individual users.

Figure 21 Security Policies panel



The following table describes the fields on this panel:

Table 17 Security Policies fields

Attribute	Value	Description
Entry Policy tab		
Disable telset login	check box	When selected, specifies when users cannot access the system through any telset interface. Default: unchecked Tip: If this is enabled, and DHCP changes the system IP address, you can determine the new IP address by way of the OAM port.
Disable post-login message	check box	When checked, specifies that the post-login security warning will not open on login. Default: not checked
Post login message	text	Displays the post-login security warning. The warning can be edited to customize the message for your system.
Nortel Support		

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Challenge key		Specifies an alphanumeric key. This key is part of the access information your service technician requires to remotely access your system. Default: trust no one. If you change the default string, retain a record of the new string so that Nortel Technical Support can access your system during a support service call. This key must be at least one character long to allow Nortel support operation.
Show/Hide	check box	When checked, displays asterisks to hide the characters used in the challenge key. Default: not checked.
Local Authentication Policy tab		
Credential Complexity		
Credential Type	Element Manager: Alphanumeric Telset: Numeric	Specifies the variety of characters an alphanumeric password must have. The required number of each type is defined by the complexity level. Note: User IDs are not case-sensitive. Telset interface passwords must be numerical. Password complexity for these passwords defines how many unique digits are required.
Minimum User ID length	Element Manager: Alphanumeric 1-32 Telset: Numeric 1-16	Specifies the minimum number of characters that the system requires for each type of credential.
Minimum password length	Element Manager: Alphanumeric 1-32 Telset: Numeric 1-16	Specifies the minimum number of characters that must be entered for a new password. Note: Alphanumeric passwords are case-sensitive. Note: This setting must be the same as or greater than the complexity level setting. Example: If you have a complexity level of two, two different types of characters or two unique numbers, the password must be at least two characters long.
Password Complexity Level (Element Manager)	0 1 2 3 4	Defines the number of character types required for an alphanumeric password. Default: 3 0: No complexity checks 1: only one character type is required 2: at least two character types are required 3: at least three character types are required. 4: all four character types are required Note: A password complexity higher than 0 will ensure that the user name is not used as the password. Check minimum length setting to ensure that it is equal to or greater than the complexity level. Password complexity consists of the following types: <ul style="list-style-type: none"> • upper case alphabet (English) • lower case alphabet (English) • westernized Arabic numbers • non-alphanumeric characters (\$, !, %, ^, period, comma)

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Password Complexity Level (telset interface)	1 2 3 4 5	Specifies the number of unique digits that must be part of a telset password: 0: No complexity checks 1: one unique digit 2: two unique digits 3: three unique digits 4: four unique digits 5: prevent consecutive numbering Note: A password complexity higher than 0 will ensure that the user name is not used as the password. Check the minimum length setting to ensure that it is equal to or greater than the complexity level.
Lockout on Failed Logon		
Enable lockout	check box	When checked, specifies that enable lockout rules apply to users.
Lockout counter	digits	Specifies the number of times the user can attempt to enter an invalid password before the user is locked out. Default: 25; for increased security, set this number to 5. Refer to “View by Accounts” on page 113 (Locked Out box) and “View by Account: General” on page 115 (Login History)
Lockout duration (min)	minutes	Specifies the amount of time after the user is locked out before they are allowed to login again. Reset the lockout counter to zero. Default: 30
Lockout counter reset	minutes	Specifies the number of minutes after a lockout before the lockout counter is automatically reset to zero. Default: 30 Example: If the lockout counter reset is set at 30 minutes and a user enters invalid passwords, but does not reach the lockout counter threshold, then waits 30 minutes before trying again, the lockout counter resets and begins counting from 1 again. If the user enters invalid passwords until the lockout counter threshold is reached, the Lockout duration determines when the user can sign back onto the system.
Password Expiry		
Enable password expiry	check box	When checked, specifies that the account will expire at a specified time.
Days before password expire	up to 256	Enter the number of days the a password can remain valid before it must be changed.
Warning days before password expire		Enter the number of days prior to password expiry that a user will receive notification.
Password History		
Enable password history	checkbox	When checked, the BCM stores a list of previously used passwords and prevents users from re-using them.
Password history length	numeric value	Enter the number of previously used passwords to be stored and checked for this account to prevent password re-use.
Authentication Service Policy tab		

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Account management	drop down menu	Specifies the method used for authenticating users when they log in. Options are Local Authentication and RADIUS. If RADIUS is selected, you must also select the Enabled check box.
Server priority	Primary Secondary	Specifies which RADIUS server will be used as the primary server for authentication, and which server will be used as a secondary server to authenticate users when the primary server is unavailable.
Server name	alphanumeric	Name of the RADIUS server.
Server IP address	<IP address>	IP address of the RADIUS server.
Server Port	numeric	Port number of the RADIUS server.
Server shared secret	alphanumeric	Key required for the BCM to communicate with the RADIUS server. Nortel recommends that the key be at least 64 characters in length.
Server message timeout	numeric	Length of time to wait for the server to respond to a request for authentication before timing out. Nortel recommends a setting of 2.
Server retries	numeric	Number of times to retry connecting with the primary server before using an alternate means of authenticating the user. Nortel recommends a setting of 2.
Enabled	checkbox	When selected, specifies that RADIUS authentication will be used. You must also select this check box before the BCM will use RADIUS authentication.
Session Management Policy tab		
Session time out (min.)	minutes	Specifies the number of minutes a logged-in user account can be inactive before the system ends the session and logs out the account. If this field is left blank, the session is only ended when the user logs off.
Active sessions		
User ID	Read-only	Displays the user ID of the active session.
IP address	Read-only	Displays the IP address of the active session.
Login date	Read-only	Displays the login date of the active session.
SSL and SSH Policy tab		
SSL		
Install Web Server Certificate (SSL)	Button	Downloads application security certificates to the server where SSH is running to ensure a secure copy connection for operations like backup and restore, upgrades and patches.
SSH		
Fingerprint	alphanumeric	Displays an identifier for the application security certificate.

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Generate new SSH key-pair	Button	Opens the file system browser to allow a system-specific security certificate and the accompanying Private key to be selected for SSL.
Transfer Public Key	Button	Downloads a public security certificate or an SSH key-pair to an SFTP server.

Configuring system security policies

This section provides procedures for setting system-level security that applies to all configured users, for installing the web server certificate, and for downloading the SSH key-pair. Use the tabs on the security policies panel to perform the following procedures.

Entry Policy tab

Use the Entry Policy tab to perform the following procedure:

- [“Setting system access control policies” on page 79](#)

Local Authentication Policy tab

Use the Local Authentication Policy tab to perform the following procedures:

- [“Setting credential complexity” on page 79](#)
- [“Setting lockout policy for failed logins” on page 80](#)
- [“Setting password expiry policy” on page 81](#)
- [“Setting password history policy” on page 81](#)

Authentication Service Policy tab

Use the Authentication Service Policy tab to perform the following procedures:

- [“Setting the authentication method” on page 81](#)
- [“Configuring an authentication server” on page 82](#)

Session Management Policy tab

Use the Session Management Policy tab to perform the following procedure:

- [“Setting the idle session timeout” on page 86](#)

SSL and SSH Policy tab

Use the SSL and SSH Policy tab to perform the following procedures:

- “[Uploading a Web Server Certificate](#)” on page 86
- “[Transferring an SSH Key-Pair](#)” on page 87

Setting system access control policies

Setting system access control policies allows the administrator to set system access rules.

To set system access control policies

- 1 Select **Configuration > Administrator Access > Security Policies > Entry Policy**.
- 2 Click in the **Disable post-login** message box to prevent the Warning message from opening after login. Leave this box unchecked if you want the Warning delivered.
- 3 Enter a new warning in the **Post-login message** box, or leave the default warning in the box.
- 4 Click in the **Disable telset login** box to prevent users from having administrating the system through any telset interface.
- 5 Use the default **Nortel Challenge Key**, or enter a new one. If you enter a new Nortel Challenge Key, make a record of the challenge key you use. Check the Show/Hide box if you want to display asterisks rather than the characters used in the Challenge Key.

Setting credential complexity

Setting credential complexity allows the administrator to define the rules for password length and password complexity.

To set credential complexity

- 1 Select **Configuration > Administrator Access > Security Policies > Local Authentication Policy**.
- 2 In the **Credential Complexity** section, under the **Credential Type** column, select the credential type.
- 3 Under the **Minimum User ID Length** column, enter the required number of characters or digits for a user’s ID.
- 4 Under the **Minimum Password Length** column, enter the required number of characters or digits for the user’s password.
- 5 Under the **Password Complexity Level** column, enter a number from 1 to 5 that represents the password complexity level requirement, or enter 0 if no complexity check is required. For an alphanumeric password, the level is from 0 to 4. For a numeric password, the level is from 0 to 5.

Variable Table

Variable	Value
Complexity Level (Element Manager)	0: no complexity checks 1: only one character type is required 2: at least two character types are required 3: at least three character types are required. 4: all four character types are required A password complexity higher than 0 will ensure that the user name is not used as the password. The four character types are: <ul style="list-style-type: none"> • lowercase letters • uppercase letters • numbers • !^, @#\$%& and spaces
Complexity Level (Telset)	0: no complexity checks 1: one unique digit 2: two unique digits 3: three unique digits 4: four unique digits 5: prevent consecutive numbering (For example, 1935 or 8634971 are valid passwords. Passwords such as 1234, 3456, 2468, 8642,8765, or 9753 would be invalid.)

Setting lockout policy for failed logins

Setting Lockout on Failed Login allows the administrator to set lockout rules. Administrators can unlock accounts that have been locked out; see [“Re-enable a locked-out user” on page 94](#) for more information.

To set lockout policy for failed logins

- 1** Select **Configuration, Administrator Access, Security Policies > Local Authentication Policy**.
- 2** In the **Lockout on Failed Login** section, select the **Enable lockout** check box to enable lockout capabilities.
- 3** In the **Lockout counter** box, enter a number that represents the number of times a user can try to login with an incorrect password.
- 4** In the **Lockout duration** box, enter the number of minutes the user is locked out after the Lockout counter threshold is reached.
- 5** In the **Lockout counter reset** box, enter the number of minutes to wait to reset the Lockout counter.

Setting password expiry policy

Use this procedure to enable a password expiry policy.

To set password expiry policy

- 1 Select **Configuration, Administrator Access, Security Policies > Local Authentication Policy**.
- 2 In the **Days before password expire** box, enter the number of days that a password can be used before it expires.
- 3 In the **Warning days before password expire** box, enter the number of days prior to password expiry that the user will receive a notification.
- 4 Select the **Enable** checkbox to enable the password expiry policy.

Setting password history policy

You can use the password history feature to prevent users from re-using the same password. Administrators can configure the number of previous passwords to store and check.

To set password history

- 1 Select **Configuration, Administrator Access, Security Policies > Local Authentication Policy**.
- 2 In the **Password history** section, select the **Enable Password History** box.
- 3 In the **Password history length** box, enter the number of previous passwords to store and check for an account.

Setting the authentication method

By default, users are authenticated on the local BCM system. In a network with multiple BCM systems, you can choose to authenticate users on a centralized server using RADIUS (Remote Authentication Dial In User Service).

The BCM RADIUS client is compliant with the RADIUS protocol described in RFC 2865, and supports the following authentication and authorization functions:

- ACCESS-REQUEST messages
- ACCESS-ACCEPT messages

Other functions, such as challenge key and accounting messages, are not supported.

If you use RADIUS for authenticating and authorizing users, and the RADIUS servers are not in-service or are out-of-contact, the BCM will revert to using local authentication.

When you select RADIUS as the authentication method, user IDs and passwords will be authenticated on the RADIUS server for the following tasks:

- administration of the BCM using Element Manager
- access to the BCM website
- access to the BCM Monitor
- dial-in access to the BCM using modem or ISDN
- Contact Centre administration
- BCM Amp configuration
- IVR administration and logging
- CTE DA ProAE
- terset administration
- IP set registration
- voicemail and web-based administration
- Call Detail Recording functionality

To set the authentication method

- 1 Select **Configuration, Administrator Access, Security Policies > Authentication Service Policy**.
- 2 From the **Account Management** drop-down menu, select **Local Authentication** or **RADIUS**. If you select RADIUS, follow the procedure for [“Configuring an authentication server”](#) on page 82.

Configuring an authentication server

To authenticate users on a centralized RADIUS server, you must configure the server using Element Manager.

To configure an authentication server in Element Manager

- 1 Select **Configuration, Administrator Access, Security Policies > Authentication Service Policy**.
- 2 Select a server to be the primary authentication server. Click in each column of the table to enter the following attributes:

Column	Value
Server name	Name of the server to be used for authentication
Server IP address	IP address of the server to be used for authentication
Server Port	Port number of the server to be used for authentication

Shared Secret	Key required for the BCM to communicate with the authentication server
Server Message Timeout	Length of time to wait for the server to respond to a request for authentication before timing out
Server Retries	Number of times to retry connecting with the primary server before using an alternate means of authenticating the user.
Enabled	Check to enable the use of a RADIUS server authentication.

3 Repeat step 2 to configure the secondary server.

Vendor specific attributes

The BCM requires Vendor Specific Attributes (VSAs) to be present in RADIUS client requests. The BCM Webpage provides a RADIUS dictionary that defines the Nortel-specific attributes. The attributes in the dictionary are defined for a Funk RADIUS server; however, the RADIUS client in BCM complies with RFC 2865 and can be used on other RADIUS servers.

In an ACCESS-REQUEST message, the BCM will look for the attributes listed in Table 18.

Table 18 Attributes in an ACCESS-REQUEST message

Attribute Name	Description
NAS Identifier	The hostname of the BCM (string)
IP	The IP address of the BCM
Calling Station ID	The IP address/DN of the client attempting the request

In an ACCESS-ACCEPT message, the BCM will look for the attributes listed in Table 19.

Table 19 Attributes in an ACCESS-ACCEPT message

Attribute Name	Value	Description
RADIUS attribute type	26	Vendor specific attribute
Vendor type	562	Northern Telecom (Nortel)
Vendor attribute type	166	BCM privilege level of the user being authenticated. Enter this level as a hex integer.
Privilege level	0-36 (see Table 20)	Privilege level of user, entered in big endian (network byte order).

BCM requires the RADIUS server to provide one or more privilege levels when the user authentication is accepted. Table 20 lists the privilege levels. These must be provided as a 32-bit integer in big endian format (network byte order).

Table 20 Privilege levels

Privilege name	Value	Description
VoiceMailAdmin	0	Voice Mail Administrator
Contact Center	1	MMCC - Administrator
SBAInstaller	2	Set Based Administrator Level 4
SBASystemCoord	3	Set Based Administrator Level 3
SBASystemCoordBasic	4	Set Based Administrator Level 2
SBABasic	5	Set Based Administrator Level 1
Security	6	Security Administrator
CTEApp	7	LAN CTE DA Pro AE User
SBA - IP Set Registration	8	IP set registration privilege - from IP telephone sets
Application - BCMMonitor	9	BCM Monitor user
CDRApp	10	CDR Application Privilege
Modem Login	11	Dial-in PPP user
GuestLogin	12	Access to BCM Web pages - user level
AdminDownload	13	Administrative application download
ExclusiveAccess	14	Access to the BCM when exclusive access flag enabled.
Admin	16	Access to the BCM configuration.
DataAdmin	17	Access to the data portion of CIM/XML interface.
RemoteAccess	18	Access to remote access fields of BCM configuration.
Guest	19	Access to all of the BCM configuration for read-only access.
VoiceAdmin	20	The ability to administer the telephony portion of the BCM configuration.
BackupOperator	21	The ability to backup a BCM.
RemoteMonitoring	22	The ability to remotely connect to and manage the BCM configuration (ie. SNMP configuration).
SoftwareUpgrade	23	The ability to upgrade the BCM.
AlarmViewer	24	The ability to view the alarm screen.

Operational Logs	26	The ability to download operational logs.
Diagnostic Logs	27	Full access to download any logs.
Application - IVR	28	The ability to configure IVR on the BCM.
ISDN - Dial-in	30	The ability to use ISDN for dial-in.
WAN - Dial-in	32	The ability to use WAN for dial-in PPP access.
System - Serial Port	36	The ability to configure the BCM through the serial port.

Setting the idle session timeout

You can use the idle session timeout feature to automatically log out users who have been inactive for a specified period of time. Follow this procedure to specify the period of time before inactive sessions are timed out.

To set the idle session timeout

- 1 Select **Configuration, Administrator Access, Security Policies > Session Management Policy**.
- 2 In the **Session timeout** box, enter the number of minutes to wait after a period of inactivity before the session times out.

Uploading a Web Server Certificate

This procedure allows you to upload a private security certificate to replace the generic web certificate provided with BCM. Using a custom site-specific certificate, you can have site validation which will eliminate the security warnings.

For further information about security certificates, see [“Security certificate” on page 123](#).

To upload a Web Server Certificate

- 1 Select **Configuration, Administrator Access, Security Policies > SSL and SSH Policy**.
- 2 In the **SSL** section, click the **Install Web Server Certificate** button.
- 3 On the **Transfer Certificate** browse panel, locate and select the security certificate file.
- 4 Click the **Transfer Certificate** button.
- 5 On the **Transfer Private Key** browse panel, locate and select the private key file.
- 6 Click the **Transfer Private Key** button.
- 7 On the Install Web Server certificate window, click **OK** to install the certificate.

Transferring an SSH Key-Pair

Transferring an SSH Key-Pair allows the administrator to download a public security certificate or an SSH key-pair. The new certificate must be installed on each sftp server the BCM communicates with to ensure a secure connection for operations like backup and restore, and software updates.

To transfer an SSH Key-Pair

- 1 Select **Configuration, Administrator Access, Security Policies > SSL and SSH Policy**.
- 2 In the **SSH** section, click the **Generate New SSH Key-pair** button.
The new key is put on the computer running BCM.
- 3 Click the **Save** button.
- 4 For SSH Key-pair, click the **Transfer Public Key** button.
- 5 On the **Save** dialog box, locate and select the public key file.
- 6 Click **Save** to transfer the files.

Configuring user accounts, user groups and privileges

User Management provides procedures for managing access to both the Element Manager and to the telset configuration menus. You can control when users can log on, how much they can see, and what they can do within the configuration menus.

The Accounts and Privileges context panels allow you to:

- view the user ID and last successful login of the current user
- view user accounts and add, delete, and modify accounts
- view group profiles and add, delete, and modify groups

Job Aid

These links provide navigation to the sections of the panel for each user management item:

Panel tabs	Tasks
“Current Account” on page 111 “View by Accounts” on page 113	“Enabling and disabling exclusive access” on page 96 <ul style="list-style-type: none"> • “Adding a new user account” on page 88 • “Modifying a user account” on page 89 • “Deleting a user account” on page 90 • “Changing a user’s password” on page 91 • “Changing the current user’s password” on page 91 • “Adding callback for a dial-up user” on page 90 • “Re-enable a locked-out user” on page 94
“View by Account: General” on page 115	<ul style="list-style-type: none"> • “Enabling and disabling an account” on page 95
“View by Account: Group Membership” on page 116	<ul style="list-style-type: none"> • “Adding a user account to a group” on page 93 • “Deleting a user account from a group” on page 93
“View by Groups” on page 117	<ul style="list-style-type: none"> • “Creating a group” on page 92 • “Deleting a group” on page 92
“View by Groups: General” on page 117	<ul style="list-style-type: none"> • “Modifying group privileges” on page 92
“View by Groups: Members” on page 119	<ul style="list-style-type: none"> • “Adding a user account to a group” on page 93 • “Deleting a user account from a group” on page 93

Click on the navigation tree heading, then press F1 to access general information about user management.



Security note: This symbol is 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.

Adding a new user account

Administrators can create user accounts when the BCM is configured to authenticate users locally. After you create a new user account, you can assign groups to that account. Groups are sets of privileges based on user tasks or roles. For information about creating groups and assigning groups to accounts, see [“Creating a group” on page 92](#) and [“Adding a user account to a group” on page 93](#).

To add a new user account

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Account** tab.
- 2 Click the **Add** button.

- 3 In the **Add Account** dialog box, enter a description of the account in the **Description** field.
- 4 Enter the user's identifier in the **User ID** field.
- 5 In the **User password** field, enter the user's password.
- 6 In the **Confirm password** dialog box, enter the user's password again.
- 7 In the **Telset password** field, enter the telset password for the user.
- 8 In the **Confirm password** dialog box, enter the user's password again.
- 9 If the user is connecting through a modem, enter the number the system dials to contact the client modem in the **Modem Callback Number** field and enter a passcode in the **Modem Callback Passcode** field. Ensure you include the correct routing codes.
- 10 If the user is connecting through ISDN, enter the number the system dials to contact the client in the **ISDN Callback Number** field and enter a passcode in the **ISDN Callback Passcode** field.
- 11 Select the **Change Password on Login** checkbox to force a password change when the user logs into Element Manager.
- 12 Select the **Change Password on Login Telset** checkbox to force a password change when the user logs into Telset.
- 13 Click **OK** to save the user account.

After the account is created, the user can change their own password through the Current Account panel. Refer to [“Changing the current user's password” on page 91](#).

Modifying a user account

As an administrator, you can modify user accounts.

To modify a user account

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Account** tab.
- 2 Select an existing user on the Accounts table and click the **Modify** button.
- 3 On the Modify Account dialog box, make the changes you require.
- 4 If callback for dial-up users is required, see [“Adding callback for a dial-up user” on page 90](#).
- 5 If telset access is required, see [“Adding Telset access for a user” on page 90](#).
- 6 Click **OK** to save the user account.

Adding callback for a dial-up user

As an administrator, you can provide callback access to a user who is accessing the system through a dial-up connection.



Callback security

If a user is connecting to the system using a 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.

To add callback for a dial-up user

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Account, Remote Access** tab.
- 2 Select an existing user on the Accounts table.
- 3 If the user is connecting through a modem, enter the number the system dials to contact the client modem in the **Modem Callback Number** field and enter a passcode in the **Modem Callback Passcode** field. Ensure you include the correct routing codes.
- 4 If the user is connecting through ISDN, enter the number the system dials to contact the client in the **ISDN Callback Number** field and enter a passcode in the **ISDN Callback Passcode** field.
- 5 Click **OK**.

Adding Telset access for a user

As an administrator, you can provide an existing user with access to the system through a set-based connection.

To add Telset access for a user

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Account** tab.
- 2 Select an existing user on the Accounts table and click the **Modify** button.
- 3 In the **Telset User ID** field, enter the user's identifier.
- 4 In the **Telset Password** field, enter the user's telset password.
- 5 Re-enter the telset password in the **Confirm Password** dialog box.
- 6 Click **OK**.

Deleting a user account

As an administrator, you can delete user accounts when they are not needed.

To delete a user account

- 1 Select **Configuration, Administrator Access, Accounts and Privileges**, and click the **View by Account** tab.
- 2 Select a user on the Users table.
- 3 Click the **Delete** button.
- 4 In the confirmation box, click **Yes** to remove the user account from the system.

Changing a user's password

As an administrator, you can change a user's forgotten password, or reset the user password for each user to enforce regular password-change policy. You can also force a password change when the user logs in.



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

To change a user's password

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Account** tab.
- 2 Select the user record from the table and click **Modify**.
- 3 In the **Modify Account** window, delete the asterisks in the **Password** or **Telset password** field.
- 4 Enter a new password and click **OK**.
- 5 Re-enter the password in the **Confirm Password** dialog box.
- 6 Provide the user with this password and request that they change it as soon as possible through the Current User panel ("[Current Account](#)" on page 111) or click on **Change Password on Login** to make a password change mandatory.

Changing the current user's password

As a user or an administrator, you must change your password periodically.

To change the current user's password

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, Current Account** panel.
- 2 Select the password field that needs to be changed.

- 3 Enter a new password that conforms with the system password policies, which are defined by the administrator during system setup.
A confirmation dialog box appears.
- 4 In the confirmation dialog box, enter the new password again.
- 5 Click **OK**.
The password takes effect the next time you log in.

Creating a group

As an administrator, you can create new groups to satisfy organizational requirements.

To create a group

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Groups** tab.
- 2 Click the **Add** button.
- 3 In the **Add Group** dialog box, enter a name for the new group.
- 4 Click **OK**.
- 5 Select the new group from the **Groups** list.
- 6 In the **Group Privileges** area, click the **Add** button.
- 7 In the **Add Privilege to Group** dialog box, select one or more group privileges to assign to the group and click **OK**. See [“Default groups” on page 98](#) and [“Default access privileges excluding set-based privileges” on page 100](#) for more information.
- 8 Populate the group using [“Adding a user account to a group” on page 93](#).

Deleting a group

As an administrator, you can delete groups as organizational requirements change.

To delete a group

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Groups** tab.
- 2 Select a group and click the **Delete** button.
- 3 Click **Yes** on the confirmation box to remove the groups from the list.

Modifying group privileges

Only user-created groups can be modified; default group privileges cannot be modified.

To modify group privileges

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Groups** tab.
- 2 Select a group and then click the **General** tab.
- 3 To remove privileges, click on the **Group Privileges** tab, select one or more group privileges to delete from the existing group, and click **Delete**. A confirmation dialog box appears; click **Yes** to delete the selected items.
- 4 To add privileges, click on the **Group Privileges** tab, select one or more group privileges to add to the existing group, and click the **Add** button. See [“Default groups” on page 98](#) and [“Default access privileges excluding set-based privileges” on page 100](#) for more information.
- 5 Click **Yes** on the confirmation box to remove the groups from the list.

Adding a user account to a group

As an administrator, you can add user accounts to one or more groups to satisfy access requirements.

To add a user account to a group

- 1 Select **Configuration, Administrator Access, Accounts and Privileges**, and click the **View by Accounts** tab.
- 2 Select a user account and then click the **Group Membership** tab.
- 3 Click the **Add** button.
- 4 In the **Add Account to Group** dialog box, select one or more groups.
- 5 Click **OK**.

Deleting a user account from a group

As an administrator, you can remove user accounts from a group to limit a user’s access.

To delete a user account from a group

- 1 Select **Configuration, Administrator Access, Accounts and Privileges**, and click the **View by Accounts** tab.
- 2 Select a user account and then click the **Group Membership** tab.
- 3 Select one or more groups on the **Accounts in the Member of Groups** table.
- 4 Click the **Delete** button.
- 5 Click **OK** on the confirmation box to remove the groups from the list.

Re-enable a locked-out user

As the administrator you can re-enable a locked-out user when the user has exceeded the login retry threshold.

The system shows an enabled check box under the Locked Out column on the Users table.

To release a locked-out user

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Accounts** tab.
- 2 Select the user record with the **Locked Out status** check box checked.
- 3 Click the **Locked out** check box to clear it.

Enabling and disabling an account

As the administrator, you can enable or disable accounts on an immediate basis or a timed basis.



Security note: Remember to disable unused accounts.

To enable or disable an account immediately

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Accounts** tab.
- 2 Select the user you want to disable/enable on the Accounts table.
- 3 Under the Disabled column, either check (disable) or clear (enable) the check box for the user. The change will apply to the user's next login.

To enable or disable an account on a timed basis

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, View by Accounts** tab.
- 2 Select the user you want to disable/enable on the Accounts table.
- 3 Click in the **Account will be disabled** field, and choose the date and time the account is to be disabled.
- 4 On the General panel, ensure that **Enable account expiry** is selected.

Enabling and disabling exclusive access

As the administrator, you can enable or disable exclusive access for special activities or maintenance. The administrator performing maintenance tasks can lock the system during the maintenance period. When you enable exclusive access, this capability prevents new logins but does not affect existing logins. This functionality is available to administrators only.

To enable/disable exclusive access

- 1 Select **Configuration, Administrator Access, Accounts and Privileges, Current Account** tab.
- 2 Click **Enable Exclusive Access**.
- 3 In the **Enable Exclusive Access** dialog box, select a duration in minutes from the drop-down box that represents the amount of time you want to have exclusive access to the system.

The timer begins to count down. When it reaches zero, exclusive access ends.

- 4 If you no longer need exclusive access, click **Disable Exclusive Access** to stop the timer and end exclusive access.

User account and user group management fundamentals

This section contains information on the following topics:

- [User accounts](#) on page 96
- [Default passwords](#) on page 98
- [Default groups](#) on page 98
- [Default access privileges excluding set-based privileges](#) on page 100
- [Telset access security](#) on page 108
- [Blocking user accounts](#) on page 110

User accounts

User accounts are defined by:

- a unique user ID that is visible only to authenticating services; Element Manager IDs are alphanumeric, and Telset IDs are numeric
- a unique user name assigned for either or both the Element Manager and telset configuration that has a minimum length that you define when you set up the security policies
- a unique password assigned for any user ID that is defined. Either password must satisfy the Password Policy settings for the system that you define when you set up the security policies.
- a list of group attributes which allow the user specific access privileges in the system

After you create an account, you can assign groups to that account. Groups are sets of privileges based on user tasks or roles. For example, if you have a user who is responsible for remote monitoring, you can create an account for that user and then assign a group to the account; the group that you assign would contain the appropriate privileges for that role. The BCM has default groups available, but you can refine the privileges available within a group to suit the needs of your network. In this example, you could assign the default group called Remote Monitoring, which would allow the user to do such things as view metrics and alarms.

You can create up to 200 accounts that require privileges in Element Manager, such as IPSec and PPP. This number does not include accounts supported for voicemail users, contact center agents, and IVR administrators.

The User ID of the account profiles created through the set based interface cannot be modified through the Element Manager.

Two default user accounts are provided:

- The nnadmin account is read only and cannot be deleted or disabled
- The nnguest account provides customers with web-only access. All access to the Apache web server requires a valid administrator username and password

Auditing for user accounts includes:

- creation date, time, and the user ID that created the account
- modify date, time, and the user ID that modified the account
- expiry date and time, if enabled
- login history, including failed attempts and the date and time of the last successful attempt
- an audit log that tracks logged-in user transactions, including user account changes

Remote users can have a callback number assigned as well. This feature allows authentication of remote users calling in through a modem. After authentication, the BCM will call the user back at the number specified.

Nortel recommends that each user have a separate user account (User Name) with a unique password. These are set up by a user with administrator privileges in the Element Manager. The password only shows up as asterisks on the Element Manager panel. If the password is lost, the administrator can reset the password for the user by re-entering the password in the user account. Each user can access their own user information and change their password. User accounts can be disabled, either manually or through dated expiry.

On the telset administration menu (F9*8), only the administrator (SBAInstaller) can enable or disable the telset user IDs and modify or delete telset user passwords.

Default passwords

The following table lists the available default passwords for the Element Manager interface, the telset interface, and the voice mail interface.

Table 21 Default passwords

User ID	Default password	Telset ID	Default telset password	Function	Available at startup?
nnadmin	PlsChgMe!	738662	266344	Read-only installer/system administrator	yes
nnguest	nnguest			Read-only web-only access	yes
		738266	266344	Set-based installer level	no
		738727	727587	Set-based administration	no
		738236	23646	Set-based coordinator functions	no
		738227	22742	Set-based basic access	no
voicemailadmin	PlsChgMe!	738862	266344	Voicemail admin*	no
–	setup	–	–	Router	no

*This account is not created by default. You must add a voicemail account using F9*8.

New accounts are created from the startup profile with a default password of Time4Chg!



Security note: The default Administrator password has full access to the system. The default password should be changed as soon as the initial system setup is complete and system function is verified.

Default groups

The BCM comes with a number of default read-only groups that provide a predetermined set of access privileges. You can assign additional privileges to groups. Table 22 lists the default privilege levels for each default group, which are described in [“Default access privileges excluding set-based privileges” on page 100](#) and [“Telset access security” on page 108](#).

Table 22 Default user account groups

Group Name	Privileges	Notes
SBA Installer	SBAInstaller IP Set Registration	SBA - Installer group access privileges on page 109 IP Set Registration access privileges on page 102
SBA Coordinator+	SBASystemCoord	SBA - System Coordinator+ group access privileges on page 109
SBA Coordinator	SBASystemCoordBasic Guests	SBA - System Coordinator group access privileges on page 109 Guests access privileges on page 104
SBA Basic	SBABasic	SBA - Basic group access privileges on page 110
Voice & Contact Center	VoiceMailAdmin	Only access to voicemail/contact center administration if this is the only group assigned to a user account. Voice Mail & Contact Center access privileges on page 100.

Table 22 Default user account groups (Continued)

Group Name	Privileges	Notes
Contact Center	Contact Center	Only access to the Contact Centre application is available if this is the only group assigned to a user account. Contact Center access privileges on page 101
CDR Application	CDRApp	Only access to the call detail record functions is available if this is the only group assigned to a user account. CDR Appl access privileges on page 102
CTE Application	CTEAppl	CTE Appl access privileges on page 101
BCM Monitor	BCMMonitorAppl	BCMMonitor Appl access privileges on page 102
Administrator	IP Set Registration BCMMonitorApp CDRApp PPP AdminDownload Exclusive Access Admin DataAdmins Remote Access Voice Admins Backup Operators Software Upgrade Alarm Viewer SBA Installer Security CTE Appl Operational Logs Diagnostic Logs VoiceMail and Contact Center Application IVR Network IPsec Modem dial out ISDN dial in ISDN dial out WAN dial in WAN dial out PPOE dial in PPOE dial out System Serial Port	IP Set Registration access privileges on page 102 BCMMonitor Appl access privileges on page 102 CDR Appl access privileges on page 102 PPP Access access privileges on page 102 Admin Download access privileges on page 103 Exclusive Access access privileges on page 103 Admin access privileges on page 103 DATA Admins group access privileges on page 103 Remote Access access privileges on page 104 Voice Admins access privileges on page 104 Backup Operators access privileges on page 105 Software Upgrade access privileges on page 105 Alarm Viewer access privileges on page 106 SBA - Installer group access privileges on page 109 Security access privileges on page 101 CTE Appl access privileges on page 101 Operational Logs access privileges on page 106 Diagnostic Logs access privileges on page 106 Voice Mail & Contact Center access privileges on page 100 Application IVR access privileges on page 106 Network IPsec access privileges on page 106 Modem dial out access privileges on page 106 ISDN dial in access privileges on page 107 ISDN dial out access privileges on page 107 WAN dial in access privileges on page 107 WAN dial out access privileges on page 107 PPPoE dial in access privileges on page 107 PPPoE dial out access privileges on page 108 System serial port access privileges on page 108
Data Administrator	DATAAdmins	DATA Admins group access privileges on page 103
Remote Access	PPP RemoteAccess	PPP Access access privileges on page 102 Remote Access access privileges on page 104
Guests	Guests	Guests access privileges on page 104
Voice Administrator	IP Set Registration VoiceAdmins Alarm Viewer	IP Set Registration access privileges on page 102 Voice Admins access privileges on page 104 Alarm Viewer access privileges on page 106

Table 22 Default user account groups (Continued)

Group Name	Privileges	Notes
Power Users	IP Set Registration DATAAdmins VoiceAdmins Alarm Viewer VoiceMail and Contact Center	IP Set Registration access privileges on page 102 DATA Admins group access privileges on page 103 Voice Admins access privileges on page 104 Alarm Viewer access privileges on page 106 Voice Mail & Contact Center access privileges on page 100
Backup Operators	Security BackupOperators	Security access privileges on page 101 Backup Operators access privileges on page 105
Security	Security AdminDownload Alarm Viewer Diagnostic Logs Operational Logs	Security access privileges on page 101 Admin Download access privileges on page 103 Alarm Viewer access privileges on page 106 Diagnostic Logs access privileges on page 106 Operational Logs access privileges on page 106
Admin Download	AdminDownload	Admin Download access privileges on page 103
Guest Download	GuestDownload	Can access the BCM web page for application downloads and user documentation. Guest Download access privileges on page 102
Remote Monitoring	Remote Monitor Alarm Viewer Operational Logs	Remote Monitoring access privileges on page 105 Alarm Viewer access privileges on page 106 Operational Logs access privileges on page 106
IPSec User	Network IPSec	Network IPSec access privileges on page 106
Software Upgrade	Software Upgrade	Software Upgrade access privileges on page 105

Default access privileges excluding set-based privileges

The group privileges further refine access availability to groups and users. You can assign more than one privilege to a group and more than one group to a user account. The group with the most privileges defines what the user can access.

For instance, the Admin group has all privileges, therefore, if this group is assigned to the user, any other group assignments with less access are superseded.

The default privileges are arranged as profiles with access privileges. Access privileges for each profile are listed in the sections below.

Voice Mail & Contact Center access privileges

- SBA -Voice Mail
- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Applications - Voice Messaging
EM - CONFIG - Applications - Contact Center
- Web Documentation - User Documentation
- BCM Applications - Applications - CallPilot Manager

- Web - User Applications

Contact Center access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM Applications - Applications - CallPilot Manager
- Web - User Applications

Security access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Administrator Access - Accounts and Privileges
- EM - CONFIG - Administrator Access - Security Policies
- EM - CONFIG - Administrator Access - SNMP
- EM - CONFIG - Administrator Access - Dial In
- EM - CONFIG - Administrator Access - Dial Out
- EM - CONFIG - Telephony - Call Security
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - General - SNMP Trap Setting
- EM - ADMIN - General - Service Manager
- EM - ADMIN - Utilities - Reset
- EM - ADMIN - Software Management - Software Inventory Panel (read-only)
- Web Documentation - User Documentation
- Diagnostic Logs - Diagnostic Log Transfer - Diagnostic Only component logs
- SSL Certificate Transfer - Certificate Transfer - SSL Certificate & SSH Key upload / download
- Web - User Applications

CTE Appl access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM Applications - Applications - CTE DA Pro AE
- Web - User Applications

IP Set Registration access privileges

- SBA - IP Set Registration
- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications

BCMMonitor Appl access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- BCM Applications - Applications - BCM Monitor
- Web - User Applications

CDR Appl access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM Applications - Applications - Call Detail Recording
- Web - User Applications

PPP Access access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- RAS - Applications - PPP
- Web - User Applications

Guest Download access privileges

- Web Documentation - User Documentation
- Web Application Download - Web Download - Callpilot Unified Messaging
- Web Application Download - Web Download - Desktop Assistant
- Web Application Download - Web Download - Desktop Assistant Pro
- Web Application Download - Web Download - 2050 Soft Phone
- Web Application Download - Web Download - Personal Call Manager
- Web Application Download - Web Download - Lan CTE Client

Admin Download access privileges

- Web Documentation - User Documentation
- Web Documentation - Admin Documentation
- Web Application Download - Web Download - Element Manager
- Web Application Download - Web Download - NCM for BCM
- Web Application Download - Web Download - Callpilot Unified Messaging
- Web Application Download - Web Download - Desktop Assistant
- Web Application Download - Web Download - Desktop Assistant Pro
- Web Application Download - Web Download - 2050 Soft Phone
- Web Application Download - Web Download - Personal Call Manager
- Web Application Download - Web Download - Lan CTE Client
- Web Application Download - Web Download - BCM Monitor
- Web Application Download - Web Download - CDR Client Wrapper Utility
- Web Application Download - Web Download - SSH

Exclusive Access access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications

Admin access privileges

- all privileges

DATA Admins group access privileges

- EM - CONFIG - System - IP Subsystem
- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Administrator Access - Dial In
- EM - CONFIG - Administrator Access - Dial Out
- EM - CONFIG - Resources - Media Gateways
- EM - CONFIG - Data Services- DHCP Server Settings
- EM - CONFIG - Data Services- Class 1 Router
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - Utilities - BCM Monitor

- EM - ADMIN - Utilities - Ping
- EM - ADMIN - Utilities - Trace Route
- Web Documentation - User Documentation
- Web - User Applications

Remote Access access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Administrator Access - SNMP
- EM - CONFIG - Administrator Access - Dial In
- EM - CONFIG - Administrator Access - Dial Out
- EM - ADMIN - General - SNMP Trap Destinations
- Web Documentation - User Documentation

Guests access privileges

- Read-only access to all but Utilities, Backup and Restore, and Log Management
- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications

Voice Admins access privileges

- EM - CONFIG - System - Identification
- EM - CONFIG - System - Time and Date
- EM - CONFIG - System - Keycodes
- EM - CONFIG - System - IP Subsystem
- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Resources - all
- EM - CONFIG - Telephony - all
- EM - CONFIG - Data Services - DHCP Server Setting
- EM - CONFIG - Applications - LAN CTE
- EM - CONFIG - Applications - Voice Messaging
- EM - CONFIG - Applications - Contact Center
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - Utilities - Inventory

- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - System Status - Qos Monitor
- EM - ADMIN - System Status - NTP Metrics
- EM - ADMIN - Telephone Metrics - all
- EM - ADMIN - Utilities - BCM Monitor
- EM - ADMIN - Utilities - Reboot
- EM - ADMIN - Software Management - all as read only
- Web Documentation - User Documentation

Backup Operators access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - ADMIN - Backup and Restore - Admin - Backup
- EM - ADMIN - Backup and Restore - Admin - Restore
- Web Documentation - User Documentation
- Web - User Applications

Remote Monitoring access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - ADMIN - General - Alarm as read only
- EM - ADMIN - General - Alarm Setting as read only
- EM - ADMIN - General - SNMP Trap Destinations
- EM - ADMIN - General - Service Manager as read only
- EM - ADMIN - General - Inventory as read only
- EM - ADMIN - System Status - Qos Monitor
- EM - ADMIN - System Status - UPS Metrics as read only
- EM - ADMIN - System Status - NTP Metrics as read only
- EM - ADMIN - Telephone Metrics - all
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- Web - User Applications

Software Upgrade access privileges

- EM - CONFIG - Administrator Access - Current User

- EM - ADMIN - Utilities - Reboot
- EM - ADMIN - Software Management - all
- Web Documentation - User Documentation
- Web - User Applications

Alarm Viewer access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - General - Inventory
- Web Documentation - User Documentation
- Web - User Applications

Operational Logs access privileges

- Web Documentation - User Documentation
- EM - ADMIN - Log Management- Operational Logs
- Web - User Applications

Diagnostic Logs access privileges

- Web Documentation - User Documentation
- EM - ADMIN - Log Management- Diagnostic Logs
- Web - User Applications

Application IVR access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications

Network IPSec access privileges

- EM - CONFIG - Administrator Access - Current User
- RAS - Application - IPSec

Modem dial out access privileges

- EM - CONFIG - Administrator Access - Current User

- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out via analog modem

ISDN dial in access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial in via ISDN

ISDN dial out access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out via ISDN

WAN dial in access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial in via analog WAN

WAN dial out access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out via WAN

PPPoE dial in access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial in via PPPoE

PPPoE dial out access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out via PPPoE

System serial port access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- Web - User Applications
- EM - configure basic parameters

Telset access security

You can use the Telset administration interface (FEATURE 9*8) to activate or deactivate the telset default access user accounts. You can also use this interface to change the password for these accounts. For further information about using telset features, see the *Telset Admin Guide*.

The Telset group privileges apply specifically to the following telset interfaces:

- FEATURE 9*8 (Administrator access only)
- FEATURE **266344 (**CONFIG) (telephony interface)
- FEATURE 983 (CallPilot interface)

These interfaces are meant to be used only as supplementary configuration portals. You can also block access to these interfaces when you set up the system Security Policies.

Table 23 Default Telset access

Configuration Heading	Parameters	Comments
System	ID	A read-only field in Feature 9*8 used for keycode entry.
	Region	Uses Feature ** PROFILE on the set. See Norstar documentation.
IPADDRESS	Dynamic	
	Address	
	Subnet	
	Dfltgw	
License	FILE Keycode data	Uses Keycodes that can be entered one at a time through Feature 9*8 .

Table 23 Default Telset access

Configuration Heading	Parameters	Comments
TelephonyStartup	Template	Uses Feature ** STARTUP on telset within 15 minutes of a bootup of BCM. See Norstar documentation.
	StartDN	Uses Feature ** STARTUP on telset within 15 minutes of a bootup of BCM. See Norstar documentation.
VOICEMAILSTARTUP	ATTENDANTDN	Uses Feature 983 the first time you initialize CallPilot. See CallPilot documentation.
	UISTYLE	Uses Feature 983 the first time you initialize CallPilot. See CallPilot documentation.
	LANGUAGE	Uses Feature 983 the first time you initialize CallPilot. See CallPilot documentation.

Telset group access privileges

There are four set-based group access privileges. These are listed in order of greatest to least access privileges with SBA - Installer being the group with the greatest privileges.

SBA - Installer group access privileges

- SBA - Feature 9*8
- SBA - Installer Rights
- IP Set Registration (when IP set registration is configured and a global password setting is used)
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM Applications - User Applications

SBA - System Coordinator+ group access privileges

- SBA - Coordinator Plus Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM Applications - User Applications

SBA - System Coordinator group access privileges

- SBA - Coordinator Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation

- BCM Applications - User Applications

SBA - Basic group access privileges

- SBA - Basic Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM Applications - User Applications

Blocking user accounts

There are different ways that you can block user access to the system based on your security and administrative requirements.

- Primarily, you can block unauthorized access by ensuring that you change all default passwords once the system is set up and verified.
- You can also block user access by simply changing the password. Note that you must retain a record of the password, since this information is not displayed either on the Element Manager panel or in the programming record file.
- You can increase the complexity required for both Element Manager and telset passwords to make it more difficult for unauthorized users to inadvertently guess the correct password. Complexity is increased by increasing the type of characters that are required and by increasing the minimum length of the password.
- You can set up the system to lock out a user if the password is entered incorrectly a (configurable) number of times. You can unlock the account through the user account record, or the user can wait for the lockout timer to run out before attempting to log on again. The user account shows the last time a user failed to logon.
- You can set a user account to automatically expire on a given date.
- You can manually disable the account. If the user is currently logged in, this takes effect at the next log-in.
- If you only want to decrease the amount of system access, you can delete groups and reassign groups with lower access privileges to the user account.

The administrator performing maintenance tasks can lock the system during the duration of the maintenance. Any user already logged in remains logged in, but would not be able to log in again until the Exclusive Access timer runs out.

Accounts and Privileges panel

This section describes the tabs and fields available on the Accounts and priveleges panel.

Current Account

The Current Account context panel provides a summary of user information about the person currently signed into the Element Manager.

Figure 22 Accounts and Privileges: Current Account panel

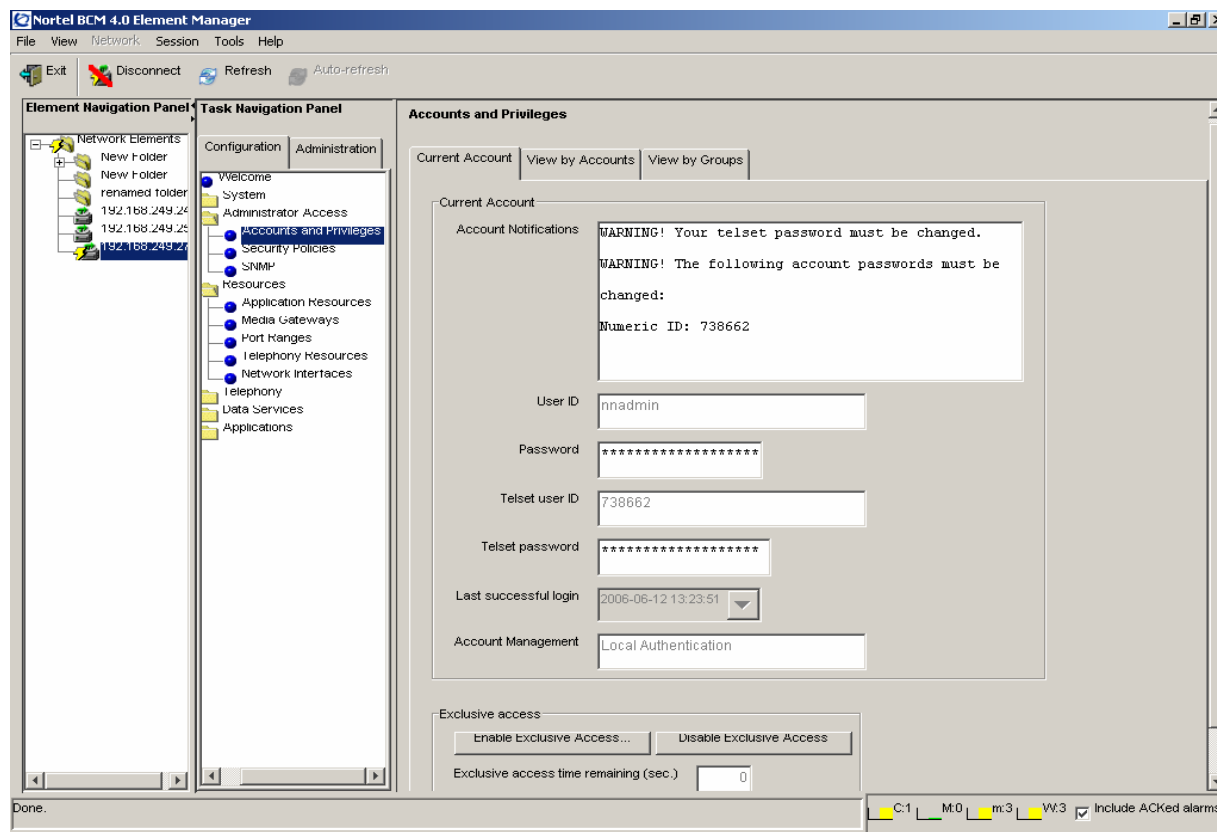


Table 24 describes each field on the Current Account context panel.

Table 24 Current Account fields

Attribute	Value	Description
Account Notifications	read-only	This field displays account notifications, such as notifications of password expiries.
User ID	read-only	A read-only field that can only be changed on the user accounts panel by a user with administrator privileges
Password	alphanumeric	Requires a password entry that contains all the security requirements. Refer to “Complexity Level (Element Manager)” on page 80. Note: Changes to the password take effect at the next login.
Telset user ID	read-only	A read-only field, and can only be changed on the user accounts panel by a user with administrator privileges

Table 24 Current Account fields (Continued)

Attribute	Value	Description
Telset password	numeric	Requires a numeric password entry that is unique for each user. These strings must satisfy the security requirements. Refer to “Complexity Level (Telset)” on page 80 . Note: This password takes effect at the next login.
Last Successful log-in	read-only	A read-only field that indicates the last date and time the user account was used to log on to the system.
Account Management	read-only	Displays the method used to authenticate the user session: local authentication, or centralized authentication through a RADIUS server.
Exclusive access time remaining	numeric minutes	Specifies the amount of time left before other users are allowed to log on to the system. Visible only to users with administrator-level privileges.
Buttons		
Enable Exclusive Access		This button is visible only to users with exclusive access privileges. Opens the Enable Exclusive Access dialog box from which you enter the amount of time that you want to have exclusive access to the system. Exclusive Access does not disable the access of users who are currently logged in.
Disable Exclusive Access		Stops the exclusive access timer and allow other users back onto the system. This button is visible only to users with exclusive access privileges.

View by Accounts

The View by Accounts context panel contains the table that defines individual user accounts. On these panels, you define how the system identifies the user. You also define what privileges the user has by assigning the user to groups.

You can add, delete, or modify user account information from this panel. When you add or modify a user, you can enter a password for both the Element Manager interface and the telset interface.

Figure 23 Accounts and Privileges, View by Accounts context panel

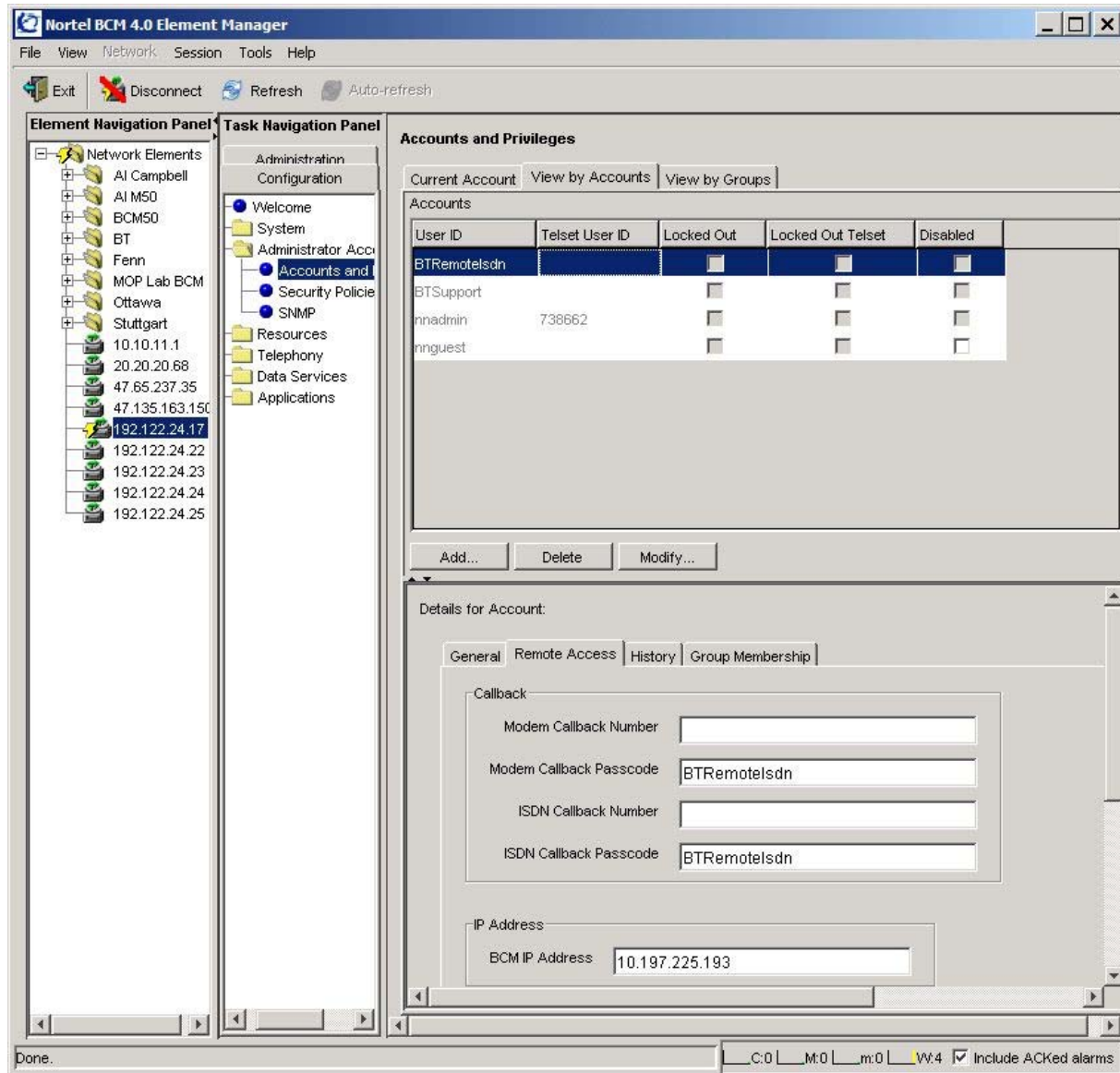


Table 25 describes each field on the View by Accounts panel.

Table 25 View by Accounts fields

Attribute	Value	Description
User ID	alphanumeric	Displays the accounts by User ID
Telset User ID	numeric	Displays the accounts by Telset User ID
Locked Out	checkbox	Indicates whether or not the user has been locked out. When checked , the user cannot access the system. This field becomes checked when a user enters an incorrect password too many times, and the system locks the user account. The user either has to wait for the lockout timer to run out, or an administrator can unlock the user's access using "Re-enable a locked-out user" on page 94 .
Locked Out Telset	checkbox	Indicates whether or not the user has been locked out. When checked , the user cannot access the system. This field becomes checked when a user enters an incorrect password too many times, and the system locks the user account. The user either has to wait for the lockout timer to run out, or an administrator can unlock the user's access using "Re-enable a locked-out user" on page 94 .
Disabled	checkbox	Indicates whether a user account has been disabled. When checked , the user cannot access the system. This field becomes checked when the account expiry date is reached. Refer to "Enabling and disabling an account" on page 95 .
Buttons		
Add		Opens the Add Account dialog box
Delete		Deletes the selected user account
Modify		Opens the Modify Account dialog box



Security note: You cannot delete the nadmin user; therefore, ensure that you change the default password as soon as possible after system setup. Keep a record of the password in a safe place.

If you select a user on the Users list, two more panels appear in the lower frame:

- The General panel allows you to see the current status of the account. See ["View by Account: General" on page 115](#)
- The Group Membership panel allows you to associate the account to group profiles, which determines what type of access the user has. See ["View by Account: Group Membership" on page 116](#).

View by Account: General

The General panel provides user account information and account control settings.

Table 26 describes each field on this panel.

Table 26 View by Accounts: General fields

Attribute	Value	Description
Description	alphanumeric	Displays the descriptive name and information for the user or the user function. This field may be left blank.
Account Expiry		
Enable account expiry	check box	When selected, specifies that the user account is scheduled to automatically expire at the specified date and time.
Account will be disabled on	date	Specifies the date and time when the user account will expire. The pull-down menu opens a calendar.
Account Textual Credentials		
Change password on login	check box	When selected, forces a user to change his or her password when logging in.
Password expiry	drop-down menu	Specifies the date to force a password change.
Account Telset Credentials		
Change password on login	check box	When selected, forces a Telset user to change his or her password when logging in.
Password expiry	drop-down menu	Specifies the date to force a Telset password change.

View by Account: Remote Access

The Remote Access panel provides callback settings for verifying user information.

Table 27 describes each field on this panel.

Table 27 View by Accounts: Remote Access

Attribute	Value	Description
Modem Callback Number	telephone #	Specifies the number the system will call to verify the dial-up user access
Modem Callback Passcode	User ID	Specifies the passcode the system uses to confirm the callback is legitimate
ISDN Callback Number	telephone #	Specifies the number the system will call to verify the ISDN user access
ISDN Callback Passcode	User ID	Specifies the passcode the system uses to confirm the callback is legitimate
IP Address		
BCM IP Address	IP address	Specifies the PPP IP address of the BCM when connecting with analog modem or ISDN terminal adaptors.

View by Account: History

The History panel provides user account and login histories and account control settings.

Table 28 describes each field on this panel.

Table 28 View by Accounts: History fields

Attribute	Value	Description
Account history		
Account created	read-only	Specifies the date that the user record was added.
Created by		Specifies the userID of the person who added the user account.
Last Modified	read-only	Specifies the date the user record was last modified.
Modified by		Specifies the userID of the person who last modified the account.
Login history		
Last successful login	read-only	Specifies the date the user last successfully logged on to either the Element Manager.
Failed login count	read-only	Specifies the number of times the user tried and failed to log on before successfully logging in or being locked out. If the count matches the failed login threshold, a value of true is displayed in the Locked Out column on the Accounts table.
Last failed login	read-only	Specifies the date that the user last tried and failed to logon.
From	read-only	Element Manager: Displays the IP address of the Element Manager
Telset login history		
Last successful login	read-only	Specifies the date the user last successfully logged on to Telset.
Failed login count	read-only	Specifies the number of times the user tried and failed to log on before successfully logging in or being locked out. If the count matches the failed login threshold, a value of true is displayed in the Locked Out column on the Accounts table.
Last failed login	read-only	Specifies the date that the user last tried and failed to logon.
From	read-only	Telset: Displays the DN of the telephone used to log into the system.

View by Account: Group Membership

The Group Membership panel allows you to associate the user account with one or more functional groups. The user will have all the privileges assigned to each group that is added to the list.

Table 29 describes each field on this panel.

Table 29 Group membership fields

Attribute	Value	Description
Account is Member of Groups	Default groups	Lists groups the user is a member of. Refer to “Default groups” on page 98 for a list of the default groups and the privileges associated with each. Note: Groups are added, modified or deleted from the “View by Groups” on page 117 panel.

Table 29 Group membership fields

Attribute	Value	Description
Buttons		
Add		Opens the Add Account dialog box. Choose the group or groups with the appropriate access privileges for the user. Note: You cannot add user accounts to groups with read-only privileges.
Delete		Deletes the user account from the selected group.

View by Groups

The View by Groups panel allows you to add or delete members from group profiles.

The Groups panel lists all the groups currently available in the system.

Table 30 describes each field on this panel.

Table 30 View by Groups fields

Attribute	Description
Groups	Lists all the defined groups. Refer to “Default groups” on page 98 for a list of the default groups and the privileges associated with each.
Buttons	
Add	Opens the Add Group dialog box. Allows the creation of custom groups that provide combinations of privileges not covered by the default groups.
Delete	Opens the Confirm Delete dialog box. Allows for the deletion of any group, with the exception of the Admin Group.

For more details about groups, refer to the panels described in [“View by Groups: General” on page 117](#).

View by Groups: General

For a selected entry in the Groups table ([“View by Groups” on page 117](#)), you can use the General details panel to define which system privileges are assigned to this group, and to users assigned with this group.

This panel also provides status information for the group.

Table 31 describes each field on this panel.

Table 31 View by Groups: General panel fields

Attribute	Value	Description
Group History		
Group created	read-only	Specifies the date the group account was created
Created by		Specifies the user who created the account

Table 31 View by Groups: General panel fields (Continued)

Attribute	Value	Description
Last modified	read-only	Specifies the last date the group account was changed
Modified by		Specifies the user who performed the changes
Privileges: Group Privileges		
Privilege	read-only	Lists the system access privileges that are allowed to members of the selected group
Actions:		
Add		Opens the Add Privilege to Group dialog box. Allows the privilege to be added to the group
Delete		Opens the Confirm Delete dialog box. Allows the privilege to be deleted from a group

View by Groups: Members

For a selected group in the Groups table (“View by Groups” on page 117), you can use the Members panel to assign the group to existing user accounts and to view which accounts have the selected group assigned.

Table 32 describes each field on this panel.

Table 32 View by Groups: Group Membership fields

Attribute	Value	Description
Description	read-only	Lists the user accounts in the selected group.
User ID	alphanumeric	Displays the accounts by User ID.
Telset User ID	numeric	Displays the accounts by Telset User ID.
Buttons:		
Add		Opens the Add Account to Group dialog box. Allows the user account to be added to the selected group.
Delete		Deletes the selected user account from the selected group.

BCM security fundamentals

This section provides an overview of the following BCM security policies:

- secure network protocols and encryption
- security audits
- system security considerations
- firewalls
- security certificate
- site authentication

This section also lists the other panels in the Element Manager that provide topic-specific security.

Security on other Configuration panels

- SNMP
- NTP
- Modem
- PPP
- Certificates
- Telephony scheduled services
- Telephony call security
- Hospitality
- Call Detail Recording

- DHCP server
- Router
- Voice messaging
- LAN CTE

Security on Administration panels

- Alarms
- Alarm settings
- SNMP trap destinations
- Service manager
- Backup and Restore
- Logs
- Software Management

Security on Applications panels

- Desktop Assistant
- DA Pro
- i2050 software phone
- Personal Call Manager
- LAN CTE Client
- CDR, BCM Monitor
- NCM

Secure network protocols and encryption

The BCM uses the following network protocols for Operation, Administration and Maintenance (OAM) in a secured mode:

- CIM/XML is the main management protocol used by the BCM and is only available through an authenticated and authorized SSL connection. User access is controlled, based on assigned privilege levels.
- Multiple data transfer protocols are supported for the various applications including, SCP, SAMBA, and FTP.
- SSH is used by customer support personnel for troubleshooting purposes only. There are special authentication parameters for this interface.

Security audits

A security log file is created at system startup to record user logins and transactions. This log is rolled each day and kept until the maximum log size is reached. When the maximum size is reached, the oldest record is deleted to make room for the newest record. For information about managing logs, see [Chapter 12, “Managing BCM Logs,” on page 345](#).

Administrators can view security logs using the Log Management capabilities found under the Administration tab.

Each security log record contains:

- the time of the event
- the user ID
- a summary of the action performed in the `configchange.systemlog`

System security considerations

To define security parameters for the system and for users, you must consider what level of security you need 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.



Security Note: Nortel recommends changing all default system passwords after the system is up and running and operation is verified.

Considerations

Consider the following:

- Do you want administrative users to be able to access the system through the telset configuration menus?
- How much access to the Element Manager interface are users allowed?
Access is based on user privileges defined through user group membership. There is one default Element Manager administrator account, *nadmin*. This account has a default telset user ID and password. There is also a read-only guest default account (*nnguest*), which does not have a default telset user ID and password. You can delete the guest account to increase security if you wish.
- Do you need to have a temporary account that expires?
- How long do you want the Element Manager to remain open if there is no input from the user?
- How long do you want a user account to be locked out after a specified number of incorrect passwords are entered?
- How complex do you want user IDs and passwords to be in terms of length and character requirements?
- Do you want modem access to use callbacks?

- Do you require the added security of a private SSL certificate?



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.



Note: There is also a Nortel support default user which cannot be deleted or modified. This account is set up to allow Nortel troubleshooting technicians to access areas of the system that are not available to other users. You can change the default challenge key, but be sure to retain a record of the change so that support technicians can access your system. For more information, talk to your Nortel service representative.

Firewalls

Secured communications over a WAN require firewall protection. Depending on the hardware being used and the type of security being employed, specific firewall rules must be set to enable communication between the BCM and the Element Manager.

If the firewall is enabled, add the following rule:

- Source address: Element Manager IP address or “Any.” This is the IP address of the system that the Element Manager resides on.
- Destination address: BCM LAN IP address.
- Service type: TCP:5989, 443 and 80 (port number for CIM/XML, https, and http)
- Action: forward

You must configure CIM/XML services for NAT using the following rules:

- Name: CIM/XML
- Start port: 5989
- End port: 5989
- Server IP address: BCM LAN IP address

Security certificate

The BCM is delivered with a generic SSL security certificate. The self-signed certificate that is included in BCM enables SSL encryption functionality, providing the necessary encryption keys.

There is also a facility to generate SSH certificates which are required in the setup of a SSH server if SCP is used as a transfer method.

Understanding BCM SSL certificate properties

When you first log on to the Element Manager, a security alert appears, which indicates site validation of the default certificate.

This security alert does not appear if you:

- add a site-specific certificate
- suppress the message on your client browser

If you want a site-specific certificate, obtain a site certificate for your system from a CA (Certificate Authority) vendor. Certificate files must use the .PEM format. When you are provided with a certificate and a private security key, these must be installed on the BCM.



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.

Site authentication

Site authentication is not provided with the generic SSL certificate. This means that the generic SSL certificate is not signed by a recognized signing authority.

However, the SSL certificate used by the http server may be upgraded to a customer's private SSL certificate, which offers site certification along with the encryption. Site authentication requires system-specific information such as an IP address, company name, and so on. A site-specific certificate ensures that when users point their web browser at the SSL web interface, the user is no longer asked to accept the certificate.

If the default BCM generic SSL certificate is used, the user is prompted to accept an unsigned

Chapter 5

Using the BCM Hardware Inventory

This chapter describes how to use the BCM Hardware Inventory. The Hardware Inventory task in the BCM Element Manager displays information about the BCM system, including:

- connected expansion units
- populated Media Bay Modules (MBMs)
- attached telephone devices

You can view the information in the Hardware Inventory remotely, using Simple Network Management Protocol (SNMP) management systems and the Entity Management Information Base (MIB), RFC2737.

About the BCM Hardware Inventory

The BCM Hardware Inventory panel provides information about the BCM physical system. There are three tabs on the main Hardware Inventory panel:

Table 2 Hardware Inventory panel

Tab	Description
System	Provides information about the key components of the BCM. For more information, see “Viewing and updating information about the BCM system” on page 126 .
PCI cards	Provides information about the type of PCI card, manufacturer and model.
Devices	Provides information about any non-BCM components connected to the system. For more information, see “Viewing information about devices” on page 131 .
Additional information	Provides manufacturer details about the BCM. For more information, see “Viewing additional information about the BCM hardware inventory” on page 132 .



Note: You can also add information about certain devices, such as an asset ID and location information, to facilitate tracking of the BCM hardware inventory in asset management systems.



Note: You can save all of the information configured and displayed on the Hardware Inventory panels as a programming record. See [“Saving programming records” on page 57](#) for information about how to generate this record.

Viewing and updating information about the BCM system

You can view and update certain information about the BCM main unit using the System tab in the BCM Element Manager. The System tab is divided into three areas:

- Main chassis
- Expansion unit
- Media bay modules
- Fiber expansion media bay modules
- Other Information

You can save inventory information to a file using the Programming Record. See [“Saving programming records” on page 57](#).

Viewing and updating information about the BCM main unit

You can view information about the BCM main unit, such as the Nortel part number, the System ID, and other information. See Table 33.



Note: Fields marked with an asterisk (*) can also be remotely queried by SNMP using the Entity MIB.

Table 33 BCM main chassis fields

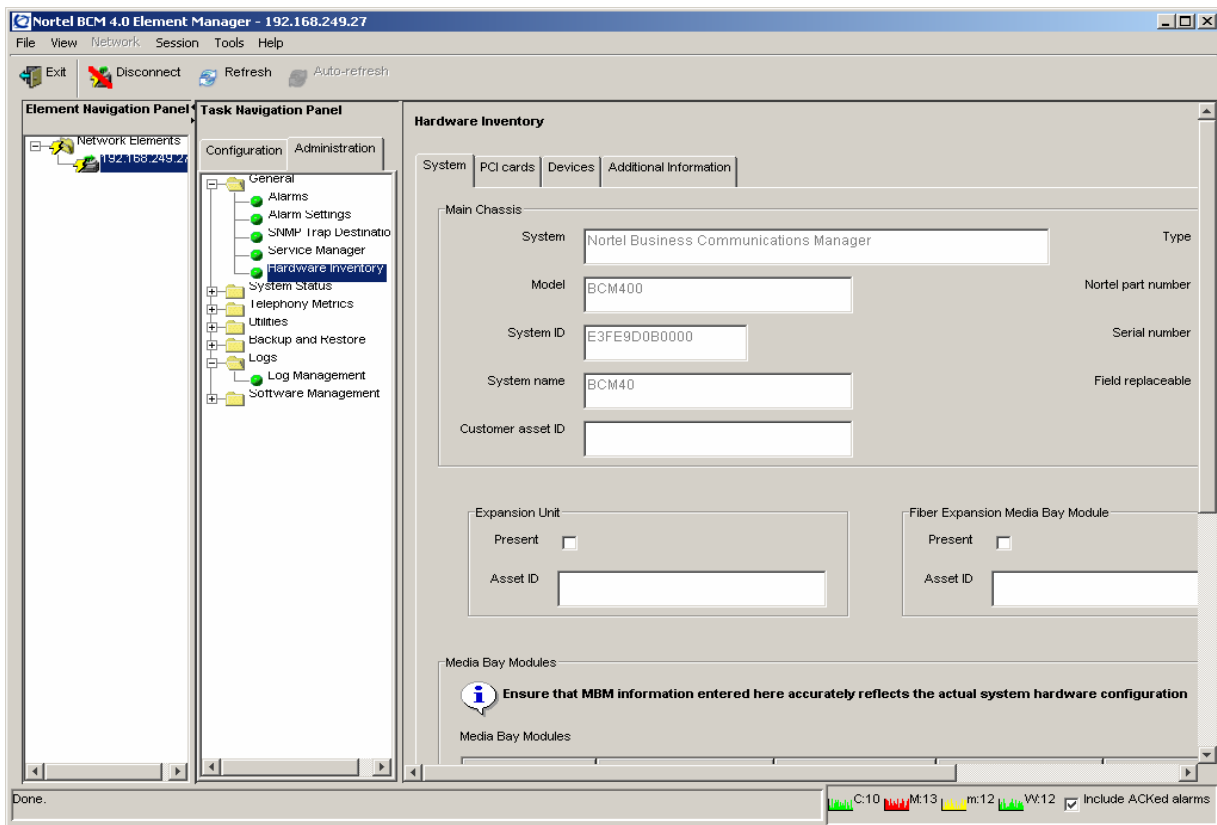
Field Name	Field Description	Field Value	Read/Write
System*	An arbitrary string that uniquely identifies the Physical Element and serves as the Element's key	Nortel BCM Communications Server	Read
Type*	The type of the physical entity	Chassis	Read
Model*	A textual description of the object	example 'BCM Telephony Only'	Read
Nortel part number*	The Nortel part number used to order the system	NT <xxxxxx>	Read
System ID	A unique string that identifies this specific instance of the element	System ID which is Mac #1	Read
Serial number	The serial number to the BCM unit	Nortel System Serial Number	Read
System name*	A user-friendly name for the object	System name of the BCM	Read
Field replaceable*	Indicates if the entity is considered a Field Replaceable Unit by the supplier	True (if checked)	Read
Customer asset ID*	Customer-defined tracking number	Initially zero	Write

You can add or update the customer asset ID associated with the BCM main unit.

To view or update information about the BCM main chassis

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The **Hardware Inventory** panel opens and displays the **System** tab.
- 3 View the information displayed in the **BCM main chassis** area.
- 4 If you want to add or update the asset ID for the BCM main unit, enter an asset ID in the **Customer Asset ID** field.

Figure 24 Hardware Inventory



Viewing and updating BCM expansion unit information

The BCM expansion unit area in the System tab provides information about the expansion unit connected to the BCM main unit, if any. If an expansion unit is present and populated with an MBM, this information is also provided.

Table 34 provides information about the fields in the BCM expansion unit area.



Note: Asterisk (*) items can also be remotely queried by SNMP using the Entity MIB.

Table 34 Expansion unit area and Fiber expansion media bay module area

Column Name	Column Description	Column Value	Read/Write
Present	Indicates if an expansion unit to main unit is present	Yes (if checked)	Read
Asset ID*	Customer defined tracking number	Initially zero	Write

To view or update expansion unit information

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The Hardware Inventory panel opens, and displays the **BCM System** tab.
- 3 View the information displayed in the **Expansion unit** area and the **Fiber expansion media bay module** area.
- 4 If you want to add or update the asset ID, enter an asset ID in the **Customer Asset ID** field.

Viewing and updating information about media bay modules

The Media Bay Modules area on the System tab displays information about media bay modules associated with the BCM system, including:

- a description of the MBM
- details about the MBM
- hardware revision information
- the chassis that the MBM is contained in
- the asset ID

While some of the information displayed is read-only, there are fields where you can add information about the MBM to create a record of the hardware at each site. Table 35 provides information about the fields in the MBM area.

Table 35 Media Bay Modules information

Column Name	Column Description	Read/Write
Description	Displays a description of the MBM configured in the system.	Read
Details	Use the pull-down menu to identify details about the MBM, such as whether it is a DSM16 or DSM32.	Write
Hardware Revision	Displays the hardware revision of the MBM.	Read
Contained In	Use the pull-down menu to indicate whether the MBM is installed in the main chassis, an expansion unit, or FEM.	Write
Asset ID	Enter the asset ID of the MBM.	Write

To view or update other information about the media bay modules

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The Hardware Inventory panel opens. The BCM **System** tab is displayed.
- 3 View the information displayed in the **Media bay modules** area.
- 4 If you want to add or update information about the owner or administrator of the BCM system, enter information in the **Owner Name** field.
- 5 Add or update information about the media bay modules in the following fields: **Details, Contained In,** and **Asset ID**.



Note: The information recorded on this panel can be queried by any SNMP management system that supports Entity MIB.

Viewing and updating other information about the BCM system

The Other Information area in the System tab displays other information associated with this particular BCM system, such as:

- the name of the administrator and their contact information
- the location of the BCM system

You can add or update this information. The date on which this information is updated is displayed BCM area, in accordance with “LastChangeTime” of the Entity MIB.

Table 36 lists the fields displayed in the Other Information area.

Table 36 Other Information fields

Field Name	Field Description	Field Value	Read/Write
Owner name	The owner’s name or any other information, such as the administrator’s name and contact information	Up to 256 characters	Write
Location of this system	The location of the system	Up to 256 characters	Write
Last change to this panel	Date and time when the information was last modified	example ‘2004-04-16 09:12:00’	Read

To view or update other information about the BCM main unit

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The Hardware Inventory panel opens. The BCM **System** tab is displayed.
- 3 View the information displayed in the **Other Information** area.

- 4 If you want to add or update information about the owner or administrator of the BCM system, enter information in the **Owner Name** field.
- 5 If you want to add or update information about the location of BCM system, enter information in the **Location of the System** field.

Viewing information about PCI cards

The PCI Cards tab displays information about the PCI cards that are part of the BCM system. The tab displays the following information:

- name of the PCI card
- a description of the card (model information)
- the manufacturer of the card.

When you select a PCI card from the table, the details panel displays the following additional information:

- MSC ID
- serial number

Figure 25 PCI Cards tab

The screenshot shows the Nortel BCM 4.0 Element Manager interface. The main content area displays the PCI Cards tab with a table of installed cards. The selected card, MSC, is highlighted in blue. Below the table, the details panel for the MSC card shows the MSC ID (E3FE9D0B0000) and Serial Number (53007150). The MS-PEC Information table shows the card is installed in Slot 3 with Hardware ID 4 and both DSP1 and DSP2 are Enabled.

PCI Card	Description	Manufacturer
MSC	Motorola Audio I/O Controller (MIDI)	Nortel
Network Card	Intel Corp. 82801E Ethernet Controller 0	Intel Corp
Network Card	Intel Corp. 82801E Ethernet Controller 1	Intel Corp
WAN Card	PCI device 12aa5600 (SDL Communications, Inc.)	SDL Communications, Inc.

Description	Location(Slot)	HardwareID	DSP1	DSP2
Empty	Slot2		Not Supported	Not Supported
Empty	Slot4		Not Supported	Not Supported
MS-PEC 3	Slot3	4	Enabled	Enabled

To view information about PCI cards

- 1 Select Administration > General > Hardware Inventory.
The Hardware Inventory panel opens.
- 2 Click the **PCI Cards** tab.
- 3 Select a PCI Card from the table and view the information displayed in the details panel.

Viewing information about devices

The Devices tab displays information about all devices attached to the BCM. These devices may include:

- digital sets
- analog devices
- IP sets, including IP clients

You can view all Directory Numbers (DNs) and the type of set associated with the DN. Table 37 lists the fields in the Attached Devices table.

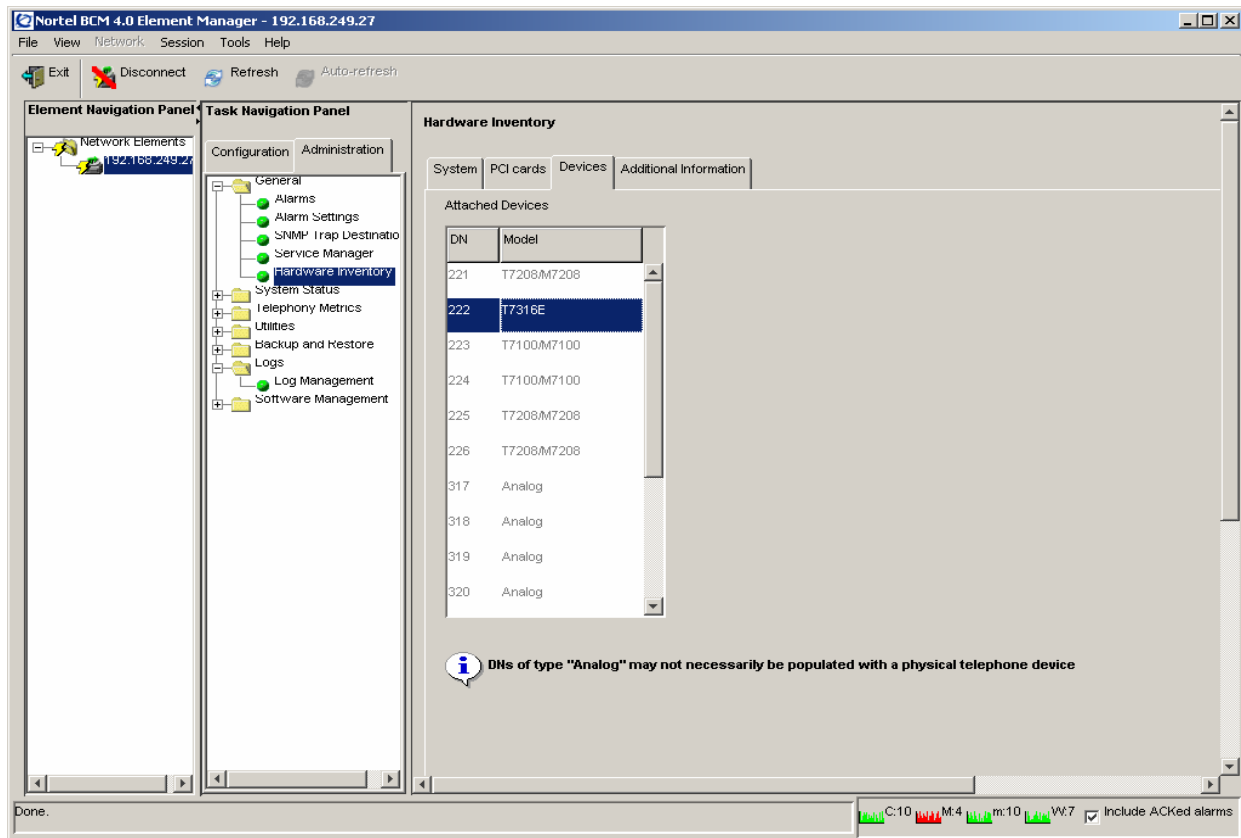


Note: DN of type “Analog” are not necessarily be populated with a physical telephone device.

Table 37 Attached Devices fields

Header Name	Header Description	Field Value	Read/Write
DN	Directory Number	In accordance with DN numbering system	Read
Model	Type of device or set	example 'T7316' or 'I2004'	Read

Figure 26 Hardware Inventory Devices tab



To view information about attached devices

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The Hardware Inventory panel opens.
- 3 Click the **Devices** tab.
The **Devices** tab opens.
- 4 View the information displayed in the **Attached Devices** table.

Viewing additional information about the BCM hardware inventory

The Additional Information tab displays additional information about the BCM main unit, such as:

- details about the manufacturer and the manufacture date
- hardware version details
- serial number details

You require this information only when a field issue requires the identification of certain systems.

Table 38 lists the fields displayed in the Additional Information tab. Items marked as read-only are detected by the BCM. For items that are not auto-detected, the Element Manager provides checkboxes, pull-down menus, and fields that the administrator can populate to indicate that these resources are present.

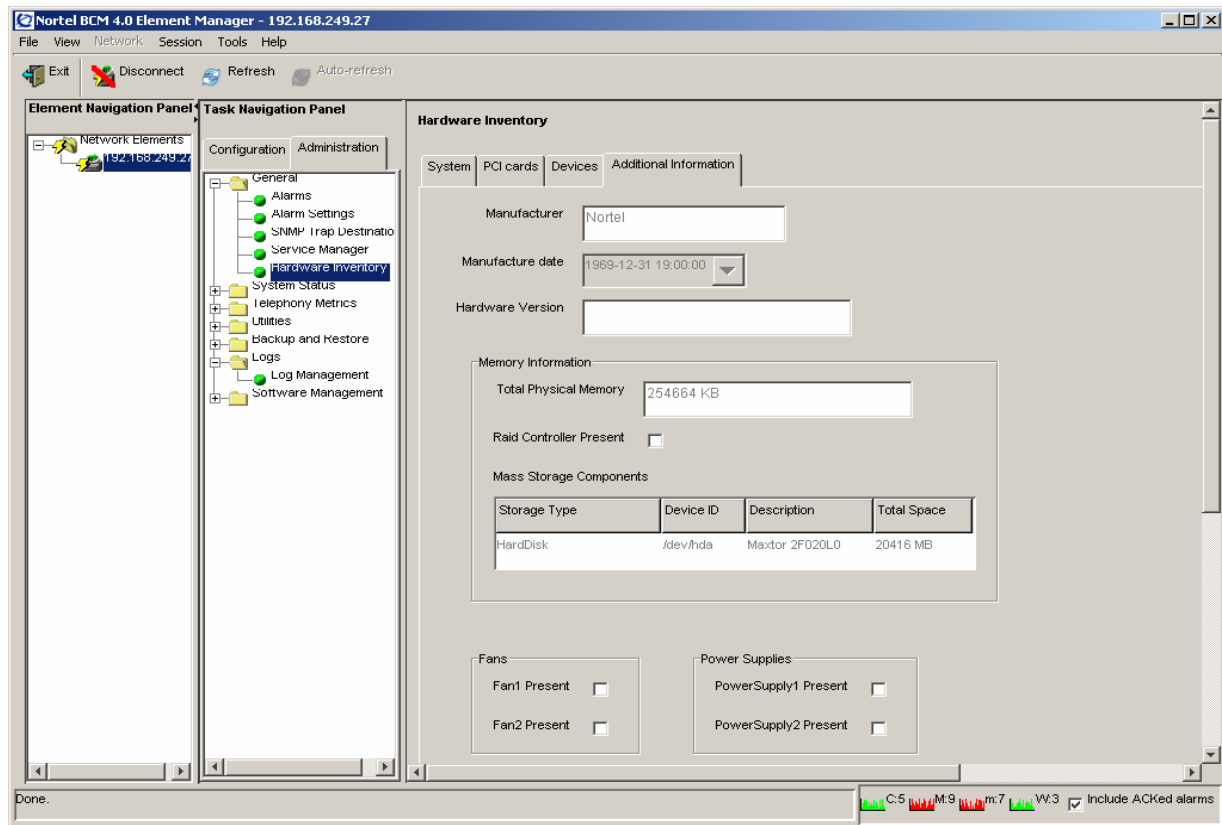


Note: Asterisk (*) items can also be remotely queried by SNMP using the Entity MIB.

Table 38 Additional BCM main unit Information fields

Field Name	Read/Write
Manufacturer*	Read
Manufacture date	Read
Hardware version*	Read
Memory Information	
Total physical memory	Read
Raid controller present	checkbox
Mass storage components	
Storage type	Read
Device ID	Read
Description	Read
Total space	Read
Fans*	
Fan 1 Present	checkbox
Fan 2 Present	checkbox
Power Supplies*	
Power supply 1 present	checkbox
Power supply 2 present	checkbox
Digital Mobility Systems	
Description	Read/Write
Asset ID	Read/Write

Figure 27 Hardware Inventory Additional Information tab



To view additional information about the BCM hardware inventory

- 1 In the BCM Element Manager, connect to a BCM device.
- 2 Select **Administration, General, Hardware Inventory**.
The Hardware Inventory panel opens.
- 3 Click the **Additional Information** tab.
The **Additional Information** tab opens.
- 4 View the information displayed in the **Additional BCM main unit Information** area.

Chapter 6

Managing BCM with SNMP

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks. SNMP-compliant devices, called agents, store meta-data in Management Information Bases (MIBs) and provide this data to SNMP requesters.

You can use external SNMP clients, such as HP OpenView, to monitor the BCM system by means of read-only SNMP requests.

This chapter provides information about:

- BCM support for SNMP
- configuring BCM SNMP settings
- using SNMP to send traps

Overview of BCM support for SNMP

This chapter provides information about SNMP support provided by the BCM main unit.

The BCM main unit supports the following versions of SNMP:

- SNMP v1 — the first implementation of SNMP; this version supports such protocols as IP
- SNMP v2C — provides improved efficiency and error handling
- SNMP v3 — provides improvements in security and privacy

Using the BCM Element Manager, you can select which versions of SNMP you want the BCM agent to support. For more information, see [“Configuring SNMP settings”](#).

Management Information Bases provide access to the managed objects of a system and specify the format of traps. BCM supports the following MIBs:

- RFC-1213 — MIB II
- RFC 2863 — Interface MIB
- RFC 2737 — Entity MIB
- RFC 2790 — Host MIB
- SmallSiteEvent MIB for traps
- OSPFv2 (RFC1850)
- RIPv2 (RFC1724)
- RFC-2261 — SNMP framework

For information about supported MIBs, how to install MIBs, and how to view SNMP traps, see [“Management Information Bases” on page 389](#).

BCM supports read-only SNMP requests, even for SNMP variables that display as read-write. BCM does not support configuration through SNMP. Variables that are not supported are displayed as “0”.

Configuring SNMP settings

You can use the BCM Element Manager to configure the BCM SNMP agent. You can configure:

- general SNMP settings
- community strings
- service access points
- SNMP trap destinations

You can save a record of SNMP settings using the programming record. For more information, see [“Saving programming records” on page 57](#).

Configuring general SNMP settings

You can configure general SNMP settings, including:

- enabling and disabling the SNMP agent
- enabling and disabling versions of the SNMP agent
- defining access permissions
- adding and deleting SNMP management stations

You can create a list of SNMP managers who are permitted to query the BCM system by specifying their IP addresses. If you have specified SNMP managers, the BCM SNMP agent will respond only to SNMP requests from those IP devices.

To configure the BCM SNMP agent

- 1 Start the BCM Element Manager.
- 2 In the **Network Element** navigation panel, select a BCM element.
- 3 Log on to the BCM by clicking the **Connect** button.
- 4 When the BCM Element Manager has connected to the device, click the **Configuration** tab in the **Task** panel.
- 5 Open the **Administrator Access** folder, and then click **SNMP**.
- 6 Click the **General** tab.
The **General** panel is displayed.
- 7 Configure the **SNMP Agent** settings.

Table 39 SNMP Agent Settings

Attribute	Action
Engine ID	The engine ID is the SNMP agent's engine ID. This field is read-only and is for information purposes only.
Port Number	The port number is a read-only field that shows the SNMP agent's local port number. The port number is 161.

To configure BCM SNMP settings

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **General** tab.
The **General** panel is displayed.
- 4 In the **SNMP Settings** area, click the **Modify** button.
The **Modify SNMP Settings** dialog box opens.
- 5 Configure SNMP settings.

Table 40 Configure SNMP Settings Attributes

Attribute	Action
Enable SNMP Agent	Select whether to enable or disable the SNMP agent by selecting the check box.
Minimum Required Security	Select the minimum required security for SNMP. Options are: AuthNoPriv or NoAuthNoPriv. Valid for SNMP v3.
Support SNMP v1	Select the check box to enable SMNP version 1.
Support SNMP v2C	Select the check box to enable SMNP version 2C.
Support SNMP v3	Select the check box to enable SMNP version 3.

The following combinations of SNMP versions are allowed:

- Option 1: SNMP v1 and SNMP v2C. These versions are similar in capability and operation.
- Option 2: SNMP v3 only. This option provides more stringent security protection than option 1 does.
- Option 3: SNMP v1, v2C, and v3. This option ensures that the BCM can interact with any SNMP agent manager.

- 6 Click the **OK** button.

Adding an SNMP manager to the BCM SNMP manager list



Note: If you configure an SNMP manager with an IP address of 0.0.0.0, the SNMP agent will respond to SNMP queries from all stations.



Caution: If you add more than five SNMP management stations, the SNMP service may degrade system performance.

To add an SNMP manager to the BCM SNMP manager list

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **General** tab.
The **General** panel is displayed.
- 4 In the **SNMP Manager List** area, click the **Add** button.
The **Add Manager** dialog box opens.
- 5 Configure the manager list attributes.

Table 41 SNMP Manager Attributes

Attribute	Action
Manager IP Address	<p>Enter the IP address of the SNMP manager that you want to authorize to query the BCM system.</p> <p>The IP address must correspond to the PC where the SNMP manager software is installed. Do not use the dynamic IP address that the PC receives when the dial-up link activates (when the BCM initiates dialing). Using the dynamic IP address causes the removal of the required static route.</p> <p>The format for the IP address is X.X.X.X:P, where P is the port.</p> <p>Setting the IP address to 0.0.0.0 authorizes all SNMP managers to query the system.</p>

- 6 Click the **OK** button.

To delete an SNMP manager

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **General** tab.
The **General** panel is displayed.
- 4 In the **SNMP Manager List** area, select a manager in the Manager IP Address table.
- 5 Click the **Delete** button.
A confirmation message opens.
- 6 Click the **Yes** button.
The manager is removed from the Manager IP Address table.

Configuring SNMP community strings

An SNMP community string is a value, similar to a user ID or a password, that allows access to a device's statistics. SNMP managers send a community string along with each SNMP request. If the community string is correct, the BCM responds with the requested information. If the community string is incorrect, the BCM discards the request and does not respond.

Community strings are used for SNMP v1 and v2C only.

BCM ships from the factory with community strings set. It is standard practice for network managers to change all the community strings to prevent outsiders from seeing information about the internal network. Before you can send SNMP messages to an SNMP workstation, you must configure community strings.

You can define the value of a community string, as well as the type of access. You can also delete a community string.



Caution: Although there is no limit for the number of SNMP communities that you can set, Nortel recommends that you limit the number of SNMP communities to a maximum number of 5. Limiting the number of SNMP communities will reduce degradation of system performance.

To add a community string

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Community Strings** tab.
The **Community Strings** panel is displayed.
- 4 Click the **Add** button.
The **Add Community String** dialog box is displayed.
- 5 Specify the community string attributes.

Table 42 SNMP Community String Attributes

Attribute	Action
Community String	Enter the entry name used as a key to uniquely identify an individual community entry on the SNMP agent.
Type of Access	Specify the read and write access for this community. Available options are Read Only and Read/Write.

- 6 Click the **OK** button.
The community string is added to the **Community Strings** table.

To delete a community string value

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Community Strings** tab.
The **Community Strings** panel is displayed.
- 4 In the Community Strings table, select the community string that you want to delete.
- 5 Click the **Delete** button.
A confirmation message is displayed.
- 6 Click **Yes**.
The community string is removed from the Community Strings table.

Configuring service access points

Service access points are associated with the enhanced security and privacy features of SNMP v3. The Service Access Point tab is not visible if SNMPv3 is not selected on the SNMP General Settings tab.

You can view and configure the following parameters associated with service access points.

- the user name associated with the service access point
- the authentication protocol
- the type of access
- the encryption protocol
- the authentication pass phrase
- the privilege pass phrase

You can add, modify, and delete service access points.

To add a service access point

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Service Access Points** tab.
The **Service Access Points** panel is displayed.
- 4 Click the **Add** button.
The **Add Service Access Point** dialog box opens.

- 5 Configure the Add Service Access Point attributes.

Table 43 Add Service Access Point Attributes

Attribute	Action
User Name	Enter the name of the user associated with the service access point.
Authentication Protocol	Select the authentication protocol. Options are: None, MD5, SHA.
Type of Access	Select the type of access. Options are: Read Only and Read/Write.
Encryption	Select the encryption. Options are: None, DES, 3DES, AES.
Engine ID	Enter an engine ID when you add a user that will be used for SNMP v3 communications. The engine ID is made up of hexadecimal digits with a colon separating each digit. Leave the engine ID blank when you add a user that will have access to the MIB, or in the case of SNMP v3 MIB queries.

- 6 Click the **OK** button.
The service access point is added to the **Service Access Point** table.

To configure pass phrases for a service access point

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Service Access Points** tab.
The **Service Access Points** panel is displayed.
- 4 Select a community string in the **Service Access Points** table.
Details are displayed in the **Details** pane.
- 5 Configure the pass phrases..

Table 44 Pass Phrase Attributes

Attribute	Action
Authentication Pass Phrase	Enter the Authentication pass phrase for the service access point. Press the Tab key when you have entered the phrase.
Privilege Pass Phrase	Enter the Privilege pass phrase for the service access point. Press the Tab key when you have entered the phrase.

- 6 In the confirm password dialog, re-enter the authentication password.
- 7 Click the **OK** button, and then press the Tab key.
- 8 In the confirm password dialog, re-enter the privilege password.
- 9 Click the **OK** button, and then press the Tab key.

To view details associated with a service access point

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Service Access Points** tab.
The **Service Access Points** panel is displayed.
- 4 Select a community string in the **Service Access Points** table.
Details are displayed in the **Details** pane, including the encrypted authentication pass phrase and the encryption pass phrase.

To delete a service access point

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Service Access Points** tab.
The **Service Access Points** panel is displayed.
- 4 In the **Service Access Points** table, select a service access point.
- 5 Click the **Delete** button.
A confirmation dialog box opens.
- 6 Click the **Yes** button.
The selected service access point is deleted from the **Service Access Points** table.

To modify a service access point

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **Service Access Points** tab.
The **Service Access Points** panel is displayed.
- 4 In the **Service Access Points** table, select a service access point.
- 5 Click the **Modify** button.
The **Modify Service Access Point** dialog box opens.
- 6 Configure the Modify Service Access Point attributes.

Table 45 Modify Service Access Points Attributes

Attribute	Action
User Name	Enter the name of the user associated with the service access point.
Authentication Protocol	Select the authentication protocol. Options are: None, MD5, SHA.
Type of Access	Select the type of access. Options are: Read Only and Read/Write.

- 7 Click the **OK** button.
The modified service access point is displayed in the **Service Access Points** table.

Configuring SNMP trap destinations

An SNMP trap is a signal that tells the SNMP manager that an event has occurred on the system. The SNMP system enables SNMP traps to be generated based on all or some events and alarms generated on the BCM system. Any information that is displayed in the Alarms panel can generate an SNMP trap. For information about the Alarms panel, see [“Using the Alarms Panel” on page 150](#).

BCM alarms that meet the SNMP trap criteria are forwarded to the SNMP trap reporting interface according to defined trap community strings. SNMP trap notifications are displayed in your SNMP trap software.

SNMP traps are generated by the BCM if you have enabled SNMP for specific BCM alarms. You configure SNMP settings using the Alarm Settings task in the Element Manager.

You can configure the following attributes associated with a trap destination:

- the name of the trap destination
- the host address of the trap destination
- the port
- the SNMP version
- the community string (for SNMP v1 and v2C only)
- the user name (for SNMP v3 only)

For information about administering SNMP trap destinations, see [“Viewing and modifying SNMP trap destinations”](#).



Note: You can configure and administer SNMP trap destinations in both the Configuration tab and the Administration tab of the BCM Element Manager. This allows operators who manage BCM faults to configure SNMP trap destinations without having to access the SNMP settings on the Configuration panel. SNMP must be enabled on the SNMP General panel if you want to configure and use SNMP trap destinations from the SNMP Trap Destinations panel on Administration panel.

To add a trap destination

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **SNMP Trap Destinations** tab.
The **SNMP Trap Destinations** panel is displayed.
- 4 Click the **Add** button.
The **Add Trap Destination** dialog box opens.

- 5 Configure the Add Trap Destination attributes.

Table 46 Add Trap Destination Attributes

Attribute	Action
Name	Enter a name for the trap.
Host	Enter the IP address of the trap destination.
Port	Enter the UDP port number from which the trap will be sent. The default value is 162.
SNMP Version	Select the version of the SNMP Agent for the trap. Options are: v1/v2C, and v3.
Community String	Enter the community string to use for the SNMP trap.
User Name	For v3 only, enter the user name for the SNMP trap.

- 6 Click the **OK** button.
The new trap destination is displayed in the **Trap Destinations** table.



Note: When the SNMP agent is restarted, the System Uptime is reset. The SNMP agent is restarted whenever you reboot the system, make an SNMP configuration change, or enable/disable the SNMP agent.

Viewing and modifying SNMP trap destinations

Once you have configured SNMP settings, you can view and administer SNMP trap destinations. You can delete and modify SNMP trap destinations.



Note: You can configure and administer SNMP trap destinations in both the Configuration tab and the Administration tab of the BCM Element Manager. This allows operators who manage BCM faults to configure SNMP trap destinations without having to access the SNMP settings on the Configuration panel. SNMP must be enabled on the SNMP General panel if you want to configure and use SNMP trap destinations from the SNMP Trap Destinations panel on Administration panel.

To modify a trap destination

- 1 Click the **Configuration** tab.
- 2 Open the **Administrator Access** folder, and then click **SNMP**.
- 3 Click the **SNMP Trap Destinations** tab.
The **SNMP Trap Destinations** panel is displayed.
- 4 In the **Trap Destinations** table, select a trap destination.
- 5 Click the **Modify** button.
The **Modify Trap Destination** dialog box opens.

6 Configure the Modify Trap Destination attributes.

Table 47 Modify Trap Destination Attributes

Attribute	Action
Name	Enter a name for the trap.
Host	Enter the IP address of the trap destination.
Port	Enter the UDP port number from which the trap will be sent. The default value is 162.
SNMP Version	Select the version of the SNMP Agent for the trap. Options are: v1/v2C, and v3.
Community String	Enter the community string to use for the SNMP trap.
User Name	For v3 only, enter the user name for the SNMP trap.

7 Click the **OK** button.

The modified trap destination is displayed in the **Trap Destinations** table.

To delete a trap destination

1 Click the **Configuration** tab.

2 Open the **Administrator Access** folder, and then click **SNMP**.

3 Click the **SNMP Trap Destinations** tab. The **SNMP Trap Destinations** panel is displayed.

4 In the **Trap Destinations** table, select a trap destination.

5 Click the **Delete** button. A confirmation dialog box opens.

6 Click the **Yes** button. The trap destination is deleted from the **Trap Destinations** table.

Auto-SNMP dial-out

The auto-SNMP dial-out service allows you to use an analog modem or ISDN channel to deliver alarms to a specified destination.

To use auto-SNMP dialout, you must perform the following tasks:

- assign remote access privileges to an account
- create a dial-up interface
- configure the dial-up interface to use a static route, or to use a dial-out number
- add an SNMP trap destination

For information about how to assign remote access privileges to an account, see [“Adding a user account to a group” on page 93](#). For information about how to create and configure a dial-up interface as a primary connection for auto-SNMP dial-out, refer to the *BCM 4.0 Networking Configuration Guide* (N0060606). To add an SNMP trap destination, see [“Configuring SNMP trap destinations” on page 143](#).

Alarm severity levels

The terminology used for alarm severity levels in the Alarms panel and in SNMP traps is not the same. Table 48 lists Alarms panel terminology and the equivalent SNMP trap type.

Table 48 Terminology used for alarm severity levels

Alarm Banner	SNMP Trap Type
Critical	Error
Major	Error
Minor	Warning
Warning	Information
Information	Information

While the BCM fault management system denotes the source of an alarm as “ComponentID”, the SNMP system denotes the sources of this information as a trap of source “eventSource”.

Chapter 7

Using the BCM Fault Management System

This chapter contains information about managing alarms generated by the BCM system and administering alarm settings.

The chapter provides information about the following:

- an overview of BCM fault management tools
- an overview of BCM alarms
- alarms and log files
- administering alarms
- configuring alarm settings
- BCM alarm list
- alarm severities

Overview of BCM fault management

You can view and manage real-time alarms generated by the BCM system. Alarms arise from components that are running on the system; these alarms indicate faults or informational conditions that may require resolution from the system administrator. Examples of alarm conditions include:

- a T1 circuit on the system is down
- a service running on the BCM has been stopped by an administrator

Alarm information can be delivered to you by any of the following means:

- the Alarms Panel in the BCM Element Manager
- the Alarm Banner in the BCM Element Manager
- core telephony alarms show on the alarm set
- Simple Network Management Protocol (SNMP) traps for remote management of faults
- LEDs on the BCM main unit

You can manage alarms and alarm information by:

- configuring alarm settings, for example filtering alarms so that only the desired subset of alarms are displayed in the BCM Element Manager Alarms Panel or sent as SNMP traps
- administering alarms, for example acknowledging selected alarms and clearing the alarm log

You can keep a record of alarm settings using the programming record. For information about using the programming record, see [“Saving programming records” on page 57](#).

About BCM alarms

Alarms are generated by software components that are running on the BCM system, and cover BCM services and applications.

Each component has a range of alarm IDs, so that each BCM alarm has a unique alarm ID. Table 49 lists the components and the alarm ID ranges.

Table 49 BCM components and Alarm ID ranges

BCM Component	Alarm ID Range
Core Telephony	0–999
Operating System	1000–1999
Software Updates	2000–2999
Persistent Data Repository	5000–5999
Date and Time	6000–6999
Modem Call Control	8000–8999
Service Manager	10000–10999
Platform Status Monitor	11000–11999
Backup and Restore	12000–12999
UPS	13000–13999
Configuration Change	16000–16999
System Set Based Admin	17000–17999
Startup Profile	19000–19999
System Authentication	30000–30999
Keycodes	31000–31999
Media Services Manager	40000–40999
CTE	41000–41999
Call Detail Recording	42000–42999
Voice CTI	43000–43999
IVR	46000–46999
Unistim Terminal Proxy Server	50000–50999
PVQM	50501–50999
VoIP Gateway	51000–51999
Media Path Server	52000–52999
Media Gateway Server	53000–53999
IP Telephony Provider	56000–56999
Survivable Remote Gateway	57000–57999
LAN Driver	60000–60999
ALG	64000–64999

Alarms and log files

All alarms that appear in the BCM Element Manager Alarms Panel are logged in the `alarms.systemlog` file. This file is capped at 1 MB in size; when the file reaches this size, a new `alarms.systemlog` file is started. The BCM keeps the current file as well as three previous files. The file is also capped and a new file is started when the BCM system is rebooted.

You can retrieve the `alarms.systemlog` files (the current file plus the three previous files) from the BCM system using the Log Management task in the BCM Element Manager. You can view the files using the BCM Log Browser. For more information, see [Chapter 12, “Managing BCM Logs,” on page 345](#).

Alarm severities

Alarm severities are as follows:

Table 50 Alarm Severities

Alarm Severity	Description
Critical	Immediate corrective action is required due to conditions such as loss of service, loss of bandwidth, outage, loss of data, and/or functionality
Major	Urgent corrective action is required due to conditions such as pending loss of service, outage, loss of data, and/or functionality
Minor	Corrective action is required to prevent eventual service-affecting degeneration
Warning	Indicates the detection of a potential or impending service-affecting condition and that some diagnostic action is required
Information	Indicates audit-type information, such as configuration changes

By default, alarms are displayed in the Alarm Banner. The BCM sends SNMP traps for alarms with a severity of Major and Critical.

Table 51 provides the default mapping of each severity level against the Alarms Panel, alarms set, LEDs, and SNMP.

Table 51 Default mapping of severity levels

Alarm Severity	Alarms Panel	LEDs	SNMP	Alarm Set (core telephony alarms only)
Critical	Yes	Yes	Yes	Yes
Major	Yes	Yes	Yes	Yes
Minor	Yes	No	No	No
Warning	Yes	No	No	No
Information	Yes	No	No	No

Administering alarms

Alarm information can be delivered to you by any of the following means:

- the Alarms Panel in the BCM Element Manager
- the Alarm Banner in the BCM Element Manager
- the alarm set (core telephony alarms only)
- Simple Network Management Protocol (SNMP) traps for remote management of faults
- LEDs on the BCM main unit

Using the Alarms Panel

You can view real-time alarm information using the Alarms Panel in the BCM Element Manager. Each alarm has a unique identifier. Alarms are displayed in the Alarms table, sorted by date and time by default, with the newest at the top of the table. The Alarms table displays from 50 to 400 alarms. For information about modifying the maximum number of alarms that are displayed, see [“Configuring alarm settings”](#).

The Alarms table contains the following elements:

- Time — the date and time of the alarm
- Alarm ID — the unique alarm ID associated with the alarm
- Severity — the severity of the alarm (Critical, Major, Minor, Warning, and Information)
- Problem Description — a description of the alarm condition
- Component ID — the process that has generated the alarm, in a 3-part DN format. The component ID always identifies the system as a BCM, includes the name of the system that generated the alarm, and identifies the component that generated the alarm. In this way, remote monitoring stations can easily identify what type of system generated an SNMP trap and which system generated the trap.
- Alarm Acked — indicates whether the alarm has been acknowledged in the BCM Element Manager

When you select an alarm in the table, a Details panel is displayed for the selected alarm. The Details panel displays the following information:

- Time — the date and time of the alarm
- Problem Description — a description of the alarm condition
- Problem Resolution — the course of action for the alarm

You can acknowledge an alarm to indicate that the alarm has been taken care of. You can specify whether to include acknowledged alarms in the Alarm Banner so that the alarm count remains concise. For more information about the Alarm Banner, see [“Using the Alarm Banner” on page 152](#).

To view an alarm

When you view an alarm on the alarms panel, you can change the order of the columns in the table and you can sort alarms. For example, you may want to sort alarms by Component ID and Alarm ID.

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarms** task.
The **Alarms** page opens.
- 3 In the Alarms Panel table, select an alarm.
The **Alarm Details** panel displays below the Alarms table.
- 4 To change the order of columns in the Alarm table, select a column and drag it left or right to the desired location, and release it.
- 5 To view a column by ascending or descending order, click the column heading.
- 6 To sort columns, right-click a column heading.
The **Sort** dialog box opens.
- 7 Sort columns as required, and then click the **OK** button.
The columns in the Alarm table are sorted according to your specifications.

To acknowledge an alarm

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarms** task.
The **Alarms** panel opens.
- 3 In the Alarms table, select the alarm you want to acknowledge.
The **Alarm Details** panel is displayed below the Alarms table.
- 4 On the **Alarms Details** panel, click the **Acknowledge Alarm** button.
A check box appears in the **Alarm ACKed** column in the Alarms table for this alarm.

Acknowledging the alarm does not clear the alarm; it indicates only that the alarm has been noted.

Clearing the alarm log



Caution: Clearing the alarm log clears the alarms in the Alarms Panel, as well as from BCM memory. Therefore, alarms will no longer be available for viewing by any other BCM Element Manager clients connected to the BCM. To view alarms, access the Alarm log.

To clear the alarm log

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarms** task.
The **Alarms** panel opens.

- 3 On the **Alarms** panel, click the **Clear Alarm Log** button.
The Alarms table is cleared. Any new alarms will be displayed after the next alarm polling interval.

Using the Alarm Banner

You can use the Alarm Banner in the BCM Element Manager to view current alarm counts and recent alarm activity on the BCM system. The Alarm Banner appears on the bottom-right corner of the BCM Element Manager window. The Alarm Banner is visible at all times, so you do not have to navigate to the Alarms panel to view alarms. If you notice a change in alarm conditions in the Alarm Banner — for example a red spike in the Critical category — you can navigate to the Alarms Panel to view the actual alarm.

The screenshot displays the Nortel BCM 4.0 Element Manager interface. The main window is titled "Nortel BCM 4.0 Element Manager - 192.168.249.27". The interface is divided into several panels:

- Element Navigation Panel:** Shows a tree view of network elements, including "Network Elements" and "192.168.249.27".
- Task Navigation Panel:** Contains tabs for "Configuration" and "Administration". Under "Administration", there is a "General" section with sub-items: "Alarms", "Alarm Settings", "SNMP Trap Destination", "Service Manager", and "Hardware Inventory".
- Alarms Panel:** Displays a table of recent alarms. The table has columns for "Time", "Alarm Acked", "Alarm ID", "Severity", and "Problem Description".
- Alarm Banner:** Located at the bottom right, it shows "Alarm Details" for a specific alarm. The details include:
 - Time: Thu Sep 15 13:14:27 EDT 2005
 - Problem description: User logon User=nnadmin Host=207.179.154.62:4695
 - Comp=CIM
 - Problem resolution: No Action Required.

At the bottom of the window, there is a status bar with the text "Done." and a small alarm banner showing counts for Critical (C:6), Major (M:6), Minor (m:3), and Warning (W:9) alarms, along with a checkbox for "Include ACKed alarms".

Time	Alarm Acked	Alarm ID	Severity	Problem Description
2005-09-15 13:14:27	<input type="checkbox"/>		30200 Information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 13:07:55	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 13:05:28	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 13:05:19	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 13:03:14	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 12:56:35	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695
2005-09-15 12:56:21	<input type="checkbox"/>		30202 minor	User failed to login User=nnadmin Host=207.179.154.62:4695
2005-09-15 12:04:50	<input type="checkbox"/>		30200 information	User logon User=nnadmin Host=207.179.154.62:4695

The Alarm Banner provides counts of Critical, Major, Minor, and Warning alarms; Information alarms are not included. You can specify whether to include acknowledged alarms in the Alarm Banner.

Each alarm severity counter has a graph, which represents a data sample of the last 20 polling intervals. The graph has a color to indicate a data change. The colors are as follows:

Table 52 Alarm graph colors

Color	Indicates
Green	There are no alarms of this severity, or there are alarms of this severity but the count has decreased since the last polling interval.
Yellow	There are alarms of this severity, but they are older than at least 1 polling interval.
Red	A new alarm has occurred since the last polling interval.

The system polls for new alarms every 30 seconds by default.

If you clear the alarm log from the BCM Element Manager, the alarms displayed on the Alarm Banner are also cleared and reset to 0.

To include or omit acknowledged alarms in the Alarm Banner

Select or clear the **Include ACKed Alarms** check box in the Alarm Banner.

Using the alarm set

You can view core telephony alarms on a telephone set on the BCM system. This allows a system administrator to monitor alarm activity without having a BCM Element Manager and a personal computer.

Core telephony alarms are displayed on the alarm set by default; you cannot configure specific alarms to display or suppress. When you view the Alarms table, the Enable Alarm Set column is displayed as a read-only field.

You can specify the telephone to serve as the alarm set in the BCM Element Manager. The telephone set used for alarms must have a 2-line display and three soft keys.

The alarm set displays an alarm as follows:

XXXXX-YYYY

Where XXXXX is the alarm ID and YYYY is additional alarm information.

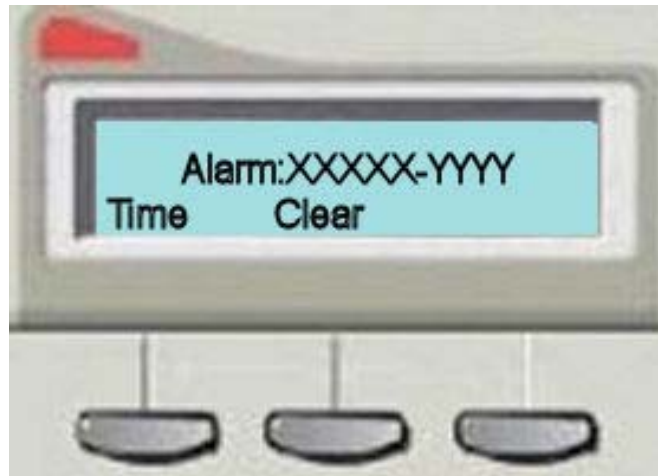
The following options are available when an alarm is generated to the alarm set:

- Time — indicates the date and time when the alarm occurred
- Clear — use this soft key to remove the alarm from the alarm set.



Note: Clearing an alarm from the alarm set does not change the status of alarms on the BCM Element Manager or reset the LEDs on the front panel of the unit.

Figure 28 shows an example of an alarm on the alarm set.

Figure 28 Alarm set alarm

To specify the alarm set

- 1 Click the **Configuration** tab.
- 2 Open the **Telephony** folder.
- 3 Open the **Global Settings** folder, and then click the **Feature Settings** task.
The **Feature Settings** page opens.
- 4 In the **Feature Settings** area, enter the DN of the telephone set that you want to use for the alarm set in the **Alarm Set** field.

To clear an alarm from the alarm set

On the alarm set, press the **Clear** soft key. The alarm is cleared from the alarm set.



Note: Clearing an alarm from the alarm set does not change the status of alarms on the BCM Element Manager or reset the LEDs on the front panel of the unit.

Alarms and LEDs

When an alarm condition occurs on the system, the Status LED on the front of the BCM main unit changes to reflect the alarm condition. In normal operation, both LEDs are green. All alarms with a severity of Major and Critical change the Status LED to solid red on the BCM front panel, except in the event of a Failed Startup Profile, which is indicated by a flashing red LED.

Using the BCM Element Manager, you can reset the Status LEDs on the front panel of the BCM to a normal state.



Note: Once the Status LED has changed to red in response to a Critical or Major alarm condition, it remains in the alarmed state until you reset it using the BCM Element Manager.

To reset the Status LED

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarms** task.
The **Alarms** panel opens.
- 3 On the **Alarms** panel, click the **Reset LEDs** button.
The Status LED on the front panel of the BCM is reset from red to normal operation green.

Using SNMP traps

You can use an SNMP trap manager to remotely monitor BCM alarms via SNMP traps. A trap is an indication from the BCM system to configured trap managers that an alarm has occurred in the BCM system. Any BCM alarm can generate an SNMP trap but by default, only critical and major alarms generate an SNMP trap.

If you want the BCM to send SNMP traps, you must first configure the SNMP agent using the BCM Element Manager. You must enable an SNMP agent and then configure how the system handles SNMP trap notifications. For information about configuring SNMP settings, see [“Configuring SNMP settings” on page 136](#).

The BCM system uses the Small Site Events Management Information Base (MIB) for alarms. The trap format is specified in this MIB. You capture and view traps using any standard SNMP fault monitoring framework or trap watcher. For information about the Small Site Events MIB, see [“Management Information Bases” on page 389](#).

By default, the BCM sends SNMP traps for alarms with a severity of Major and Critical. The only exception is PVQM alarms; for these alarms, the BCM send SNMP traps for all severity levels. You can change the default alarms that are set for SNMP to limit the volume and type of SNMP information, and to control essential information that is transferred on the network. For information about how to change the default alarms, see [“To enable or disable SNMP traps for alarms” on page 156](#).

Configuring alarm settings

Although the BCM system provides a default mapping of alarms that are displayed in the Alarms table and that are sent as an SNMP trap, you may want to monitor additional alarms using either of these means, or you may want to reduce the number of alarms that are displayed in the Alarms table or sent via SNMP traps. You can specify how each alarm is handled, according to your business requirements.

You can specify the following settings for alarms:

- the maximum number of alarms to display in the Alarms Panel (from 50 to 400)
- whether to enable or disable SNMP traps for selected alarms; by default, all Critical and Major alarms are sent as SNMP traps if you have specified one or more trap destinations
- whether to display selected alarms in the Alarms table; by default all Critical, Major, Minor, and Warning alarms are displayed in the Alarms table
- whether to display selected alarms on the alarm set; by default, only core telephony Critical and Major alarms are sent to this set

You can also test a selected alarm. This allows you to test whether the LED or SNMP traps are functioning as expected. Testing an alarm generates an alarm in the system. Alarms generated using the Test Alarm feature are identified in the Alarms table by the words “Test Event” in the alarm Problem Description field.

For information about using SNMP to monitor the BCM system, see [Chapter 6, “Managing BCM with SNMP,”](#) on page 136.

To enable or disable SNMP traps for alarms

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarm Settings** task.
The **Alarm Settings** panel opens.
- 3 In the Alarms table, select an alarm.
- 4 In the **Enable SNMP Trap** column, select or clear the check box to enable or disable SNMP traps for the selected alarm. If you select the check box for a selected alarm, an SNMP trap will be generated if that particular alarm condition occurs.

To enable or disable viewing of selected alarms in the Alarms table

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarm Settings** task.
The **Alarm Settings** panel opens.
- 3 In the Alarms table, select an alarm.
- 4 In the **Enable GUI View** column, select or clear the check box to enable or disable a view of the selected alarm in the Alarms Panel. If you clear the check box for a selected alarm, the alarm will not be displayed in the Alarms table if that particular alarm condition occurs in the system.

To test an alarm

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Alarm Settings** task.
The **Alarm Settings** panel opens.

- 3 In the Alarms table, select an alarm.
- 4 Click the **Test Alarm** button.
In the Alarms table, “Test Event” is displayed in the alarm Problem Description field.



Note: When you click the Test Alarm button, you will see an alarm indication on the BCM Element Manager, or through SNMP. Test alarms are not displayed on the alarm set.

List of BCM alarms

Table 53 lists BCM alarms. The table includes the default handling of each alarm with respect to the Alarms table, the alarm set, LEDs, and SNMP traps.

You can customize whether each alarm appears in the Alarms table or is sent as an SNMP trap in accordance with your business requirements.

Table 53 BCM Alarm List

#	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm	SNMP	LED	Alarm Set
1	18	minor	Core Telephony	Core Telephony - Unable to process calls.	Reboot system and contact your local support group.	Yes	No	No	No
2	31	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failed.	Power down the system and check the DTM hardware and the expansion chassis connections. If problem persists replace the DTM or expansion chassis hardware.	Yes	Yes	Yes	Yes
3	32	critical	Core Telephony	Core Telephony - BRI module is primary clock instead of DTM module.	Configure the DTM module as primary clock in your system. BRI clock specifications are not acceptable for DTM connections to the public network.	Yes	Yes	Yes	Yes
4	33	critical	Core Telephony	Core Telephony - Cold restart has occurred causing loss of telephony data.	Check configuration change logs to see if this was user initiated. If not contact your local support group.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

5	34	warning	Core Telephony	Core Telephony - Media Bay Module firmware download started.	No Action Required.	Yes	No	No	No
6	35	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failure.	Power down the system and check the expansion chassis connections. Check for corresponding alarm 31 or 79 to determine which module is having issues. If problem persists replace corresponding hardware.	Yes	Yes	Yes	Yes
7	36	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failure.	Power down the system and check the expansion chassis connections. Check for corresponding alarm 31 or 79 to determine which module is having issues. If problem persists replace corresponding hardware.	Yes	Yes	Yes	Yes
8	37	critical	Core Telephony	Core Telephony - Failure to download market profile/protocol data from the Persistent Data Repository.	Restart system and contact your local support group.	Yes	Yes	Yes	Yes
9	39	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption in the market profile area.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

10	40	critical	Core Telephony	Core Telephony - "Unavailable Seconds Error" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
11	41	critical	Core Telephony	Core Telephony - "Loss of Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
12	42	critical	Core Telephony	Core Telephony - "Loss of Frame" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
13	43	critical	Core Telephony	Core Telephony - "Alarm Indication Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

14	44	critical	Core Telephony	Core Telephony - "Remote Alarm Indication" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
15	45	critical	Core Telephony	Core Telephony - "Loss of Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
16	46	critical	Core Telephony	Core Telephony - "Alarm Indication Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
17	47	critical	Core Telephony	Core Telephony - "Remote Alarm Indication" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

18	50	critical	Core Telephony	Core Telephony - A digital station module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital station module. If the problem persists, replace the module.	Yes	Yes	Yes	Yes
19	51	critical	Core Telephony	Core Telephony - A trunk media bay module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. If the problem persists, replace the module.	Yes	Yes	Yes	Yes
20	52	critical	Core Telephony	Core Telephony - A trunk media bay module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. If the problem persists, replace the module.	Yes	Yes	Yes	Yes
21	54	warning	Core Telephony	Core Telephony - Media Bay Module firmware download started.	No Action Required.	Yes	No	No	No
22	55	warning	Core Telephony	Core Telephony - Media Bay Module firmware download complete.	No Action Required.	Yes	No	No	No
23	61	critical	Core Telephony	Core Telephony - A trunk media bay module is programmed as the wrong module type.	Check that the correct module type is programmed for the expansion chassis.	Yes	Yes	Yes	Yes
24	62	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption in the auto answer area.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

25	63	critical	Core Telephony	Core Telephony - No DTMF receivers available.	If this happens more than once in a 5 minute span check that any auto answer or DISA configured trunks are operating properly. If they are not operating properly reboot the system and contact your local support group.	Yes	Yes	Yes	Yes
26	67	critical	Core Telephony	Core Telephony - Invalid trunk media bay module connected to an expansion chassis.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. Check that the hardware being used is supported in the market your have selected in Core Telephony. If the problem persists, replace the module.	Yes	Yes	Yes	Yes
27	68	critical	Core Telephony	Core Telephony - Unsupported set/peripheral connected.	Disconnect the set/peripheral from the port and reconnect it to a valid port. If the problem persists replace the set/peripheral.	Yes	Yes	Yes	Yes
28	69	critical	Core Telephony	Core Telephony - General software error.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
29	71	warning	Core Telephony	Core Telephony - Emergency transfer relay activated indicating a power issue or Core Telephony down condition.	No Action Required.	Yes	No	No	No
30	72	critical	Core Telephony	Core Telephony - TEI request on ISDN device on system.	Disconnect all station side ISDN devices. If problem persists contact your local support group.	Yes	Yes	Yes	Yes

Table 53 BCM Alarm List

31	75	critical	Core Telephony	Core Telephony - Digital trunking clock in free run.	Check your cabling from any DTM modules to the external network. Get your network provider to check the circuit.	Yes	Yes	Yes	Yes
32	77	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes	Yes
33	79	critical	Core Telephony	Core Telephony - ASM firmware download error.	Power down the system and check the ASM hardware and the expansion chassis connections. If problem persists replace the ASM or expansion chassis hardware.	Yes	Yes	Yes	Yes
34	194	critical	Core Telephony	Core Telephony - Low Level Operating error.	Restart system and contact your local support group.	Yes	Yes	Yes	Yes
35	224	critical	Core Telephony	Core Telephony - Error after restore of data.	Attempt another restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes	Yes
36	247	critical	Core Telephony	Core Telephony - Digital station loop error.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	Yes	Yes	Yes
37	260	minor	Core Telephony	Core Telephony - Line presence test failure on system startup due to no battery feed on a trunk line.	Verify all trunks lines are connected to the system and in working condition. If not disable/enable the trunk interfaces. If problems persists contact your local support group.	Yes	No	No	No

Table 53 BCM Alarm List

38	262	minor	Core Telephony	Core Telephony - No dialtone on trunk line during seizure.	Check the trunk interfaces to see if dialtone is present. If no dialtone is present contact your network provider.	Yes	No	No	No
39	263	minor	Core Telephony	Core Telephony - Invalid disconnect sequence error on an analog trunk line.	Check the analog trunk interfaces to ensure all lines are operating correctly. If a trunk is showing busy with no active calls disable the trunk interface and re-enable it. If problems persist contact your local support group.	Yes	No	No	No
40	265	minor	Core Telephony	Core Telephony - Outgoing trunk could not be seized. Handshake between the system and network failed.	Check the trunk interfaces to ensure all lines are operating correctly. If a trunk is not able to be used contact your network provider.	Yes	No	No	No
41	270	minor	Core Telephony	Core Telephony - Set initialization error from an invalid message from the set.	If the event occurs more than once in a 5 minute span then disconnect the set in question. If problem stops replace set and check cable between set and system.	Yes	No	No	No
42	271	minor	Core Telephony	Core Telephony - A set is trying to initialize that has incompatible firmware on the system.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	No	No	No

Table 53 BCM Alarm List

43	323	minor	Core Telephony	Core Telephony - "Degraded Minute" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
44	324	minor	Core Telephony	Core Telephony - "Severely Errored Second" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
45	325	minor	Core Telephony	Core Telephony - "Errored Second" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
46	326	minor	Core Telephony	Core Telephony - "Slip Underflow" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No

Table 53 BCM Alarm List

47	327	minor	Core Telephony	Core Telephony - "Slip Overflow" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
48	328	minor	Core Telephony	Core Telephony - "Line Code Violation" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
49	329	minor	Core Telephony	Core Telephony - "Loss of Signal" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
50	330	minor	Core Telephony	Core Telephony - "Loss of Frame" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No

Table 53 BCM Alarm List

51	331	minor	Core Telephony	Core Telephony - "Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
52	332	minor	Core Telephony	Core Telephony - "Remote Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
53	333	minor	Core Telephony	Core Telephony - "Loss of Frame" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
54	334	minor	Core Telephony	Core Telephony - "Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No

Table 53 BCM Alarm List

55	335	minor	Core Telephony	Core Telephony - "Remote Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No	No
56	336	information	Core Telephony	Core Telephony - The Digital Trunk T1/E1/PRI has recovered.	No Action Required.	Yes	No	No	No
57	367	minor	Core Telephony	Core Telephony - Digital Trunk Media bay module reset.	Determine whether this alarm occurred due to the system rebooting. If the system was not rebooting when the alarm occurred, then contact your local support group.	Yes	No	No	No
58	372	warning	Core Telephony	Core Telephony - Clocking on the Digital Trunk Media bay module has changed sources.	No Action Required.	Yes	No	No	No
59	401	minor	Core Telephony	Core Telephony - Digital station loop initialization error.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	No	No	No
60	608	minor	Core Telephony	Core Telephony - Unsupported set/peripheral connected.	Verify that all types of attached sets/peripherals initialize and function. Remove any unsupported set types.	Yes	No	No	No

Table 53 BCM Alarm List

61	639	minor	Core Telephony	Core Telephony - CAP/KIM error while retrieving key information.	Check the system for CAP/KIM modules and reset them. If the problem persists contact your local support group.	Yes	No	No	No
62	799	minor	Core Telephony	Core Telephony - ISDN call processing error.	No Action Required.	Yes	No	No	No
63	894	minor	Core Telephony	Core Telephony - DASS2/DPNSS error on a DTM module.	Check that the DASS2/DPNSS circuit is online. If it is not disable/enable the expansion chassis and try to get the circuit back online. If problem persists contact your local support group.	Yes	No	No	No
64	901	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption.	Restore a known good backup into the system to get it back online and contact your local support group.	Yes	Yes	Yes	Yes
65	949	minor	Core Telephony	Core Telephony - BRI protocol call control error.	Get a protocol trace of the BRI loop using BCM monitor and contact your local support group.	Yes	No	No	No
66	999	warning	Core Telephony	Core Telephony - Unknown alarm.	Contact your local support group.	Yes	No	No	No
67	1001	major	Operating System	Operating System - Major operating system error (Kernel Oops).	Contact your local support group.	Yes	Yes	Yes	N/A
68	1002	critical	Operating System	Operating System - Critical operating system error (Kernel panic).	Contact your local support group.	Yes	Yes	Yes	N/A
69	2100	information	Software Updates	Software Update - Software update applied successfully.	No Action Required.	Yes	No	No	N/A
70	2101	information	Software Updates	Software Update - Software upgrade applied successfully.	No Action Required.	Yes	No	No	N/A
71	2102	information	Software Updates	Software Update - Software update started.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

72	2103	information	Software Updates	Software Update - Software upgrade started.	No Action Required.	Yes	No	No	N/A
73	2104	information	Software Updates	Software Update - Software update scheduled.	No Action Required.	Yes	No	No	N/A
74	2105	information	Software Updates	Software Update - Scheduled software update completed.	No Action Required.	Yes	No	No	N/A
75	2106	information	Software Updates	Software Update - Software update removed.	No Action Required.	Yes	No	No	N/A
76	2300	critical	Software Updates	Software Update - Software update failed to apply.	Contact your local support group.	Yes	Yes	Yes	N/A
77	2301	major	Software Updates	Software Update - Software update failed to transfer files.	Retry software update and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
78	2302	critical	Software Updates	Software Update - Software upgrade failed to apply.	Contact your local support group.	Yes	Yes	Yes	N/A
79	2303	major	Software Updates	Software Update - Failed to remove software update.	Retry removal of software update and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
80	2304	major	Software Updates	Software Update - Software update invalid signature or corrupt file. Retry file transfer.	Retry software update and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
81	5001	critical	Persistent Data Repository	Persistent Data Repository - Could not start Persistent Data Repository. No resources available. This will cause many components to fail to start with the proper configuration.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

82	5002	critical	Persistent Data Repository	Persistent Data Repository - Could not open Persistent Data Repository. Reverting to last saved file. Will mean configuration will not be current on the system.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	Yes	Yes	N/A
83	5003	critical	Persistent Data Repository	Persistent Data Repository - Could not open Persistent Data Repository. Reverting to default file. Will mean configuration will be default on the system.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	Yes	Yes	N/A
84	6000	minor	Date and Time	Date and Time - Time has been updated by CoreTel.	No Action Required.	Yes	No	No	N/A
85	6004	critical	Date and Time	Date and Time - Time service initialization failed.	Contact your local support group.	Yes	Yes	Yes	N/A
86	6007	minor	Date and Time	Date and Time - Time adjustment detected which is larger than provisioned.	Confrim the date/ time is correct on the system.	Yes	No	No	N/A
87	6008	minor	Date and Time	Date and Time - NTP client unable to contact server.	Confirm the NTP server is available on the network.	Yes	No	No	N/A
88	6010	critical	Date and Time	Date and Time - Real time clock on system not working properly.	Don't reboot the system and contact your local support group.	Yes	Yes	Yes	N/A
123	10002	critical	Service Manager	Service Manager - CallPilot has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10102 or 10302. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

124	10003	critical	Service Manager	Service Manager - IP Terminal Service (UTPS) has stopped unexpectedly. This will affect service on all IP terminals on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10103 or 10303. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
126	10005	critical	Service Manager	Service Manager - Voice over IP Gateway (feps) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10105 or 10305. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
127	10006	critical	Service Manager	Service Manager - Quality of Service Monitor (qmond) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10106 or 10306. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
128	10007	critical	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10107 or 10307. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
130	10008	critical	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has stopped unexpectedly. This will affect CallPilot, System Set Based Admin and IVR. Service Manager is attempting to restart the service.	Check for corresponding alarm 10108 or 10308. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
132	10010	critical	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10110 or 10310. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

133	10011	critical	Service Manager	Service Manager - Computer Telephony Service (Cte) has stopped unexpectedly. This will affect LAN CTE and the Line Monitor in BCM Monitor. Service Manager is attempting to restart the service.	Check for corresponding alarm 10111 or 10311. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
134	10012	critical	Service Manager	Service Manager - Line Monitor Service (lms) has stopped unexpectedly. This will affect the Line Service Manager - Monitor in BCM Monitor. Service Manager is attempting to restart the service.	Check for corresponding alarm 10112 or 10312. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
135	10013	critical	Service Manager	Service Manager - Media Services Manager (Msm) has stopped unexpectedly. This will affect all telephony operations on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10113 or 10313. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
136	10014	critical	Service Manager	Service Manager - Media Path Server (mps) has stopped unexpectedly. This will affect all IP Telephony. Service Manager is attempting to restart the service.	Check for corresponding alarm 10114 or 10314. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
137	10015	critical	Service Manager	Service Manager - Media Gateway Server (mgs) has stopped unexpectedly. This will affect all IP Telephony. Service Manager is attempting to restart the service.	Check for corresponding alarm 10115 or 10315. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

138	10016	critical	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has stopped unexpectedly. This will affect any management done to running services or startup of non-running services. Service Manager is attempting to restart the service.	Check for corresponding alarm 10116 or 10316. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
139	10017	critical	Service Manager	Service Manager - Keycode Service (cfsserver) has stopped unexpectedly. This will affect the ability to enter any new keycodes. Service Manager is attempting to restart the service.	Check for corresponding alarm 10117 or 10317. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
140	10018	critical	Service Manager	Service Manager - Time Service (tmwservice) has stopped unexpectedly. This will affect the synchronization of time in the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10118 or 10318. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
141	10019	critical	Service Manager	Service Manager - Platform Status Monitor (psm) has stopped unexpectedly. This will affect the monitoring of system hardware and drivers. Service Manager is attempting to restart the service.	Check for corresponding alarm 10119 or 10319. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

142	10020	critical	Service Manager	Service Manager - Web Server (httpd) has stopped unexpectedly. This will affect the onbox web pages, downloads and documentation. Service Manager is attempting to restart the service.	Check for corresponding alarm 10120 or 10320. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
143	10021	critical	Service Manager	Service Manager - On Box Management Framework (owcimomd) has stopped unexpectedly. Element Manager will be unable to connect with the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10121 or 10321. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
144	10023	critical	Service Manager	Service Manager - MSC Driver (MscService) has stopped unexpectedly. This will affect normal operation of all services that interact with CoreTel. Service Manager is attempting to restart the service.	Check for corresponding alarm 10123 or 10323. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
145	10024	critical	Service Manager	Service Manager - IP Terminal Service (EchoServer) has stopped unexpectedly. This will affect IP terminals from operating properly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10124 or 10324. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

146	10025	critical	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has stopped unexpectedly. This will affect the ability to download new firmware to IP terminals. Service Manager is attempting to restart the service.	Check for corresponding alarm 10125 or 10325. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
147	10026	critical	Service Manager	Service Manager - CoreTel Logging (LogManagement) has stopped unexpectedly. This will affect the logging of CoreTel. Service Manager is attempting to restart the service.	Check for corresponding alarm 10126 or 10326. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
148	10027	critical	Service Manager	Service Manager - DNS Services (named) has stopped unexpectedly. This will affect the system from proper DNS name resolution. Service Manager is attempting to restart the service.	Check for corresponding alarm 10127 or 10327. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
149	10028	critical	Service Manager	Service Manager - Integrated Wan (Wan) has stopped unexpectedly. This will affect the ability to use ISDN dial up services on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10128 or 10328. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

150	10029	critical	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has stopped unexpectedly. This will affect the ability to use a doorphone on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10129 or 10329. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
151	10030	critical	Service Manager	Service Manager - Reporting for Contact Center Service (CCRSAppServer) has stopped unexpectedly. This will affect the ability to use Reporting for Contact Center. Service Manager is attempting to restart the service.	Check for corresponding alarm 10130 or 10330. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
152	10031	critical	Service Manager	Service Manager - Reporting for Contact Center Database Service (postgresql) has stopped unexpectedly. This will affect the ability to use Reporting for Contact Center. Service Manager is attempting to restart the service.	Check for corresponding alarm 10131 or 10331. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A
153	10032	critical	Service Manager	Service Manager - IP Music Service (BcmAmp) has stopped unexpectedly. This will affect the ability to use IP music. Service Manager is attempting to restart the service.	Check for corresponding alarm 10132 or 10332. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

154	10033	minor	Service Manager	Service Manager - IP Music Service (ToneSrvr) has stopped unexpectedly. This will affect the ability to use IP music. Service Manager is attempting to restart the service.	Check for corresponding alarm 10133 or 10333. This can be caused by changing music sources. If service doesn't restart then reboot system and contact your local support group..	Yes	No	No	N/A
155	10034	minor	Service Manager	Service Manager - Net Link Manager Service (nlmd) has stopped unexpectedly. This will affect the default IP route of your system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10134 or 10334. If service doesn't restart then reboot system and contact your local support group.	Yes	No	No	N/A
157	10102	critical	Service Manager	Service Manager - CallPilot has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
158	10103	critical	Service Manager	Service Manager - IP Terminal Service (UTPS) has stopped unexpectedly and could not be restarted by service manager. This will affect service on all IP terminals on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
160	10105	critical	Service Manager	Service Manager - Voice over IP Gateway (feps) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
161	10106	critical	Service Manager	Service Manager - Quality of Service Monitor (qmond) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

162	10107	critical	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
164	10108	critical	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has stopped unexpectedly and could not be restarted by service manager. This will affect CallPilot, System Set Based Admin and IVR.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
166	10110	critical	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
167	10111	critical	Service Manager	Service Manager - Computer Telephony Service (Cte) has stopped unexpectedly and could not be restarted by service manager. This will affect LAN CTE and the Line Monitor in BCM Monitor.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
168	10112	critical	Service Manager	Service Manager - Line Monitor Service (lms) has stopped unexpectedly and could not be restarted by service manager. This will affect the Line Monitor in BCM Monitor.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

169	10113	critical	Service Manager	Service Manager - Media Services Manager (Msm) has stopped unexpectedly and could not be restarted by service manager. This will affect all telephony operations on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
170	10114	critical	Service Manager	Service Manager - Media Path Server (mps) has stopped unexpectedly and could not be restarted by service manager. This will affect all IP Telephony.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
171	10115	critical	Service Manager	Service Manager - Media Gateway Server (mgs) has stopped unexpectedly and could not be restarted by service manager. This will affect all IP Telephony.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
172	10116	critical	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has stopped unexpectedly and could not be restarted by service manager. This will affect any management done to running services or startup of non-running services.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
173	10117	critical	Service Manager	Service Manager - Keycode Service (cfserver) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to enter any new keycodes.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

174	10118	critical	Service Manager	Service Manager - Time Service (tmwservice) has stopped unexpectedly and could not be restarted by service manager. This will affect the synchronization of time in the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
175	10119	critical	Service Manager	Service Manager - Platform Status Monitor (psm) has stopped unexpectedly and could not be restarted by service manager. This will affect the monitoring of system hardware and drivers.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
176	10120	critical	Service Manager	Service Manager - Web Server (httpd) has stopped unexpectedly and could not be restarted by service manager. This will affect the onbox web pages, downloads and documentation.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
177	10121	critical	Service Manager	Service Manager - On Box Management Framework (owcimomd) has stopped unexpectedly and could not be restarted by service manager. Element Manager will be unable to connect with the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
178	10122	critical	Service Manager	Service Manager - Service Manager (monit) has stopped unexpectedly.	Check for corresponding alarm 10322 to indicate a restart. If 10322 doesn't happen then reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

179	10123	critical	Service Manager	Service Manager - MSC Driver (MscService) has stopped unexpectedly and could not be restarted by service manager. This will affect normal operation of all services that interact with CoreTel.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
180	10124	critical	Service Manager	Service Manager - IP Terminal Service (EchoServer) has stopped unexpectedly and could not be restarted by service manager. This will affect IP terminals from operating properly.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
181	10125	critical	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to download new firmware to IP terminals.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
182	10126	critical	Service Manager	Service Manager - CoreTel Logging (LogManagement) has stopped unexpectedly and could not be restarted by service manager. This will affect the logging of CoreTel.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

183	10127	critical	Service Manager	Service Manager - DNS Services (named) has stopped unexpectedly and could not be restarted by service manager. This will affect the system from proper DNS name resolution.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
184	10128	critical	Service Manager	Service Manager - Integrated Wan (Wan) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use ISDN dial up services on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
185	10129	critical	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use a doorphone on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
186	10130	critical	Service Manager	Service Manager - Reporting for Contact Center Service (CCRSAppServer) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use Reporting for Contact Center.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

187	10131	critical	Service Manager	Service Manager - Reporting for Contact Center Database Service (postgresql) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use Reporting for Contact Center.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
188	10132	critical	Service Manager	Service Manager - IP Music Service (BcmAmp) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use IP music.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
189	10133	critical	Service Manager	Service Manager - IP Music Service (ToneSvr) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use IP music.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A
190	10134	critical	Service Manager	Service Manager - Net Link Manager Service (nlmd) has stopped unexpectedly and could not be restarted by service manager. This will affect the default IP route of your system.	Reboot system and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

192	10202	Warning	Service Manager	Service Manager - CallPilot has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No	N/A
193	10203	Warning	Service Manager	Service Manager - IP Terminal Service (UTPS) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect service on all IP terminals on the system.	No Action Required.	Yes	No	No	N/A
195	10205	Warning	Service Manager	Service Manager - Voice over IP Gateway (feps) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No	N/A
196	10206	Warning	Service Manager	Service Manager - Quality of Service Monitor (qmond) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

197	10207	Warning	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No	N/A
201	10210	Warning	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No	N/A
202	10211	Warning	Service Manager	Service Manager - Computer Telephony Service (Cte) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect LAN CTE and the Line Monitor in BCM Monitor.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

203	10212	Warning	Service Manager	Service Manager - Line Monitor Service (lms) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the Line Monitor in BCM Monitor.	No Action Required.	Yes	No	No	N/A
204	10213	Warning	Service Manager	Service Manager - Media Services Manager (Msm) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all telephony operations on the system.	No Action Required.	Yes	No	No	N/A
205	10214	Warning	Service Manager	Service Manager - Media Path Server (mps) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all IP Telephony.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

206	10215	Warning	Service Manager	Service Manager - Media Gateway Server (mgs) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all IP Telephony.	No Action Required.	Yes	No	No	N/A
207	10216	Warning	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect any management done to running services.	No Action Required.	Yes	No	No	N/A
208	10217	Warning	Service Manager	Service Manager - Keycode Service (cfserver) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to enter any new keycodes.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

209	10218	Warning	Service Manager	Service Manager - Time Service (tmwservice) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the synchronization of time in the system.	No Action Required.	Yes	No	No	N/A
210	10219	Warning	Service Manager	Service Manager - Platform Status Monitor (psm) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the monitoring of system hardware and drivers.	No Action Required.	Yes	No	No	N/A
211	10220	Warning	Service Manager	Service Manager - Web Server (httpd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the onbox web pages, downloads and documentation.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

212	10221	Warning	Service Manager	Service Manager - On Box Management Framework (owcimomd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. Element Manager will be unable to connect with the system.	No Action Required.	Yes	No	No	N/A
213	10223	Warning	Service Manager	Service Manager - MSC Driver (MscService) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect normal operation of all services that interact with CoreTel.	No Action Required.	Yes	No	No	N/A
214	10224	Warning	Service Manager	Service Manager - IP Terminal Service (EchoServer) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect IP terminals from operating properly.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

215	10225	Warning	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to download new firmware to IP terminals.	No Action Required.	Yes	No	No	N/A
216	10226	Warning	Service Manager	Service Manager - CoreTel Logging (LogManagement) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the logging of CoreTel.	No Action Required.	Yes	No	No	N/A
217	10227	Warning	Service Manager	Service Manager - DNS Services (named) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the system from proper DNS name resolution.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

218	10228	Warning	Service Manager	Service Manager - Integrated Wan (Wan) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use ISDN dial up services on the system.	No Action Required.	Yes	No	No	N/A
219	10229	Warning	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use a doorphone on the system.	No Action Required.	Yes	No	No	N/A
220	10230	Warning	Service Manager	Service Manager - Reporting for Contact Center Service (CCRSAppServer) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use Reporting for Contact Center.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

221	10231	Warning	Service Manager	Service Manager - Reporting for Contact Center Database Service (postgresql) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use Reporting for Contact Center.	No Action Required.	Yes	No	No	N/A
222	10232	Warning	Service Manager	Service Manager - IP Music Service (BcmAmp) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use IP music.	No Action Required.	Yes	No	No	N/A
223	10233	Warning	Service Manager	Service Manager - IP Music Service (ToneSrvr) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use IP music.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

224	10234	Warning	Service Manager	Service Manager - Net Link Manager Service (nlmd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the default IP route of your system.	No Action Required.	Yes	No	No	N/A
226	10302	Information	Service Manager	Service Manager - CallPilot has been successfully restarted.	No Action Required.	Yes	No	No	N/A
227	10303	Information	Service Manager	Service Manager - IP Terminal Service (UTPS) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
229	10305	Information	Service Manager	Service Manager - Voice over IP Gateway (feps) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
230	10306	Information	Service Manager	Service Manager - Quality of Service Monitor (qmond) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
231	10307	Information	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
232	10308	Information	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
234	10310	Information	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has been successfully restarted.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

235	10311	Information	Service Manager	Service Manager - Computer Telephony Service (Cte) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
236	10312	Information	Service Manager	Service Manager - Line Monitor Service (lms) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
237	10313	Information	Service Manager	Service Manager - Media Services Manager (Msm) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
238	10314	Information	Service Manager	Service Manager - Media Path Server (mps) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
239	10315	Information	Service Manager	Service Manager - Media Gateway Server (mgs) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
240	10316	Information	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
241	10317	Information	Service Manager	Service Manager - Keycode Service (cfserver) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
242	10318	Information	Service Manager	Service Manager - Time Service (tmwservice) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
243	10319	Information	Service Manager	Service Manager - Platform Status Monitor (psm) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
244	10320	Information	Service Manager	Service Manager - Web Server (httpd) has been successfully restarted.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

245	10321	Information	Service Manager	Service Manager - On Box Management Framework (owcimomd) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
246	10322	Information	Service Manager	Service Manager - Service Manager (monit) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
247	10323	Information	Service Manager	Service Manager - MSC Driver (MscService) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
248	10324	Information	Service Manager	Service Manager - IP Terminal Service (EchoServer) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
249	10325	Information	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
250	10326	Information	Service Manager	Service Manager - CoreTel Logging (LogManagement) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
251	10327	Information	Service Manager	Service Manager - DNS Services (named) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
252	10328	Information	Service Manager	Service Manager - Integrated Wan (Wan) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
253	10329	Information	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has been successfully restarted.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

254	10330	Information	Service Manager	Service Manager - Reporting for Contact Center Service (CCRSAppServer) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
255	10331	Information	Service Manager	Service Manager - Reporting for Contact Center Database Service (postgresql) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
256	10332	Information	Service Manager	Service Manager - IP Music Service (BcmAmp) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
257	10333	Information	Service Manager	Service Manager - IP Music Service (ToneSvr) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
258	10334	Information	Service Manager	Service Manager - Net Link Manager Service (nlmd) has been successfully restarted.	No Action Required.	Yes	No	No	N/A
260	10906	Information	Startup Sequence	System Startup - Operating system and alarm subsystem available. Power LED = solid red; Status LED = Off.	No Action Required.	Yes	No	No	N/A
262	10907	Information	Startup Sequence	System Startup - Telephony and Voicemail active. Power LED = solid red; Status LED = blinking green.	No Action Required.	Yes	No	No	N/A
263	10908	Information	Startup Sequence	System Startup - Element Manager is available. Power LED = solid green; Status LED = flashing green.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

264	10909	Information	Startup Sequence	System Startup - Startup complete. Service Manager and Scheduling Services available. Power LED = solid green; Status LED = solid green.	No Action Required.	Yes	No	No	N/A
265	10999	major	Startup Sequence	System Startup - AutoCoreUpload FAILED....!	Contact your local support group.	Yes	Yes	Yes	N/A
266	11002	Information	Platform Status Monitor	Platform Status Monitor - Power recovered.	No Action Required. Recovery alarm for corresponding alarms 11200 and 11400.	Yes	No	No	N/A
267	11003	Information	Platform Status Monitor	Platform Status Monitor - Hard drive space recovered.	No Action Required. Recovery alarm for corresponding alarms 11201.	Yes	No	No	N/A
268	11004	Information	Platform Status Monitor	Platform Status Monitor - Memory recovered.	No Action Required. Recovery alarm for corresponding alarm 11202	Yes	No	No	N/A
269	11005	Information	Platform Status Monitor	Platform Status Monitor - CPU load recovered.	No Action Required. Recovery alarm for corresponding alarm 11203.	Yes	No	No	N/A
270	11006	Information	Platform Status Monitor	Platform Status Monitor - LAN recovered.	No Action Required. Recovery alarm for corresponding alarm 11204.	Yes	No	No	N/A
271	11011	Information	Platform Status Monitor	Platform Status Monitor - Local Temperature recovered.	No Action Required. Recovery alarm for corresponding alarms 11209 and 11405.	Yes	No	No	N/A
272	11012	Information	Platform Status Monitor	Platform Status Monitor - Remote Temperature recovered.	No Action Required. Recovery alarm for corresponding alarms 11210 and 11406.	Yes	No	No	N/A
273	11014	Information	Platform Status Monitor	Platform Status Monitor - Fan recovered.	No Action Required. Recovery alarm for corresponding alarms 11212 and 11408.	Yes	No	No	N/A

Table 53 BCM Alarm List

279	11200	minor	Platform Status Monitor	Platform Status Monitor - failed to read Power.	Reboot system and if problem persists contact your local support group.	Yes	No	No	N/A
280	11201	major	Platform Status Monitor	Platform Status Monitor - Hard drive near capacity.	Contact local support group for assistance in recovering drive space.	Yes	Yes	Yes	N/A
281	11202	major	Platform Status Monitor	Platform Status Monitor - Memory near capacity.	Contact local support group for assistance in analyzing memory usage.	Yes	Yes	Yes	N/A
282	11203	minor	Platform Status Monitor	Platform Status Monitor - CPU load above threshold.	Use BCM Monitor for real-time view of CPU activity. Monitor for alarm 11005 to indicate CPU recovered. If problem persists, contact local support group.	Yes	No	No	N/A
283	11204	major	Platform Status Monitor	Platform Status Monitor - 1. rx_byte/sec greater than 50% of LAN%% speed, 2. tx_byte/sec greater than 50% of LAN%% speed, 3. rx_errors/sec of LAN%% > %%%, 4. tx_errors/sec of LAN%% > %%%, 5. rx_dropped/sec of LAN%% > %%%, 6. tx_dropped/sec of LAN%% > %%%	Verify that Customer LAN is performing as expected.	Yes	Yes	Yes	N/A
284	11209	major	Platform Status Monitor	Platform Status Monitor - Failed to read Local Temperature.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes	N/A
285	11210	major	Platform Status Monitor	Platform Status Monitor - Failed to read Remote Temperature.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

286	11212	major	Platform Status Monitor	Platform Status Monitor - Fan Below Tolerance.	Check Fan operation as fan is apparently not working correctly. If alarm persists, replace fan.	Yes	Yes	Yes	N/A
292	11250	major	Platform Status Monitor	Platform Status Monitor - The size of XXX Log file is greater than 16MB, XXX Log file will be deleted to recover /var/log partition.	Contact your local support group.	Yes	Yes	Yes	N/A
293	11400	major	Platform Status Monitor	Platform Status Monitor - Power %##% Failed.	Verify that external power is per operational limits. If alarm persists, contact your local support group.	Yes	Yes	Yes	N/A
294	11405	critical	Platform Status Monitor	Platform Status Monitor - Local Temperature above tolerance.	Check Fan operation and room temperature as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes	N/A
295	11406	critical	Platform Status Monitor	Platform Status Monitor - Remote Temperature above tolerance.	Check Fan operation and room temperature as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes	N/A
296	11408	critical	Platform Status Monitor	Platform Status Monitor - Fan speed is reading 0 for over 1 minute.	Check Fan operation as fan is apparently malfunctioning. If alarm persists, replace fan.	Yes	Yes	Yes	N/A
298	11502	critical	Platform Status Monitor	Platform Status Monitor - System out of Memory.	Contact your local support group for assistance in analyzing memory condition.	Yes	Yes	Yes	N/A
299	12001	major	Backup and Restore	Backup and Restore - Backup file could no be renamed.	Contact your local support group.	Yes	Yes	Yes	N/A
300	12002	major	Backup and Restore	Backup and Restore - Backup type is incorrect for its filesystem location.	Use a good backup to attempt the restore	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

301	12003	major	Backup and Restore	Backup and Restore - This backup type can not be restored.	Use a good backup to attempt the restore	Yes	Yes	Yes	N/A
302	12004	major	Backup and Restore	Backup and Restore - Internal error. Could not find associated connection definition.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
303	12005	major	Backup and Restore	Backup and Restore - Internal error. Could not create a file.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
304	12006	major	Backup and Restore	Backup and Restore - Internal error. Could not build the dynamic rule file.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
305	12007	major	Backup and Restore	Backup and Restore - Internal general error.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
306	12008	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Try a different backup file.	Yes	No	No	N/A
307	12009	major	Backup and Restore	Backup and Restore - Could not connect to the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes	N/A
308	12010	minor	Backup and Restore	Backup and Restore - Could not authenticate with the ftp site.	Check your login credentials to the FTP server	Yes	No	No	N/A
309	12011	minor	Backup and Restore	Backup and Restore - Could not change ftp modes on the ftp site.	Check your FTP server configuration	Yes	No	No	N/A
310	12012	major	Backup and Restore	Backup and Restore - Could not send the file to the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

311	12013	major	Backup and Restore	Backup and Restore - Could not retrieve the file from the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes	N/A
312	12014	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes	N/A
313	12015	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes	N/A
314	12016	warning	Backup and Restore	Backup and Restore - Backup is busy serving another request.	No Action Required.	Yes	No	No	N/A
315	12017	warning	Backup and Restore	Backup and Restore - File integrity error. Contents altered since creation.	Use a different backup file	Yes	No	No	N/A
316	12018	major	Backup and Restore	Backup and Restore - Internal error. Database could not be backed-up.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes	N/A
317	12019	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No	N/A
318	12020	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No	N/A
319	12021	major	Backup and Restore	Backup and Restore - Internal error. Could not shadow data.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes	N/A
320	12022	major	Backup and Restore	Backup and Restore - File is not recognizable. The signature is the wrong length.	Use a different backup file and if problem persists contact your local support group	Yes	Yes	Yes	N/A
321	12023	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Use a different backup file and if problem persists contact your local support group	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

322	12024	major	Backup and Restore	Backup and Restore - Internal error. Compression incorrectly specified in configuration file.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes	N/A
323	12025	major	Backup and Restore	Backup and Restore - Internal error. Component in configuration file not recognized.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes	N/A
324	12026	major	Backup and Restore	Backup and Restore - Internal error. Unrecognized transfer mechanism.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes	N/A
325	12027	critical	Backup and Restore	Backup and Restore - File could not be copied to USB device.	Check the USB connection and flash device	Yes	Yes	Yes	N/A
326	12028	minor	Backup and Restore	Backup and Restore - File is incompatible with current software.	Use a backup from a supported software version	Yes	No	No	N/A
327	12029	major	Backup and Restore	Backup and Restore - Internal error. Could not restore the database.	Attempt another restore and if problem persists contact your local support group	Yes	Yes	Yes	N/A
328	12030	minor	Backup and Restore	Backup and Restore - File could not be transferred by sftp.	Check your login credentials to the SFTP server	Yes	No	No	N/A
329	12031	minor	Backup and Restore	Backup and Restore - File could not be transferred to the shared folder.	Check your login credentials to the shared folder	Yes	No	No	N/A
330	12032	major	Backup and Restore	Backup and Restore - Could not use the USB device.	Check the USB connection and space on the flash device	Yes	Yes	Yes	N/A
331	12033	minor	Backup and Restore	Backup and Restore - Could not detach the USB device.	Check the USB connection and flash device	Yes	No	No	N/A
332	12034	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No	N/A

Table 53 BCM Alarm List

333	12035	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No	N/A
334	12036	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No	N/A
335	12037	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No	N/A
336	12038	minor	Backup and Restore	Backup and Restore - A backup file does not exist.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No	N/A
337	12041	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No	N/A
338	12042	major	Backup and Restore	Backup and Restore - The voicemail service could not be started.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
339	12043	major	Backup and Restore	Backup and Restore - The voicemail service could not be stopped.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
340	12044	major	Backup and Restore	Backup and Restore - The CTI service could not be restarted.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
341	12045	major	Backup and Restore	Backup and Restore - The voicemail clean-up failed.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

342	12046	major	Backup and Restore	Backup and Restore - The IVR service could not be stopped.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
343	12047	major	Backup and Restore	Backup and Restore - The IVR service could not be started.	Attempt another backup or restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
344	12048	major	Backup and Restore	Backup and Restore - The backup archive was not created on a compatible device type.	Attempt another restore from a compatible backup.	Yes	Yes	Yes	N/A
345	12049	major	Backup and Restore	Backup and Restore - Core telephony failed to backup its data.	Attempt another backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
346	12050	major	Backup and Restore	Backup and Restore - Handset administration is prohibited during this operation.	Attempt administration after the backup/restore is complete.	Yes	Yes	Yes	N/A
347	12051	major	Backup and Restore	Backup and Restore - The operation cannot complete because core telephony is restarting.	Attempt another backup/restore when Core Telephony is restarted.	Yes	Yes	Yes	N/A
348	12052	major	Backup and Restore	Backup and Restore - Core telephony failed to restore its data.	Attempt another restore and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
349	12053	major	Backup and Restore	Backup and Restore - The core telephony data is invalid and cannot be restored.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
350	12054	major	Backup and Restore	Backup and Restore - The core telephony data image size is invalid and cannot be restored.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

351	12055	major	Backup and Restore	Backup and Restore - The core telephony data header is invalid and cannot be restored.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
352	12056	major	Backup and Restore	Backup and Restore - Core telephony cannot write to NVRAM. The restore cannot complete.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
353	12057	major	Backup and Restore	Backup and Restore - Core telephony cannot restart the MPE timer. The restore cannot complete.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
354	12058	major	Backup and Restore	Backup and Restore - Core telephony is missing critical data. The restore cannot complete.	Attempt another restore with a valid backup and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
355	12202	Information	Backup and Restore	Backup and Restore - Onbox Backup/Log collection has completed.	No Action Required.	Yes	No	No	N/A
356	12203	Information	Backup and Restore	Backup and Restore - Backup/Log files have been successfully transferred off box.	No Action Required.	Yes	No	No	N/A
357	12204	Information	Backup and Restore	Backup and Restore - Restore has started.	No Action Required.	Yes	No	No	N/A
358	12205	Information	Backup and Restore	Backup and Restore - Restore has completed successfully.	No Action Required.	Yes	No	No	N/A
359	12206	Information	Backup and Restore	Backup and Restore - Restore has rebooted the system to complete its operation.	No Action Required.	Yes	No	No	N/A
360	13002	Information	UPS	UPS - Power failure.	Check local power connected to the system.	Yes	No	No	N/A
361	13003	Information	UPS	UPS - Running on UPS batteries.	Check local power connected to the system.	Yes	No	No	N/A

Table 53 BCM Alarm List

362	13004	warning	UPS	UPS - Battery power exhausted.	Check local power connected to the system.	Yes	No	No	N/A
363	13005	warning	UPS	UPS - Reached run time limit on batteries.	Check local power connected to the system.	Yes	No	No	N/A
364	13006	warning	UPS	UPS - Battery charge below low limit.	Check batteries in UPS and replace if needed.	Yes	No	No	N/A
365	13007	warning	UPS	UPS - Reached remaining time percentage limit on batteries.	No Action Required.	Yes	No	No	N/A
366	13008	warning	UPS	UPS - Failed to kill the power! Attempting a REBOOT!	Check USB connection to UPS.	Yes	No	No	N/A
367	13009	Information	UPS	UPS - Initiating system shutdown!.	System is going down due to power failures. Check local power connected to the system.	Yes	No	No	N/A
368	13010	Information	UPS	UPS - Power is back. UPS running on mains.	No Action Required.	Yes	No	No	N/A
369	13011	Information	UPS	UPS - Users requested to logoff.	No Action Required.	Yes	No	No	N/A
370	13012	major	UPS	UPS - Battery failure. Emergency.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes	N/A
371	13013	major	UPS	UPS - UPS battery must be replaced.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes	N/A
372	13014	Information	UPS	UPS - Remote shutdown requested.	No Action Required.	Yes	No	No	N/A
373	13015	major	UPS	UPS - Communications with UPS lost.	Check USB connection to UPS.	Yes	Yes	Yes	N/A
374	13016	Information	UPS	UPS - Communications with UPS restored.	No Action Required.	Yes	No	No	N/A
375	13017	Information	UPS	UPS - Self Test switch to battery.	No Action Required.	Yes	No	No	N/A
376	13018	Information	UPS	UPS - Self Test completed.	No Action Required.	Yes	No	No	N/A
377	13019	warning	UPS	UPS - Master not responding.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

378	13020	Information	UPS	UPS - Connect from master.	No Action Required.	Yes	No	No	N/A
379	13021	Information	UPS	UPS - Mains returned. No longer on UPS batteries.	No Action Required.	Yes	No	No	N/A
380	16001	Information	Configuration Change	Configuration Change - Configuration Change has occurred.	No Action Required.	No	No	No	N/A
381	17002	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn=Y, login success.	No Action Required.	No	No	No	N/A
382	17003	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn Y logged off.	No Action Required.	No	No	No	N/A
383	17004	Information	System Set Based Admin	System Set Based Admin - UserId=X, user account created/deleted successfully, Dn=Y.	No Action Required.	Yes	No	No	N/A
384	17006	Information	System Set Based Admin	System Set Based Admin - UserId=X, password changed successfully, Dn=Y.	No Action Required.	Yes	No	No	N/A
385	17007	Information	System Set Based Admin	System Set Based Admin - DHCP client enabled for eth1.	No Action Required.	Yes	No	No	N/A
386	17008	Information	System Set Based Admin	System Set Based Admin - DHCP client disabled for eth1.	No Action Required.	Yes	No	No	N/A
387	17009	Information	System Set Based Admin	System Set Based Admin - IP=%s, ip address changed successfully.	No Action Required.	Yes	No	No	N/A
388	17010	Information	System Set Based Admin	System Set Based Admin - MASK=%s, subnet mask changed successfully.	No Action Required.	Yes	No	No	N/A
389	17011	Information	System Set Based Admin	System Set Based Admin - Gateway=X, ip gateway changed successfully.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

390	17012	Information	System Set Based Admin	System Set Based Admin - Keycode validated.	No Action Required.	Yes	No	No	N/A
391	17013	Information	System Set Based Admin	System Set Based Admin - Reboot required.	No Action Required.	Yes	No	No	N/A
392	17015	Information	System Set Based Admin	System Set Based Admin - Modem Enabled/Disabled.	No Action Required.	Yes	No	No	N/A
393	17100	warning	System Set Based Admin	System Set Based Admin - System Set Based Admin general warning alarm.	Problem exists using System Set Based Admin. If problem persists contact your local support group.	Yes	No	No	N/A
394	17111	warning	System Set Based Admin	System Set Based Admin - UserID = X, password changed failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
395	17112	warning	System Set Based Admin	System Set Based Admin - UserID = X, user account creation failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
396	17113	warning	System Set Based Admin	System Set Based Admin - UserID = X, user account deletion failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
397	17120	warning	System Set Based Admin	System Set Based Admin - Key code activation failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
398	17121	warning	System Set Based Admin	System Set Based Admin - Key code set failed.	Log back into System Set based admin to verify keycode. If problem persists contact your local support group.	Yes	No	No	N/A

Table 53 BCM Alarm List

399	17130	warning	System Set Based Admin	System Set Based Admin - Get modem PDR value failed.	Log back into System Set based admin to verify modem settings. If problem persists contact your local support group.	Yes	No	No	N/A
400	17131	warning	System Set Based Admin	System Set Based Admin - Set modem PDR value failed.	Log back into System Set based admin to verify modem settings. If problem persists contact your local support group.	Yes	No	No	N/A
401	17140	warning	System Set Based Admin	System Set Based Admin - LAN ip address change failed, ip = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
402	17141	warning	System Set Based Admin	System Set Based Admin - LAN subnet mask change failed, mask = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
403	17142	warning	System Set Based Admin	System Set Based Admin - LAN Gateway change failed, gateway = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No	N/A
404	17200	critical	System Set Based Admin	System Set Based Admin - System Set Based Admin general critical alarm.	Problem exists using System Set Based Admin. If problem persists contact your local support group.	Yes	Yes	Yes	N/A
405	19002	critical	Startup Profile	Startup Profile - Startup Profile had 1 or more errors when trying to apply.	Check log file on USB device.	Yes	Yes	Yes	N/A
406	19010	Information	Startup Profile	Startup Profile - Startup Profile completed successfully.	No Action Required.	Yes	No	No	N/A
407	19101	warning	Startup Profile	Startup Profile - Startup Profile failed to apply because previous log file exists on USB device.	Delete existing log file on USB to continue.	Yes	No	No	N/A

Table 53 BCM Alarm List

408	30100	major	System Authentication	System Authentication - User Locked out.	Check user account for potential security issues.	Yes	Yes	Yes	N/A
409	30101	information	System Authentication	System Authentication - User Lockout ended.	No Action Required.	Yes	No	No	N/A
410	30200	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=Z.	No Action Required.	No	No	No	N/A
411	30201	information	System Authentication	System Authentication - User logoff User=X Comp=SBA.	No Action Required.	No	No	No	N/A
412	30202	minor	System Authentication	System Authentication - User failed to login User=X Host=Y Comp=Z.	Monitor user activity for lockout condition. If concerned, check "Last successful login" timestamp on View by Accounts panel.	Yes	No	No	N/A
413	30203	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=WWW.	No Action Required.	Yes	No	No	N/A
414	30300	information	System Authentication	System Authentication - Account created.	No Action Required.	Yes	No	No	N/A
415	30301	information	System Authentication	System Authentication - Account updated.	No Action Required.	Yes	No	No	N/A
416	30302	information	System Authentication	System Authentication - Account password changed.	No Action Required.	Yes	No	No	N/A
417	30303	information	System Authentication	System Authentication - Account enabled.	No Action Required.	Yes	No	No	N/A
418	30304	information	System Authentication	System Authentication - Account deleted User=X Comp=Y.	No Action Required.	Yes	No	No	N/A
419	30400	information	System Authentication	System Authentication - Group Created.	No Action Required.	Yes	No	No	N/A
420	30401	information	System Authentication	System Authentication - Group member added.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

421	30402	information	System Authentication	System Authentication - Group member removed.	No Action Required.	Yes	No	No	N/A
422	30403	information	System Authentication	System Authentication - Group Deleted.	No Action Required.	Yes	No	No	N/A
423	30404	information	System Authentication	System Authentication - Group permissions modified.	No Action Required.	Yes	No	No	N/A
424	30601	major	System Authentication	System Authentication - RADIUS Server is not able to be used for authentication.	Check connectivity to RADIUS server and configuration.	Yes	Yes	Yes	N/A
425	30602	Information	System Authentication	System Authentication - RADIUS server in contact.	No Action Required.	Yes	No	No	N/A
426	31006	critical	Keycodes	Keycodes - invalid license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
427	31007	critical	Keycodes	Keycodes - unknown license file status.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
428	31019	warning	Keycodes	Keycodes - failed to find component (<component handle>).	Ensure component is running properly and if problem persists contact your local support group.	Yes	No	No	N/A
429	31045	critical	Keycodes	Keycodes - failed to open file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
430	31052	critical	Keycodes	Keycodes - failed to open license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
431	31055	critical	Keycodes	Keycodes - failed to read system id.	Reboot the system and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
432	31056	critical	Keycodes	Keycodes - cannot find system id tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
433	31057	critical	Keycodes	Keycodes - failed to read sequence number.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
434	31058	critical	Keycodes	Keycodes - cannot find sequence tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

435	31059	critical	Keycodes	Keycodes - failed to read key type.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
436	31062	critical	Keycodes	Keycodes - failed to read key code <keycode size>.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
437	31063	critical	Keycodes	Keycodes - failed to find key code.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	N/A
438	31067	critical	Keycodes	Keycodes - failed to find component for feature.	Ensure component is running properly and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
439	31068	critical	Keycodes	Keycodes - invalid data range for feature (<feature code> <feature data>).	Contact your local support group.	Yes	Yes	Yes	N/A
440	31079	critical	Keycodes	Keycodes - wrong system id.	Check the system ID in your licensing configuration.	Yes	Yes	Yes	N/A
441	31089	critical	Keycodes	Keycodes - wrong sequence number.	Check the sequence number in your licensing configuration.	Yes	Yes	Yes	N/A
442	31130	warning	Keycodes	Keycodes - Keycode could not be activated.	Check requirements for the keycode and if the problem persists contact your local support group.	Yes	No	No	N/A
443	40002	information	Media Services Manager	MSM - DSP initialized.	No Action Required.	Yes	No	No	N/A
444	40003	critical	Media Services Manager	MSM - Unable to communicate with DSP.	Reboot system and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
445	40004	warning	Media Services Manager	MSM - DSP audit failed.	Contact your local support group.	Yes	No	No	N/A
446	40005	critical	Media Services Manager	MSM - DSP reset.	If alarm 40002 proceeds this then no action required otherwise contact your local support group.	Yes	Yes	Yes	N/A
447	41001	major	CTE	CTE - Cte table corruption.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

448	41002	major	CTE	CTE - Unsupported KSU.	Restart system and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
449	41003	major	CTE	CTE - Incorrect state index in the state machine.	Contact your local support group.	Yes	Yes	Yes	N/A
450	41004	warning	CTE	CTE - Error replying to licensing process.	Check your licensing information.	Yes	No	No	N/A
451	41005	minor	CTE	CTE - Error getting feature from list in licensing process.	Check your licensing information.	Yes	No	No	N/A
452	41006	warning	CTE	CTE - Error processing Data Status in licesning process.	Check your licensing information.	Yes	No	No	N/A
453	42200	warning	Call Detail Recording Transfer	CDR Transfer minor error.	Check your configuration parameters.	Yes	No	No	N/A
454	42500	critical	Call Detail Recording Transfer	CDR Transfer initialization error.	Contact your local support group.	Yes	Yes	Yes	N/A
455	42501	critical	Call Detail Recording Transfer	CDR Transfer processing error.	Check your configuration parameters and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
456	42502	critical	Call Detail Recording Transfer	CDR Transfer working error.	Check your configuration parameters and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
457	43002	warning	Voice CTI	Voice CTI no voice channels allocated.	Contact your local support group.	Yes	No	No	N/A
458	43003	critical	Voice CTI	Voice CTI unable to regsigter with MSM.	Contact your local support group.	Yes	Yes	Yes	N/A
459	43004	critical	Voice CTI	Voice CTI subcomponent failure.	Contact your local support group.	Yes	Yes	Yes	N/A
460	43005	critical	Voice CTI	Voice CTI software error.	Contact your local support group.	Yes	Yes	Yes	N/A
461	43006	warning	Voice CTI	Voice CTI application did not register properly.	Contact your local support group.	Yes	No	No	N/A

Table 53 BCM Alarm List

462	43008	information	Voice CTI	Voice CTI - More than 20 percent voice file space available.	No Action Required.	Yes	No	No	N/A
463	43009	warning	Voice CTI	Voice CTI - Less than 20 percent voice file space available.	Check voice mailboxes for excessive messages and if problem persists contact your local support group.	Yes	No	No	N/A
464	43010	critical	Voice CTI	Voice CTI - Less than 5 percent voice file space available.	Check voice mailboxes for excessive messages and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
465	46800	information	IVR Provider	IVR Provider - Node number has been successfully changed to <node number>.	No Action Required.	Yes	No	No	N/A
466	46801	information	IVR Provider	IVR Provider - Prompt <prompt> has been deleted successfully.	No Action Required.	Yes	No	No	N/A
467	46802	information	IVR Provider	IVR Provider - Prompt <prompt> has been loaded successfully.	No Action Required.	Yes	No	No	N/A
468	46803	information	IVR Provider	IVR Provider - Host Access License loaded successfully.	No Action Required.	Yes	No	No	N/A
469	46804	information	IVR Provider	IVR Provider - Configuration file <file> has been successfully transferred to the folder <folder>.	No Action Required.	Yes	No	No	N/A
470	46805	information	IVR Provider	IVR Provider - Configuration file <file> has been successfully transferred from the folder <folder>.	No Action Required.	Yes	No	No	N/A
471	46806	information	IVR Provider	IVR Provider - Ran IVR advanced command <command>.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

472	46807	information	IVR Provider	IVR Provider - Host access license <license> has been deleted successfully.	No Action Required.	Yes	No	No	N/A
473	46850	warning	IVR Provider	IVR Provider - Starting IVR process <process> failed.	Contact your local support group.	Yes	No	No	N/A
474	46851	warning	IVR Provider	IVR Provider - Stopping IVR process <process> failed.	Contact your local support group.	Yes	No	No	N/A
475	46852	warning	IVR Provider	IVR Provider - No IVR node number was set.	Contact your local support group.	Yes	No	No	N/A
476	46853	warning	IVR Provider	IVR Provider - CFS keycode initialization failed, rc=<return code>.	Contact your local support group.	Yes	No	No	N/A
477	46854	warning	IVR Provider	IVR Provider - CFS callback registration failed, rc=<return code>.	Contact your local support group.	Yes	No	No	N/A
478	46855	warning	IVR Provider	IVR Provider - Running IVR advanced command <command> failed.	Contact your local support group.	Yes	No	No	N/A
479	46856	warning	IVR Provider	IVR Provider - Loading prompt <prompt> failed.	Contact your local support group.	Yes	No	No	N/A
480	46857	warning	IVR Provider	IVR Provider - Deleting prompt <prompt> failed.	Contact your local support group.	Yes	No	No	N/A
481	46858	warning	IVR Provider	IVR Provider - Changing node number from <node> to <node> failed.	Contact your local support group.	Yes	No	No	N/A
482	46859	warning	IVR Provider	IVR Provider - Deleting host access license <license> failed.	Contact your local support group.	Yes	No	No	N/A
483	46860	warning	IVR Provider	IVR Provider - Loading configuration file <filename> failed, the file is read-only.	Contact your local support group.	Yes	No	No	N/A

Table 53 BCM Alarm List

484	46861	warning	IVR Provider	IVR Provider - Loading configuration file <filename> failed, the file is invalid.	Contact your local support group.	Yes	No	No	N/A
485	46900	major	IVR Provider	IVR Provider - Reading file failed, file = <file>.	Contact your local support group.	Yes	Yes	Yes	N/A
486	46901	major	IVR Provider	IVR Provider - Opening file failed, file = <file>.	Contact your local support group.	Yes	Yes	Yes	N/A
487	46902	major	IVR Provider	IVR Provider - Copying file failed, src = file, dst = <file>.	Contact your local support group.	Yes	Yes	Yes	N/A
488	46903	major	IVR Provider	IVR Provider - Moving file failed, file = <file>.	Contact your local support group.	Yes	Yes	Yes	N/A
489	46904	major	IVR Provider	IVR Provider - Writing to file failed, file = <file>.	Contact your local support group.	Yes	Yes	Yes	N/A
490	46905	major	IVR Provider	IVR Provider - Memory allocation failed.	Contact your local support group.	Yes	Yes	Yes	N/A
492	50001	critical	Unistim Terminal Proxy Server	The UTPS cannot determine whether or not the BCM is running in SRG mode. Without that information, the UTPS cannot continue: aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
493	50002	critical	Unistim Terminal Proxy Server	The UTPS cannot determine whether or not the BCM is running in SRG mode. Without that information, the UTPS cannot continue: aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
494	50003	critical	Unistim Terminal Proxy Server	UTPS failed to initialize itself because of an internal error. The UTPS is aborting.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

495	50004	critical	Unistim Terminal Proxy Server	UTPS has determined that the SRG keycode has been applied but the SRG process is not running properly. UTPS is aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
496	50005	critical	Unistim Terminal Proxy Server	UTPS has determined that the SRG process is not running but cannot determine whether or not the SRG keycode has been applied - the UTPS cannot continue without that information; aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
497	50006	critical	Unistim Terminal Proxy Server	UTPS failed to establish a link to the SRG process. Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
498	50007	critical	Unistim Terminal Proxy Server	UTPS opened a link with the SRG process but failed to get the SRG keycode information: Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
499	50008	critical	Unistim Terminal Proxy Server	UTPS has lost its link to the SRG process and can no longer continue - terminating.	Contact your local support group.	Yes	Yes	Yes	N/A
500	50009	critical	Unistim Terminal Proxy Server	UTPS waited for SRG process to supply SRG keycode information but no response was received - terminating.	Contact your local support group.	Yes	Yes	Yes	N/A
501	50010	critical	Unistim Terminal Proxy Server	UTPS failed to create socket on UDP port << utpsPort << . Terminating with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

502	50011	critical	Unistim Terminal Proxy Server	UTPS failed to retrieve vital information about the network adaptors present on the BCM. UTPS is aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
503	50012	critical	Unistim Terminal Proxy Server	The published IP address has just been changed - the UTPS will restart and start using the new published IP address.	Contact your local support group.	Yes	Yes	Yes	N/A
504	50013	critical	Unistim Terminal Proxy Server	UTPS failed to obtain the detailed terminal list from the core telephony engine. The detailed error description is: << detailedString.	Contact your local support group.	Yes	Yes	Yes	N/A
505	50014	critical	Unistim Terminal Proxy Server	UTPS failed to retrieve vital information about the UDP socket used to communicate with IP sets. terminating with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
506	50015	critical	Unistim Terminal Proxy Server	The UTPS couldn't find the network adaptor that is bound to the published IP address - aborting.	Contact your local support group.	Yes	Yes	Yes	N/A
507	50050	critical	Unistim Terminal Proxy Server	The UTPS experienced an internal error preventing it from properly handling incoming connection requests from IP sets - aborting.	Contact your local support group.	Yes	Yes	Yes	N/A
508	50060	critical	Unistim Terminal Proxy Server	An exception was caught trying to initialize the EPF layer - aborting.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

509	50061	critical	Unistim Terminal Proxy Server	UTPS failed to initialize the EPF layer. Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
510	50062	critical	Unistim Terminal Proxy Server	An unidentified fatal error occurred inside EPF layer - terminating.	Contact your local support group.	Yes	Yes	Yes	N/A
511	50064	critical	Unistim Terminal Proxy Server	The Media Path Management sub-system unexpectedly became offline - terminating.	Contact your local support group.	Yes	Yes	Yes	N/A
512	50065	critical	Unistim Terminal Proxy Server	UTPS failed to initialize the EPF layer - terminating with MPSMI return code of << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
513	50101	major	Unistim Terminal Proxy Server	UTPS is unable to initialize the NNU security interface. << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
514	50102	major	Unistim Terminal Proxy Server	ERROR: Application::Run returned << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
515	50103	major	Unistim Terminal Proxy Server	Unable to update the feature table in the PDR (error << ret <<).	Contact your local support group.	Yes	Yes	Yes	N/A
516	50104	major	Unistim Terminal Proxy Server	tPerDNConfiguration::ListenerDnChanged could not find entry for DN << oldDn.	Contact your local support group.	Yes	Yes	Yes	N/A
517	50105	major	Unistim Terminal Proxy Server	Attempting to save jitter for the invalid DN of << dn.	Contact your local support group.	Yes	Yes	Yes	N/A
518	50106	major	Unistim Terminal Proxy Server	Attempting to save codec for the invalid DN of << dn.	Contact your local support group.	Yes	Yes	Yes	N/A
519	50108	major	Unistim Terminal Proxy Server	Error << errorCode << writing advertisementlogo \ << logo << \ to PDR.	Contact your local support group.	Yes	Yes	Yes	N/A
520	50109	major	Unistim Terminal Proxy Server	Error << errorCode << changing registration flag in registry.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

521	50110	major	Unistim Terminal Proxy Server	Error << errorCode << changing global password flag in registry.	Contact your local support group.	Yes	Yes	Yes	N/A
522	50111	major	Unistim Terminal Proxy Server	Error << errorCode << attempting to store registration password in registry.	Contact your local support group.	Yes	Yes	Yes	N/A
523	50112	major	Unistim Terminal Proxy Server	Error << errorCode << changing AutoAssignDN flag in registry.	Contact your local support group.	Yes	Yes	Yes	N/A
524	50113	major	Unistim Terminal Proxy Server	Failed to send message; cannot process OAM command.	Contact your local support group.	Yes	Yes	Yes	N/A
525	50114	major	Unistim Terminal Proxy Server	terminalIdentifier << Could not register terminal with UNIStimIOHandler .	Contact your local support group.	Yes	Yes	Yes	N/A
526	50115	major	Unistim Terminal Proxy Server	terminalIdentifier << : No public media address available - EchoServer may be down or misconfigured.	Contact your local support group.	Yes	Yes	Yes	N/A
527	50116	major	Unistim Terminal Proxy Server	failed to insert << element << in m_mapInstantiate dTerminals.	Contact your local support group.	Yes	Yes	Yes	N/A
528	50117	major	Unistim Terminal Proxy Server	Firmware download session rejected. Reason is << rejectionCause.	Contact your local support group.	Yes	Yes	Yes	N/A
529	50118	major	Unistim Terminal Proxy Server	UTPS has failed to authenticate the supplied user ID due to an internal error - error code = << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
530	50119	major	Unistim Terminal Proxy Server	UTPS has failed to authenticate the supplied user ID due to an internal error - error code = << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

531	50120	major	Unistim Terminal Proxy Server	Attempt to Hot Desk << dnToHighjack << from << hijackerDn << has failed [Debug information << sessionId << << errorCode <<].	Contact your local support group.	Yes	Yes	Yes	N/A
532	50121	major	Unistim Terminal Proxy Server	Attempt to Hot Desk << dnToHighjack << from << HighjackerDn << has failed because 'stand-by Hot Desking service' could be started [Debug information << sessionId << << errorCode <<].	Contact your local support group.	Yes	Yes	Yes	N/A
533	50122	major	Unistim Terminal Proxy Server	Hot Desking Session initiated by << highjackerDn << has failed to start with internal error.	Contact your local support group.	Yes	Yes	Yes	N/A
534	50123	major	Unistim Terminal Proxy Server	HotDesking session termination between << Dn1 << and << Dn2 << failed : internal data structure out of synch.	Contact your local support group.	Yes	Yes	Yes	N/A
535	50124	major	Unistim Terminal Proxy Server	HotDesking session termination between << Dn1 << and << Dn1 << failed : cannot find standby Hot Desking session.	Contact your local support group.	Yes	Yes	Yes	N/A
536	50125	major	Unistim Terminal Proxy Server	Lost Connection to SRG.	Contact your local support group.	Yes	Yes	Yes	N/A
537	50192	major	Unistim Terminal Proxy Server	AppFwCriticalSection::init osCreateEvent rc = << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
538	50193	major	Unistim Terminal Proxy Server	AppFwCriticalSection::init osCreateEvent rc = << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

539	50194	major	Unistim Terminal Proxy Server	AppFwCriticalSection::MessageToSelf osReceiveError << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
540	50195	major	Unistim Terminal Proxy Server	AppFwCriticalSection::Acquire osReceiveError << errorCode.	Contact your local support group.	Yes	Yes	Yes	N/A
541	50196	major	Unistim Terminal Proxy Server	In Application::InitializationComplete but NnuServiceInitialized returned << errorCode << APPLICATION WILL BE SHUT DOWN.	Contact your local support group.	Yes	Yes	Yes	N/A
542	50197	major	Unistim Terminal Proxy Server	Application::Run caught unspecified exception: FORCING EMERGENCY SHUTDOWN.	Contact your local support group.	Yes	Yes	Yes	N/A
543	50198	major	Unistim Terminal Proxy Server	Application::Run caught exception: << exceptionType << FORCING EMERGENCY SHUTDOWN.	Contact your local support group.	Yes	Yes	Yes	N/A
544	50300	information	Unistim Terminal Proxy Server	** Running the DEBUG version of UTPS, version << UtpsVersion.	No Action Required.	Yes	No	No	N/A
545	50301	information	Unistim Terminal Proxy Server	** Running the RELEASE version of UTPS, version << UtpsVersion.	No Action Required.	No	No	No	N/A
546	50302	information	Unistim Terminal Proxy Server	BCM running in SRG/BCM mode.	No Action Required.	Yes	No	No	N/A
547	50303	information	Unistim Terminal Proxy Server	Terminal << dn << is being deregistered from OAM.	No Action Required.	Yes	No	No	N/A
548	50304	information	Unistim Terminal Proxy Server	The IP Terminal at << IpAddress << is NOT configured to connect to the BCM's published IP address - please correct the IP Terminal's configuration.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

549	50305	information	Unistim Terminal Proxy Server	System running in SRG mode.	No Action Required.	Yes	No	No	N/A
550	50306	information	Unistim Terminal Proxy Server	System NOT running in SRG mode.	No Action Required.	No	No	No	N/A
551	50307	information	Unistim Terminal Proxy Server	SRG Connection Re-established.	No Action Required.	Yes	No	No	N/A
552	50308	information	Unistim Terminal Proxy Server	Terminal << dn << : firmware version being upgraded from << oldFirmwareVersion << to << newFirmwareVersion.	No Action Required.	Yes	No	No	N/A
553	50501	information	Unistim Terminal Proxy Server	Packet Loss Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
554	50502	warning	Unistim Terminal Proxy Server	Packet Loss Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A

Table 53 BCM Alarm List

555	50503	minor	Unistim Terminal Proxy Server	Packet Loss Violation Unacceptable <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>,eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
556	50504	information	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>,eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
557	50505	warning	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>,eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
558	50506	minor	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Unacceptable: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>,eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A

Table 53 BCM Alarm List

559	50507	information	Unistim Terminal Proxy Server	Round Trip Delay Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
560	50508	warning	Unistim Terminal Proxy Server	Round Trip Delay Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
561	50509	minor	Unistim Terminal Proxy Server	Round Trip Delay Violation Unacceptable: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
562	50510	information	Unistim Terminal Proxy Server	Listening R Factor Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A

Table 53 BCM Alarm List

563	50511	warning	Unistim Terminal Proxy Server	Listening R Factor Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>,eSD <>,aNL <>,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No	N/A
564	51010	warning	VoIP Gateway	VoIP Gateway configuration parameters not found.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	No	No	N/A
565	51014	information	VoIP Gateway	VoIP Gateway succeeded to ping gatekeeper address.	No Action Required.	Yes	No	No	N/A
566	51015	warning	VoIP Gateway	VoIP Gateway failed to ping gatekeeper address.	Check that the gatekeeper is configured correctly, and is accessible. The system will keep trying to make contact with the gatekeeper at 3 minute intervals.	Yes	No	No	N/A
567	51016	warning	VoIP Gateway	VoIP Gateway remote gateway mismatch.	Verify the remote gateway is supported for interoperability.	Yes	No	No	N/A
568	51020	critical	VoIP Gateway	VoIP Gateway failed to initialize h.323 stack.	Contact your local support group.	Yes	Yes	Yes	N/A
569	51024	major	VoIP Gateway	VoIP Gateway can't communicate with QoS monitor.	Check the status of the QoS monitor in Element Manager.	Yes	Yes	Yes	N/A
570	51100	major	VoIP Gateway	VoIP Gateway rejected call setup attempt from DN <DN> to DN <DN>: <reason>.	Ensure the codecs are setup properly in the system. If problem persists use BCM monitor to trace an unsuccessful call and contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

571	51101	major	VoIP Gateway	VoIP Gateway dropped connected call from DN <DN> to DN <DN>: <reason>.	The call has dropped, possibly due to incompatible codecs, network errors, or protocol problems. If problem persists contact your local support group.	Yes	Yes	Yes	N/A
572	51102	information	VoIP Gateway	All 2 keycoded trunks in-use on the <interface name> interface.	This happens when all VoIP trunk ports are busy. If this continues more VoIP Trunk licenses should be added.	Yes	No	No	N/A
573	51103	warning	VoIP Gateway	Call rejected, due to all 2 keycoded trunks being in-use on the <interface name> interface.	This happens if a call is not accepted because all VoIP trunk ports are busy. If this continues more VoIP Trunk licenses should be added.	Yes	No	No	N/A
574	51901	critical	VoIP Gateway	VoIP Gateway serious system error.	Contact your local support group.	Yes	Yes	Yes	N/A
576	51903	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes	N/A
577	51904	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes	N/A
578	52000	critical	Media Path Server	MPS unable to allocate memory. MPS service aborted.	Reboot system and if problem persists contact your local support group.	Yes	Yes	Yes	N/A
579	52001	critical	Media Path Server	MPS unable to initialize MPSMI. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	N/A
580	52002	critical	Media Path Server	MPS unable to connect to MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	N/A
581	52003	critical	Media Path Server	MPS unable to open FUMP channels. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	N/A
582	52004	critical	Media Path Server	MPS FUMP channel not ready. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

583	52005	critical	Media Path Server	MPS reset by network manager.	Contact your local support group.	Yes	Yes	Yes	N/A
584	52006	critical	Media Path Server	MPS received connection lost from MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	N/A
585	52007	critical	Media Path Server	MPS unable to create event. MPS service failed to start.	Contact your local support group.	Yes	Yes	Yes	N/A
586	52008	critical	Media Path Server	MPS unable to initialize NNU messaging framework.	Contact your local support group.	Yes	Yes	Yes	N/A
587	52009	critical	Media Path Server	MPS unable to initialize message loop thread.	Contact your local support group.	Yes	Yes	Yes	N/A
588	52013	warning	Media Path Server	MPS codec incompatible, call dropped.	Contact your local support group.	Yes	No	No	N/A
589	52014	warning	Media Path Server	MPS endpoint registration failed.	Contact your local support group.	Yes	No	No	N/A
590	53000	critical	Media Gateway Server	MGS Exception software error.	Contact your local support group.	Yes	Yes	Yes	N/A
591	53001	critical	Media Gateway Server	MGS shutting down due to gateway creation failure.	Contact your local support group.	Yes	Yes	Yes	N/A
592	53002	critical	Media Gateway Server	MGS shutting down due to gateway initialization error.	Contact your local support group.	Yes	Yes	Yes	N/A
593	53003	critical	Media Gateway Server	MGS shutting down due to a fatal error.	Contact your local support group.	Yes	Yes	Yes	N/A
594	53004	critical	Media Gateway Server	MGS shutting down due to MSM communication failure.	Contact your local support group.	Yes	Yes	Yes	N/A
595	53005	critical	Media Gateway Server	MGS shutting down due to MPS communication failure.	Contact your local support group.	Yes	Yes	Yes	N/A
596	53006	critical	Media Gateway Server	MGS shutting down due to resource limits query failure.	Contact your local support group.	Yes	Yes	Yes	N/A
597	53007	critical	Media Gateway Server	MGS shutting down due to configuration query failure.	Contact your local support group.	Yes	Yes	Yes	N/A

Table 53 BCM Alarm List

598	53008	critical	Media Gateway Server	MGS MediaTransport Received bad ports: <port1> <port2>.	Contact your local support group.	Yes	Yes	Yes	N/A
599	53009	critical	Media Gateway Server	MGS MediaTransport Codec and/or frames per packet mismatch <details>.	Contact your local support group.	Yes	Yes	Yes	N/A
600	53010	critical	Media Gateway Server	MGS MediaTransport: Transport mismatch <details>.	Contact your local support group.	Yes	Yes	Yes	N/A
601	53011	critical	Media Gateway Server	MGS MsmProxy:: <interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes	N/A
602	53012	critical	Media Gateway Server	MGS <entity>:: <interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes	N/A
603	53018	critical	Media Gateway Server	MGS ResourceMediaController::(<OID=<oid> >) DSP Task Lost.	Contact your local support group.	Yes	Yes	Yes	N/A
604	53019	information	Media Gateway Server	MGS Shutting down due to IP address change.	No Action Required as service manager will restart.	Yes	No	No	N/A
605	56003	major	IP Telephony Provider	IP Telphony Provider fatal error was detected.	Contact your local support group.	Yes	Yes	Yes	N/A
606	56004	minor	IP Telephony Provider	IP Telphony Provider error was detected.	Contact your local support group.	Yes	No	No	N/A
607	56005	major	IP Telephony Provider	IP Telphony Provider software exception.	Contact your local support group.	Yes	Yes	Yes	N/A
608	56006	minor	IP Telephony Provider	IP Telphony Provider shutting down due to fatal error.	Contact your local support group.	Yes	No	No	N/A
609	57002	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Test Local Mode.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

610	57003	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware is out of sync with Main Office Call Server.	Check your firmware on the system to ensure it's the same revision as the main office.	Yes	No	No	N/A
611	57004	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Set Firmware Upgrade in Progress.	No Action Required.	Yes	No	No	N/A
612	57005	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Normal Mode – Set Redirected to Main Office.	No Action Required.	Yes	No	No	N/A
613	57006	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Redirection Pending (Set on call).	No Action Required.	Yes	No	No	N/A
614	57007	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware Upgrade Pending (Set on call).	No Action Required.	Yes	No	No	N/A
615	57008	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Main Office Parameters Not Provisioned.	Check your local configuration in the system.	Yes	No	No	N/A
616	57250	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (1) – No endpoint in Gatekeeper database.	Check your configuration in the main office.	Yes	No	No	N/A
617	57251	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (2) – ID unknown within the Call Server.	Check your configuration in the main office.	Yes	No	No	N/A

Table 53 BCM Alarm List

618	57252	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (3) – Endpoint in Gatekeeper database is Originating Call Server.	Check your configuration in the main office.	Yes	No	No	N/A
619	57253	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Net Connect Server Unreachable.	Check your local configuration, network connectivity and ensure the main office is on line.	Yes	Yes	Yes	N/A
620	57500	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Main Office TPS Unreachable.	Check your local configuration, network connectivity and ensure the main office is on line.	Yes	Yes	Yes	N/A
621	57501	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware is not available on the SRG.	Check your firmware on the system to ensure it's the same revision as the main office.	Yes	Yes	Yes	N/A
622	57750	critical	Survivable Remote Gateway	Survivable Remote Gateway - SRG terminated unexpectedly.	Contact your local support group.	Yes	Yes	Yes	N/A
623	60005	critical	LAN Driver	LAN Driver - Duplicate IP address detected on startup of LAN interface.	Check in diagnostics logs for messages log for further information. Also Check your network to ensure no other devices are using the same IP address as the system.	Yes	Yes	Yes	N/A
624	64001	information	Net Link Manager	Net Link Manager Service is Started.	No Action Required.	No	No	No	N/A
625	64002	information	Net Link Manager	Net Link Manager Service is Stopped.	Go to Configuration->Resources->NW Interfaces->Global Settings Tab and start Netlink Manager Service.	No	No	No	N/A
626	64003	warning	Net Link Manager	Net Link Manager, Backup Started.	Check the primary link connectivity and configuration.	Yes	No	No	N/A
627	64004	warning	Net Link Manager	Net Link Manager, Fast Backup.	Check the primary link connectivity and configuration.	Yes	No	No	N/A

Table 53 BCM Alarm List

628	64005	information	Net Link Manager	Net Link Manager, recovering back to permanent.	No Action Required.	Yes	No	No	N/A
629	65000	information	Voice Enabled WAN Stack	No WANIC500/520 Cards found.	Check if WAN Card is installed.	Yes	No	No	N/A
630	65001	critical	Voice Enabled WAN Stack	Failed to initialize linkprotocol for wan1.	(1) Check the connectivity. (2) Check protocol configuration. (3) Check remote end configuration/state.	Yes	Yes	Yes	N/A
631	65002	critical	Voice Enabled WAN Stack	Failed to initialize linkprotocol for wan2.	(1) Check the connectivity. (2) Check protocol configuration. (3) Check remote end configuration/state.	Yes	Yes	Yes	N/A
632	65003	information	Voice Enabled WAN Stack	wan1 link up.	No Action Required.	Yes	No	No	N/A
633	65004	major	Voice Enabled WAN Stack	wan1 link down.	(1) Check the connectivity. (2) Check protocol configuration. (3) Check remote end configuration/state.	Yes	Yes	Yes	N/A
634	65005	information	Voice Enabled WAN Stack	wan2 link up.	No Action Required.	Yes	No	No	N/A
635	65006	major	Voice Enabled WAN Stack	wan2 link down.	(1) Check the connectivity. (2) Check protocol configuration. (3) Check remote end configuration/state.	Yes	Yes	Yes	N/A
636	66001	information	Routing Stack	Unknown message received from kernel.	No Action Required.	Yes	No	No	N/A
637	66002	warning	Routing Stack	OSPF TE: cannot update TE LSA for interface.	Check OSPF Configuration.	Yes	No	No	N/A
638	66003	warning	Routing Stack	Opaque originate failed for router-TLV.	No Action Required.	Yes	No	No	N/A
639	66004	warning	Routing Stack	Cannot find area in the configured list to delete.	Check OSPF configuration for the area.	Yes	No	No	N/A
640	66005	information	Routing Stack	OSPF : Delete link-TLV instance not found.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

641	66006	information	Routing Stack	OSPF: Delete router-TLV area not found.	No Action Required.	Yes	No	No	N/A
642	68000	warning	DNS	Domain Name Service - Started.	No Action Required.	No	No	No	N/A
643	68001	warning	DNS	Domain Name Service - Stopped.	No Action Required.	Yes	No	No	N/A
644	69000	warning	WebCache	Apache Cache Mode Enabled.	No Action Required.	Yes	No	No	N/A
645	69001	warning	WebCache	Apache Cache Mode Disabled.	No Action Required.	Yes	No	No	N/A
646	70001	information	Modem	Incoming dialup connection is successfully established with UserName X.	No Action Required.	Yes	No	No	N/A
647	70002	warning	Modem	Authentication failure for incoming modem connection.	Check Users Dial-In Credentials.	Yes	No	No	N/A
648	70003	warning	Modem	Authentication Protocol Mis-match for Modem Connection.	Check if both the ends of a connection have at least one Authentication Protocol in common.	Yes	No	No	N/A
649	70005	warning	Modem	Peer refused to authenticate.	Check configuration for authentication on both ends.	Yes	No	No	N/A
650	70006	warning	Modem	Peer rejected username/ password for the dialout connection on interface X.	Check username, password.	Yes	No	No	N/A
651	70007	minor	Modem	Outgoing connection could not be made due to modem error.	Check configuration, physical connectivity and state of the dialout line. Try to reconnect after some time (about 60 secs).	Yes	No	No	N/A
652	70008	minor	Modem	Link protocol negotiation failed.	Check the PPP configuration on both the sides.	Yes	No	No	N/A
653	70009	warning	Modem	The peer system failed (or refused) to authenticate itself. Aborting the callback.	Check callback credentials for the dialin user.	Yes	No	No	N/A

Table 53 BCM Alarm List

654	70010	information	Modem	Callback User X. Performing Callback.	No Action Required.	Yes	No	No	N/A
655	70013	information	Modem	Modem Card Detection.	No Action Required.	Yes	No	No	N/A
656	70014	information	Modem	Server assigned the local ip address by overriding the configured ip address.	No Action Required.	Yes	No	No	N/A
657	71001	information	ISDN	Incoming dialup connection is successfully established with UserName X.	No Action Required.	Yes	No	No	N/A
658	71002	warning	ISDN	Authentication failure for incoming ISDN connection.	Check Users Dial-in credentials.	Yes	No	No	N/A
659	71003	warning	ISDN	Authentication protocol mis-match for ISDN connection.	Check if both the ends of the connection have atleast one Authentication protocol in common.	Yes	No	No	N/A
660	71004	warning	ISDN	Peer refused to authenticate.	Check configuration for authentication on both ends.	Yes	No	No	N/A
661	71005	warning	ISDN	Peer rejected username/ password for the dialout connection on interface X.	Check username, password.	Yes	No	No	N/A
662	71008	information	ISDN	Callback User X. Performing Callback.	No Action Required.	Yes	No	No	N/A
663	71009	information	ISDN	Some ISDN channels of the dialout interface are busy.	No Action Required.	Yes	No	No	N/A
664	71010	information	ISDN	Server assigned the local ip address by overriding the configured ip address.	No Action Required.	Yes	No	No	N/A
665	72000	information	IPSec	IPSecProviderAgent Service started. Mgmt IP: <ipaddress>.	No Action Required.	No	No	No	N/A

Table 53 BCM Alarm List

666	72001	information	IPSec	IPSecProviderAgent Service stopped.	No Action Required.	No	No	No	N/A
667	72002	information	IPSec	IPSec SA Established on <local IP> with <remote IP>: <encryption> outbound SPI: <hex> inbound SPI: <hex>.	No Action Required.	Yes	No	No	N/A
668	72003	information	IPSec	ISAKMP SA Established on <local IP> with <remote IP>.	No Action Required.	Yes	No	No	N/A
669	72004	information	IPSec	Deleting ISAKMP SA from <local IP> to <remote IP>.	No Action Required.	Yes	No	No	N/A
670	72005	minor	IPSec	Could not initiate Quick Mode from <local IP> to <remote IP>.	Ensure local and remote configurations are correct.	Yes	No	No	N/A
671	72006	minor	IPSec	PFS required on <local IP> but not provided by <remote IP>.	Ensure PFS is configured on the remote endpoint.	Yes	No	No	N/A
672	72007	information	IPSec	Received Delete ISAKMP SA message on <local IP> from <remote IP>.	No Action Required.	Yes	No	No	N/A
673	72008	information	IPSec	Received Delete IPSec SA message on <local IP> from <remote IP>.	No Action Required.	Yes	No	No	N/A
674	72009	information	IPSec	Oakley <mode> Mode proposal accepted on <local IP> from <remote IP>.	No Action Required.	Yes	No	No	N/A
675	72010	minor	IPSec	IPSec connection request Rejected on <local IP>. Maximum number of IPSec Tunnels reached.	Disconnect non needed tunnels or wait until one disconnects.	Yes	No	No	N/A
676	72011	information	IPSec	Deleting IPSec SA on <local IP> with <remote IP>: <encryption> outbound SPI: <hex> inbound SPI: <hex>.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

677	72012	warning	IPSec	VPN Client: Account Disabled. IPSec Connection Request Rejected on <local IP> from <remote IP>.	Check configuration as VPN Client is disabled in Element Manager.	Yes	No	No	N/A
678	72013	warning	IPSec	VPN Client: Account already in use. IPSec Connection Request Rejected on <local IP> from <remote IP>.	Check where account is being used and have them disconnect or use a different account to connect.	Yes	No	No	N/A
679	72014	warning	IPSec	VPN Client: Account not found. IPSec Connection Request Rejected on <local IP> from <remote IP>.	Check configuration for VPN client accounts.	Yes	No	No	N/A
680	72015	information	IPSec	Changed Management IP Address to <ipaddress>.	No Action Required.	Yes	No	No	N/A
681	72016	information	IPSec	BCM has no IP Address on the IPSec Client private network: IP Address: <IP Address> IP Mask: <Subnet Mask>.	No Action Required.	Yes	No	No	N/A
682	72017	information	IPSec	The IP Address of the PC running the IPSec client <IP Address> is on the private network <Network>.	No Action Required.	Yes	No	No	N/A
683	72018	information	IPSec	BCM interface that IPSec client is trying to connect to <IP Address> is on the private network <Network>.	No Action Required.	Yes	No	No	N/A
684	72019	information	IPSec	Starting Password/ QOTD Server on IP Address: <IP Address>.	No Action Required.	No	No	No	N/A
685	72020	information	IPSec	Idle Timeout detected on IPSec SA between: local:<Local endpoint IP address>, remote:<remote endpoint IP Address>.	No Action Required.	Yes	No	No	N/A

Table 53 BCM Alarm List

686	73001	warning	PPPoE	Peer refused to authenticate.	Check for configuration of Authentication on both ends.	Yes	No	No	N/A
687	73002	warning	PPPoE	Peer rejected username/ password for the dialout connection on interface X.	Check username, password.	Yes	No	No	N/A
688	73003	minor	PPPoE	Link protocol negotiation failed.	Check the PPP configuration on both the sides.	Yes	No	No	N/A
689	73004	information	PPPoE	Server assigned the local ip address by overriding the configured ip address.	No Action Required.	Yes	No	No	N/A
690	74000	warning	NAT and IP Policy Filters	NAT and IP Policy Filters - Interface <interface> has been in 'init' state for too long.	Verify the interface is up and can send and receive traffic. Try disabling and enabling the interface.	Yes	No	No	N/A
691	74001	warning	NAT and IP Policy Filters	NAT and IP Policy Filters - Default outbound link speed used for interface <interface>.	The outbound link speed for the interface must be configured.	Yes	No	No	N/A
692	74002	major	NAT and IP Policy Filters	NAT and IP Policy Filters - Cannot create DSC interface <interface>.	Verify system memory.	Yes	Yes	Yes	N/A
693	74003	warning	NAT and IP Policy Filters	NAT and IP Policy Filters - Active interfaces count mismatch with DSC Kernel Loadable Module: <data> versus <data>.	Understand if either a DSC Provider Agent or DSC Kernel Loadable Module patch has been applied. If this is the case, then the user need not take action. Otherwise, send logs and alarm data to support.	Yes	No	No	N/A

Table 53 BCM Alarm List

694	74004	major	NAT and IP Policy Filters	NAT and IP Policy Filters - DSC Kernel Loadable Module is not responding.	Understand if either a DSC Provider Agent or DSC Kernel Loadable Module patch has been applied. If this is the case, then the user need not take action. Otherwise, send logs and alarm data to support.	Yes	Yes	Yes	N/A
695	74005	major	NAT and IP Policy Filters	NAT and IP Policy Filters - Error reading rule data in PDR for <data>. The <data> <data> rule has been removed.	Either manually recreate the rule, or restore a backed up version of the data. If the problem persists contact your local support group.	Yes	Yes	Yes	N/A
696	74100	major	NAT and IP Policy Filters	NAT and IP Policy Filters - DSCMERR: DSC Module Error Code: <code>, Data: <data>.	Contact your local support group.	Yes	Yes	Yes	N/A
697	74101	warning	NAT and IP Policy Filters	NAT and IP Policy Filters - DSCMALA(74101) : <data>: H225 setup message exceeds TCP segment buffer. Data: <data>.	The number of codec choices needs to be reduced. This will reduce the size of the setup message	Yes	No	No	N/A
698	74102	information	NAT and IP Policy Filters	NAT and IP Policy Filters - DSCMALA(74102) : <data>: H225 TCP segment collection timeout. Data: <data>.	No Action Required.	Yes	No	No	N/A
699	74103	warning	NAT and IP Policy Filters	NAT and IP Policy Filters - DSCMALA(74103) : The maximum number of stateful IP Policy Filter sessions has been exceeded.	No Action Required.	Yes	No	No	N/A

Chapter 8

Using the BCM Service Management System

You can use the BCM Element Manager to view and administer the services that run on the BCM system.

This chapter provides:

- an overview the BCM service management system
- a list of BCM services
- information about how to start, stop, and restart BCM services

Overview of the BCM service management system

You can view details about the services that run on the BCM system, including:

- the name of a service
- whether a service is enabled to automatically start up
- the status of the service running on the BCM

You can also administer services by starting, stopping, and restarting certain services.



Caution: Use the BCM Services Manager only as directed by Nortel Technical Support. Improper use of the BCM Services Manager may adversely affect system operation.

You can keep a record of BCM services using the programming record. For more information, see [“Saving programming records” on page 57](#).

BCM services

Table 54 lists BCM services.

Table 54 BCM Services

Service Name	Description
BackupRestoreProviderAgent	Cimom Provider
BCM_DCMPProviderAgent	Cimom Provider
BCM_DNSProvider Agenet	Cimom Provider
BCM_Doorphone	Doorphone Service
BCM_DoorphoneProviderAgent	Cimom Provider
BCM_HostProviderAgent	Cimom Provider

Table 54 BCM Services

Service Name	Description
BCM_IPMusicProviderAgent	Cimom Provider
BCM_ISDNProviderAgent	Cimom Provider
BCM_LicenseProviderAgent	Cimom Provider
BCM_LogProviderAgent	Cimom Provider
BCM_MIB2ProviderAgent	Cimom Provider
BCM_ModemDialUpProviderAgent	Cimom Provider
BCM_NetLinkMgrProviderAgent	Cimom Provider
BCM_NetworkInterfacesProviderAgent	Cimom Provider
BCM_NetworkStatisticsProviderAgent	Cimom Provider
BCM_PPPOEProviderAgent	Cimom Provider
BCM_RoutingProviderAgenet	Cimom Provider
BCM_SecurityProviderAgent	Cimom Provider
BCM_SNMPPProviderAgent	Cimom Provider
BCM_SSMPProviderAgent	Cimom Provider
BCM_TimeServiceProviderAgent	Cimom Provider
BCM_TimeZoneSettingProviderAgent	Cimom Provider
BCM_WANProviderAgent	Cimom Provider
BCM_WebCacheProviderAgent	Cimom Provider
BcmAmp	IP Music Player
BCMCoreUploadProviderAgent	Cimom Provider
BCMPerfMonProviderAgent	Cimom Provider
BCMSystemProviderAgent	Cimom Provider
BCMUPSPProviderAgent	Cimom Provider
BCMWebProviderAgent	Cimom Provider
btraceserver	Plug-in for Authentication and Routing Management for BT
CallPilotProviderAgent	Cimom Provider
CCRSAppServer.exe	Reporting for Call Centre Service
CDRProviderAgent	Cimom Provider
CDRService	Call Detail Recording Service
cfserver	Component Feature Service
core_file_monitor	
coreauthservice	
CoreTelProviderAgent	Cimom Provider
cron	Cron Scheduler
Cte	Computer Telephony Engine
ctiserver	Computer Telephony Integration

Table 54 BCM Services

Service Name	Description
dhcpcd	DHCP Provider Daemon
DHCPProviderAgent	Cimom Provider
DiaLogger	System Logging Mechanism
feps	Functional Endpoint Proxy Server (VoIP Gateway)
HGMetrics Reporter	Hunt Group Metrics
HotDesking	Used with IP Sets
httpd	HTTP Daemon
InventoryProviderAgent	Cimom Provider
IPSecProviderAgent	Cimom Provider
IpTelProviderAgent	Cimom Provider
LanCteProviderAgent	Cimom Provider
LANProviderAgent	Cimom Provider
lms	Line Monitor Server
LogManagement	Log Management Server
mgs	Media Gateway Server
mps	IP Telephony—Media Path
Msm	Media Services Manager
MsmProviderAgent	Cimom Provider
NnuScheduler	System Scheduler
owcimomd	Open Wbem Cimom Server Daemon
Pdrd	Persistence Data Repository Service
postgresql	Database used for Reporting for Contact Center
qmond	QoS Monitor
RAIDProviderAgent	Cimom Provider
securityservice	Authentication and Authorization
SoftwareUpdateProviderAgent	Cimom Provider
ssba	System Set Based Admin Service (Feature 9*8)
sshd	Secure Shell Daemon
ssmd	
SyslogListener	Syslog Receiver
tmwservice	Time Service
ToneSrvr	IP Music Service
UftpServer	
utps	UniSTIM Terminal Proxy Server (IP Sets)
voicemail	Voicemail Process
WAN	

To view details about services

- 1 Start the BCM Element Manager.
- 2 In the **Element** pane, select an element.
- 3 Click the **Connect** button.
The **Task** pane is displayed.
- 4 Click the **Administration** tab.
- 5 Open the **General** folder, and then click the **Service Manager** task.
The **Service Manager** page opens. Services are displayed in the Services table.

Starting, stopping, and restarting services

You can stop any of the services that are running on the BCM system.



Caution: Use the BCM Services Manager only as directed by Nortel Technical Support. Improper use of the BCM Services Manager may adversely affect system operation.

To stop a service

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Service Manager** task.
The **Service Manager** page opens. Services are displayed in the Services table.
- 3 In the Services table, select a service.
- 4 Click the **Stop** button.
A confirmation dialog box opens.
- 5 Click **Yes**.
In the Services table, **Stopped** is displayed in the **Status** column for the stopped service.

To restart a service

- 1 Click the **Administration** tab.
- 2 Open the **General** folder, and then click the **Service Manager** task.
The **Service Manager** page opens. Services are displayed in the Services table.
- 3 In the Services table, select a stopped service.
- 4 Click the **Restart** button.
A confirmation dialog box opens.
- 5 Click **Yes**.
In the Services table, **Running** is displayed in the **Status** column for the restarted service.

Chapter 9

Monitoring BCM Status and Metrics

You can use the Element Manager to view detailed information about the performance of the BCM and about the performance of system resources.

This chapter provides information about the following:

- system status
- telephony metrics

About the system status

Using the Element Manager, you can monitor overall system performance and other performance-related information.

You monitor system status using the following tools:

- LED Status
- QoS Monitor
- UPS Status
- NTP Metrics
- Interface Metrics
- Disk Mirroring
- QoS Metrics

LED Status

The System Status Monitor displays the status of the following LEDs:

- power
- hard disk
- status
- MSC
- WAN
- modem
- NICs
- Temp
- Fan

Click the Refresh button to update the display.

Figure 29 Monitoring the LED status

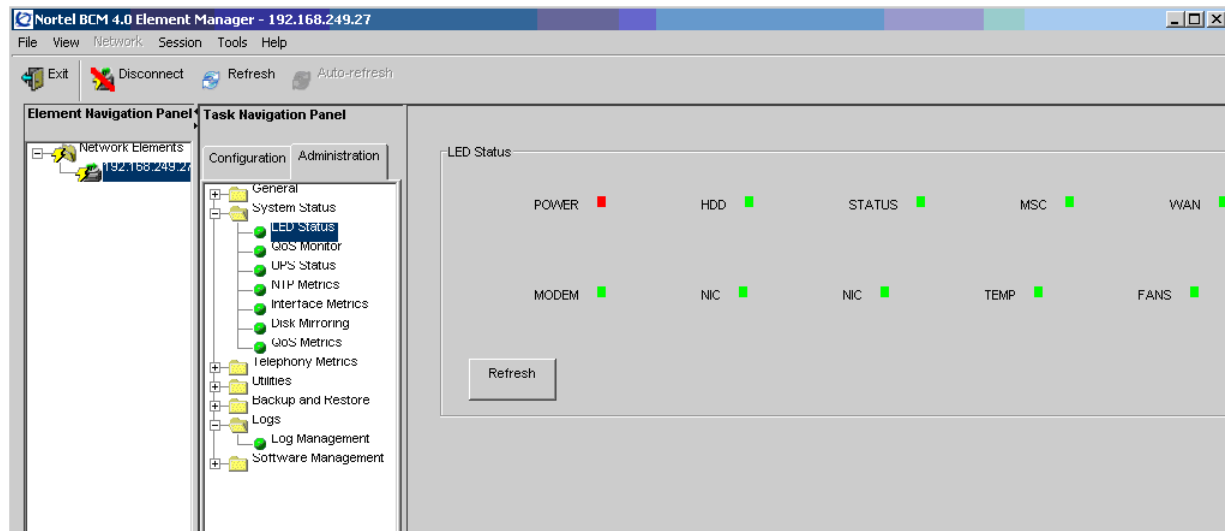


Table 55 summarizes the possible operating states of the LEDs.

Table 55 Base function tray system status LED states

LED	Description	LED states
Power	Indicates the status of all power components. The Power LED is used with the Status LED to show startup conditions. An LED that monitors a component will also show a fault in combination with the Power LED.	Green ON – normal operation Red ON – an excessive voltage deficiency or a component failure (such as a redundant power supply module) Red ON – a critical alarm has occurred
HDD	Indicates access to the system hard disk.	Green ON – hard disk activity detected This LED lights when the HDD is accessed. If the systems does not need to read or write to the HDD the LED is off.
Status	Indicates the system status. Six non-blinking LEDs in the center indicate monitoring software is not active.	Green ON – all monitored services are functioning Green FLASH – failure in one or more telephony services Green OFF – not all services are working
MSC	PCI Device/MSC	Green ON – device is present and operating properly Green FLASH – driver is not running Green OFF – device is defective or not present

Table 55 Base function tray system status LED states

LED	Description	LED states
WAN	PCI Device/WAN1 + WAN2	Green ON – device is present and operating properly Green FLASH – driver is not running Green OFF – device is defective or not present
Modem	PCI Device/Modem	Green ON – device is present and operating properly Green FLASH – driver is not running Green OFF – device is defective or not present
LAN 1	PCI Device/LAN 1	Green ON – device is present and operating properly Green FLASH – driver is not running Green OFF – device is defective or not present
LAN 2	PCI Device/LAN 2	Green ON – device is present and operating properly Green FLASH – driver is not running Green OFF – device is defective or not present
Temp	Monitors the main unit and CPU temperature.	Green ON – normal Red ON – sensor is non-operational or temperature is out of range. Note: Red LED indicates a possible fan failure.
Fan	Monitors the status of the fans.	Green ON – all installed fans are working Red ON – sensor failure or there is a problem with at least one fan

QoS Monitor

QoS Monitor monitors the quality of service (QoS) of IP trunk services. The tool periodically monitors the delay and packet-loss of IP networks between two peer gateways. The main objective of the QoS Monitor is to allow new IP telephony calls to fall back to the PSTN if the voice quality of the IP network falls below the specified transmit threshold.

For information about setting the transmit threshold, see the *BCM 4.0 Networking Configuration Guide* (N0060606). You can set the threshold in the Element Manager in the Telephony Resources panel.

Configuring the QoS Monitor

You configure the QoS Monitor using the QoS Monitor panel on the Administration tab. You can configure the following:

- the monitoring mode
- logging parameters

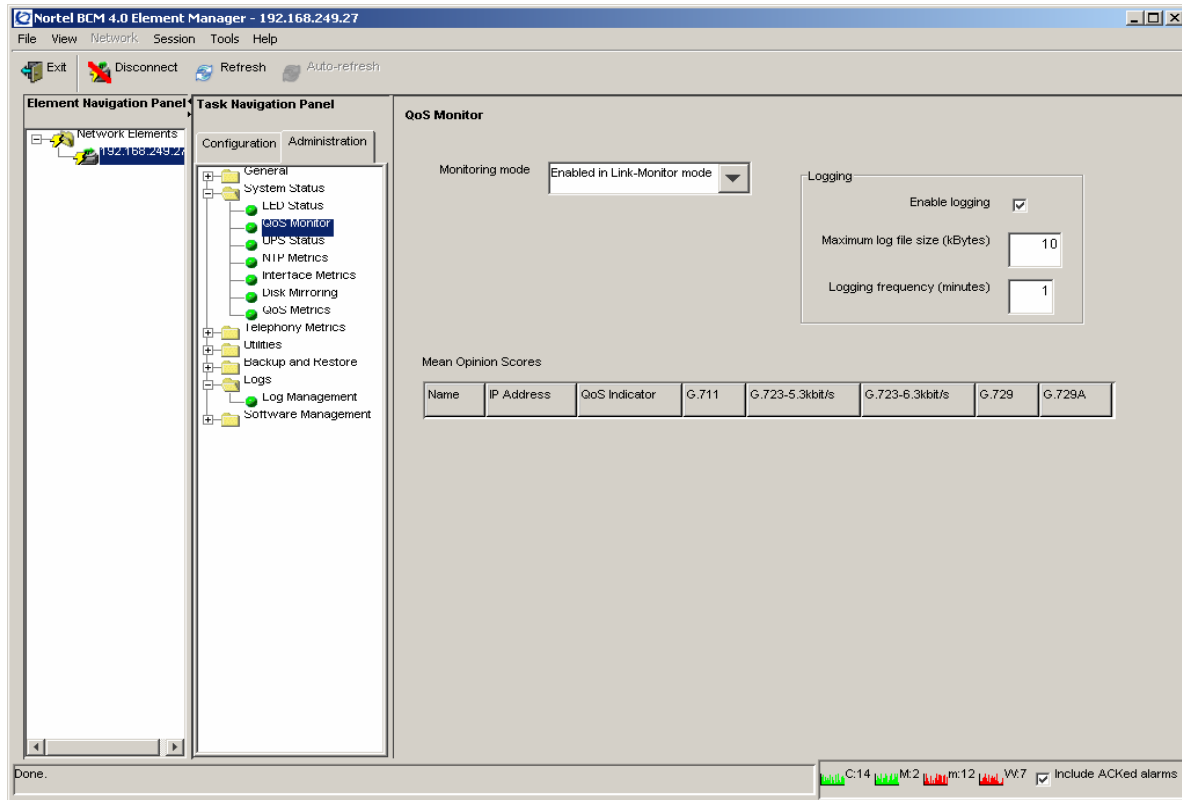
To configure monitoring mode

- 1 On the Navigation tree, click the **Administration** tab, **System Status**, and **QoS Monitor**.
- 2 Configure the monitoring mode attributes.

Table 56 Monitoring Mode attributes

Attribute	Action
Disabled	—
Link-Monitor Mode	Continuously test the connection between the BCM and remote endpoints.
QoS-Monitor Mode	Select this option if you want to calculate MOS values for each endpoint, determine whether the connection has fallen below a specific threshold, send MOS scores to FCAPS applications, and create a log history of the MOS scores.

Figure 30 QoS Monitoring mode



To configure logging attributes

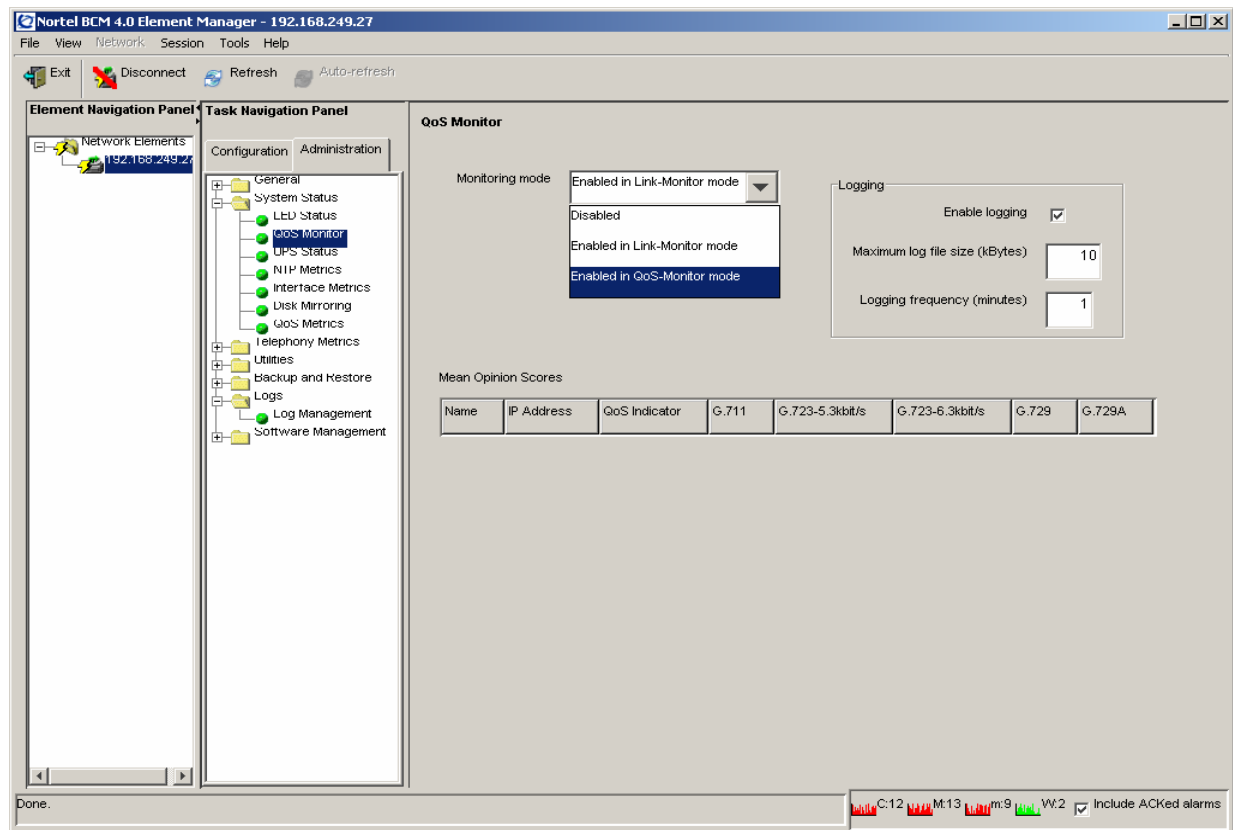
- 1 On the Navigation tree, click the **Administration** tab, **System Status**, and **QoS Monitor**.
- 2 Configure logging attributes.

Table 57 Logging attributes

Attribute	Action
Enable Logging	Enable the check box if you want to enable the logging of MOS scores.
Maximum log file size	Enter a value for the maximum size of the log file, from 1 to 10240 kilobytes (KB). The default is 10 KB.
Logging Frequency	Enter the time interval between each MOS log: 1 to 1440 minutes. The default is 1 minutes.

- 3 Press the **Tab** key to save the settings.

Figure 31 QoS Logging attributes



To view the QoS monitoring information

The Mean Opinion Scores table displays the current network quality described as a Mean Opinion Score (MOS) for each IP destination. You can view the MOS mapping. Unlike the BCM 3.x where both transmit and receive values were reported, the QoS Monitor collects only the transmit values.

Table 58 lists the fields displayed in the Mean Opinion Score table.

Table 58 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 Indicator	Displays a text description of the current MOS value. The MOS values can be Poor, Fair, Good or Excellent.
G.711	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).

Table 58 Mean Opinion Score descriptions (Continued)

Attribute	Description
Name	Displays the name of the Remote Gateway
G.723-5.3kbit/s	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.723-6.3kbit/s	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.729	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.729A	Displays the current MOS value calculated when using a G.729A 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).

To refresh the QoS monitor data

To update the MOS table with the most current values, select **View > Refresh**, press F5, or select the Refresh icon from the toolbar.

UPS Status

The BCM can support an Uninterruptible Power Supply (UPS) device to ensure continuous operation during power interruption and failure conditions. The UPS feature provides power source monitoring and battery backup so that critical system functionality required to maintain and provide warning time to either correct the problem or to activate a contingency plan for impacted services is possible. UPS is described in the *BCM200/400 BCM 4.0 Installation and Maintenance Guide* (N0060612), and the *BCM 4.0 Installation Checklist and Quick Start Guide* (N0060603).

The UPS connects and communicates with the BCM through USB. Enabling the UPS feature requires plugging the UPS USB cable into the BCM USB connector before powering up the BCM. The UPS must be present during the boot up process for the BCM to function.

This section provides the procedure that describes how [“To access UPS Status”](#).

To access UPS Status

- 1 To access the UPS Status, open the Element Manager, click the **Administration** tab, click **System Status** in the directory tree, and then click **UPS Status**.

The **UPS Status** then displays.

The UPS Status panel confirms that a UPS is connected including model and serial number, its current status, and provides a read out of the current values. Additionally, an indication is given whether the value is within the normal range or not.

The UPS Status panel tracks occurrences of alarms pertaining to UPS operation. These alarms are also sequentially viewable in the Alarm panel. The metrics correspond to alarms in the BCM and appear in the alarm panel as well. See [Figure 32](#).

Figure 32 UPS Status Monitor

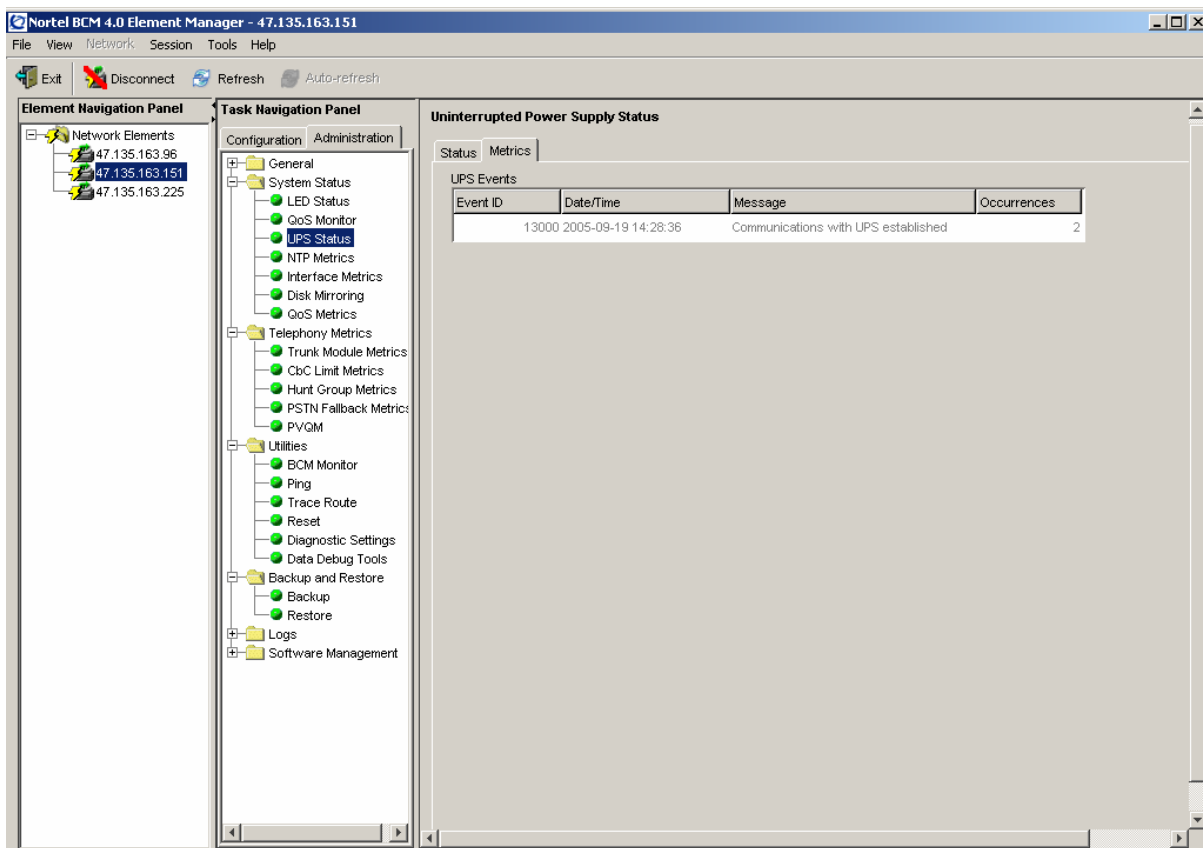
The screenshot shows the Nortel BCM 4.0 Element Manager interface. The main window is titled 'Nortel BCM 4.0 Element Manager - 47.135.163.151'. The interface is divided into three main sections:

- Element Navigation Panel:** Shows a tree view of network elements with IP addresses 47.135.163.96, 47.135.163.151, and 47.135.163.225.
- Task Navigation Panel:** Contains a tree view of tasks under 'Configuration' and 'Administration'. The 'UPS Status' task is selected.
- Uninterrupted Power Supply Status:** The main content area, split into 'Status' and 'Metrics' tabs. The 'Metrics' tab is active, showing a table of current values and their status.

Current Values	Value	Status
Load capacity (%)	9.70	Normal
Battery charge (%)	100	Normal
Battery charge time left (min)	123	Normal
Temperature (C)	25.20	Normal
Line frequency (Hz)	60.00	Normal
Output voltage (Volts)	118.00	Normal
Input voltage (Volts)	118.00	Normal
High transfer - Line maximum (Volts)	127	Normal
Low transfer - Line minimum (Volts)	106	Normal
Normal battery voltage (Volts)	24	Normal
Current battery voltage (Volts)	27.70	Normal

- 2 To check the metrics of the UPS, click the **Metrics** tab. It displays the information on the panel.

Figure 33 UPS Status page



NTP Metrics

Using Network Time Protocol (NTP), you can configure the time on the BCM indirectly from a single time server. NTP is a network protocol designed to synchronize the clocks of computers over an IP network. The NTP Metrics provide an overview of the integrity of the NTP time source.



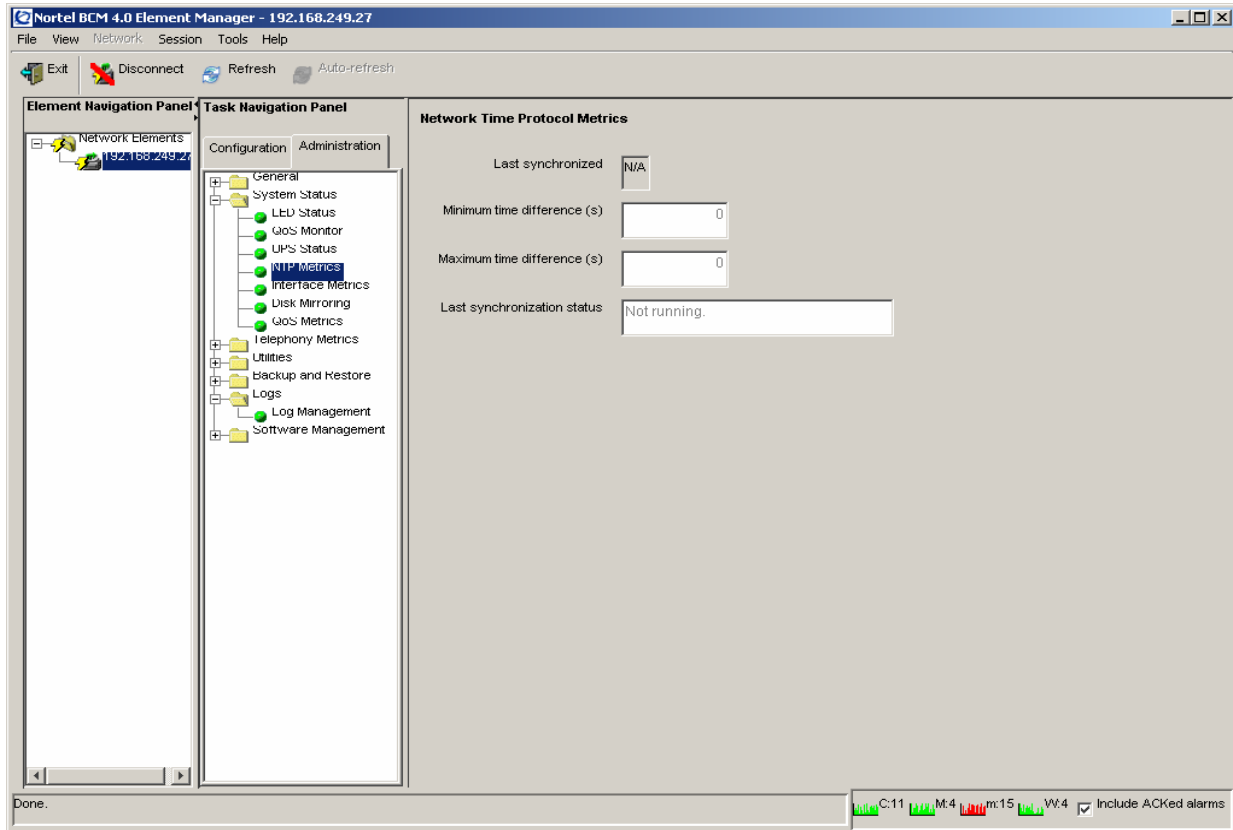
Note: If the BCM clock control has not been configured to use NTP (Configuration>System>Date & Time), then the NTP Metrics panel displays no data.

This section provides the procedure [“To access the NTP Metrics”](#).

To access the NTP Metrics

- 1 Open the Element Manager, click the **Administration** tab, click **System Status** and then select **NTP Metrics** in the navigation tree. See [Figure 34](#).

Figure 34 NTP Metrics



The **NTP Metrics** panel displays information contained in [Table 59](#).

Table 59 NTP Statistics

Parameter Name	Description
Minimum time difference (s)	The minimum time change that occurred since NTP was running
Maximum time difference (s)	The maximum time difference that occurred since NTP was running
Last Synchronized	When the last synchronization occurred
Last Synchronization Status	The results of the last synchronization: successful or unsuccessful. If unsuccessful the reason for the failure is given: failed to contact, or failed security check. A status of Not Running indicates that NTP is not configured.

Interface Metrics

You can monitor information about the network interfaces in your system. The **Interface Metrics** panel displays information contained in Table 60.

Table 60 Interface Metrics

Type	Interface Name	% Total Rx BW	% Total Tx BW
Type of interface connected, such as LAN, WAN, or modem	Name of interface	Percentage of received bandwidth	Percentage of transmitted bandwidth

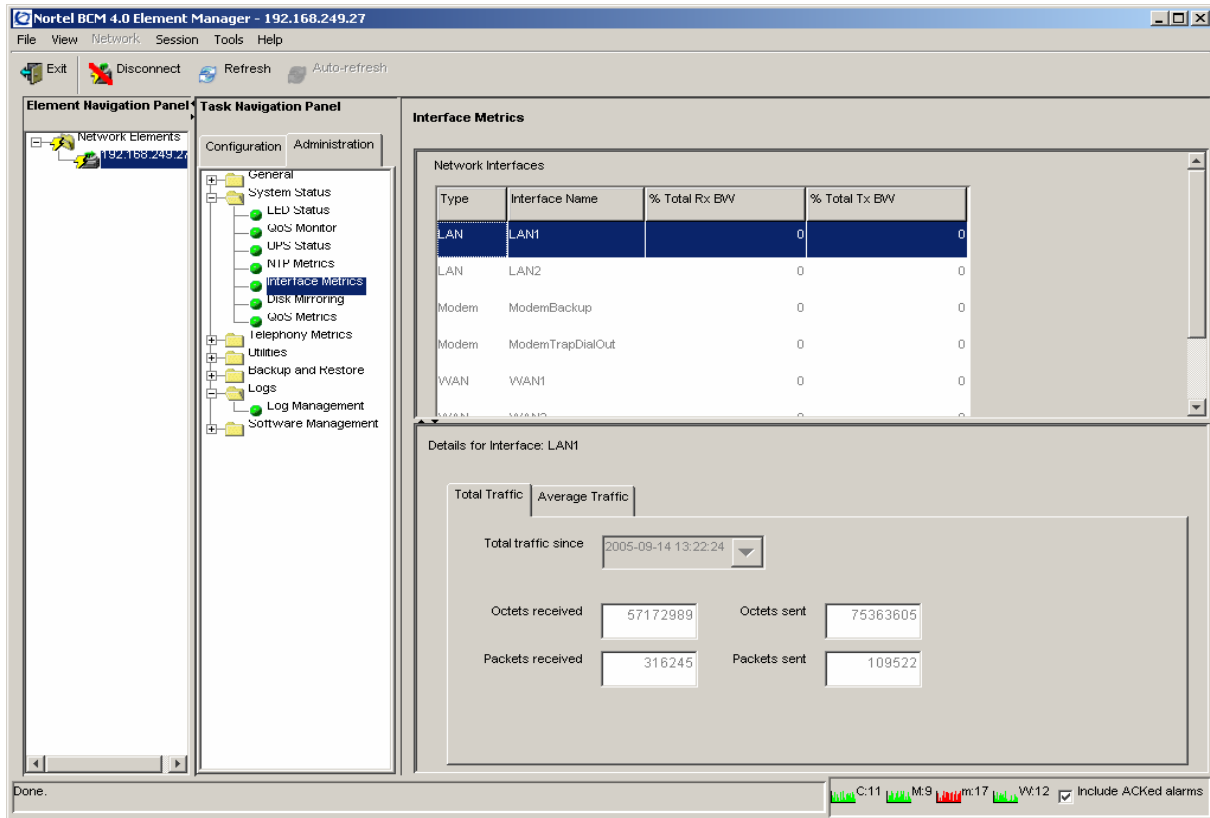
You can view the network interfaces by selecting **Configuration > Network Interfaces**. For more information about configuring network interfaces, see the *BCM 4.0 Networking Configuration Guide* (N0060606).

To view Interface Metrics

Use this procedure to display interface metrics.

- 1 Open the Element Manager, select **Administration > System Status > Interface Metrics** in the navigation tree. See [Figure 34](#).
- 2 Select an interface from the **Network Interfaces** table.

Figure 35 Interface Metrics



When you select an interface, the details panel displays two additional tabs: Total Traffic, and Average Traffic. Table 61 lists the metrics that each tab displays.

Table 61 Total traffic and average traffic

Metric	Description
Total traffic	
Since	Start time for collecting metrics
Total number of octets received	The total number of octets received since the start time
Total number of octets sent	The total number of octets sent since the start time
Total number of packets received	The total number of packets received since the start time
Total number of packets sent	The total number of packets received since the start time
Average traffic	
Average (per second) from	Start date for calculating average
To	End date for calculating average
Average number of octets received (per second)	The average number of octets received during the specified time period.

Table 61 Total traffic and average traffic

Metric	Description
Average number of octets sent (per second)	The average number of octets sent during the specified time period.
Average number of packets received (per second)	The average number of packets received during the specified time period.
Average number of packets sent (per second)	The average number of packets sent during the specified time period.

Disk Mirroring

If you are using disk mirroring to provide redundancy in your system, you can use the Disk Mirroring panel to monitor the status of the hard drives used for disk mirroring.

The Disk Mirroring panel contains Settings information and Status information. Table 62 describes the fields on the panel.

Table 62 Information about Disk Mirroring

Field	Description
Settings	
Operation mode	The options are Mirror Mode, Mirror Only, and Primary Only
Beep on drive failure	The interval between beeps when a drive fails. The options are: Every 5 seconds, Every 30 seconds, Continuously, and Disabled.
Button	
Test beep	Click on the button to test the warning beep.
Status	
Operational status	Read-only. Displays the status of the disk mirroring equipment. When operating correctly, the status is Drives are Identical.
Primary disk status	Read-only. Status may be Passed, Failed, or N/A.
Mirror disk status	Read-only. Status may be Passed, Failed, or N/A.
Rebuild status	Read-only. Displays the progress of the rebuild of mirror data. Status may be Idle or Started.

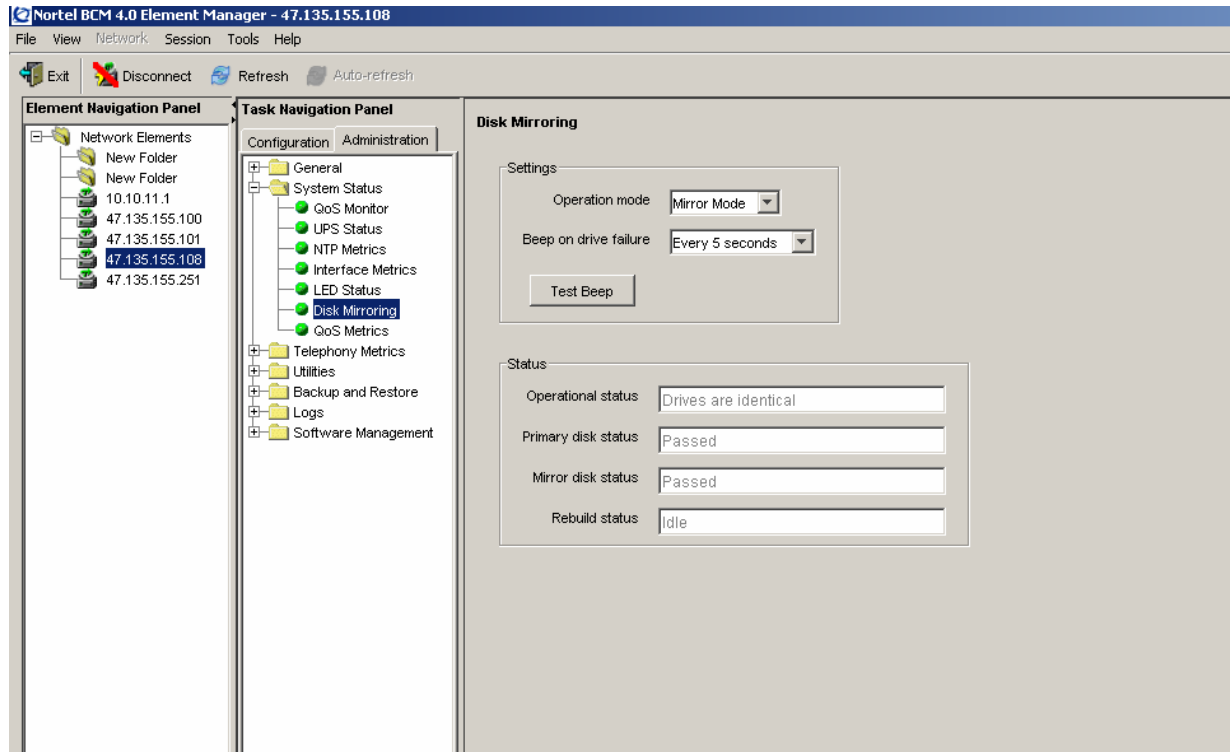
For additional information about choosing an operation mode for disk mirroring, see the *BCM200/400 BCM 4.0 Installation and Maintenance Guide* (N0060612) and the *BCM 4.0 for BCM1000 Installation and Maintenance Guide Addendum* (N0060603).

To monitor Disk Mirroring

Use this procedure to monitor disk mirroring.

- 1 Open the Element Manager, select **Administration > System Status > Disk Mirroring** in the navigation tree.
- 2 See [Figure 34](#).

Figure 36 Disk Mirroring



QoS Metrics

The QoS Metrics panel allows you to monitor QoS metrics in three ways: globally, on a per-interface basis, or on a per-account basis. For information about how to access these metrics, follow the procedures contained in this section:

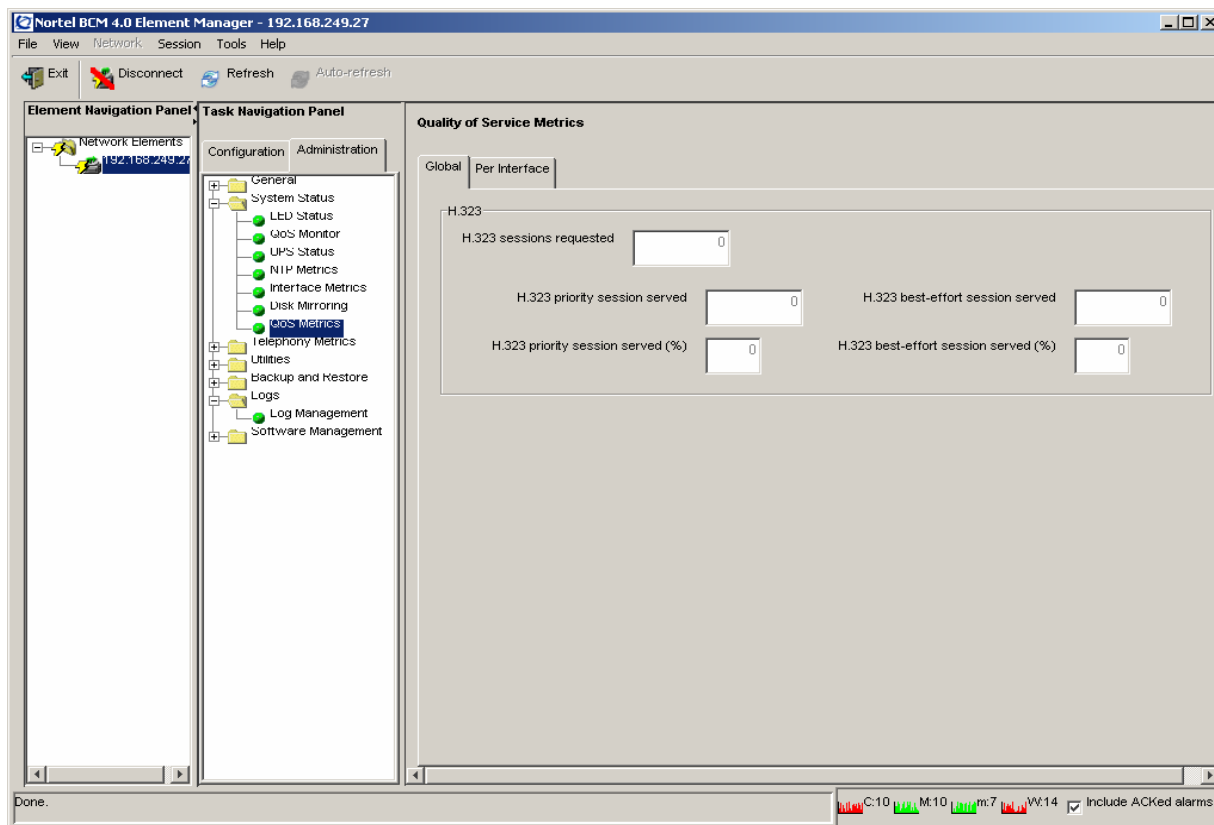
- [“To view global QoS metrics” on page 259](#)
- [“To view per interface QoS metrics” on page 260](#)

To view global QoS metrics

Use this procedure to display global metrics for H.323 sessions.

- 1 Open the Element Manager, select **Administration > System Status > QoS Metrics > Global** in the navigation tree. See [Figure 34](#).

Figure 37 Global QoS metrics



The **Global** tab in the **QoS Metrics** panel displays information contained in [Table 63](#).

Table 63 Global QoS Metrics

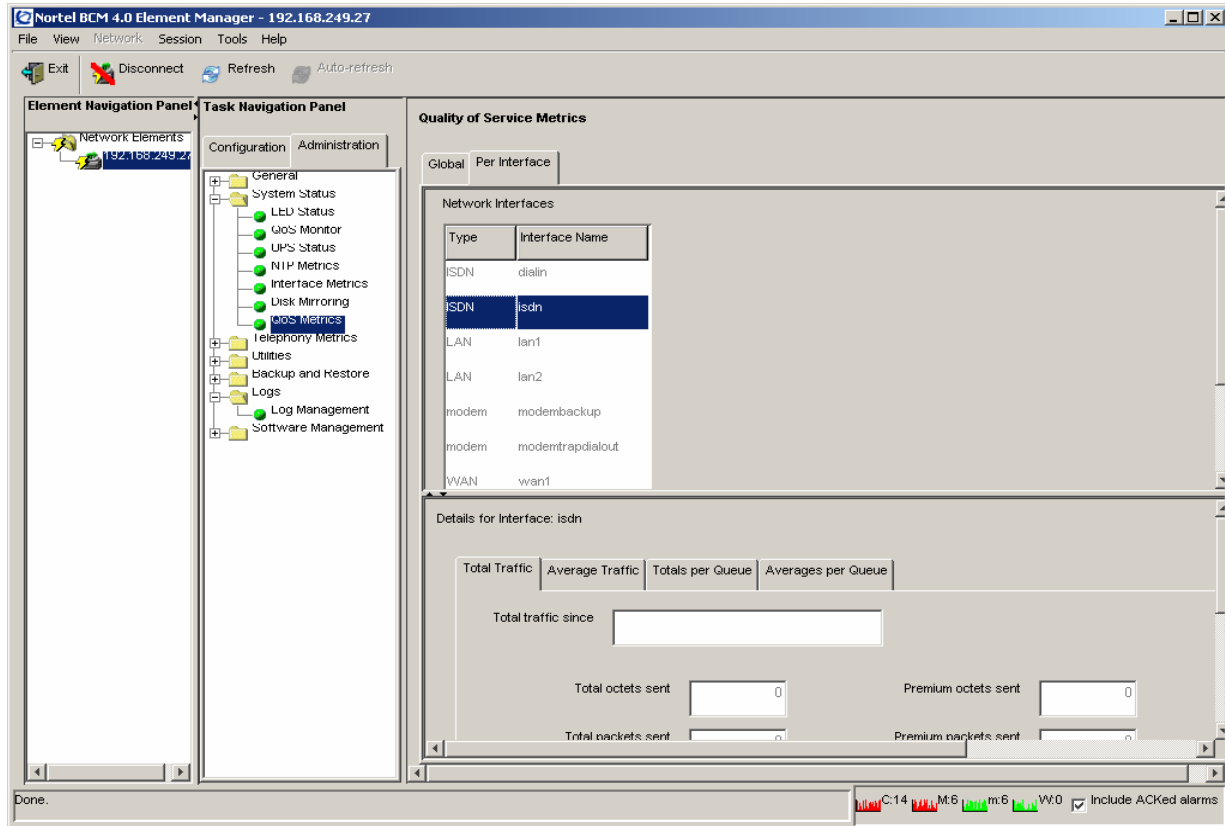
Metric Name	Description
H.323 sessions requested	Total number of all H.323 sessions requested
H.323 priority sessions served	Total number of H.323 priority sessions served
H.323 priority sessions served (%)	Percentage of H.323 priority sessions served
H.323 best-effort session served	Total number of H.323 best-effort session served
H.323 best-effort session served (%)	Percentage of H.323 best-effort session served

To view per interface QoS metrics

Use this procedure to display QoS metrics for a specific interface.

- 1 Open the Element Manager, select **Administration > System Status > QoS Metrics > Per Interface** in the navigation tree.
- 2 Select an in interface from the Network Interfaces table.
See [Figure 34](#).

Figure 38 Per Interface QoS metrics



The details panel displays information about the selected interface under four different tabs:

- Total Traffic, as described in Table 64
- Average Traffic, as described in Table 65
- Totals Per Queue, as described in Table 66
- Averages Per Queue, as described in Table 67

Table 64 Total traffic tab

Metric Name	Description
Total traffic since	Start date for collecting metrics
Total octets sent	Total Number of
Premium octets sent	Number of premium octets sent

Table 64 Total traffic tab

Metric Name	Description
Best effort octets sent	Number of best effort octets sent
Total packets sent	Total number of packets sent
Premium packets sent	Number of premium packets sent
Best effort packets sent	Number of best effort packets sent
Total packets within guarantee	Total number of packets within the guarantee
Premium packets within guarantee	Number of premium packets within the guarantee
Best effort packets within guarantee	Number of best effort packets within the guarantee
Total packets over guarantee	Total number of packets over the guarantee
Premium packets over guarantee	Number of premium packets over the guarantee
Best effort packets over guarantee	Number of best effort packets over the guarantee
Total packets dropped	Total number of packets dropped
Premium packets dropped	Number of premium packets dropped
Best effort packets dropped	Number of best effort packets dropped

Table 65 Average traffic tab

Metric Name	Description
Average traffic from	Start date used for calculating averages
To	End date used for calculating averages
Total octets sent	Total Number of
Premium octets sent	Number of premium octets sent
Best effort octets sent	Number of best effort octets sent
Total packets sent	Total number of packets sent
Premium packets sent	Number of premium packets sent
Best effort packets sent	Number of best effort packets sent
Total packets within guarantee	Total number of packets within the guarantee
Premium packets within guarantee	Number of premium packets within the guarantee
Best effort packets within guarantee	Number of best effort packets within the guarantee
Total packets over guarantee	Total number of packets over the guarantee
Premium packets over guarantee	Number of premium packets over the guarantee
Best effort packets over guarantee	Number of best effort packets over the guarantee
Total packets dropped	Total number of packets dropped

Table 65 Average traffic tab

Metric Name	Description
Premium packets dropped	Number of premium packets dropped
Best effort packets dropped	Number of best effort packets dropped

Table 66 Totals per queue

Metric Name	Description
Total traffic since	Start date used for calculating totals
Queue	The number of the queue
Class of query	The type of query
Octets sent	Number of octets sent
Packets sent	Number of packets sent
Packets within guarantee	Number of packets within the guarantee
Packets over guarantee	Number of packets over the guarantee
Packets dropped	Number of packets dropped

Table 67 Averages per queue

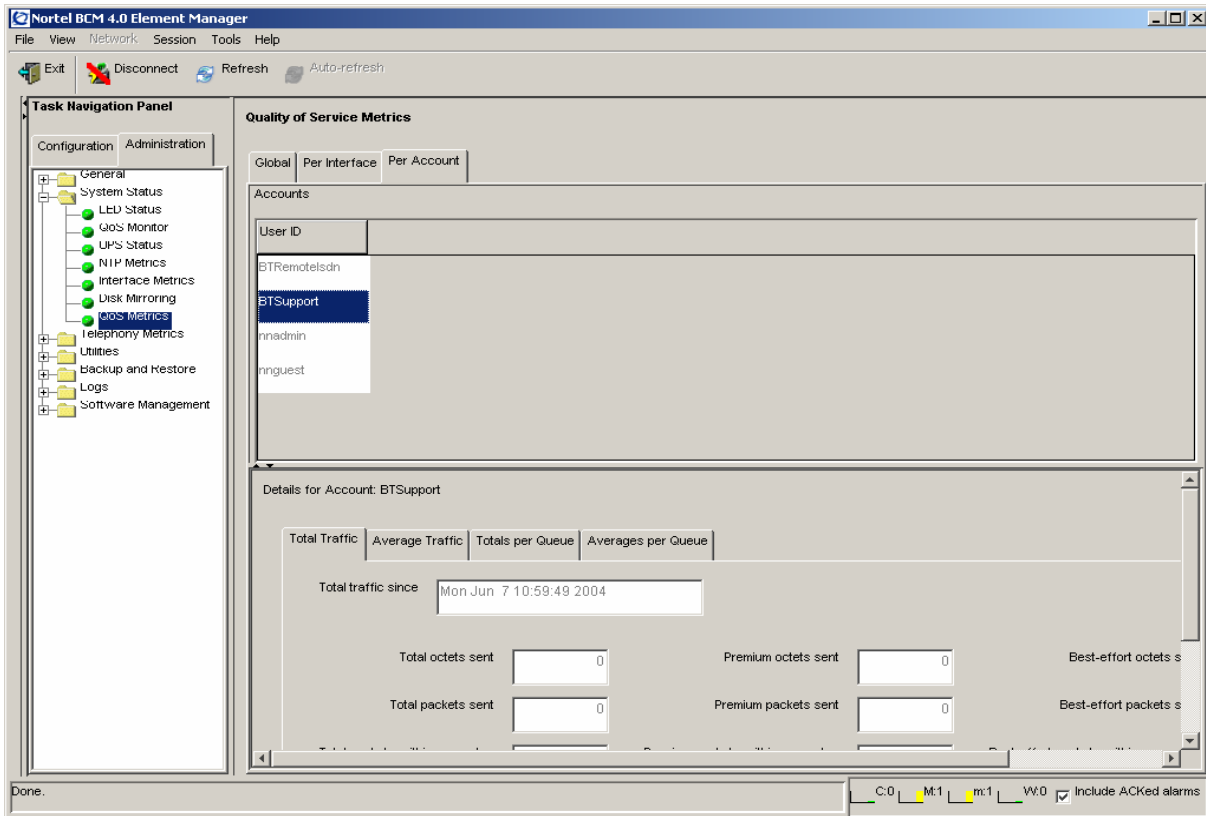
Metric Name	Description
Average traffic from	Start date used for calculating averages
To	End date used for calculating averages
Queue	The number of the queue
Class of query	The type of query
Octets sent	Number of octets sent
Packets sent	Number of packets sent
Packets within guarantee	Number of packets within the guarantee
Packets over guarantee	Number of packets over the guarantee
Packets dropped	Number of packets dropped

To view per account QoS metrics

Use this procedure to display QoS metrics for a specific account. These metrics are available for dial-up accounts only.

- 1 Open the Element Manager, select **Administration > System Status > QoS Metrics > Per Account** in the navigation tree.
- 2 Select an account from the Accounts table, as shown in [Figure 39](#).

Figure 39 Per Account QoS Metrics



The details panel displays information about the selected account under four different tabs:

- Total Traffic, as described in Table 68
- Average Traffic, as described in Table 69
- Totals Per Queue, as described in Table 70
- Averages Per Queue, as described in Table 71

Table 68 Total traffic tab

Metric Name	Description
Total traffic since	Start date for collecting metrics
Total octets sent	Total Number of octets sent
Premium octets sent	Number of premium octets sent
Best effort octets sent	Number of best effort octets sent
Total packets sent	Total number of packets sent
Premium packets sent	Number of premium packets sent
Best effort packets sent	Number of best effort packets sent
Total packets within guarantee	Total number of packets within the guarantee
Premium packets within guarantee	Number of premium packets within the guarantee

Table 68 Total traffic tab

Metric Name	Description
Best effort packets within guarantee	Number of best effort packets within the guarantee
Total packets over guarantee	Total number of packets over the guarantee
Premium packets over guarantee	Number of premium packets over the guarantee
Best effort packets over guarantee	Number of best effort packets over the guarantee
Total packets dropped	Total number of packets dropped
Premium packets dropped	Number of premium packets dropped
Best effort packets dropped	Number of best effort packets dropped

Table 69 Average traffic tab

Metric Name	Description
Average traffic from	Start date used for calculating averages
To	End date used for calculating averages
Total octets sent	Total Number of octets sent
Premium octets sent	Number of premium octets sent
Best effort octets sent	Number of best effort octets sent
Total packets sent	Total number of packets sent
Premium packets sent	Number of premium packets sent
Best effort packets sent	Number of best effort packets sent
Total packets within guarantee	Total number of packets within the guarantee
Premium packets within guarantee	Number of premium packets within the guarantee
Best effort packets within guarantee	Number of best effort packets within the guarantee
Total packets over guarantee	Total number of packets over the guarantee
Premium packets over guarantee	Number of premium packets over the guarantee
Best effort packets over guarantee	Number of best effort packets over the guarantee
Total packets dropped	Total number of packets dropped
Premium packets dropped	Number of premium packets dropped
Best effort packets dropped	Number of best effort packets dropped

Table 70 Totals per queue

Metric Name	Description
Total traffic since	Start date used for calculating totals
Queue	The number of the queue
Class of query	The type of query
Octets sent	Number of octets sent
Packets sent	Number of packets sent
Packets within guarantee	Number of packets within the guarantee
Packets over guarantee	Number of packets over the guarantee
Packets dropped	Number of packets dropped

Table 71 Averages per queue

Metric Name	Description
Average traffic from	Start date used for calculating averages
To	End date used for calculating averages
Queue	The number of the queue
Class of query	The type of query
Octets sent	Number of octets sent
Packets sent	Number of packets sent
Packets within guarantee	Number of packets within the guarantee
Packets over guarantee	Number of packets over the guarantee
Packets dropped	Number of packets dropped

Telephony Metrics

The following sections provide a general overview of the Element Manager Telephony Metrics headings.

The Telephony Metrics folder groups together a number of BCM system status tracking different aspects of Telephony services.

This overview describes the following general process information:

- [“Trunk Module Metrics” on page 266](#)
- [“CbC limit metrics” on page 272](#)
- [“ Hunt Group Metrics” on page 274](#)
- [“PSTN Fallback Metrics” on page 276](#)
- [“Proactive Voice Quality Management” on page 277](#)

Trunk Module Metrics

When you need to find out information about a trunk module, you can determine the status of any of the settings under the trunk modules headings. To correct a problem you may need to enable or disable a port, a module, or an entire bus.

This section provides the following procedures:

- “[To view Trunk Module status](#)” on page 266
- “[Disabling or enabling a B channel setting](#)” on page 268
- “[Provisioning a PRI B-channel](#)” on page 268
- “[Trunk Module CSU statistics](#)” on page 269

To view Trunk Module status

The Trunk Module Metrics panel allows you to view the status of digital trunk 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 Trunk Module selection to disable and enable modules and devices.

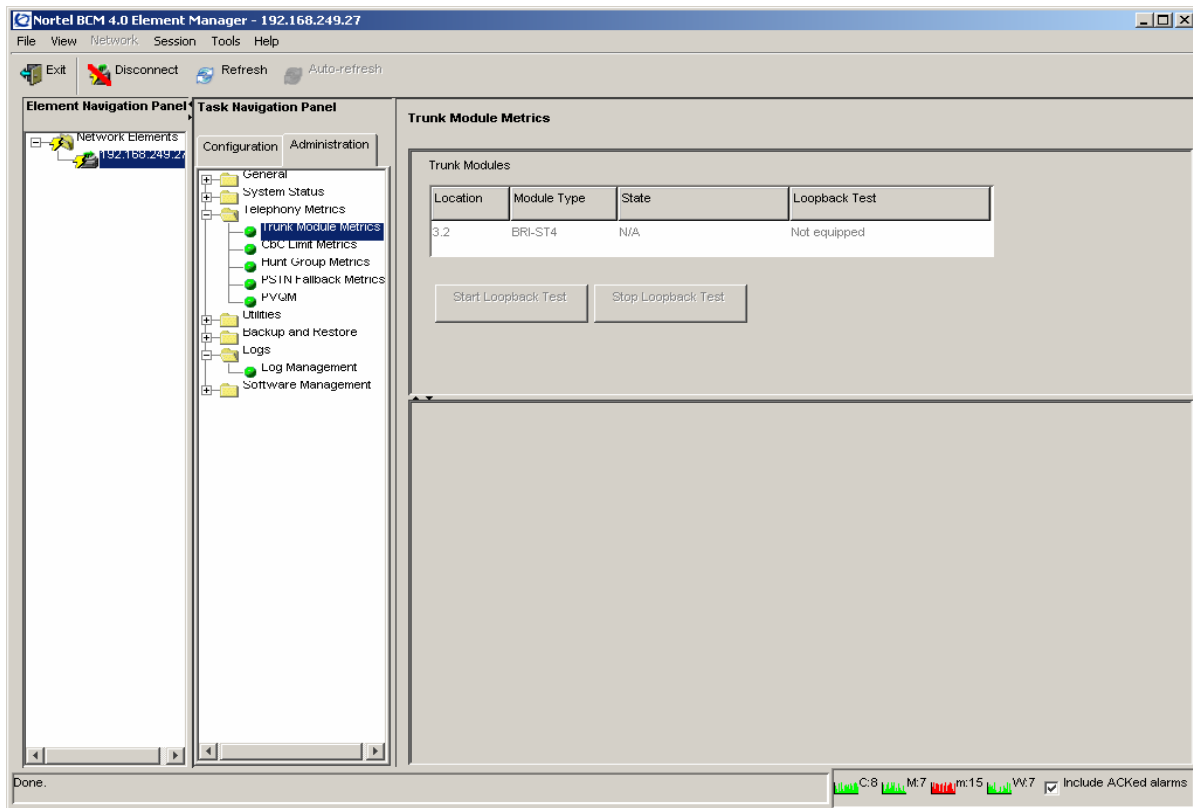
Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module state:

- 1 On the Element Manager navigation tree, select **Administration > Telephony Metrics > Trunk Module Metrics**.

The window displays the expansion locations for the modules connected to the system.

- 2 Select the module that you want to view. For example, **Expansion 1**. See [Figure 40](#).

Figure 40 Viewing Trunk Module metrics



- 3 Click **Start Loopback Test** button to start the network test without having to remove the BCM.
- 4 Select a loopback type. The options are:
 - payload
 - line
 - card edge
 - continuity
- 5 Click **Stop Loopback Test** when done the test of the network.

When you click on a module in the process above, a new menu appears, **Details for Module: <number>** with the following tabs:

- CSU Alarms
- CSU Alarm History
- Performance
- Performance History
- D-Channel
- B-Channels

Viewing Performance History information

The Performance History tab displays the performance information over 15-minute intervals collected in the past 24 hours. The performance information collected includes the number of errored seconds, severely errored seconds, and unavailable seconds over each 15-minute interval.

- 1 On the navigation tree, click **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Click the **Performance History** tab to view metrics information.

Viewing D-Channel information

This tab displays trunk module metrics for the D-channel. D-channel metrics display when a BRI trunk module is configured on the system.

- 1 On the navigation tree, click **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Click the **D-channel** tab to view metrics information.

Disabling or enabling a B channel setting

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

To disable or enable a B channel setting

- 1 On the navigation tree, click **Administration > Telephony Metrics > Trunk Module Metrics**.

The window displays **Expansion 1** or **Expansion 2**.

- 2 Click heading of the bus you want to view. For example, click **Expansion 1**.
- 3 Click the tab in the lower menu marked B-Channels.
- 4 Click the B channel you want to enable or disable (**B1** or **B2**).
- 5 Then select **Enable** or **Disable**.

If you are disabling the channel, you are prompted by a dialog box to confirm your action. The State field indicates the mode of operation for the port. If the port is enabled, this field is blank unless a device is physically connected.

Provisioning a PRI B-channel

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. If you do not have all of the PRI B channels, disable all the B-channels that you do not need.

Nortel recommends that the number of lines that are deprovisioned on a DTM (configured as PRI) be the same as the number of B-channels that are disabled. For example, if the DTM is on Expansion 1, when B-channels 13-23 are disabled, you should deprovision lines 77 to 87.

To provision a PRI B-channel

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose an expansion 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 CSU statistics

Each trunk module has an internal channel service unit (CSU). When enabled, the internal CSU monitors the quality of the received T1 signal and provides performance statistics, alarm statistics, and diagnostic information.

Trunk modules must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information, refer to:

- [“Statistics collected by the system” on page 269](#)
- [“Enabling the internal CSU” on page 270](#)
- [“To check the performance statistics” on page 270](#)
- [“To check the CSU alarms” on page 271](#)
- [“To check carrier failure alarms” on page 271](#)
- [“To check bipolar violations” on page 271](#)
- [“To check short-term alarms” on page 272](#)
- [“To check defects” on page 272](#)
- [“CbC limit metrics” on page 272](#)

Statistics collected by the system

The system accumulates three performance parameters:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined according to TIA-547A. Errored seconds are enhanced to include control slip (CS) events. Only near-end performance data is recorded.

The internal CSU continuously monitors the received signal and detects four types of transmission defects:

- any active carrier failure alarms (CFA), such as loss of signal (LOS), out of frame (OOF), alarm indication signal (AIS), and remote alarm indication (RAI)

- the number of bipolar violations that occurred in the last minute
- any defects that occurred in the last minute, such as loss of signal (LOS), out of frame (OOF), and alarm indication signal (AIS)
- the number of milliseconds of short-term alarms in the last minute, such as loss of signal (LOS), out of frame (OOF), alarm indication signal (AIS), and remote alarm indication (RAI). A short term alarm is declared when the detected defects persist for tens of milliseconds.

A carrier failure alarm (CFA) is a duration of carrier system outage. CFA types reported can be mapped to CFAs defined in TIA-547A and TR62411 as shown in Table 72.

Table 72 Carrier failure alarms

Business Communications Manager	TIA-547A	TR62411
LOS CFA	RED CFA	RED CFA
OOF CFA	RED CFA	RED CFA
AIS CFA	RED CFA	AIS CFA
RAI CFA	YELLOW CFA	YELLOW CFA

The criteria for declaring and clearing the alarms is selectable to meet those in TIA-547A or TR64211. You can also view Carrier Failure Alarms as Core Telephony Alarms in the Alarm Viewer.

Enabling the internal CSU

Use the following procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

To enable the internal CSU

- 1 Choose **Configuration, Resources, Telephony Resources**.
The window displays the expansion modules.
- 2 Choose the appropriate expansion module. For example, select Expansion 1.
- 3 For the selected module, choose the **Trunk Module Parameters** tab.
- 4 In the T1 Parameters section, select the Internal CSU check box to enable the Internal CSU.

To check the performance statistics

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose the appropriate expansion module that contains the module that you want to check.
- 3 Choose **Performance** tab.

- 4 The **Current interval** displays the duration of the current 15-minute interval of the selected card, the number of errored seconds (ES), the number of severely errored seconds (SES) and the number of unavailable time seconds (UAS).
- 5 Click the **24-hour summary** heading for an overall summary of the previous 24 hours.
The Number of intervals, Errored Seconds, Severely Errored Seconds, Unavailable Seconds appear in the summary.
- 6 Click the **Reset Statistics** button to reset any new settings.
The system displays a message indicating that this will remove all of the statistics.
- 7 Select **OK** to erase all the current statistics and begin collecting statistics again.

Checking trunk module alarms

To check the CSU alarms

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose an expansion module.
- 3 Click the **CSU Alarms** tab.

The display shows all the active alarms of the types LOS (loss of signal), OOF (out of Frame), RAI (Remote alarm indicator) or AIS (Alarm indication signal). For more information on these types of transmission defects, refer to [“Statistics collected by the system” on page 269](#).

To check carrier failure alarms

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose an expansion module.
- 3 Click the **CSU Alarm History** tab.

The display shows LOS (loss of signal), OOF (out of Frame), AIS (Alarm indication signal), and RAI (Remote alarm indicator). For more information on these types of transmission defects, refer to [“Statistics collected by the system” on page 269](#).

- 4 Choose the type of alarm you wish to view. For example, LOS (Loss Of Signal).
- 5 Click the drop-down menu to select a time period.

The display shows the Start time of the period.

To check bipolar violations

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose an expansion module.
- 3 Click the **CSU Alarms** tab.

The display shows the number of bipolar violations that occurred in the last minute.

To check short-term alarms

- 1 Choose **Administration, Telephony Metrics, Trunk Module Metrics**.
- 2 Choose an expansion module.
- 3 Click the **CSU Alarms** tab.

The display shows the short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute.

To check defects

- 1 Choose **Administration > Telephony Metrics > Trunk Module Metrics**.
- 2 Choose a an expansion module.
- 3 Click the **CSU Alarms** tab.

The display shows the first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute.

To view CSU Alarm History

- 1 Choose **Administration, Trunk Modules**.
- 2 Choose an expansion module.
- 3 Click the **CSU Alarm History** tab.

The display shows all the alarms

- 4 To view a specific alarm, click the **Alarm Name**.

The display shows all the occurrences of that Alarm

CbC limit metrics

Call-by-call service (CbC) on public PRI protocol (NI-2) allows a PBX to use channels more effectively by expanding or contracting the number of channels available to different call types such as INWATS, OUTWATS, Foreign Exchange (FX), and tie lines.

The call-by-call service is a method of offering and receiving services to Customer Premises Equipment (CPE) on ISDN PRI without the use of dedicated circuits (i.e. interface or B-channels). The Call-By-Call service conveys signaling information over an ISDN Primary Rate Interface (PRI) that indicates, on a per-call basis, the specific service type required to complete the call.

Once the feature is configured, use the CbC Limit metrics panel to monitor denied call activity for each service on each line pool.

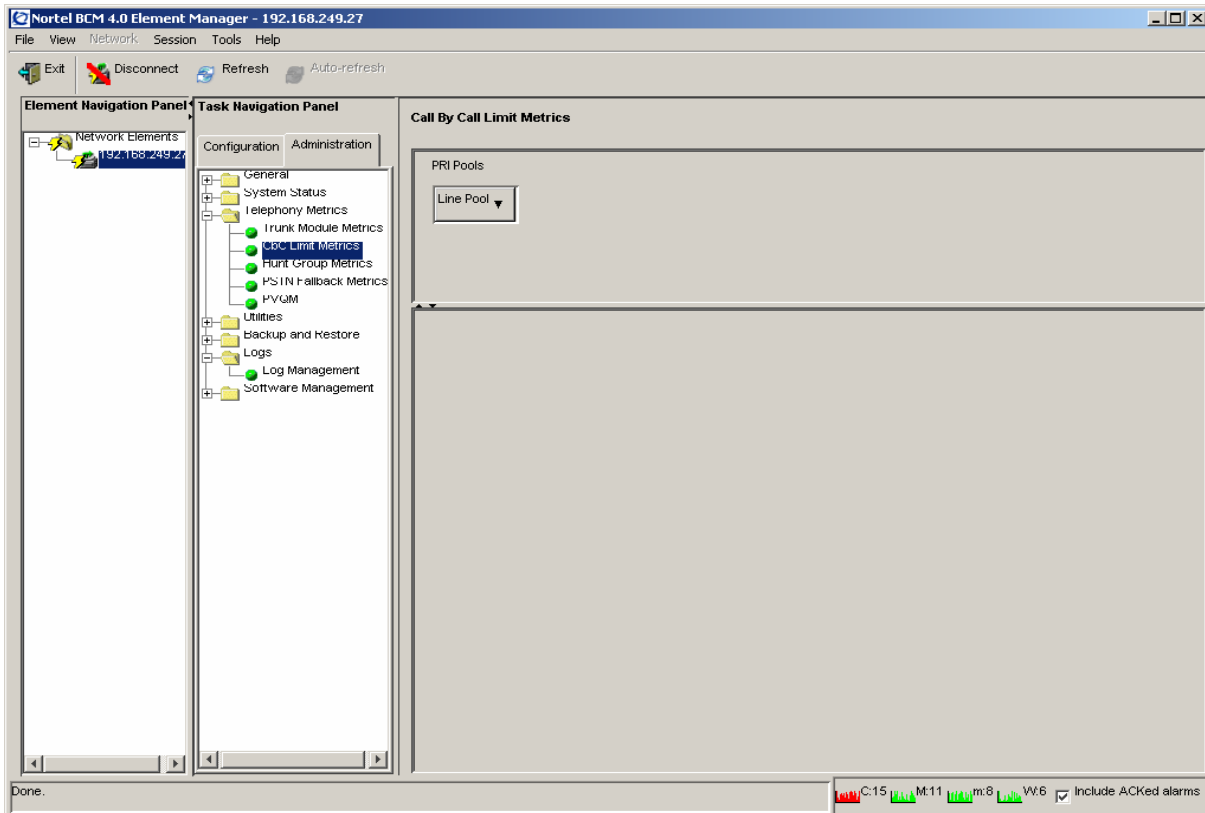
PRI lines that support call-by-call services have maximum and minimum call limits for each service. Use this panel to view reports for the services. These limits are set as part of the numbering plan programming.

This section provides the [“To access the CbC limit metrics”](#) procedure.

To access the CbC limit metrics

- 1 To access the CbC metrics, in the Element Manager, click the **Administration** tab, click the **Telephony Metrics** and then **CbC Limit Metrics** in the navigation tree.
- 2 To assess the capacity of the PRI call services on your system, on the **Call by Call Metrics** table, select the line pool for which you want to view CbC traffic.
- 3 See [Figure 41](#).

Figure 41 Call By Call limit metrics



The denied call details for each type of service supported by the line pool is displayed. See [Figure 42](#) on page 274.

Figure 42 Denied calls details

Details for Pool: ROstr01				
Calls denied because CbC limits were exceeded				
Service Type	INCOMING due to Outgoing Min ▲	due to Incoming Max	OUTGOING due to Incoming Min	due to Outgoing Max
First	1	1	1	1
Second	2	2	2	2
Third	3	3	3	3
First	4	4	4	4

Table 73 describes each field on the two CbC metrics panels.

Table 73 Details for a Line Pool

Attribute	Value
Call By Call Limit Metrics table	
Line Pool	Read-only. The pool of lines that call-by-call limits are applied to.
Calls denied because CbC limits were exceeded table	
Service Type	Read-only. The type of service that the limits apply to.
INCOMING due to Outgoing Min.	Read-only. The number of incoming calls that have been blocked due to the call-by-call limits.
due to Incoming Max.	Read-only. The number of incoming calls that have been blocked due to the call-by-call limits.
Outgoing due to Incoming Min.	Read-only. The number of outgoing calls that have been blocked due to the call-by-call limits.
due to Outgoing Max.	Read-only. The number of outgoing calls that have been blocked due to the call-by-call limits.
Actions	
Clear	To clear the table so you can start a monitoring period: <ol style="list-style-type: none"> 1. Click on the Action menu item. 2. Select Clear. 3. Close the panel. 4. If you determine that the call denials are too numerous, increase lines that support the affected service type.

Hunt Group Metrics

Hunt groups provide a service where incoming calls ring on a targeted group of telephones called a Hunt group. When you designate a Hunt group, you define the group as a unique Directory Number (DN). This DN receives and distributes calls to the telephones assigned to the group.

This section provides the procedure for “To access the Hunt Group metrics”.



Note: You can include Hunt Group hourly metrics files with the CDR data files when they are transferred to the central server. For more information on configuring this option, refer to the *Call Detail Recording System Configuration Guide* (N0060599).

To access the Hunt Group metrics

To access the Hunt Group metrics to evaluate total call processing by hunt group member:

- 1 In the Element Manager, select the **Administration** tab, then the **Telephony Metrics** and **Hunt Group Metrics** in the navigation tree. See [Figure 43 on page 275](#).

Figure 43 Hunt Group Metrics Table

The screenshot shows the Nortel BCM 4.0 Element Manager interface. On the left is the Element Navigation Panel with a tree view where 'Hunt Group Metrics' is selected. The main area displays a table of Hunt Groups and a details panel for the selected group (01).

Hunt Group	Name	Total Calls	Answered: Total	Answered: Avg %	Answered: Avg Time (s)	Abandoned:
01	HG01	0	0	0	0	0
02	HG02	0	0	0	0	0
03	HG03	0	0	0	0	0
04	HG04	0	0	0	0	0
05	HG05	0	0	0	0	0
06	HG06	0	0	0	0	0

Details for Hunt Group: 01

Last Reset Time: 2005-09-15 11:59:20

Reset

Table 74 describes each field on the panel.

Table 74 Hunt Group Metrics fields

Attribute	Value	
Hunt Groups table		
Hunt group name	Read-only	Name of hunt group
Name	Read-only	Name entered on DN record

Table 74 Hunt Group Metrics fields (Continued)

Attribute	Value	
Total calls	Read-only	Total number of calls
Answered: Total	Read-only	Total number of answered calls
Answered Average%	Read-only	Average number of answered calls
Answered: Average time (s)	Read-only	Average answer time in seconds
Abandoned: Total	Read-only	Total number of abandoned calls
Abandoned: Average%	Read-only	Average number of abandoned calls
Busy: Total	Read-only	Total number of busy calls
Busy: Average%	Read-only	Average number of busy calls
Overflow: Total	Read-only	Total number of overflow calls
Overflow: Average%	Read-only	Average number of overflow calls
Time in Queue:	Read-only	Time in queue
Details		
Last Reset time	Read-only	Time and date format depends country profile of system.
Reset	<ol style="list-style-type: none"> 1. On the Hunt Groups table, select the hunt group member for which you want to reset the metrics. 2. In the lower frame, click the Reset button. 3. Click OK on the confirmation dialog box. 	

PSTN Fallback Metrics

When trunks are out of service, traffic can be switched to PSTN fallback lines. You can view how many fallback attempts and fallback failures occur within a specific period using the PSTN Fallback Metrics panel.

This section provides the procedure [“To access PSTN Fallback metrics”](#).

To access PSTN Fallback metrics

- 1 In the Element Manager, select the **Administration** tab, then click the **Telephony Metrics** and **PSTN Fallback Metrics** in the navigation tree.

The **PSTN Fallback metrics** display immediately. See [Figure 44 on page 277](#).

Figure 44 Fallback Metrics panel

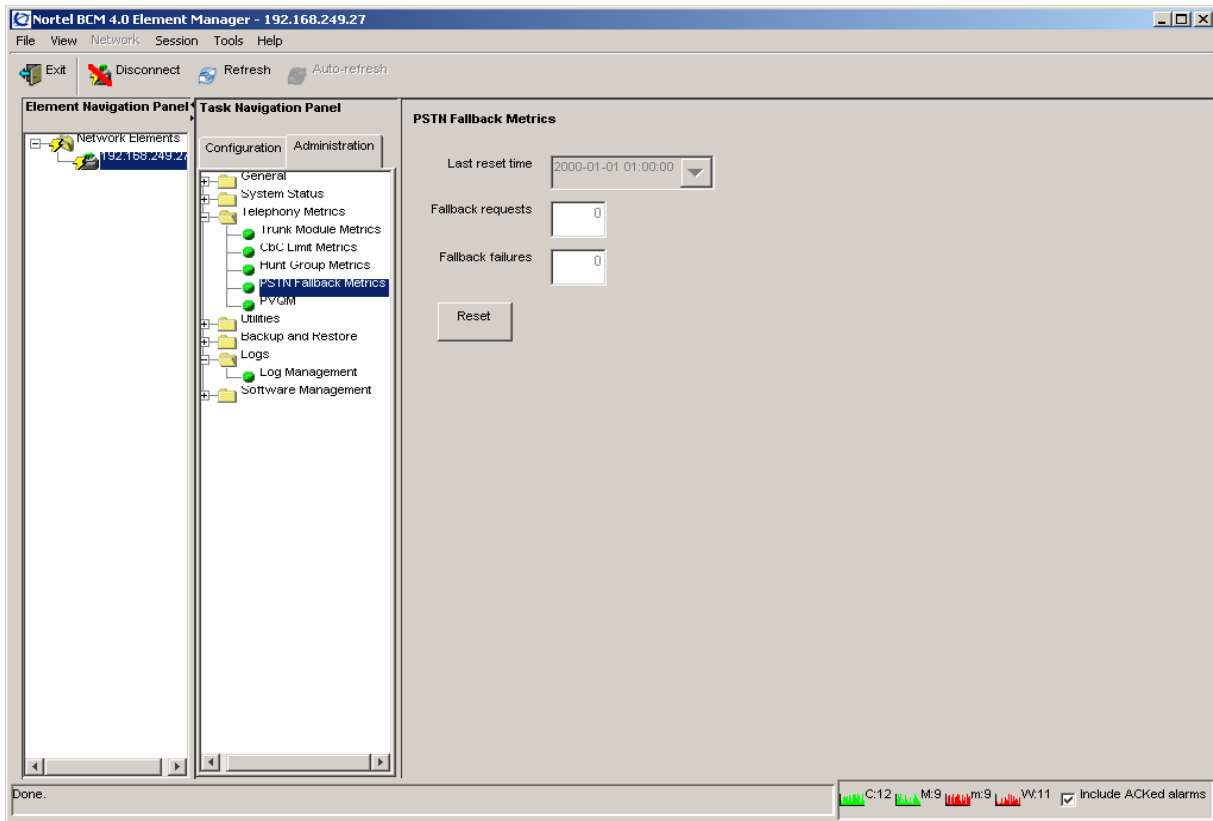


Table 75 describes each field on the panel.

Table 75 PSTN Fallback Metrics fields

Attribute	Value	Description
Last reset time	<read-only>	This is the date and time the metrics table was last reset.
Fallback requests	<read-only>	The number of calls that were not able to route through the preferred trunk.
Fallback failures	<read-only>	The number of calls that were not able to route through the fallback trunk. Note: If there is no fallback trunk assigned, all fallback requests will fail.
Actions		
Reset	Click this button to clear out the metrics table. The Last reset time will display the current date and time.	

Proactive Voice Quality Management

Proactive Voice Quality Management (PVQM) metrics allow you to monitor the quality of VoIP calls. You can also use the PVQM metrics to diagnose infrastructure problems in your network.

You can use PVQM to configure and report threshold violations for the following voice quality metrics:

- packet loss—packets lost in transit due to errors or network failures
- inter arrival jitter—the variable delay on a packet as it traverses a network
- round trip delay
- listening R—the transmission quality as experienced by the user; this metric reflects the segment of the call that is carried over the RTP session

There are two thresholds for PVQM metrics: Warning, and Unacceptable. A violation of the Warning threshold indicates that the voice quality is reduced but is still within an acceptable range. A violation of the Unacceptable threshold indicates a severe degradation in voice quality.

PVQM is fully supported on Phase 2 IP sets. Phase 1 IP sets support only the following PVQM metrics: packet loss, inter arrival jitter, and round trip delay. Table 76 lists the IP Phones that support PVQM.

Table 76 PVQM support

IP Set Type	Description
IP Phone 2001	Phase 2 firmware
IP Phone 2002	Phase 1 and Phase 2 firmware
IP Phone 2004	Phase 1 and Phase 2 firmware
IP Phone 2050	PC-based soft client
IP Phone 2007	Phase 2 firmware
IP Phone 1120E	Phase 2 firmware
IP Phone 1140E	Phase 2 firmware

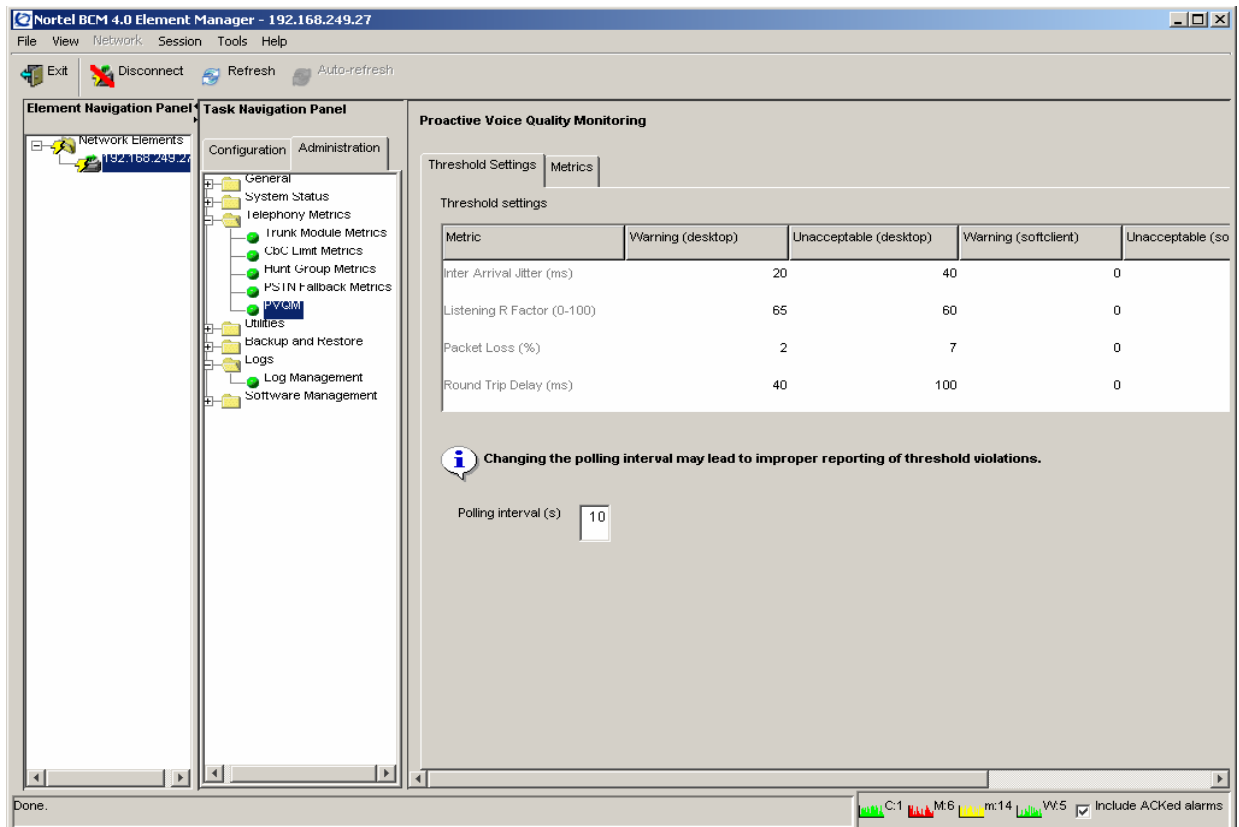
This section provides procedures [“To configure PVQM threshold settings”](#) and [“To access PVQM metrics”](#), and also provides information about [PVQM alarms](#).

To configure PVQM threshold settings

- 1 In the Element Manager, select the **Administration** tab, then click the **Telephony Metrics > PVQM > Threshold Settings** in the navigation tree.

The **Proactive Voice Quality Monitoring panel** displays. See [Figure 44 on page 277](#).

Figure 45 PVQM panel



2 Configure the threshold value for each PVQM metric. The options are:

- warning (desktop)
- warning (soft client)
- unacceptable (desktop)
- unacceptable (soft client)



Note: The term “desktop” indicates IP sets that are desktop models. The term “soft client” indicates IP sets that are software applications, such as the 2050 and the 2050MVC. Since desktop IP sets may provide better voice quality than software-based IP sets, you can specify different threshold levels for each type of IP set.

Table 79 describes the settings.

Table 77 PVQM threshold settings

Metric	Description	Value Range	Default Value for Warning thresholds	Default Value for Unacceptable thresholds
Packet Loss Rate	The fraction of RTP data packets from the source lost since the beginning of the call, expressed as a percentage.	0-100	1%	5%
Inter-arrival Jitter	The inter-arrival time of incoming RTP packets, as defined in RFC 1889. Expressed in milliseconds.	0-1000	50 ms	500 ms
RTCP Round Trip Delay	The round trip time of incoming RTP packets, as defined in RFC 1889. Measured in milliseconds.	0-1000	300 ms	500 ms
Listening R Factor	A scale from 0 (lowest quality) to 100 (highest quality) according to ITU-T G.107.	0-100	65	n/a

3 Configure the polling interval.

PVQM alarms

If an alarm is generated to report a threshold violation, additional information is included in the alarm to indicate the source of the alarm and provide other troubleshooting information.

Table 78 lists the abbreviations used in the alarm text to present this additional information.

Table 78 PVQM alarm information

Abbreviation	Attribute	Value	Description
cT	codec type	alphanumeric	Vocoder type used on this call
eT	endpoint type	S or D	S indicates softclient D indicates desktop
nLR	network loss rate	percentage, scaled by 256 (e.g. 354 = 1.4%)	Rate of network packet loss
dR	average discard rate	percentage, scaled by 256	Average rate of discards due to jitter
bD	burst loss density	percentage, scaled by 256	Density of lost and discarded packets during burst periods
bL	burst length	milliseconds	Average length of bursts
gD	gap loss density	percentage, scaled by 256	Density of lost and discarded packets during gap periods
gL	average length of gap	milliseconds	average length of gap

Table 78 PVQM alarm information

Abbreviation	Attribute	Value	Description
eSD	end system delay	milliseconds	Average end system delay on the call
aNL	noise level	dBm	Measured received silent period noise level
aSP	average signal level	dBm	Measured received signal level during talk spurts
rTT	local round trip time average	1/65536 of a second	Average round trip time on the call

For a list of the alarms generated by PVQM threshold violations, refer to [About BCM alarms](#) on page 148 and [List of BCM alarms](#) on page 157.

When a PVQM threshold is violated, the traps generated by the BCM can also be used by the AppManager VoIP performance monitoring product from NetIQ.

To access PVQM metrics

- 1 In the Element Manager, select the **Administration** tab, then click the **Telephony Metrics** and **PVQM > Metrics** in the navigation tree.

The **PVQM metrics** panel displays.

Figure 46 PVQM Metrics panel

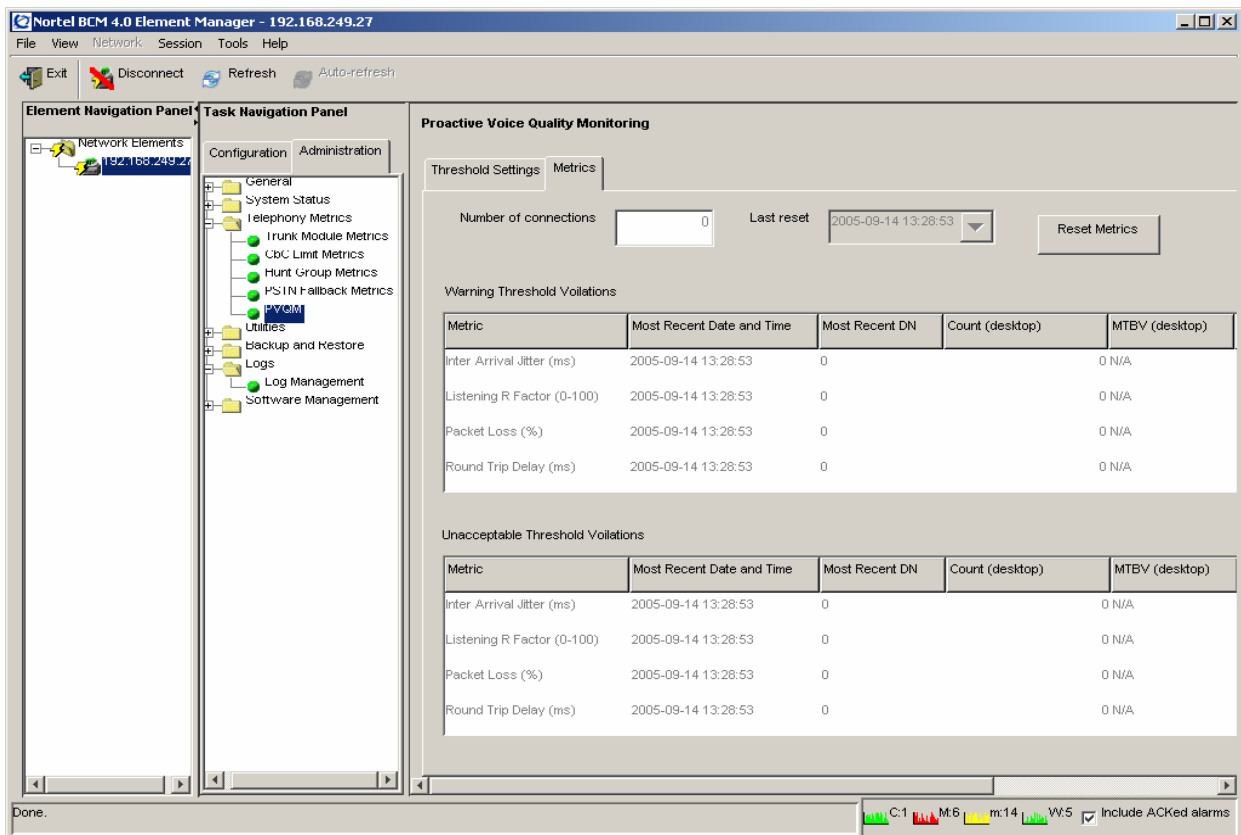


Table 79 describes each field on the panel.

Table 79 PVQM Metrics fields

Attribute	Value	Description
Number of connections	<read-only>	Displays the total number of connections by IP sets on the system since the last reset. This count includes non-interactive features such as dial tones, call progress tones, and music on hold.
Last rest	<read-only>	Displays the time of the last reset.
Most recent date and time	<read-only>	Displays the time of the most recent threshold violation.
Most recent DN	<read-only>	Displays the DN of the most recent threshold violation.
Desktop count	<read-only>	Displays the number of times a desktop client violated a threshold.
Soft client count	<read-only>	Displays the number of times a soft client violated a threshold.
Mean time between violations (MTBV) for desktop	<read-only>	Displays the mean time between threshold violations of a particular metric for desktop clients (measured in seconds).
Mean time between violations (MTBV) for soft client	<read-only>	Displays the mean time between threshold violations of a particular metric for soft clients (measured in seconds).

Table 79 PVQM Metrics fields

Attribute	Value	Description
Actions		
Reset Metrics		Click this button to clear out the metrics table. The Last reset time will display the current date and time.

Chapter 10

BCM Utilities

This chapter contains information about the utilities that are part of the BCM Element Manager. These utilities provide information about the BCM system, so that you can monitor and analyze system status and performance.

BCM utilities are:

- BCM Monitor
- Ping
- Trace Route
- Ethernet Activity
- Reset
- Diagnostic Settings
- Data Networking Utilities

About BCM Monitor

BCM Monitor is a stand-alone diagnostic application that the system administrator can use to view real-time system and IP telephony information about BCM200, BCM400, and BCM1000 systems.

BCM Monitor is included with the installation of the BCM Element Manager. You do not need to download the utility, unless you are an administrative user who requires access to only this management tool and you do not have or require the BCM Element Manager.

Using BCM Monitor, you can monitor the following:

- overall system status
- IP telephony functions of the BCM system, including IP device activity and VoIP session information
- utilization of resources
- operation of telephony applications (for example, Voice Mail and Contact Center)
- lines
- PRI, BRI, and IP trunks

You use BCM Monitor from a remote PC that has IP connectivity to the monitored system. You can open multiple instances of BCM Monitor on a single PC to monitor several remote BCM systems at the same time.

BCM Monitor supports BCM release 3.0 to BCM50 release 1.0. You can use BCM Monitor with BCM releases 2.5 and 2.5 FP1, but these releases provide only limited support for certain diagnostic queries. When you establish a connection with an earlier BCM system, unsupported information elements appear as “N/A” in BCM Monitor panels.

When BCM Monitor connects to a BCM system that does not support a particular information element, this is indicated by “N/A” in the relevant BCM Monitor panels.

BCM Monitor does not require significant hard disk space or memory on the client PC.

The following operating systems support BCM Monitor:

- Windows 98 SE
- Windows 2000
- Windows XP
- Citrix

When BCM Monitor is used on Windows 98, logon capabilities are reduced due to operating system limitations.

Installing BCM Monitor

BCM Monitor is included with the installation of the BCM Element Manager. You do not need to download the utility, unless you are an administrative user who requires access to only this management tool and you do not have or require the BCM Element Manager. If you do require BCM Monitor separately from the BCM Element Manager, you install the application from the BCM Web page.

The BCM Monitor provided with BCM 4.0 monitors BCM200, BCM400 and BCM1000 systems.

To install BCM Monitor separately from BCM Element Manager

- 1 On the BCM Web Page, click the **Administrator Applications** link.
The **Administrator Applications** page opens.
- 2 Click the **BCM Monitor** link.
The **BCM Monitor** page opens.
- 3 Click the **Download BCM Monitor** link.
- 4 Enter the System Administrator user name and password, and then click the **OK** button.
- 5 Select a folder where you want to store the BCM Monitor install file, and then click the **Save** button.
- 6 From your desktop, go to the folder where you saved the BCM Monitor install file, and then double-click the **BCMMonitor.exe** icon.
- 7 Follow the instructions on the installation wizard.

To remove BCM Monitor

- 1 In Windows, click the **Start** button.
- 2 Select **Control Panel**.
- 3 Double-click the **Add or Remove Programs** icon.

- 4 Select **BCM Monitor**, and then click the **Change/Remove** button.
- 5 Follow the on-panel removal instructions.

Connecting to a BCM system

For security reasons, the user on the computer on which the BCM Monitor runs must be authenticated by the BCM system.

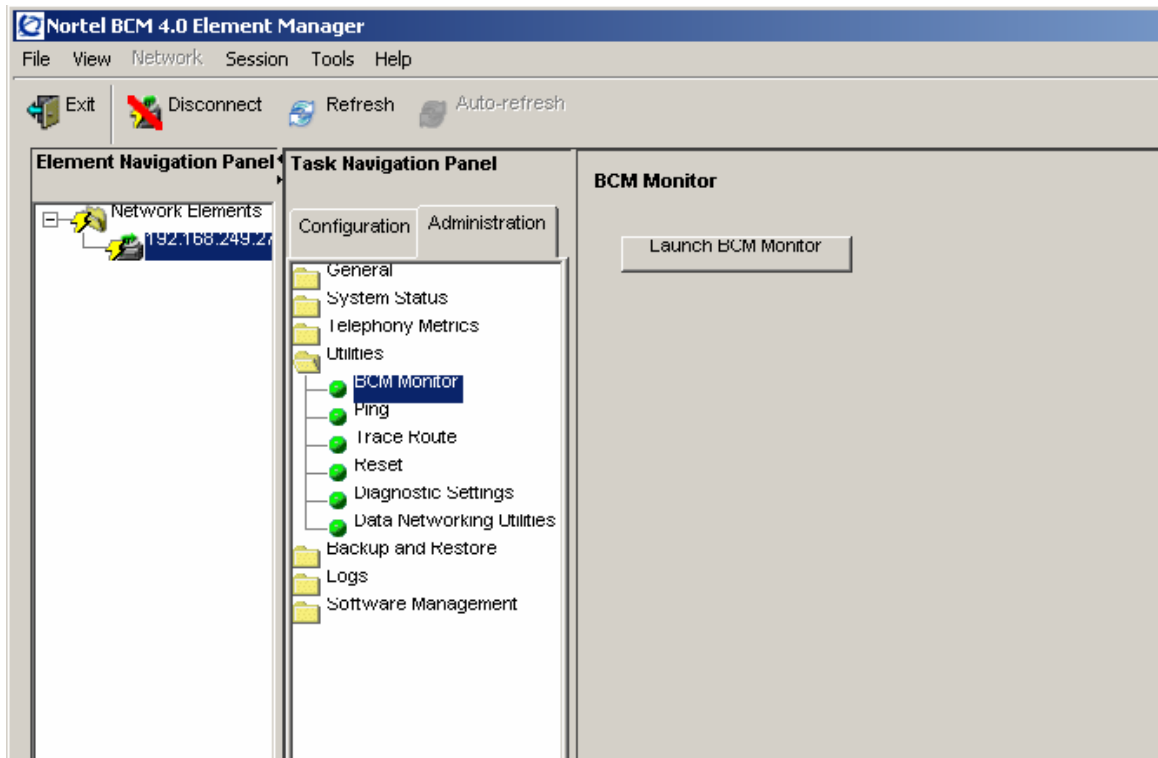
To start BCM Monitor without the BCM Element Manager

- 1 Double-click the **BCM Monitor** shortcut on your desktop or find **BCM Monitor** in your **Start/Programs** menu.
The **Enter Logon Information** window opens.
- 2 In the **System Name or IP Address** field, enter the system name of the BCM you want to monitor.
- 3 In the **Connect As** field, enter your BCM user name.
- 4 In the **Password** field, enter the password associated with your BCM user name.
- 5 Click the **Connect** button.
The **BCM Monitor** panel opens.

To start BCM Monitor from the BCM Element Manager

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **BCM Monitor**.
The BCM Monitor panel opens.

- 3 Click the **Launch BCM Monitor** button.
BCM Monitor opens and connects to the same BCM that the Element Manger is currently connected to.



Note: You can also launch the BCM Monitor from within the Element Manager by selecting **Tools > BCM Monitor**.

Disconnecting BCM Monitor from a BCM

On the **File** menu of the BCM Monitor, select **Disconnect from BCM**.
BCM Monitor disconnects from the BCM system and clears all the fields.



Note: If you do not want to connect to another BCM system, close the BCM Monitor application. This terminates the application and disconnects BCM Monitor from the BCM system.

To connect to a different BCM

- 1 On the **File** menu of the BCM Monitor, select **Disconnect from BCM**.
BCM Monitor disconnects from the BCM system and clears all fields.
- 2 On the **File** menu of the BCM Monitor, select **Connect to BCM**.
The **Enter Logon Information** window opens.

- 3 In the **System Name or IP Address** field, enter the system name of the BCM you want to monitor.
- 4 In the **Connect As** field, enter your BCM user name.
- 5 In the **Password** field, enter your password.
- 6 Click the **Connect** button.
The **BCM Monitor** panel opens.

Using BCM Monitor to analyze system status

System Administrators and support personnel can use BCM Monitor to obtain real-time troubleshooting data about the BCM system and to save data to generate system utilization and traffic reports.

BCM Monitor tabs provide information about the following:

- the overall BCM system
- utilization of resources
- operation of telephony applications (for example, Voice Mail, and Contact Center)
- lines
- PRI, BRI, and IP trunks

You can capture information about the BCM system by using:

- static snapshots
- dynamic snapshots

Static snapshots

You can capture an instantaneous snapshot of system information in a text file. You specify which BCM Monitor tab you want to capture and then save the information to the .txt file. The file name embeds the time, date, and BCM name information so that you can view the data using Microsoft Word or another application at another time.

Before you start a snapshot, you must configure static snapshot settings.

To configure static snapshot settings

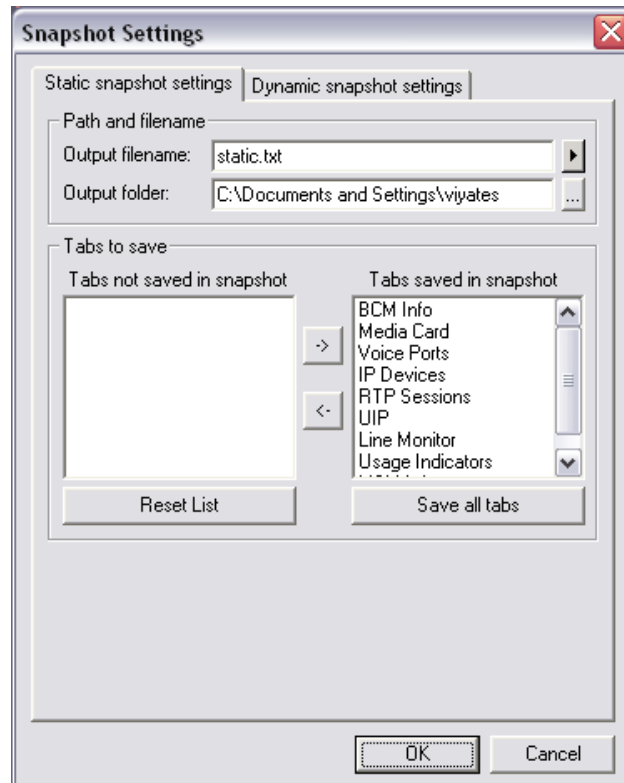
- 1 On the **File** menu, select **Snapshot Settings**.
The **Snapshot Settings** panel opens.
- 2 Click the **Static Snapshot Settings** tab.
- 3 In the **Path and Filename** area, enter the filename for the static snapshot in the **Output Filename** field. For additional options, click the Arrow button to the right of the **Output Filename** field.

4 Configure the Output Filename attributes.**Table 80** Output filename attributes

Attribute	Action
Auto-Increment Counter	Automatically increments the filename so that subsequent files do not overwrite earlier files. Adds <counter> to the filename in the Output Filename field.
BCM Name	Adds the name of the BCM to the filename. Position your cursor in the filename field where you want the name to be added. Adds <BCM name> to the filename in the Output Filename field.
Time	Adds the time to the filename. Position your cursor in the filename field where you want the name to be added. Adds <time> to the filename in the Output Filename field.
Date	Adds the date to the filename. Position your cursor in the filename field where you want the name to be added. Adds <date> to the filename in the Output Filename field.

- 5** In **Output Folder** field, enter the path of the folder where you want to store static snapshots. To browse for a folder, click the ... button to the right of the **Output Folder** field. The **Browse for Folder** dialog box opens.
- 6** Select a folder or make a new folder, and then click the **OK** button.

- 7 Select the BCM Monitor tabs that you want to include in static snapshots in the **Tabs Saved in Snapshot** box. For example, if you want snapshots to include information about voice ports, make sure that Voice Ports is included in the **Tabs Saved in Snapshot** box.



- 8 To remove tabs from the snapshots definition, select a tab from the **Tabs Saved in Snapshot** box and use the arrow button to move the tab to the **Tabs Not Saved in Snapshot** box.
- 9 Click the **OK** button.

To save a static snapshot

Once you have configured static snapshot settings, you can save static snapshot at any time.

- 1 While you are observing data on a tab, select **Save Static Snapshots** from the **File** menu, or press **CTRL S**.
All the tabs included in the snapshot definition are saved to a text file located in the folder you specified when you configured the static snapshot settings.

Dynamic snapshots

Dynamic snapshots record snapshots of system data that changes over time, such as CPU utilization and active calls. Dynamic snapshots are captured according to a frequency that you define. Once dynamic snapshots are enabled, BCM Monitor saves dynamic snapshot information to a file on your personal computer, using the comma separated value (csv) file format. You can open this file using a spreadsheet application, such as Microsoft Excel.

You can:

- specify which information you want to dynamically log
- enable or disable automated dynamic snapshots
- specify the interval of time between successive snapshots

Time intervals are specified in seconds. You can specify a maximum number of snapshots or infinite logging.

To configure dynamic snapshot settings

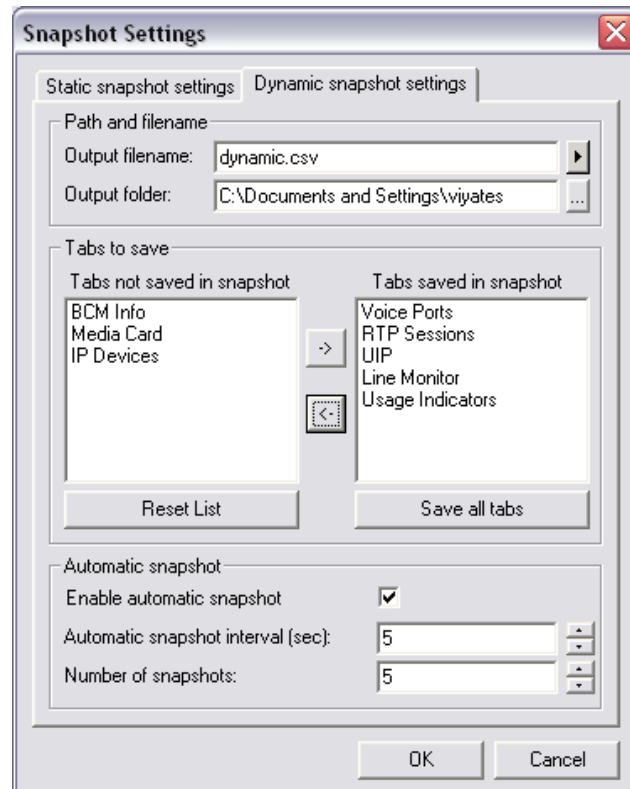
- 1 On the **File** menu, select **Snapshot Settings**.
The **Snapshot Settings** panel opens.
- 2 Click the **Dynamic Snapshot Settings** tab.
- 3 In the **Path and Filename** area, enter the filename for the dynamic snapshot in the **Output Filename** field. For additional options, click the Arrow button to the right of the **Output Filename** field.
- 4 Configure the Output Filename attributes.

Table 81 Output filename attributes

Attribute	Action
Auto-Increment Counter	Automatically increments the filename so that subsequent files do not overwrite earlier files. Adds <counter> to the filename in the Output Filename field.
BCM Name	Adds the name of the BCM to the filename. Position your cursor in the filename field where you want the name to be added. Adds <BCM name> to the filename in the Output Filename field.
Time	Adds the time to the filename. Position your cursor in the filename field where you want the name to be added. Adds <time> to the filename in the Output Filename field.
Date	Adds the date to the filename. Position your cursor in the filename field where you want the name to be added. Adds <date> to the filename in the Output Filename field.

- 5 In **Output Folder** field, enter the path of the folder where you want to store the static snapshots. To browse for a folder, click the ... button to the right of the **Output Folder** field. The **Browse for Folder** dialog box opens.
- 6 Select a folder or make a new folder, and then click the **OK** button.

- 7 Select the BCM Monitor tabs that you want to include in dynamic snapshots in the **Tabs Saved in Snapshot** box. For example, if you want the snapshots to include information about voice ports, make sure that Voice Ports is included in the **Tabs Saved in Snapshot** box.

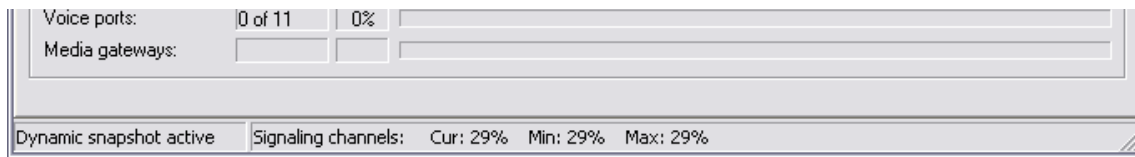


- 8 To remove a tab from the snapshots, select a tab from the **Tabs Saved in Snapshot** box and use the arrow button to move the tab to the **Tabs Not Saved in Snapshot** box.
- 9 In the **Automatic Snapshot** area, click the **Enable Automatic Snapshot** check box to enable automatic snapshots. If you disable automatic snapshots, BCM Monitor will take a single snapshot instead of a series of snapshots. If you enable automatic snapshots, the **Automatic Snapshot Interval (sec)** field and the **Number of Snapshots** field become available.
- 10 In the **Automatic Snapshot Interval (sec)** field, enter the interval in seconds between successive automatic snapshots.
- 11 In the **Number of Snapshots** field, enter the number of snapshots from 1 to Infinite.
- 12 Click the **OK** button.

Starting a dynamic snapshot

Once you have configured dynamic snapshot settings, you can start a dynamic snapshot. Once you start dynamic logging, BCM Monitor continues taking snapshots until it reaches the number of snapshots you defined when you configured dynamic snapshot settings, or until you stop a dynamic snapshot.

When you start dynamic snapshots, the BCM Monitor status bar displays “Dynamic snapshot active;” the figure below shows the status bar portion of the panel.



On the **File** menu, select **Dynamic Snapshot, Start**.

BCM Monitor starts taking snapshots and saves the snapshot data in a file located in the folder you specified when you configured the dynamic snapshot settings.

Stopping a dynamic snapshot

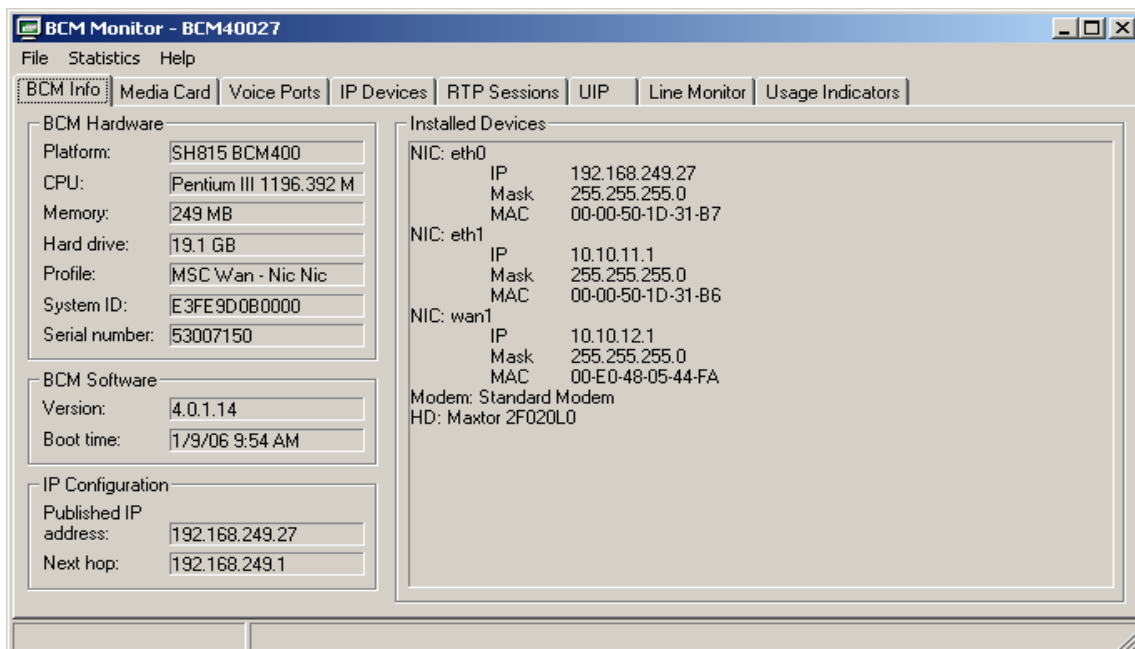
On the **File** menu, select **Dynamic Snapshot, Stop**.

BCM Info tab

The BCM Info tab displays static information about the BCM system, such as:

- information about the main hardware components of the BCM system
- software installed on the system
- IP configuration data

You can use the information on this tab to verify the software release level of the BCM, the published IP address and default gateway of the BCM main unit, the last time the BCM was rebooted, as well as IP address information about other Ethernet interfaces on the BCM main unit.



The installed devices on the BCM Info tab are displayed as follows:

- Eth0 — indicates a LAN internal to the BCM system.
- Eth1 — indicates a customer LAN. This is the LAN accessible to the customer through ports 1, and 2 on the front panel of the BCM main unit.
- WAN 1—This is a dedicated LAN port accessible as port 0, the left-most Ethernet port on the front panel of the BCM main unit.

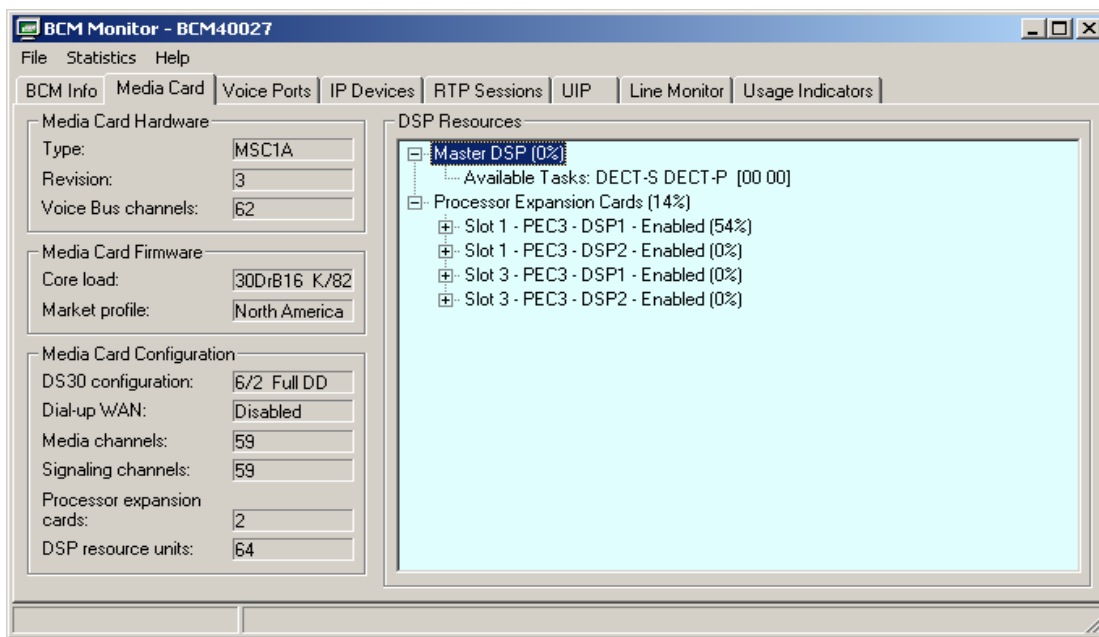
Media Card tab

The Media Card tab provides information about the telephony system of the BCM. This tab provides the following information for a BCM:

- the hardware of the BCM main unit on which the telephony software resides
- the telephony software component release level and market profile
- configuration information, such as media channels (64 Kbps B channels), and the total number of logical DSP resource units
- the available tasks and tasks in service

The Media Card tab provides the following information for BCM systems:

- Media Card hardware, including type and revision, and voice bus channels
- Media Card firmware, including core load and market profile
- configuration information, such as DS30 configuration, dialup WAN, media channels (64 kbps B channels), signaling channels (D channels), processor expansion cards, and the total number of logical DSP resource units
- the available DSP tasks and DSP tasks in-service

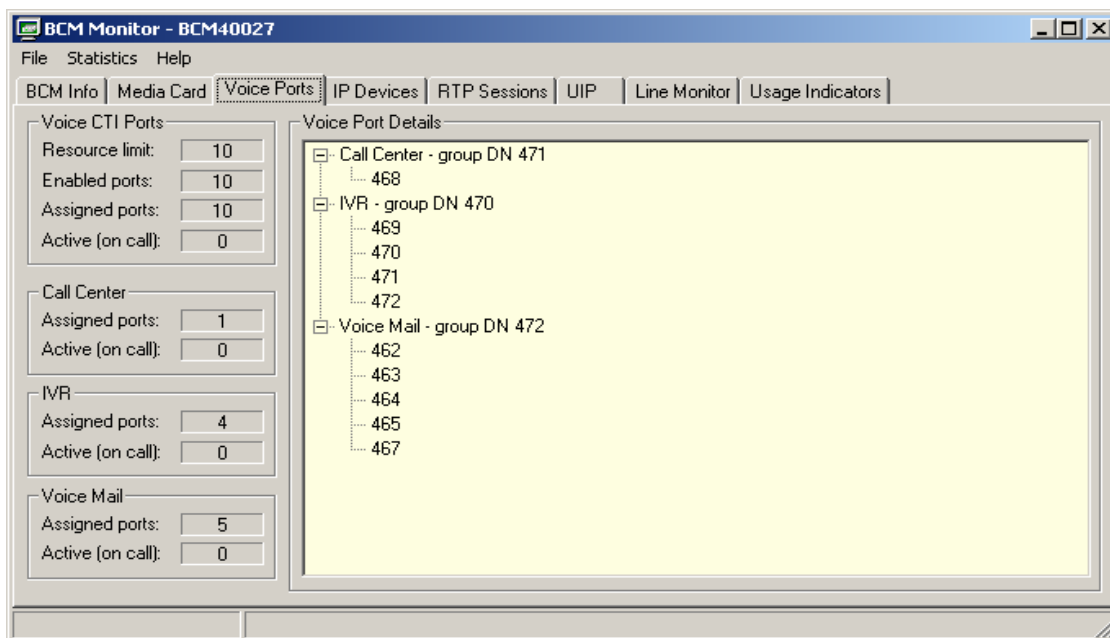


Voice Ports tab

The Voice Ports tab displays real-time information about configured voice ports. A configured voice port is a logical device used for Voice Mail, Contact Center, and IVR. Values associated with voice ports change with the usage of the switch, and are therefore well suited for dynamic logging to view trends relating to system activity.

You can use the Voice Ports tab to view the following information:

- information about voice ports used by the Voice CTI services, such as the resource limit and how many voice CTI ports are enabled and assigned
- how many Voice CTI ports are assigned to Contact Center, Voice Mail, and, for BCM3.x, to IVR
- how many assigned ports are currently active, and the DN of the user assigned to the port
- voice port details, which show information about activity on each enabled voice port



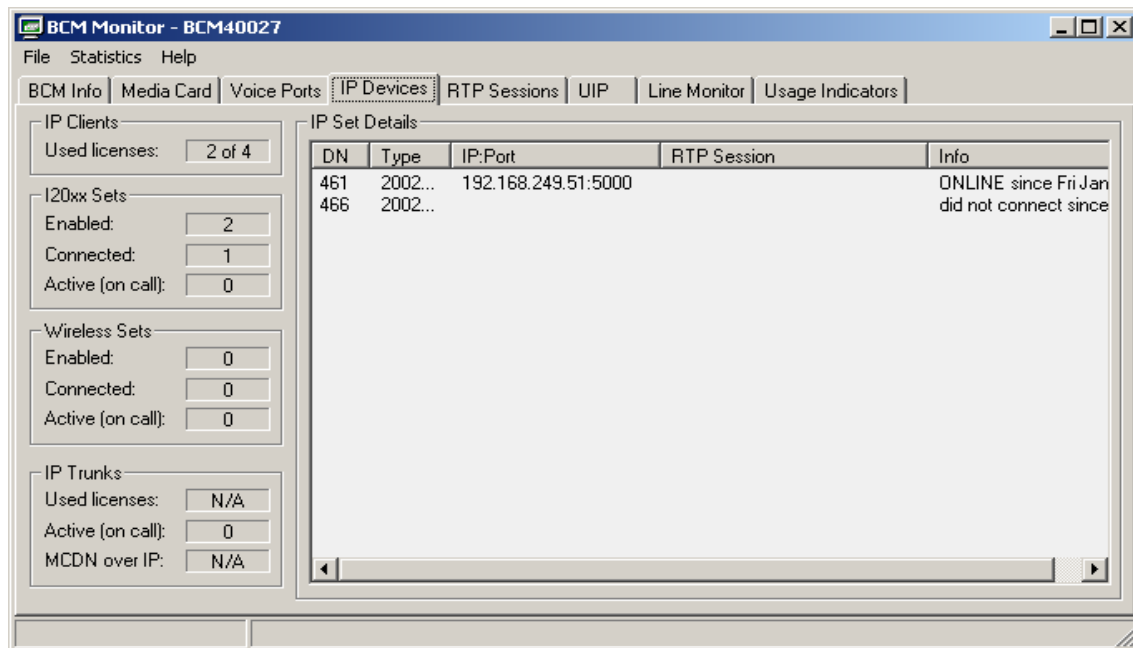
IP Devices tab

The IP Devices tab displays information about call activity associated with IP sets, wireless sets, and IP trunks. IP sets include IP clients (for example, the i2050 softphone), i200x IP sets, and wireless sets.



Note: IVR is supported on the BCM3.x release level for BCM200, BCM400, and BCM1000, but it is not supported on the BCM.

The IP Devices tab shows how many sets in each category are enabled, connected, and active. The tab displays the DN, IP address, and type of set for each active call.



RTP Sessions tab

The RTP Sessions tab shows details about RTP (Real Time Protocol over UDP) sessions, which involve either the BCM system or an IP set controlled by the BCM system.

You can use the information in this tab to monitor the direct path between two IP sets.

The tab displays information about:

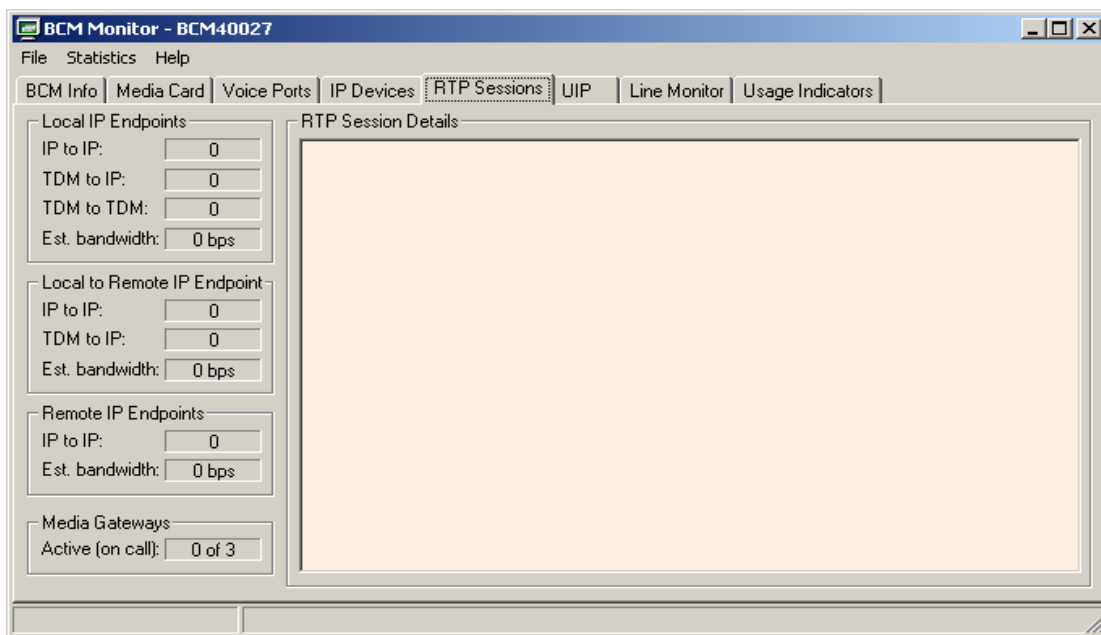
- local IP endpoints (two sets both connected to the BCM)
 - combinations of IP to IP, TDM to IP, and TDM to TDM
 - an estimate of network traffic generated by RTP sessions between TDM devices or local IP devices
- local to remote IP endpoints
 - combinations of IP to IP, TDM to IP
 - an estimate of network traffic generated by RTP sessions
- remote IP endpoints (IP to IP)
 - an estimate of network traffic generated by RTP sessions between remote IP endpoints
- the number of allocated Media Gateways that are providing a connection between a TDM device and an IP endpoint

The RTP Sessions tab also displays detailed information about active RTP sessions. The RTP Session Details area displays the following line for each active session:

```
{IP Endpoint A}{IP Trunk X}<stream info>{IP Trunk Y}{IP Endpoint B} Codec FPP
Details
```

The IP Endpoint tokens contain information about each IP endpoint (type, DN, IP address, RTP port number). The IP Trunk tokens contain information about the IP Trunk used by each endpoint (if no trunk is used, the token is omitted). The stream info token shows which RTP streams are enabled between the two endpoints. The Codec token describes the codec type used for the RTP session. The FPP shows the negotiated value of frames per packet. The Details token shows additional information about the RTP session.

BCM Monitor can display real-time RTP session statistics for sessions that involve at least one media gateway. These statistics include information about duration of the session, the number of bytes and packets sent or received per second and per session. These statistics are useful for troubleshooting packet loss or routing problems. For information about statistics, see [“Using statistical values” on page 304](#).



UIP tab

The UIP tab displays information about Universal ISDN Protocol (UIP) activity associated with IP trunks (MCDN messages), BRI loops, and PRI loops on the BCM.

You can monitor UIP modules by:

- enabling or disabling monitoring of MCDN over IP messages for calls made over IP trunks
- selecting and configuring a bus used by expansion modules
- selecting the type of ISDN module connected to the expansion unit
- enabling or disabling monitoring of loops on BRI modules connected to the expansion unit

Enabling UIP message monitoring



Caution: Monitoring UIP messages may affect the performance of the BCM system or connected peripherals. For example, if IP sets or voice ports make or receive a high number of calls over PRI trunks, monitoring UIP increases the amount of signalling data and may increase the response time for IP sets or voice ports. Therefore, it is strongly recommended that you monitor only a single UIP module at a time and restrict the monitoring time.

- 1 Click the **UIP** tab.
- 2 To enable or disable monitoring of MCDN over IP messages for calls made over IP trunks, select or clear the **MCDN over IP** check box.
- 3 To select an expansion module, select one of the following from the Bus selection field:
 - Bus 5
 - Bus 6
 - Bus 7
 - Bus 8
- 4 Select the type of ISDN module or modules:
 - PRI — enables monitoring of a DTI module
 - BRI — enables monitoring of BRI loops

For example, you can monitor UIP messages for loops 1 and 2 of a BRI module connected to Bus 5 and a PRI module connected to Bus 6. To do this, you would:

- Select Bus 5 - BRI, then select Module 1 - Loop 1
- Select Bus 5 - BRI, then select Module 1 - Loop 2
- Select Bus 6 - PRI

To disable monitoring of UIP messages

- 1 Click the **UIP** tab.
- 2 Select the module on which monitoring is to be disabled.
- 3 For the selected module, click the **Off** radio button.



Note: To disable monitoring of UIP messages for MCDN over IP, you must deselect the MCDN over IP check box.

To log UIP data

- 1 Click the **UIP** tab.
- 2 Select the **Log UIP Data** check box.

You can log UIP data to track the most recent 20 UIP messages. If you enable UIP logging, BCM Monitor writes UIP messages in log files, which are created in the log folder in the BCM Monitor startup directory. One log file is generated for each monitored system and each module or loop. Log files are named IPAddr_MCDN.log, IPAddr_PRI_BusX.log, and IPAddr_BRI_BusXModuleYLoopZ.log.

To view UIP log files

- 1 Locate the log file that is saved to the BCM Monitor startup directory.
- 2 Open the log file with a text editor, such as Notepad, or a spreadsheet application, such as Microsoft Excel.

You can view the amount of time after which monitoring of selected UIP modules will be disabled, and you can disable the monitoring timeout. If you are investigating intermittent problems, an extended monitoring period may be required. In this case, disable the monitoring timeout and enable logging of UIP data.

To configure timeout settings

- 1 Click the **UIP** tab.
- 2 To disable the timeout, select the **Disable Timeout** check box.



Caution: Before you disable the monitoring timeout, consider the potential impact on system performance if the BCM system handles a high number of PRI calls.

Viewing UIP message details

The **Universal ISDN Protocol Messages** section displays a folder for each UIP module that is enabled for monitoring. Each folder displays up to 20 most recent UIP messages. You can expand UIP messages that contain at least one information element. An information element can contain data, which you can expand as well.

Each UIP message line contains the following information:

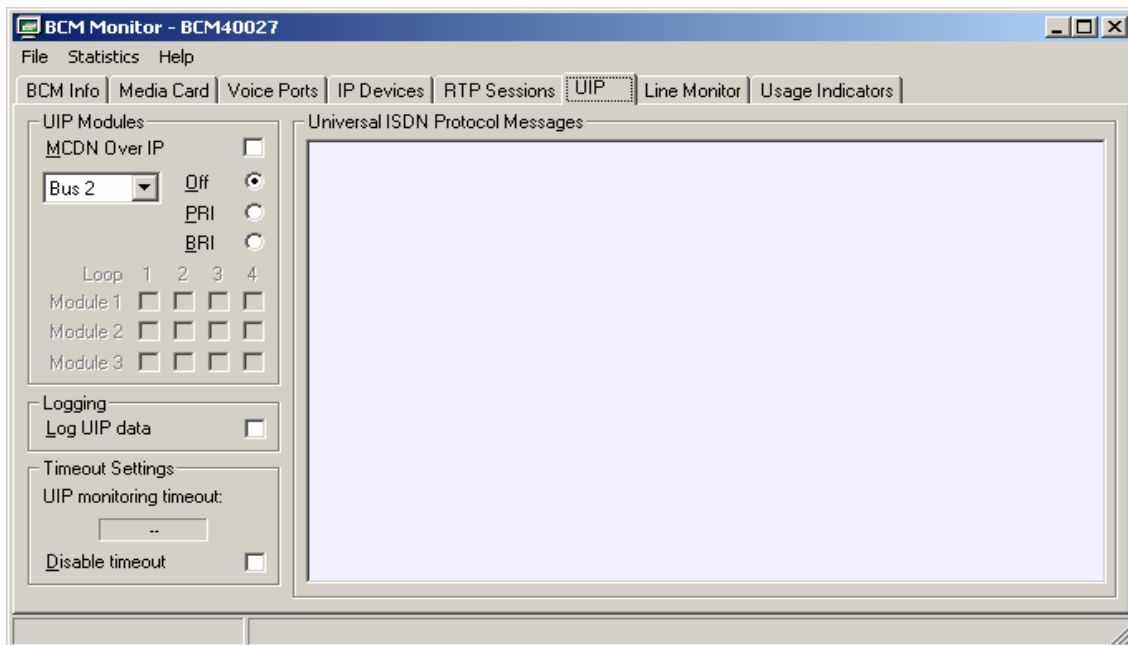
- the direction in relation to the BCM (> for incoming or < for outgoing)
- the message type (CC for Call Control, MTC for Maintenance)
- the direction in relation to the call reference origin (> Cref Origin for incoming or < CRef Origin for outgoing)
- the message name (or a hexadecimal value if the name is unknown)
- additional data extracted from information elements

To expand a UIP message

- 1 Click the **UIP** tab.
The **Universal ISDN Protocol Messages** area displays detailed information about monitored UIP modules.
- 2 In the **Universal ISDN Protocol Messages** area, double-click a UIP message.
Information elements appear below the UIP message.

To clear UIP message details

- 1 Click the **UIP** tab.
The **Universal ISDN Protocol Messages** area displays detailed information about monitored UIP modules.
- 2 In the **Universal ISDN Protocol Messages** area, right-click a UIP message or information element and select **Clear Tree**.
The entire tree is cleared from the **Universal ISDN Protocol Messages** area.



Line Monitor tab

The Line Monitor tab shows the status of lines on the BCM system. You can view the number of active lines, and view all lines on the BCM system, including inactive lines.

For all lines displayed in the line monitor area, you can view the following information:

- line name — displays the line number and line name
- direction — “Outgoing” indicates that the call originated from the BCM; “Incoming” indicates that the call originated from outside and is directed at the BCM

- start time — displays the time and date on which the call started
- user — displays the DN and name of the BCM user
- state — displays Idle if there is no active call on the line; displays Dialing if the BCM user is in the process of dialing digits to place a call; displays Alerting if a call has been received on the line and a BCM user's phone is ringing; displays Connected if the line has a connected call; displays Held if the line has a call on hold.

In the line monitor area, colours are used to indicate the state of each line:

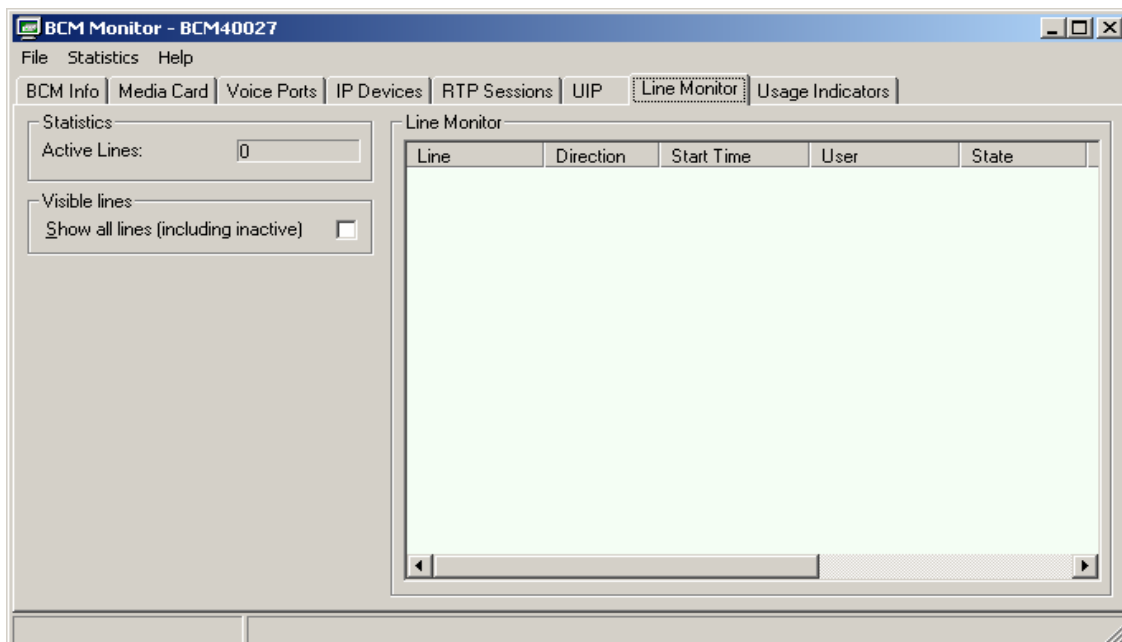
- gray represents lines that are idle
- blue represents lines that are active
- red represents lines that are alerting
- dark red represents lines that are on hold

To view all lines

1 Click the **Line Monitor** tab.

2 Click the Show All Lines (Including Inactive) check box.

The Line Monitor area displays all lines on the BCM system. For lines displayed in light gray, previous calls are shown until a new call is placed or received on that line.



Usage Indicators tab

The Usage Indicators tab displays real time information about the BCM system.

The tab displays the following information:

- BCM system data, including CPU and memory use
- resources used on the Media Card, including signaling channels, media channels, voice bus channels, and DSP resources
- active telephony devices, such as IP trunks, IP sets, voice ports, and media gateways

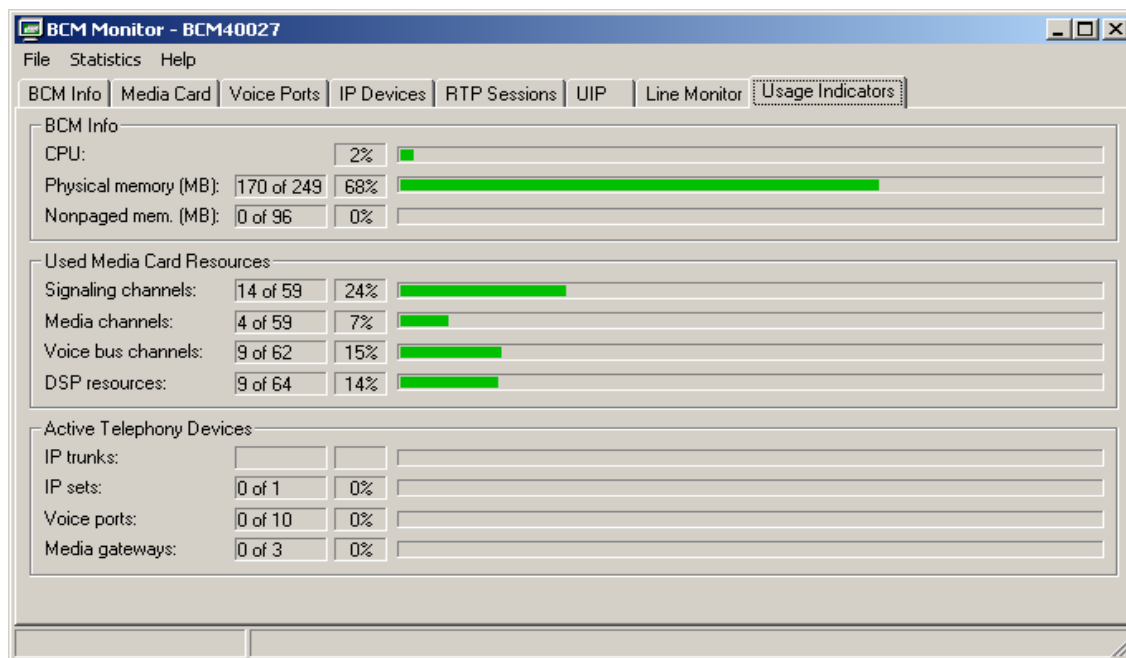
The information is displayed as an absolute figure and as a percentage of the resource used. You can capture a static snapshot of this information or log it dynamically. For more information about snapshots, see [“Using BCM Monitor to analyze system status” on page 289](#).

Usage values

Usage values are accompanied by a colored bar. [Table 82](#) describes the usage value indicators and recommended actions.

Table 82 Usage indicators

Indicator color	Indicator meaning	Recommended action
Green	Usage values are normal.	None.
Yellow	Potential resource problem.	Further investigation is recommended if an indicator remains yellow for an extended period.
Red	Critical resource problem.	Further investigation is recommended if an indicator remains red for more than a few seconds.



Using statistical values

BCM Monitor stores the minimum and maximum values for many of the statistics that appear on BCM Monitor tabs. A statistic must be a numeric value and must change over time; that is, the value cannot be a static value. Examples of statistics that have minimum and maximum values are CPU usage, Active Lines, and Enabled i20XX sets. Examples of statistics that do not have minimum and maximum values are Dial-up WAN (which is not a numeric value) and Serial Number (which is static).

The values that BCM Monitor displays are the minimum and maximum values for the current BCM Monitor session. The minimum and maximum values are reset when you exit the BCM Monitor.

You can do the following with statistical values:

- view minimum and maximum values
- view the date and time of minimum and maximum values
- reset minimum and maximum values

Viewing minimum and maximum values

Click the value on the BCM Monitor panel for which you want to view the minimum or maximum value.

The current (Cur:), minimum (Min:), and maximum (Max:) values appear on the Status bar at the bottom of the panel.

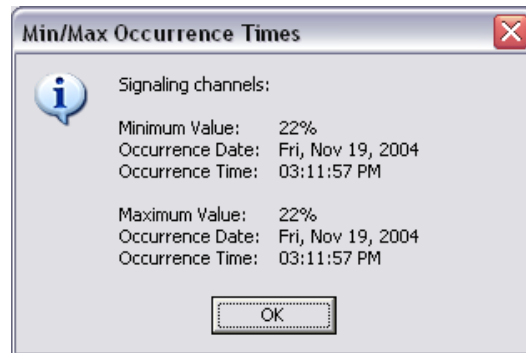
The three values remain on the Status bar until you select another value. These values also continue to change as the value for the selected statistic changes. This is useful if you want to monitor a single statistic on one panel while you are viewing the information on another panel.

Viewing the date and time of minimum and maximum values

When BCM Monitor stores the minimum and maximum value, it also stores the date and time when the minimum or maximum occur.

To view the date and time of minimum and maximum values

- 1 Select the value for which you want to view the minimum or maximum value.
- 2 From the **Statistics** menu, select **Show Min/Max Times**.
A dialog box appears with the date and time when the minimum and maximum values occurred.



- 3 Click the **OK** button to close the dialog box.

Resetting minimum and maximum values

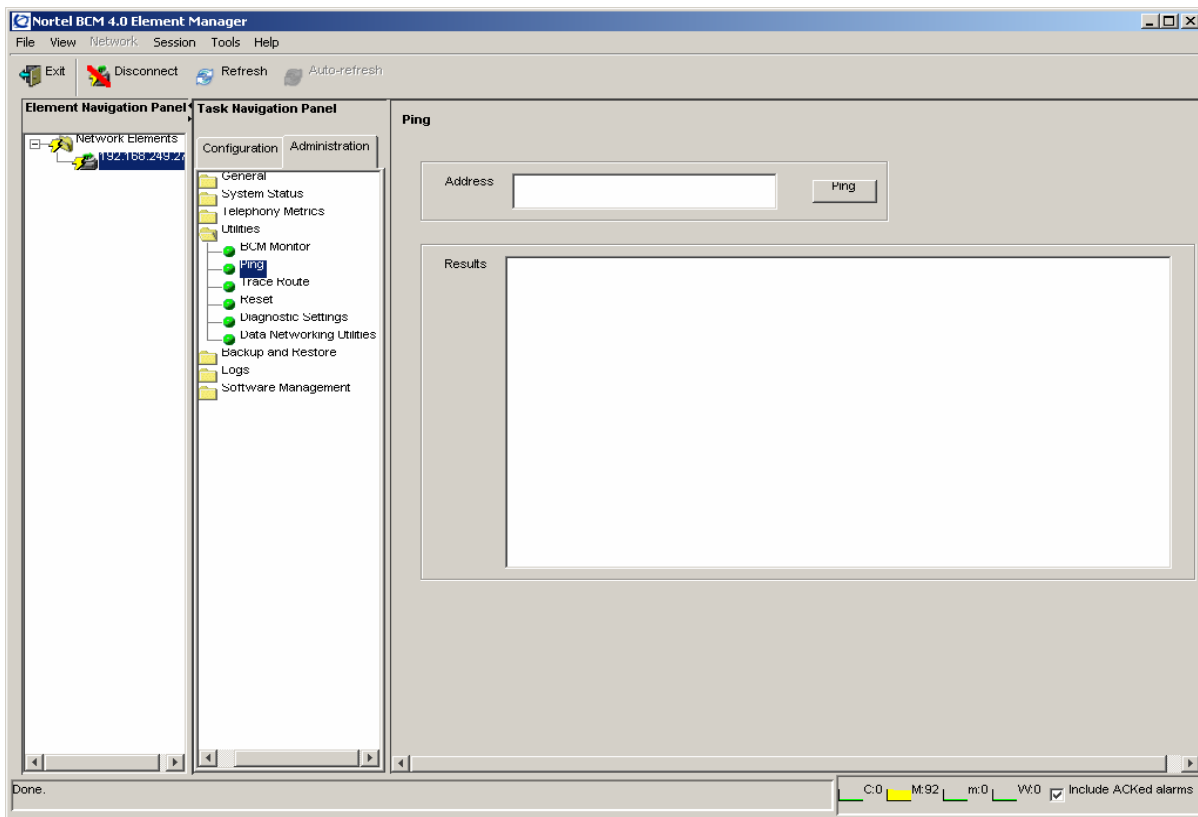
When you reset the minimum and maximum values, the current minimum and maximum values are deleted and BCM Monitor starts recording new values.

To reset the minimum and maximum values for a statistic

- 1 Click the value you want to reset.
- 2 Do one of the following:
 - a On the **Statistics** menu, click **Reset Current Min/Max**.
 - b To reset the minimum and maximum values for all statistics, select **Reset All Min/Max** from the **Statistics** menu.

Ping

Ping (Packet InterNet Groper) is a utility that you can use to verify that a route exists between the BCM and another device. Ping sends an ICMP (Internet Control Message Protocol) echo request message to a host. It expects an ICMP echo reply, which you can use to measure the round-trip time to the selected host. You can measure the percent packet loss for a route by sending repeated ICMP echo request messages.



To ping a device

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Ping**.
The **Ping** panel opens.
- 3 In the **Address** field, enter the IP address of the element you want to ping.
- 4 Click the **Ping** button.
The results appear in the **Results** area.



Note: Establishing a PPP link over a modem make take some time. If the Ping utility times out before the modem call can be established, click the Ping button again.

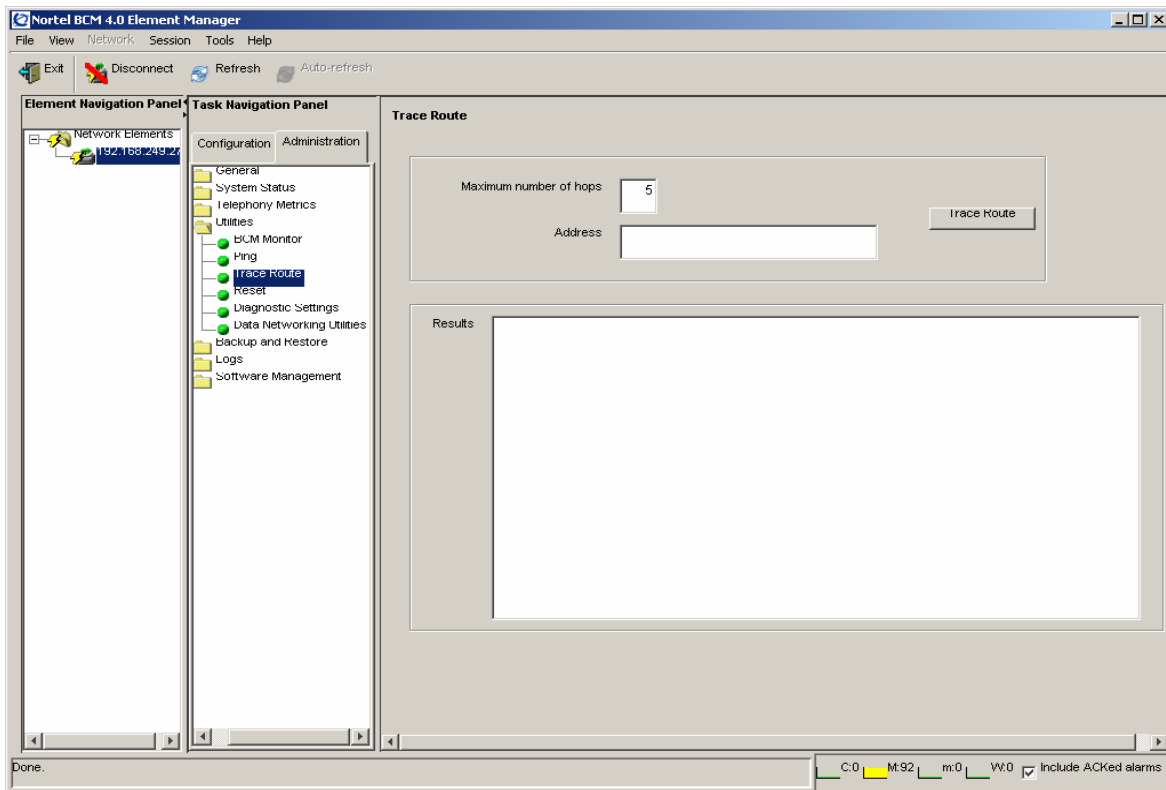
Trace Route

You can use Trace Route to measure round-trip times to all hops along a route. This helps you to identify bottlenecks in the network. Trace Route uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. Instead, a router discards the packet and returns to the originating IP address an ICMP time exceeded message.

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

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

An example trace route is as follows:



To perform a trace route

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Trace Route**.
The Trace Route panel opens.

- 3 In the **Maximum Number of Hops** field, enter the maximum number of hops on the route. The default is 5 hops.
- 4 In the **Address** field, enter the IP address of the element for which you want to perform a trace route.
- 5 Click the **Trace Route** button. The results are displayed in the **Results** area.

Reset

You can use the Reset utility to:

- reboot the BCM system
- shut down the BCM system
- perform a warm reset of telephony services
- perform a cold reset of telephony services

Table 83 lists the Reset functions.

Table 83 Reset functions

Function	Description	Impact
Reboot BCM System	Restarts the operating system of the BCM system	Temporarily stops all services on the system. Restarts all services. This operation does not affect configuration parameters or programming.
Shut down BCM system	Shut down the BCM system.	Stops all services on the BCM to allow you to power down the system safely.
Warm Reset Telephony Services	Restarts telephony services running on the BCM system	Restarts all telephony services, including LAN CTE, Voicemail, and IP telephony. This operation does not affect configuration parameters or programming.
Cold Reset Telephony Services	Resets telephony programming of the BCM system to the factory defaults for that software level	Affects all telephony services, including LAN CTE, Voicemail, and IP telephony. Telephony services restart with all telephony programming at default values for the specified region, template, and start DN, for the current software release level.

Rebooting the BCM system



Caution: Rebooting the BCM system temporarily stops all services running on the system.

To reboot the BCM

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Reset**.
The **Reset** panel opens.
- 3 Click the **Reboot BCM System** button.
A confirmation dialog box opens.
- 4 Click the **OK** button.
The operating system of the BCM restarts.

Shutting down the BCM



Caution: Rebooting the BCM system stops all services running on the system.

To shut down the BCM

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Reset**.
The **Reset** panel opens.
- 3 Click the **Shutdown BCM System** button.
A confirmation dialog box opens.
- 1 Click the **OK** button.
The operating system of the BCM shuts down.

Performing a warm reset of BCM telephony services



Caution: All active calls on the BCM system will be dropped.

To perform a warm reset of BCM telephony services

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Reset**.
The **Reset** panel opens.

- 3 Click the **Warm Reset Telephony Services** button.
A confirmation dialog box opens.
- 4 Click the **OK** button.
All telephony services are restarted, including LAN CTE, Voicemail, and IP telephony.

Performing a cold reset of BCM telephony services



Caution: Performing a cold reset of telephony services erases all telephony programming, as well as all Voice Message mailboxes and messages. Telephony services will restart with all telephony programming at default values for the specified region, template, and start DN, for the current software release level.

To perform a cold reset of BCM telephony services

- 1 Click the **Administration** tab.
- 2 Open the **Utilities** folder, and then click **Reset**.
The **Reset** panel opens.
- 3 Click the **Cold Reset Telephony Services** button.
The **Cold Reset Telephony** dialog box displays.
- 4 Configure the Cold Reset Telephony attributes.

Table 84 Configure Hard Reset Telephony attributes

Attribute	Action
Region	Specify the startup region.
Template	Specify the startup template. Options are: PBX or DID.
Start DN	Specify the startup DN. The default value is 221.
Force MSC download	Check the box to force the MSC core download.

- 5 Click the **OK** button.
All telephony services are reset, including LAN CTE, Voicemail, and IP telephony.

Diagnostic settings

Diagnostic settings is a utility that allows you to determine the level of system reporting you require for released ISDN or VoIP calls. You can choose to have no text, a simple explanation, or a detailed explanation.

This section provides the procedures [“To set Release Reasons”](#).

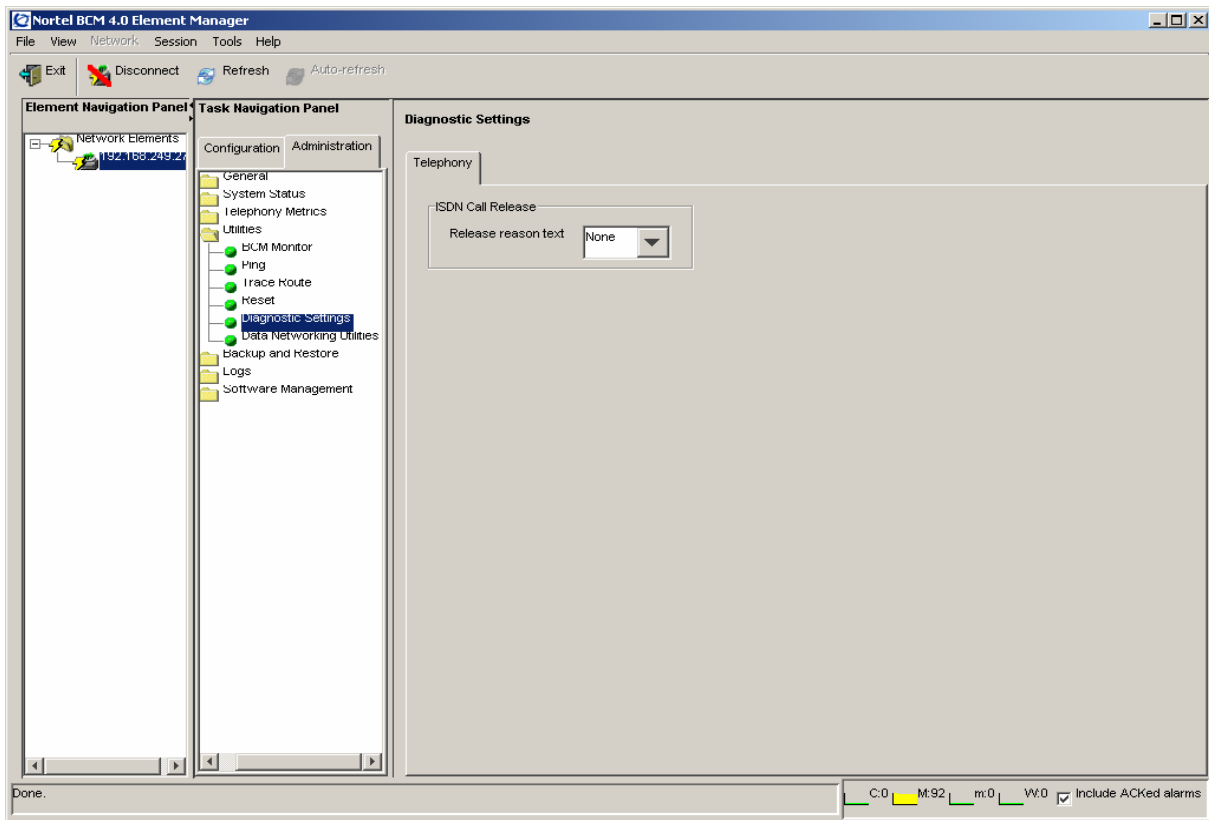
To set Release Reasons

To set Release reasons, follow these steps:

- 1 Click **Administration, Utilities, Diagnostic settings**.
- 2 Click the **Telephony** tab.

The **Release Reasons** panel appears. See [Figure 47](#).

Figure 47 Telephony diagnostic settings



- 3 From the Release Reason drop-down menu, select the level of reporting that you require. Table 85 lists the possible values for Release reasons.

Table 85 Release reasons

Attributes	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 diagnostic purposes only.

Table 85 Release reasons

Attributes	Values	Description
Detailed	No setting	A detailed explanation of the Cause code is provided.
Cause Code	check box	This check box appears when you select Simple in the Release Reason Text drop-down menu. When you select the check box, only the cause code accompanies a dropped call notification.

Data Networking Utilities

The Data Networking Utilities panel allows you to generate information needed to troubleshoot and debug the system. You can use the utility to generate the following information:

- route table
- IP stack route table
- TCP/IP network connections
- hostname
- ARP table
- IP configuration
- router IP configuration
- router IP route
- DNS address

For example, you can use the **TCP/IP network connections** command to generate a list of active internet connections.



Note: You must configure the DNS IP address before you can execute the commands on the Data Networking Utilities panel. For information about how to set the DNS IP address, see the *BCM 4.0 Networking Configuration Guide* (N0060606).

This section provides the procedure [“To use data networking utilities”](#).

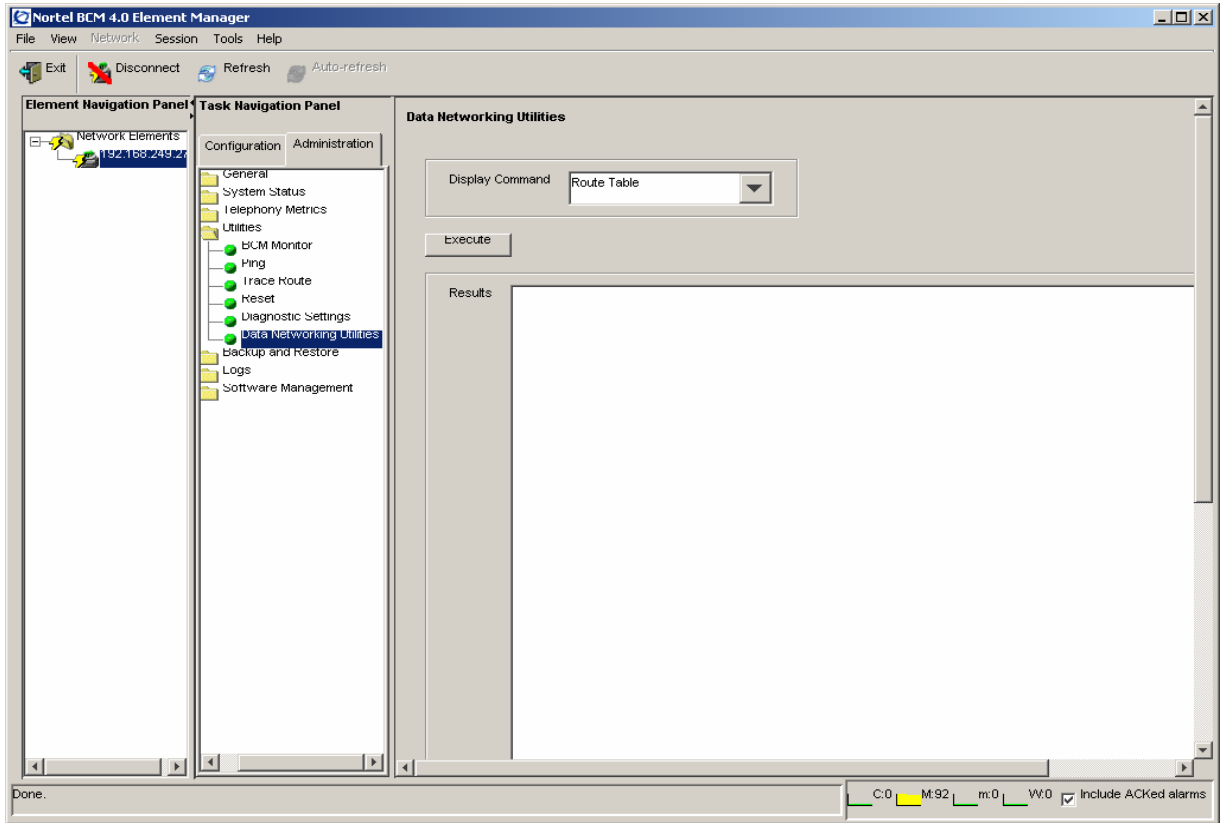
To use data networking utilities

To use the Data Networking Utilities, follow these steps:

- 1** Click **Administration > Utilities > Data Networking Utilities**.
- 2** Select a command from the **Display Command** drop-down menu.
- 3** Click the **Execute** button.

The Results panel displays data generated by the command. See [Figure 48](#).

Figure 48 Data networking utilities



Chapter 11

Backing Up and Restoring BCM Data

This chapter provides information about how to back up and restore data from the BCM system.

Overview of backing up and restoring data

Before you make administrative changes or as your BCM system accumulates information, you can backup to another location on the network. At a later time, you can restore the data to the BCM.



Note: Nortel recommends that you back up BCM data on a regular basis. In particular, you should perform a backup of the BCM and router data before you undertake major configuration changes and before you apply a software update or upgrade.

You can restore data to the same system or to a different system at the same software release level. The BCM checks the software release level of the destination system and will provide a warning if an incompatibility prevents the backup from being restored onto the selected system.

Backup and restore operations are performed by only one operator at a time to avoid conflicts with other operations. All passwords and database records included with your backup file are encrypted.

You can perform backup operations on demand or you can schedule a single backup or recurring backups. You can view the backup schedule and change it as required, and you can also save a record of the backup schedule that you set. For information about saving programming records, see [“Saving programming records” on page 57](#).

A restore operation can be performed on demand only.

Backup and restore options

You can backup and restore the settings and service data of your BCM.

During the backup procedure, you can exclude a number of optional services from the backup operation to ensure that service is not interrupted. The remainder of the services and settings are automatically included during a backup operation. Table 86 lists the components that you can choose to include or exclude from the backup operation.

Table 86 Optional components

Component	Description
IVR Configuration	Includes all IVR configuration information.
CallPilot Configuration	Includes Voicemail and ContactCenter information.
IVR Data	Includes IVR configuration, IVR data, Voicemail and ContactCenter configuration, and Voicemail and ContactCentre messages.
CallPilot Messages	Includes IVR configuration, IVR data, Voicemail and ContactCenter configuration, and Voicemail and ContactCentre messages.

Select the optional components that best fit your backup strategy. For example, if you do not want to backup personal voicemail messages, you can select the CallPilot Configuration component, which saves all CallPilot information except for personal voicemail messages.

When you perform a restore operation, you can choose to restore any optional components that were included in the backup operation. For example, if your backup included the optional IVR Data component, you can select this component during a restore operation to restore all messages, IVR data, and the IVR and voicemail configurations.

Viewing backup and restore activity

A log file tracks all backup and restore activities that occur on the system. You can retrieve and view this file in the Operational logs category. The file name is <archiver.systemlog>.

For information about logs, see [Chapter 12, “Managing BCM Logs,” on page 345](#).

About backups

A backup collects the configuration settings and the data generated during the normal operation of the BCM system.

Examples of configuration settings include:

- IP configuration details
- telephony programming
- SNMP settings
- Call Detail Recording settings
- BCM schedules (for example, the backup schedule, and the log retrieval schedule)
- greetings
- prompts

Examples of data generated during normal operations include:

- voicemail messages
- Call Detail Records
- faxes
- email text-to-speech
- envelope information



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.



Caution: The backup operation takes longer on a system with many saved voice messages. As a result, the backup archive can be quite large and can take 30 minutes or more to reach a remote server.

The BCM can accommodate a backup file that is greater than 500 MB. To minimize the size of the backup file, exclude the optional components from the backup operation. The BCM will compress sections of the backup archive when it is effective to do so. Compressing data generates a high CPU load.



Note: To manage your Voicemail options, you must use the CallPilot Manager and not the BCM Element Manager.

BCM backup file

When you perform a backup operation, the BCM creates a backup archive and stores it in a location that you specify. The archive file includes embedded archives, each of which represent a different part of the BCM system:

- archive.sig — ensures the integrity of the file
- various archive files — various archive files that contain the configuration settings and operating data

In addition to the configuration and application information, every backup operation includes the following files:

- Software Inventory — provides a snapshot of the software component release level
- Software History — provides a snapshot of the software update history

These files document the system software level from which the backup was taken. They are located in the archive softwarelevel.tar.gz.

Backup archives transferred to servers or to attached USB storage devices are named according to the system name of the BCM, the date, and the time of the backup. Archives are prefixed with Bak_. For example, an archive created on July 8, 2005 at 1:52:55 pm is named Bak_acme-melbourne_20050708T135255.tar.

For USB storage devices, an additional copy of the backup archive is stored in the file backup.tar; the BCM will reference this file during a USB restore operation. Only the most recent backup to the USB storage device is available for a restore operation. To access historical backup archives, attach the USB storage device to a personal computer and use the Restore from My Computer option.

Backup destinations

Table 87 lists the destinations to which you can back up configuration and application data. Whichever destination you choose, the backup operation replaces the BCM's own copy of the file, so that a copy of the most recent backup always remains on the BCM. You can use this to restore your BCM without transferring a backup from an external device or server.

Table 87 Backup destinations

Destination	Description
BCM	For an immediate backup, saves backup archives to the hard drive of the BCM. You cannot specify a path. Each backup rewrites any pre-existing backup of the same type.
My Computer	For an immediate backup, saves backup archives to any accessible location on the client PC on which the BCM Element Manager is installed. You can specify a name for the backup, so that the pre-existing backup is not automatically overwritten.
Network Folder	Saves data to a shared network folder. The remote server must provide a Microsoft Windows-like shared file resource and a user account with rights to create and write files in the destination location. You cannot browse the network directories to select the best destination folder, but you can specify a directory by identifying the path.
USB Storage Device	Saves backup archives to a USB storage device. The files will be written to the top directory level. You cannot specify a path to a different directory on the storage device. Each backup overwrites any pre-existing backup of the same type. A USB storage device must be formatted as FAT32.

Table 87 Backup destinations

Destination	Description
FTP Server	Saves backup archives to a File Transfer Protocol server. Credentials and backup data are sent without encryption. The remote server must provide an FTP server application and a user account with rights to allow the BCM to create and write files in the destination location. You cannot browse the FTP server to select the best destination folder, but you can specify a directory by identifying the path.
SFTP Server	Saves backup archives to an SFTP server. This method encrypts the login credentials and the data in transit. You must set up the remote SFTP server to allow the BCM to communicate with the SFTP server. The BCM system can generate a public SSH key, which you must install on the remote SFTP server. For information about SSH keys, see the chapter BCM Security.

For more information about how to access and use the storage locations, see [“BCM common file input/output processes” on page 67](#).

Before you back up BCM data, make sure that the BCM has appropriate access to the shared resource on which you will store the data. You must set full access permissions on the shared resource.



Note: When you backup to a network folder hosted in a computer running Windows 98 SE, you cannot specify an IP address in the folder name. You must specify the computer name in the network folder name. For example, enter `\\<computer>\<resource>`.

If the BCM and the network folder are on different networks, configure the BCM to use a DNS server. The Windows 98 SE computer name must be identical to the DNS hostname entry for that computer.

If the BCM does not have the same domain name as the Windows 98 SE computer, the fully qualified domain name must be specified in the folder name. For example, specify `\\computer.company.com\resource`.

Performing immediate backups

You can perform immediate backups to the following storage locations:

- BCM
- client PC
- network folder
- USB storage device
- FTP server
- SFTP sever

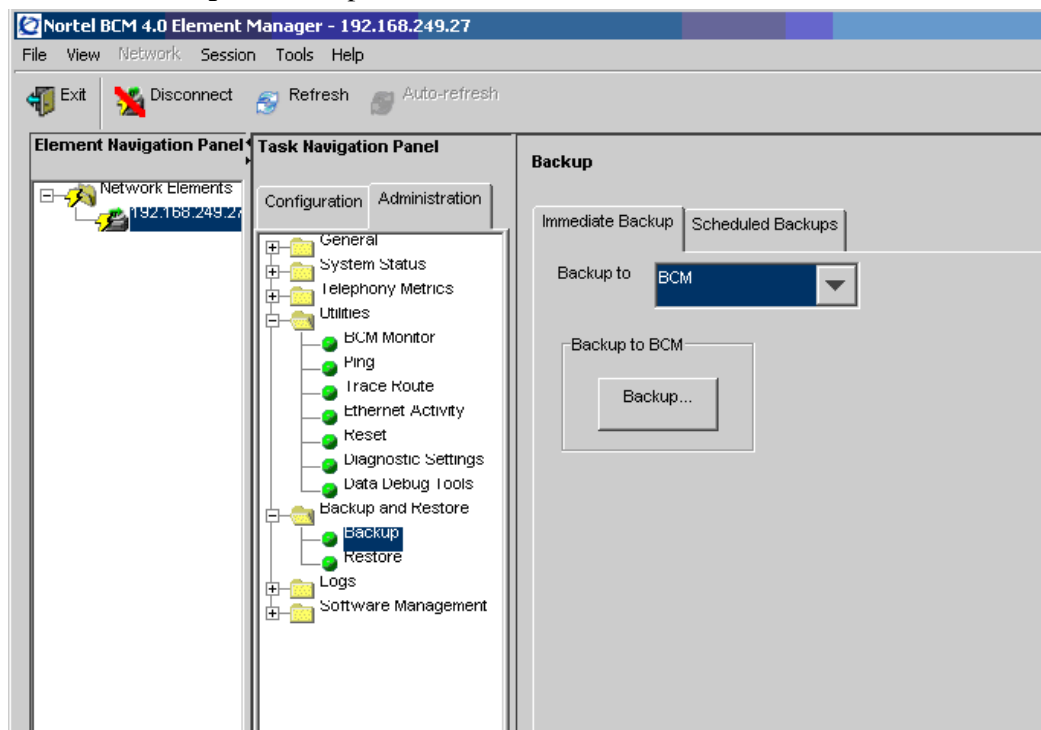
Performing an immediate backup to the BCM



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to the BCM

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab. In the **Backup To** selection field, choose **BCM**.
- 3 Click the **Backup** button.
The **Backup** window opens.



- 4 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 5 Click the **OK** button.
A warning window opens.
- 6 Click the **Yes** button to proceed.
A progress window opens. When the backup is complete, the **Backup Complete** message appears.

- 7 Click the **OK** button.

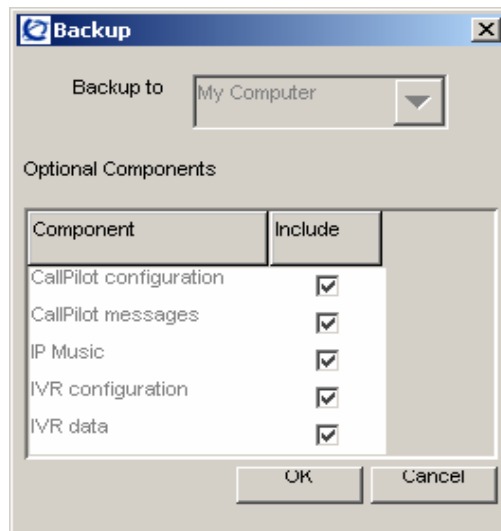
Performing an immediate backup to your personal computer



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to your personal computer

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 In the **Backup To** selection field, select **My Computer**.
- 4 Click the **Backup** button.
The **Backup** window opens.
- 5 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.



- 6 Click the **OK** button.
A warning message appears.
- 7 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Save** window opens.
- 8 Specify the directory and enter a file name in the **File Name** field. Enter a file name with a .tar extension (e.g. backup2.tar) so that you can examine the file with a utility such as WinZip. If

you do not select the folder **backup**, the new backup file will be stored in the root of this folder.

- 9 Click the **Save** button.
When the backup is complete the **Backup Complete** message appears.
- 10 Click the **OK** button.

Performing an immediate backup to a network folder



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to a network folder

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 In the **Backup To** selection field, select **Network Folder**.
- 4 Configure the Network Folder attributes.

Table 88 Configure Network Folder attributes

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and the resource name. For example, enter \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password associated with the network folder.
Directory	Enter the path to the subdirectory (optional).



Note: When you backup to a network folder hosted in a computer running Windows 98 SE, you cannot specify an IP address in the folder name. You must specify the computer name in the network folder name. For example, enter \\<computer>\<resource>.

If the BCM and the network folder are on different networks, configure the BCM to use a DNS server. The Windows 98 SE computer name must be identical to the DNS hostname entry for that computer.

If the BCM does not have the same domain name as the Windows 98 SE computer, the fully qualified domain name must be specified in the folder name. For example, specify \\computer.company.com\resource.

- 5 Click the **Backup** button.
The **Backup** window opens
- 6 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 7 Click the **OK** button.
A warning window opens.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Backup Complete** message displays.
- 9 Click the **OK** button.

Performing an immediate backup to a USB storage device



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to a USB storage device

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 In the **Backup To** selection field, select **USB Storage Device**.
- 4 Click the **Backup** button.
The **Backup** window opens.
- 5 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 6 Click the **OK** button.
A warning window opens.
- 7 Click the **Yes** button to proceed.
A progress window opens. When the backup is complete, the **Backup Complete** message displays.
- 8 Click the **OK** button.

Performing an immediate backup to an FTP server



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to an FTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 In the **Backup To** selection field, select **FTP Server**.
- 4 Configure the FTP Server attributes.

Table 89 Configure FTP Server attributes

Attribute	Action
FTP Server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the FTP server.
Directory	Enter the path to the subdirectory (optional).

- 5 Click the **Backup** button.
The **Backup** window opens.
- 6 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 7 Click the **OK** button.
A warning window opens.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Backup Complete** message displays.
- 9 Click the **OK** button.

Performing an immediate backup to an SFTP server



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform an immediate backup to an SFTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 In the **Backup To** selection field, select **SFTP Server**.
- 4 Configure the SFTP Server attributes.

Table 90 Configure SFTP Server attributes

Attribute	Action
SFTP Server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Directory	Enter the path to the subdirectory, as applicable.

- 5 Click the **Backup** button.
The **Backup** window opens.
- 6 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 7 Click the **OK** button.
A warning window opens.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Backup Complete** message displays.
- 9 Click the **OK** button.

Viewing and performing scheduled backups

You can create scheduled backups in order to perform backups at a date and time that you choose. For example, you can choose a date and time during which your business is closed. This will avoid disrupting the normal work-day routine and may allow your backup file to transfer more quickly.

You can create a schedule for a single backup operation or for operations that recur on a regular basis. You can view existing scheduled backups, as well as modify and delete them.



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

Table 91 lists the information that is displayed in the Scheduled Backups table.

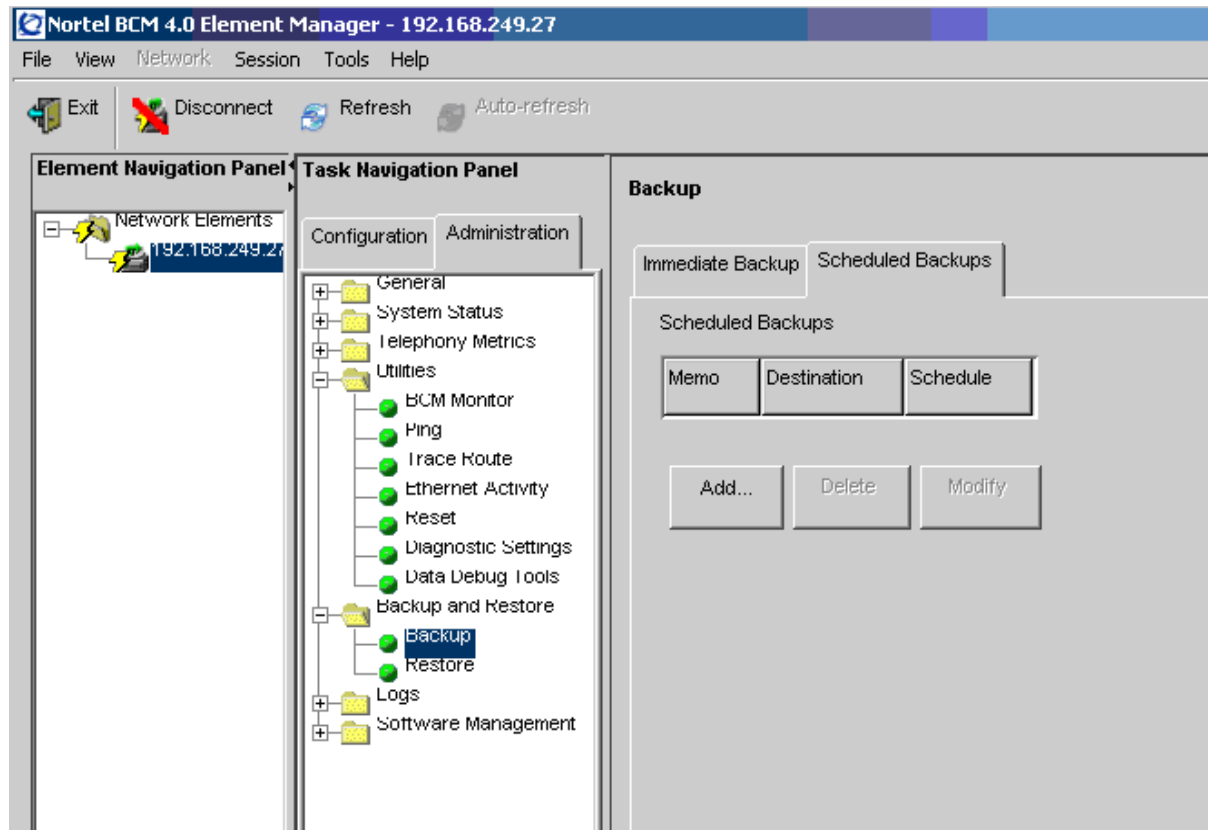
Table 91 Information displayed in the Scheduled Backups table

Column	Description
Memo	Displays the memo for the scheduled backup.
Destination	Displays the storage location for the backup file. For example, the FTP server.
Schedule	Displays the date and time at which the backup will be performed.

You can change the order of the information in the table by clicking a column heading and dragging it to a new location in the table. You can list the information in a column in ascending or descending order by clicking a column heading.

To view scheduled backups

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens. Any existing scheduled backups are displayed in the **Scheduled Backups** table.



Performing a scheduled backup to the BCM



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to the BCM

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Backup** window opens. In the **Backup To** selection field, choose BCM.

- 5 Click the **OK** button.
The **Add Scheduled Backup** window opens.
- 6 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation. Click the **OK** button.
- 7 Configure the schedule attributes.

Table 92 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often the scheduled backup is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month in which the scheduled backup is to occur.
Day of Month	Select the day of the month on which the scheduled backup is to occur.
Time	Select the time at which the scheduled backup is to occur.

- 8 Click the **OK** button.
The scheduled backup is displayed in the **Scheduled Backups** table.

Performing a scheduled backup to a network folder



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to a network folder

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Backup** window opens.
- 5 In the **Backup To** selection field, select **Network Folder**.

6 Configure the Network Folder attributes.

Table 93 Configure Network Folder attributes

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and resource name For example, \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password associated with the network folder.
Directory	Enter the path to the subdirectory (optional).

7 Click the **OK** button.

The **Add Scheduled Backup** window opens.

8 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.

9 Configure the schedule attributes.

Table 94 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often the scheduled backup is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month in which the scheduled backup is to occur.
Day of Month	Select the day of the month on which the scheduled backup is to occur.
Time	Select the time at which the scheduled backup is to occur.

10 Click the **OK** button.

The scheduled backup is displayed in the **Scheduled Backups** table.

Performing a scheduled backup to a USB storage device



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to a USB storage device

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Backup** window opens.
- 5 In the **Backup To** selection field, select **USB Storage Device**.
- 6 Click the **OK** button.
The **Add Scheduled Backup** window opens
- 7 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 8 Configure the schedule attributes.

Table 95 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often the scheduled backup is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month in which the scheduled backup is to occur.
Day of Month	Select the day of the month on which the scheduled backup is to occur.
Time	Select the time at which the scheduled backup is to occur.

- 9 Click the **OK** button.
The scheduled backup is displayed in the **Scheduled Backups** table.

Performing a scheduled backup to an FTP server



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to an FTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Backup** window opens.
- 5 In the **Backup To** selection field, select **FTP Server**.
- 6 Configure the FTP Server attributes.

Table 96 Configure FTP Server attributes

Attribute	Action
FTP Server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the FTP server.
Directory	Enter the path to the subdirectory (optional).

- 7 Click the **OK** button.
The **Add Scheduled Backup** window opens.
- 8 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 9 Configure the schedule attributes.

Table 97 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often the scheduled backup is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.

Table 97 Configure schedule attributes

Attribute	Action
Month	Select the month in which the scheduled backup is to occur.
Day of Month	Select the day of the month on which the scheduled backup is to occur.
Time	Select the time at which the scheduled backup is to occur.

10 Click the **OK** button.

The scheduled backup is displayed in the **Scheduled Backups** table.

Performing a scheduled backup to an SFTP server



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to an SFTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Backup** window opens.
- 5 In the **Backup To** selection field, select **FTP Server**.
- 6 Configure the SFTP Server attributes.

Table 98 Configure SFTP Server attributes

Attribute	Action
SFTP Server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Directory	Enter the path to the subdirectory (optional).

7 Click the **OK** button.

The **Add Scheduled Backup** window opens.

- 8 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 9 Configure the schedule attributes.

Table 99 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often the scheduled backup is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month in which the scheduled backup is to occur.
Day of Month	Select the day of the month on which the scheduled backup is to occur.
Time	Select the time at which the scheduled backup is to occur.

- 10 Click the **OK** button.
The scheduled backup is displayed in the **Scheduled Backups** table.

Modifying and deleting scheduled backups

You can modify existing scheduled backups. You can modify:

- the type of backup you want to perform (configuration or application)
- the memo for the scheduled backup
- optional components to include in the backup
- schedule details for the backup

You can also delete a scheduled backup.

Modifying a scheduled backup



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To modify a scheduled backup

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Select a scheduled backup in the **Scheduled Backups** table.
- 5 Click the **Modify** button.
The **Modify Scheduled Backup** window opens.
- 6 Modify the attributes of the scheduled backup as required. For information about how to configure the attributes, see the procedures in [“Viewing and performing scheduled backups” on page 325](#).
- 7 Click the **OK** button.
The modified backup is displayed in the **Scheduled Backups** table.

To delete a backup schedule

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Backup**.
The **Backup** panel opens and displays the **Immediate Backup** tab.
- 3 Click the **Scheduled Backups** tab.
The **Scheduled Backups** panel opens.
- 4 Select a scheduled backup in the **Scheduled Backups** table.
- 5 Click the **Delete** button.
A confirmation window opens.
- 6 Click the **Yes** button.
The scheduled backup is removed from the **Scheduled Backups** table.

Restoring BCM system data

You can restore BCM configuration and application data using the BCM Element Manager.

The restore software determines compatibility with the backup archive. Incompatible backups cannot be restored at all. Compatible backups may have incompatible sub-components which must be excluded from a Restore operation. This situation can occur if your BCM software is upgraded and a component changes the data that it includes in the backup. New backups should be made after any change to your BCM software to avoid this situation. However, it may be possible to recover data for components that have not changed from backups made prior to your software upgrade.

Restore operations are available to one user at a time, and on demand only; they cannot be scheduled.

You can retrieve the most recent backup file that you want to use for the restore operation from the BCM or from an external storage location. Nortel recommends that you always use the same storage location when you perform a restore operation. This practice will avoid potential mismatches in the backup archives. For information about storage locations, see [“Backup destinations” on page 318](#).

When you restore data, the following details are available to you:

- the size of the backup file
- the backup date
- the backup version

Restore options

You can select the components for which you want to restore configuration or application data.

You can restore a backup to a different system; for example, to quickly bring a second system into service in a new installation. In this case, not all of the configuration information in the Configuration backup is relevant to the second system. You can select whether to restore device-specific configuration information, such as network settings. You may wish to exclude certain components from being restored. For example, the network settings are often excluded from a restore operation to avoid giving two machines on your network the same identity. Backup information can be restored only to another unit that has the same software release level.

For information about applying software updates to the BCM, see [Chapter 13, “Managing BCM Software Updates,” on page 369](#).

The BCM verifies that the software release level of the unit to which the backup is being applied is consistent with the software release level of the backup file. If a potential issue is detected, the BCM Element Manager provides you with an error message.

Optional components

You can restore configuration or application data for the following optional components:

- Call Data Recording
- Call Pilot Configuration

- Call Pilot Messages
- Core Telephony
- Data Services + Network Interfaces
- Date and Time
- Doorphone
- IP Music
- IP Telephony
- IVR Configuration
- IVR Data
- Keycode
- LAN CTE
- Media Services Manager
- NAT and filters / QoS queueing
- QoS Monitor
- Security
- Scheduling
- SNMP
- Survivable Remote Gateway

Effects on the system

A restore operation is a service-affecting operation. A number of services running on the BCM system are stopped and then restarted after the data has been restored. A reboot warning is displayed if any of the components selected for restoration require a system restart. Table 100 lists the effects of restoring optional components.

Table 100 Effects of a restore operation on the system

Component	Effect
Core Telephony	System interruption.
IP Telephony	System interruption.
Keycodes	Reboots the BCM.
Network interfaces	Network interruption.

Restore operations and logs

A log file tracks all backup and restore activities that occur on the system. You can retrieve and view this file in the Operational Logs category. The file name is <archiver.systemlog>.

For information about BCM logs, see [Chapter 12, “Managing BCM Logs,” on page 345](#).

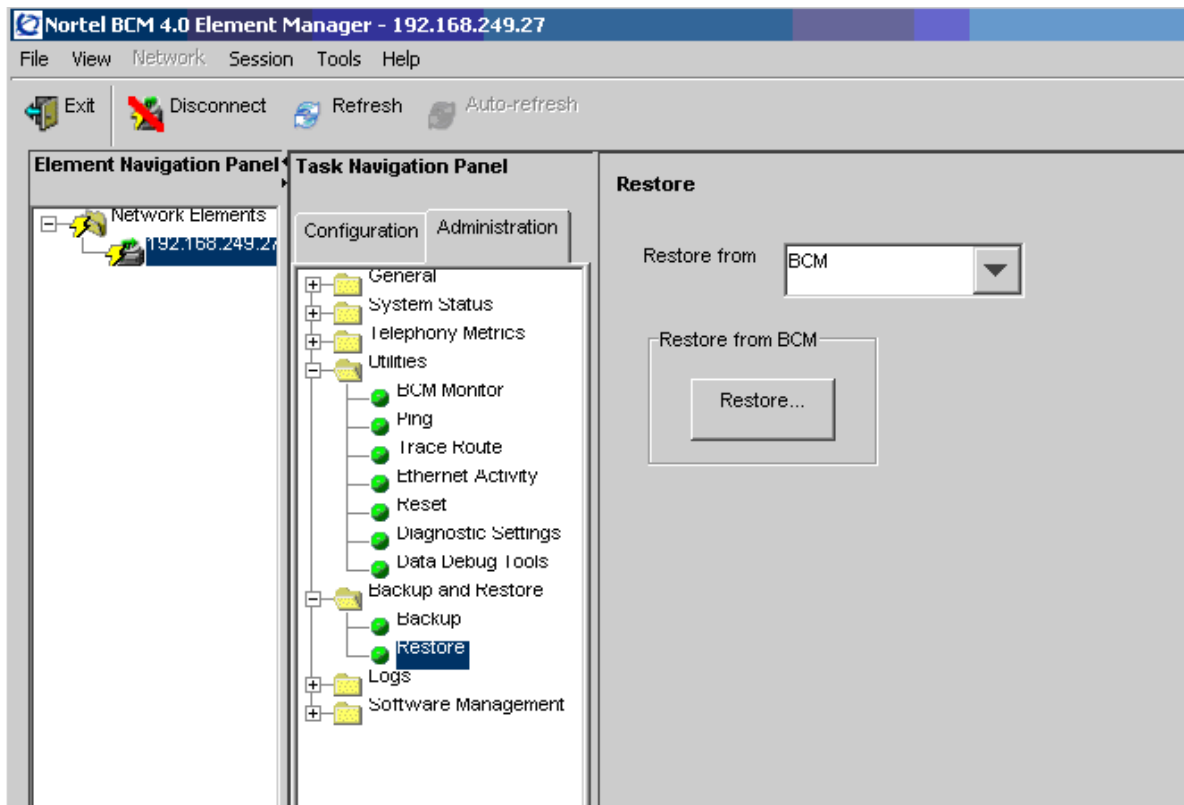
Restoring data from the BCM



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To restore data from the BCM

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens. The **Restore From** selection field has **BCM** as a default value.



- 3 Click the **Restore** button.
The **Restore From BCM** window opens.
- 4 Click the **OK** button.
The **Select Components to Restore** window opens.
- 5 Select the optional components that you want to include from the backup file.
- 6 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.

- 7 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.
- 8 Click the **OK** button.

Restoring data from your personal computer



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To restore data from your personal computer

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **My Computer**.
- 4 Click the **Restore** button.
The **Open** window opens.
- 5 Select the backup file to restore.
A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM.



Caution: When you proceed to the next step, the selected file will overwrite the backup file that is stored on the BCM. Ensure that the correct backup file is selected before proceeding.

- 6 Click the **Open** button.
The **Select Components to Restore** window opens.
- 7 Select the optional components that you want to include from the backup file.
- 8 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.
- 9 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.
- 10 Click the **OK** button.

Restoring data from a network folder



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To restore data from a network folder

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **Network Folder**.
- 4 Configure the Restore from Network Folder attributes.

Table 101 Configure Restore from Network Folder attributes

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and resource name. For example, \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password associated with the network folder.
Directory	Enter the path to the subdirectory, as applicable (optional).
File	Enter the name of the backup file.

A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM.



Caution: When you proceed to the next step, the selected file will overwrite the backup file that is stored on the BCM. Ensure that the correct backup file is selected before proceeding.

- 5 Click the **Open** button.
The **Select Components to Restore** window opens.
- 6 Select the optional components that you want to include from the backup file.
- 7 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.

- 9 Click the **OK** button.

Restoring data from a USB storage device

Your BCM supports the ability to recover using the USB device. The backup must have been created on the USB device while directly attached to a BCM. The BCM will select the most recent backup made to the USB device for the restore operation. If you want to restore an older backup archive, you must attach the USB storage device to your computer and chose the option Restore From: My Computer.



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To restore data from a USB storage device

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **USB Storage Device**.
- 4 Select the backup file to restore.
A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM.



Caution: When you proceed to the next step, the selected file will overwrite the backup file that is stored on the BCM. Ensure that the correct backup file is selected before proceeding.

- 5 Click the **Open** button.
The **Select Components to Restore** window opens.
- 6 Select the optional components that you want to include from the backup file.
- 7 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.
- 9 Click the **OK** button.

Restoring data from an FTP server



Caution: A backup operation can interrupt services running on the BCM. A warning displays whenever the backup will cause a service interruption. If you want to perform a backup that does not affect the system, you can exclude services that would be affected. Alternatively, you can include these services and perform a backup at a time when the system is typically not in use.

To restore data from an FTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **FTP Server**.
- 4 Configure the Restore from FTP Server attributes.

Table 102 Configure Restore from FTP Server attributes

Attribute	Action
FTP server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the FTP server.
Directory	Enter the path to the subdirectory, as applicable (optional).
File	Enter the name of the backup file.

A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM.



Caution: When you proceed to the next step, the selected file will overwrite the backup file that is stored on the BCM. Ensure that the correct backup file is selected before proceeding.

- 5 Click the **Open** button.
The **Select Components to Restore** window opens.
- 6 Select the optional components that you want to include in the backup file.
- 7 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.
- 8 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.

- 9 Click the **OK** button.

Restoring data from an SFTP server



Caution: A restore operation is a service-affecting operation. A number of services running on the BCM system are stopped and then restarted using the restored configuration or application data. A reboot is required if you choose Keycodes as a restore option. It takes several minutes before Voicemail is working again.

To restore data from an SFTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **SFTP Server**.
- 4 Configure the Restore from SFTP Server attributes.

Table 103 Configure Restore from SFTP Server attributes

Attribute	Action
SFTP server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Password	Enter the password associated with the SFTP server.
Directory	Enter the path to the subdirectory, as applicable.
File	Enter the name of the backup file.

A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM.



Caution: When you proceed to the next step, the selected file will overwrite the backup file that is stored on the BCM. Ensure that the correct backup file is selected before proceeding.

- 5 Click the **Open** button.
The **Select Components to Restore** window opens.
- 6 Select the optional components that you want to include from the backup file.
- 7 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.

- 8 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.
- 9 Click the **OK** button.

Restoring the factory configuration



Caution: A restore operation is a service-affecting operation. A number of services running on the BCM system will be stopped and then restarted using the restored configuration or application data. A reboot is required if you choose Keycodes as a restore option. It will take several minutes before Voicemail is working again.

To restore the factory configuration

Your BCM is delivered with a backup file that was created at the factory. This file can be a helpful starting point if you decide to completely re-configure your BCM and would like to erase the settings programmed on your device. Although you can select individual components to restore, Nortel recommends that you restore all components when using this option.

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Backup and Restore** folder, and then click **Restore**.
The **Restore** panel opens.
- 3 In the **Restore From** selection field, select **Factory Default**.
- 4 Click the **Restore** button.
The **Select Components to Restore** panel opens.
- 5 Select the optional components that you want to include from the backup archive.
- 6 Click the **OK** button.
A warning window opens and displays information about components that will be affected by the restore operation.
- 7 Click the **Yes** button to proceed.
A progress window opens. When the operation is complete, the **Restore Complete** window opens.
- 8 Click the **OK** button.

Chapter 12

Managing BCM Logs

This chapter contains information about viewing and managing log files generated by the BCM.

Overview of BCM logs

A log file is a collection of individual log events generated by the BCM. An administrator can use log files to monitor and analyze system behavior, user sessions, and events.

You manage log files by transferring selected BCM log archives from the BCM to a specified location, such as your personal computer. You can then view individual log events using the BCM Element Manager Log Browser or your usual text editor.



Note: Depending on the privileges assigned to you, you may or may not see all the log files or processes described in this chapter.

In addition to the log files generated by the BCM, the Element Manager itself generates a log file. This log is found under the Help selection of the BCM Element Manager toolbar. This log contains diagnostic information.

The BCM manages log archives and maintains generations of information depending upon size or other criteria. Generations of log files have a numbered extension such as 3.gz.

A generation of the alarms.systemlog file is created each time the BCM is rebooted or when the log file reaches the 1 MB limit.

Log types

The BCM logs are grouped in three categories:

- Operational logs
- Diagnostic logs
- Sensitive logs

Each log category contains one or more log files.

A log transfer groups all selected categories into a common archive. The embedded categories have easily identified names and are accessible to utilities such as WinZip (MS-Windows) and tar (UNIX).

When you transfer log archives, a set of additional log files is included in the log archive. These files are system information reports, which contain information about the system at the time of the log transfer.

Administrators have access to all log categories. Users who need only operational information have access to Operational and System Information logs.

Operational logs

Operational logs contain information about the BCM system and its use, such as alarm information, configuration changes, and security information. Administrators and authorized users can access Operational logs and view them using the Log Browser.

Table 104 lists the logs that belong to the Operational logs category.

Table 104 Operational logs

Log type	BCM log name	Description
Alarm log	alarms.systemlog	Records alarms that were written to the Element Manager alarm panel. Other possible alarms, if they cannot be viewed using the BCM Element Manager, are logged in the alarms diagnostic log.
Configuration change	configchange.systemlog	Records Element Manager configuration data changes by user and time
Security log	security.systemlog	Records users logging in and out as well as locked out users
	psmtest.systemlog	Records Ethernet interface activity and hard drive partitions
	psmOMS.log	Records platform status, such as operational measurements

Diagnostic logs

Diagnostic logs contain the log files generated by the BCM software components. These log files are required only if additional system information is required by Nortel Technical Support to help diagnose a BCM issue. Only an administrator can access Diagnostic logs.

Sensitive logs

Sensitive logs may contain sensitive customer information, such as personal identification numbers or bank account and credit card numbers. Users may enter sensitive information using their telephone sets, for example when performing telephone banking.

Sensitive logs are grouped in a separate category to allow the administrator to decide whether to include this category of log files in a log file transfer, depending on the nature of the connection being used for the transfer. Administrators may choose to exclude Sensitive logs when the network or the destination is not sufficiently secure or when there are other privacy or security concerns.

The Sensitive Logs category includes only three log files for core telephony, LAN CTE, and Voice CTI.



Caution: The Sensitive Logs category can become very large due to the large core telephony log files.



Security Note: Once logs are transferred to an external location, the administrator is responsible for securing the information and controlling access to it.

Additional System Information

A set of System Information files is included with every log file transfer. These are reports rather than log files, and contain a snapshot of operating state of the BCM system at the time of the log file transfer. These reports are automatically collected and included with every log file transfer.

The files included in this category are .txt files. You can open these files with an application such as WordPad or Microsoft Word, but you cannot open or view them using the BCM Element Manager Log Browser. Nortel recommends WordPad, since this application retains the column structure of the logs.

Overview of transferring and extracting log files

You use the BCM Element Manager to transfer log files from the BCM to an external location. You must transfer the log files to an external device before you can view them. If you are using the BCM Element Manager Log Browser to view the logs, you will also have to extract the log files from the log archive that is transferred from the BCM. The log archive contains a collection of log files.

When you transfer the log archives to another device, you can specify:

- the location to which you want to transfer log files, such as your personal computer or a network folder
- the category of logs you want to transfer, such as Sensitive Information logs
- a schedule for a log file transfer

You can also transfer log files using the BCM Web page if you cannot access the BCM Element Manager.

After you transfer the log archives, several options are available to you for extracting the log file information and for viewing the log files. If you are using the BCM Element Manager (recommended), the Log Browser prompts you to extract the actual log files from the .tar file. If you prefer, you can use the WinZip application to expand the .tar file into its included log files. As an alternative to using the BCM Element Manager Log Browser, you can use an application such as WordPad to view the log files.

Using the BCM Element Manager Log Browser to view extracted log files gives you the ability to view information in a way that suits you; for example, you can filter and sort information according to priority, time, message, and so on.

Transferring log files using the BCM Element Manager

Using the BCM Element Manager, you can transfer log files by using:

- an immediate log transfer
- a scheduled log transfer

You can create, modify, or delete a scheduled log transfer.

You can transfer log files to the following destinations:

- a USB storage device

- your personal computer
- a network folder
- an FTP server
- an SFTP server for secure file transfer

Log archives transferred to the servers and the USB device are named with a Log_ prefix. The system name of the BCM and the date/time are appended to the prefix. An example filename is Log_acme_20050708T101604.tar.

When you transfer log files to the computer on which your Element Manager is installed, the default location for the Logs folder is \BCMElementManager\files\logs\. You may wish to create a folder within this folder for each BCM you are managing, so that log files from a particular BCM can always be transferred to the associated log file folder on your computer.

When you are transferring the log archive to your personal computer, you may also wish to save the log archive file using the system name and date as part of the file name. This will simplify the task of locating the tar file later. For example, you may wish to save the tar file as “Log_acme20050315.tar”.

Performing immediate log archive transfers

The time required to transfer log files varies with the amount of log data being collected and the speed of your devices and network.

Performing an immediate log transfer to a USB storage device

Before you transfer a log from a USB storage device, make sure that:

- the USB storage device is formatted as a FAT32 device (attach the USB storage device to a computer with a recent MS-Windows operating system installed, right-click the USB storage device icon, and format the device to File System of FAT32)
- the USB storage device is connected to the BCM
- the capacity of the storage device is sufficient for the log archive



Note: The log archive is saved in the top-level directory. You cannot navigate a folder hierarchy on the USB device.

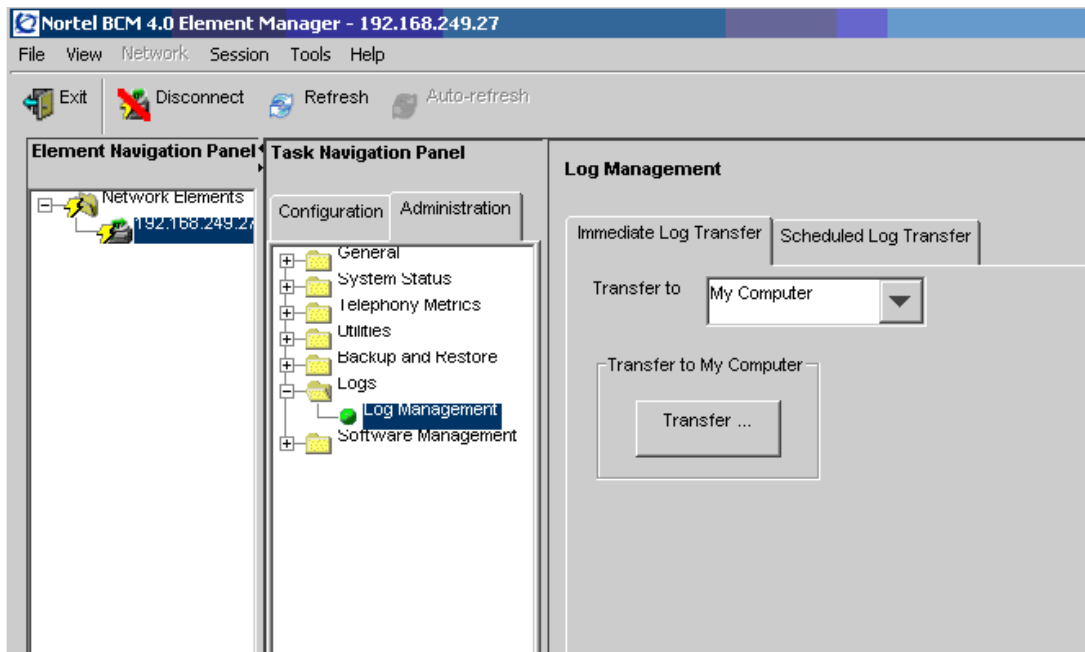


Note: Log archives written to external devices (except My Computer) have a unique name based on the timestamp. This prevents earlier log archives from being overwritten. A device will eventually reach its capacity if log archives are not manually detected.

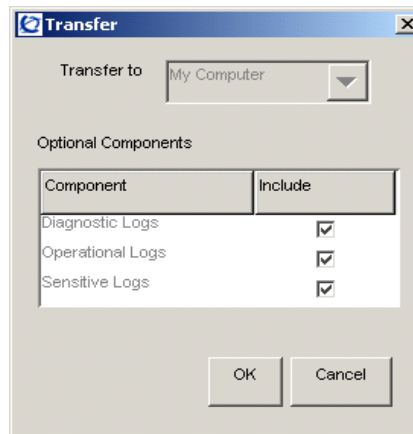
To perform an immediate log transfer to a USB storage device

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.

- 3 Click the **Immediate Log Transfer** tab.
- 4 In the **Transfer To** selection field, select **USB Storage Device**.



- 5 Click the **Transfer** button.
The **Transfer To** window opens.
- 6 Select the log file categories that you want to include in the log file transfer. All the log files associated with the selected categories will be transferred.



- 7 Click the **OK** button.
A transfer window opens and displays applicable warnings.
- 8 Click the **Yes** button to initiate the transfer.
The **Progress Update** window opens. When the log files are transferred, the **Transfer Complete** window opens.

- 9 Click the **OK** button.
The log archive is saved in the location you specified.

Performing an immediate log transfer to your personal computer



Note: The time required to transfer log files varies with the amount of log data being collected and the speed of your devices and network.

To perform an immediate log transfer to your personal computer

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.
- 3 Click the **Immediate Log Transfer** tab.
- 4 In the **Transfer To** selection field, select **My Computer**.
- 5 Click the **Transfer** button.
The **Transfer To** window opens.
- 6 Select the log file categories that you want to include in the log file.



- 7 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 8 Click the **Yes** button to initiate the transfer.
The **Progress Update** window opens. When the log archive is ready to be saved, the **Save** window opens.
- 9 Select the directory in which you want to save the log file transfer.

- 10** In the **File Name** field, enter the name of the log file followed by a .tar extension. For example, log1.tar.



Note: If you do not specify a .tar extension, the transfer proceeds and the file will be written to the specified location. The file, however, will be of an unknown type and your utilities may not operate with it. Rename the file with the extension .tar by right-clicking on the file and renaming it.

- 11** Click the **Save** button.
The **Transfer Complete** window opens.
- 12** Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

Performing an immediate log transfer to a network folder



Note: The time required to transfer log files varies with the amount of log data being collected and the speed of your devices and network.

To perform an immediate log transfer to a network folder

- 1** Click the **Administration** tab, and then open the **Logs** folder.
- 2** Click the **Log Management** task.
The **Log Management** panel opens.
- 3** Click the **Immediate Log Transfer** tab.
- 4** In the **Transfer To** selection field, select **Network Folder**.
- 5** Configure the **Transfer to Network Folder** attributes.

Table 105 Configure the Transfer to Network Folder attributes

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and the resource name. For example, enter \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password associated with the network folder.
Directory	Enter the path to the subdirectory, as applicable (optional).

- 6** Click the **Transfer** button.
The **Transfer** window opens.
- 7** Select the log file categories that you want to include in the log file transfer.
- 8** Click the **OK** button.
A confirmation window opens, and displays applicable warnings.

- 9 Click the **Yes** button to initiate the transfer.
The **Progress Update** window opens. When the log files are transferred, the **Transfer Complete** window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

Performing an immediate log transfer to an FTP server



Note: The time required to transfer log files varies with the amount of log data being collected and the speed of your devices and network.

To perform an immediate log transfer to an FTP server

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.
- 3 Click the **Immediate Log Transfer** tab.
- 4 In the **Transfer To** selection field, select **FTP Server**.
- 5 Configure the Transfer to FTP Server attributes.

Table 106 Configure Transfer to FTP Server attributes

Attribute	Action
FTP Server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the FTP server.
Directory	Enter the path to the subdirectory, as applicable (optional).

- 6 Click the **Transfer** button.
The **Transfer** window opens.
- 7 Select the log file categories that you want to include in the log file transfer.
- 8 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 9 Click the **Yes** button to initiate the transfer.
The **Progress Update** window opens. When the log files are transferred, the **Transfer Complete** window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

Performing an immediate log transfer to an SFTP server



Note: The time required to transfer log files varies with the amount of log data being collected and the speed of your devices and network.



Note: You must set up the SFTP server to allow the BCM to communicate with the SFTP server. For information about how to set up an SFTP server and about SSH keys, see [“Transferring an SSH Key-Pair”](#) on page 87.

To perform an immediate log transfer to an SFTP server

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.
- 3 Click the **Immediate Log Transfer** tab.
- 4 In the **Transfer To** selection field, select **SFTP Server**.
- 5 Configure the Transfer to SFTP Server attributes.

Table 107 Configure Transfer to SFTP Server attributes

Attribute	Action
SFTP Server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Directory	Enter the path to the subdirectory, as applicable (optional).

- 6 Click the **Transfer** button.
The **Transfer** window opens.
- 7 Select the log file categories that you want to include in the log file transfer.
- 8 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 9 Click the **Yes** button to initiate the transfer.
The **Progress Update** window opens. When the log files are transferred, the **Transfer Complete** window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

Performing scheduled log transfers

You can schedule a log transfer for a future date or for a single transfer, or for recurring future transfers. You can create multiple schedule entries. For example, you can transfer Operational logs and System Information logs on a daily basis and transfer Diagnostic and Sensitive Information logs on a weekly basis.

You can also modify or delete a scheduled log transfer.

Table 108 lists the information that is displayed in the Scheduled Log Transfer table.

Table 108 Information displayed in the Scheduled Log Transfer table

Column	Description
Memo	Displays the description of the scheduled log transfer.
Destination	Displays the storage location for the log transfer.
Schedule	Displays the date and time at which the log transfer will be transferred to the specified storage location.

For information about how to configure transfer to attributes, see the procedures in [“Performing immediate log archive transfers” on page 348](#).

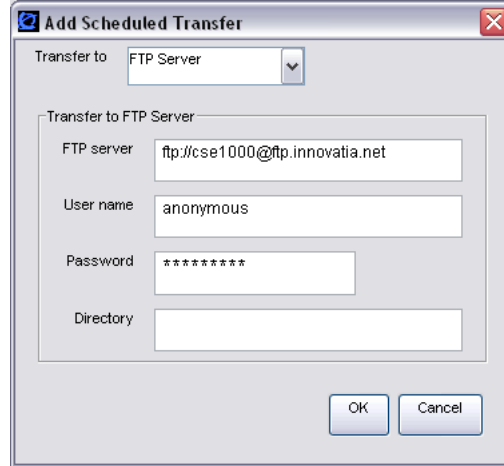


Note: You cannot schedule a log transfer to your personal computer. Use a network folder, a USB storage device, an FTP server, or an SFTP server instead.

To perform a scheduled log transfer to a storage location

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The Log Management panel opens.
- 3 Click the **Scheduled Log Transfer** tab.
The **Scheduled Log Transfer** panel opens.
- 4 Click the **Add** button.
The **Add Scheduled Transfer** window opens.
- 5 In the **Transfer To** selection field, select the location to which you want to transfer the log files:
 - Network Folder
 - USB Storage Device
 - FTP Server

- SFTP Server



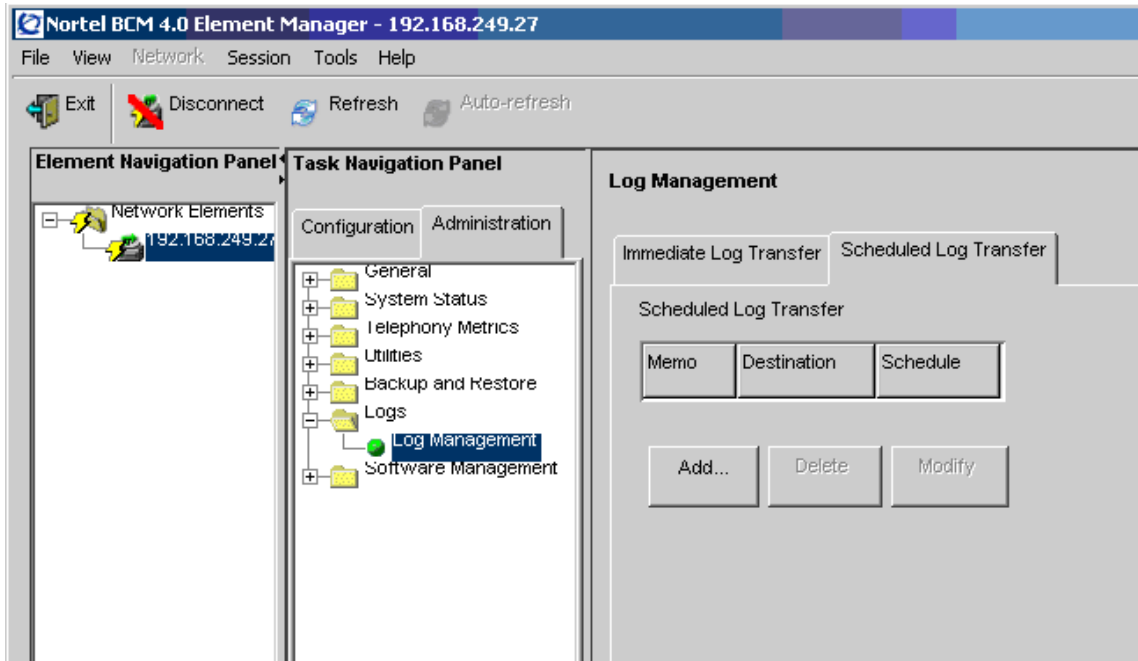
- 6 Configure the **Transfer To** attributes. For information about how to configure Transfer To attributes, see the procedures in [“Performing immediate log archive transfers”](#) on page 348.
- 7 Click the **OK** button.
The **Add Scheduled Transfer** window opens.
- 8 Select the log file categories that you want to include in the log file transfer.
- 9 Configure the schedule attributes.

Table 109 Configure schedule attributes

Attribute	Action
Memo	Enter a note for the scheduled log transfer, as applicable.
Recurrence	Select how often the scheduled transfer is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week check boxes appear so that you can select the days on which the transfer will occur.
Month	Select the month in which the scheduled transfer is to occur.
Day of Month	Select the day of the month on which the scheduled transfer is to occur.
Time	Select the time at which the scheduled transfer is to occur. Click the field to display a Time box, where you can specify the hour, minute, second, and whether the time occurs in morning or afternoon. Close the box when you have finished specifying the time.

10 Click the **OK** button.

The scheduled log transfer is displayed in the **Scheduled Log Transfer** table.



To modify a scheduled log transfer

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.
- 3 Click the **Scheduled Log Transfer** tab.
- 4 In the **Scheduled Log Transfer** table, select a scheduled log file transfer.
- 5 Click the **Modify** button.
The **Modify Scheduled Transfer** window opens.
- 6 In the **Destination** field, modify the destination as appropriate.
- 7 In the **Memo** field, modify the memo for the scheduled log transfer as appropriate.
- 8 In the **Optional Components** area, modify the log file categories you want to include or exclude from the transfer, as appropriate.
- 9 Click the **OK** button.
The modified scheduled log transfer is displayed in the **Scheduled Log Transfer** table.

To delete a scheduled log transfer

- 1 Click the **Administration** tab, and then open the **Logs** folder.
- 2 Click the **Log Management** task.
The **Log Management** panel opens.
- 3 Click the **Scheduled Log Transfer** tab.
- 4 In the **Scheduled Log Transfer** table, select a schedule.
- 5 Click the **Delete** button.
A confirmation window opens.
- 6 Click the **Yes** button.
The scheduled log transfer is deleted from the **Scheduled Log Transfer** table.

Transferring log files using the BCM Web page

You can transfer log files using the BCM Web page if you cannot access the BCM Element Manager.

When you use the BCM Web page to transfer log files, you cannot choose the log file categories that you will transfer; all the log files in all the categories will be transferred.

Using the BCM Web Page to transfer log files to your personal computer

- 1 In your web browser, type the IP address of the BCM and click the **Go** button.
The login screen opens.
- 2 Log in to the BCM using the same username and password that you use to log into a BCM using the BCM Element Manager.
The BCM Web page opens.

3 Click the **Administrators Applications** link.



- 4 Click **Retrieve Logs**.
- 5 In the **Get Logs** area, click the **Download From Here** radio button.
- 6 Click the **Submit** button.
A **Working** screen opens. When the log retrieval is complete, the screen displays “Done.”
- 7 Click the **Click Here to Download Logs** link.
The **File Download** screen opens.
- 8 Click the **Save** button.
The **Save As** screen opens.
- 9 Specify the location where you want to save the log file transfer, and enter a name for the file in the **File Name** field.
- 10 Click the **Save** button.
The file is saved.

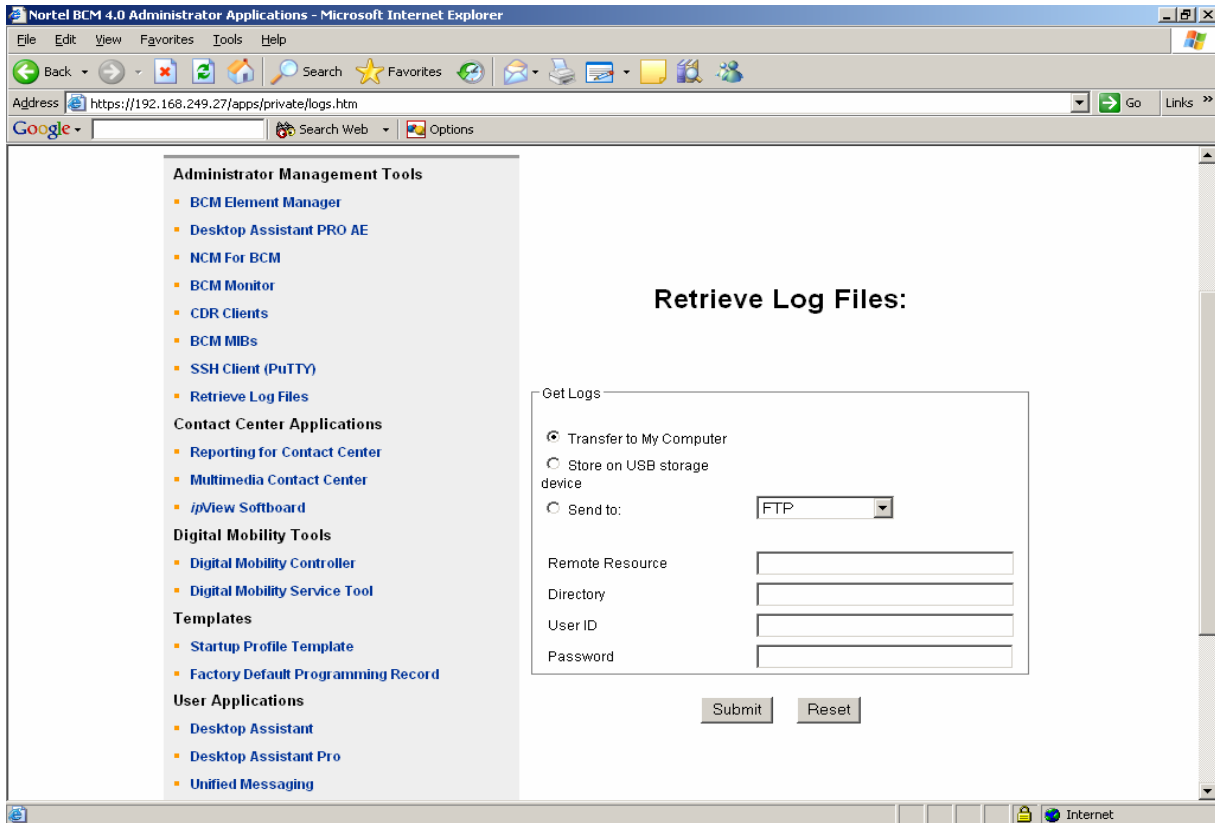
To use the BCM Web Page to transfer log files to other destinations

- 1 In your web browser, type the IP address of the BCM and click the **Go** button.
The login screen opens.
- 2 Log in to the BCM using the same user name and password that you use to log into a BCM using the BCM Element Manager.
The BCM Web page opens.
- 3 Click the **Administrators Applications** link.



- 4 Click the **Retrieve Logs** link.
- 5 In the **Get Logs** area, select a destination for the retrieved logs:
 - USB storage device
 - Send to:
 - FTP
 - SFTP

- Windows Shared Folder



- 6 If you selected a Send To option, configure the destination attributes.

Table 110 Configure destination attributes

Attribute	Action
Remote Resource	Enter the FTP or SFTP address or the network pathway, as appropriate.
UserID	Enter the user ID associated with the remote resource.
Password	Enter the password associated with the remote resource. This option does not apply when the destination is an SFTP server.

- 7 Click the **Submit** button.
A **Working** screen opens. When the log retrieval is complete, the screen displays “Done.”
- 8 Click the **Click Here to Download Logs** link.
The **File Download** screen opens.
- 9 Click the **Save** button to save the backup.tar file.
The **Save As** screen opens.
- 10 Specify the location where you want to save the zipped file, and enter a name for the file in the **File Name** field. The file must have a .tar extension. For example, log2.tar.

- 11 Click the **Save** button.
The file is saved.

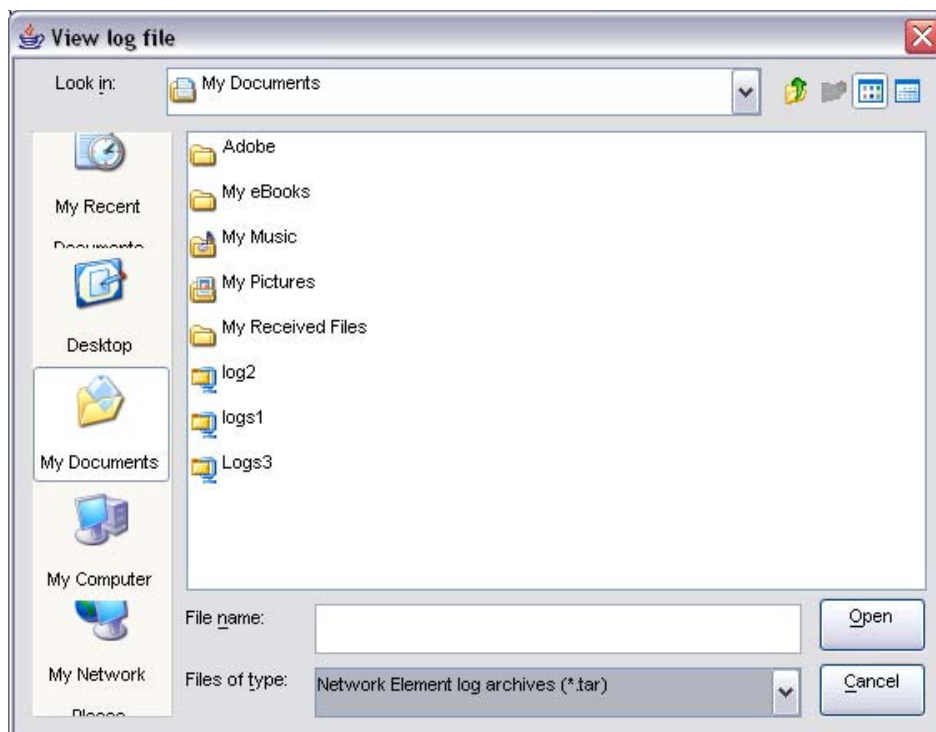
Extracting log files

Once you have transferred log files using the BCM Element Manager or the BCM Web page, you can extract the log files using the BCM Element Manager Log Browser. The log files must be extracted from the log archive before you can view them using the Element Manager Log Browser.

Before you extract log files, create a folder in your directory for each archive and then follow the procedure below to extract the archive into the appropriate folder.

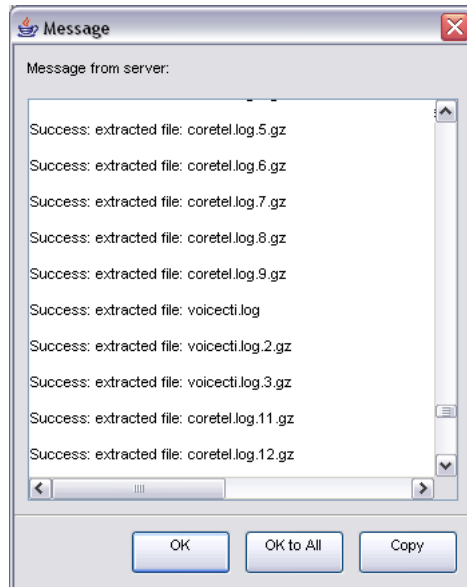
To extract log files using the BCM Element Manager

- 1 In the navigation pane, right-click a network element. The network element may be connected or disconnected.
- 2 Select **View Logs**.
The **View Log File** window opens.
- 3 Select the directory or location that contains the transferred BCM log file tar archive.
- 4 Select **Network Element log archives (*.tar)** in the **File of Type** field.
- 5 Select the archive file, and then click the **Open** button.

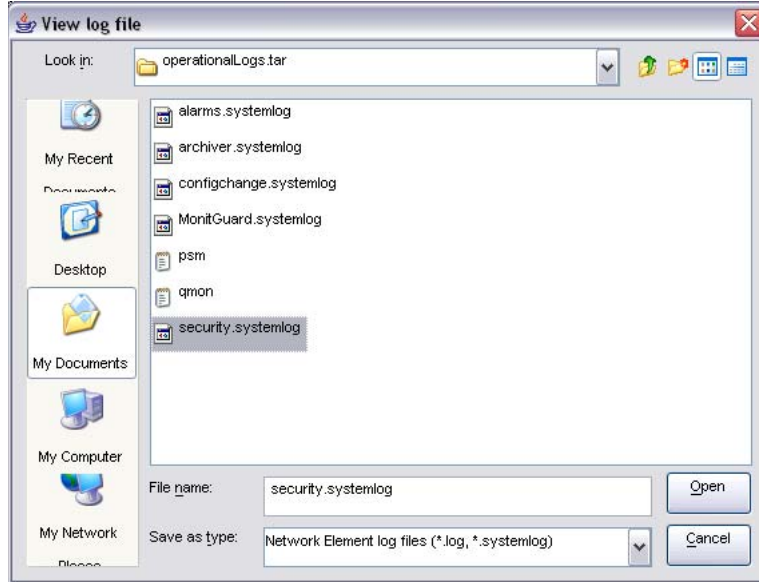


A confirmation dialog box opens.

- 6 Click the **Yes** button to extract the contents of the zipped file.
A message dialog box opens and displays a success or error message for each extracted file.



- 7 Click the **OK** button to acknowledge an individual message, or click **OK to All** to acknowledge all messages once the extraction is complete. Alternatively, you can wait until the extraction is complete, and then close the window.
Once the files are extracted, the **View Log File** window opens.
- 8 Select a log file folder, for example operationalLogs.tar. Select **.systemlog** from the **Save as Type** select field to show only log files that the Log Browser can display.
- 9 Click the **Open** button.
The log file folder opens and the log files that it contains are displayed.



- 10 Select a .systemlog file or a .log file, and click the **Open** button.
The Log Browser opens and displays retrieval results for the selected log file.

Viewing log files using the Log Browser

The Log Browser is an application that you can use to search for and view information about log events from different types of data sources. You can determine what type of information you want to see and customize how you want to display the information.

You can view the following log files using the BCM Element Manager Log Browser:

- all log files of type .systemlog
- most log files of type .log
- log files of type .txt or other file extensions that cannot be viewed using the Log Browser

You can use an application such as WordPad or Microsoft Word to view log files that you cannot view using the Log Browser.

Table 111 lists the log files that you can view using the Log Browser.

Table 111 Log files and the Log Browser

Log File	Can be viewed in the Log Browser?
Operational logs (.systemlog)	Yes
Diagnostic logs	Some can
System Information	No
Sensitive Information	Yes

The Log Browser contains the following areas:

- Retrieval Criteria area
- Retrieval Results list
- Log Details area

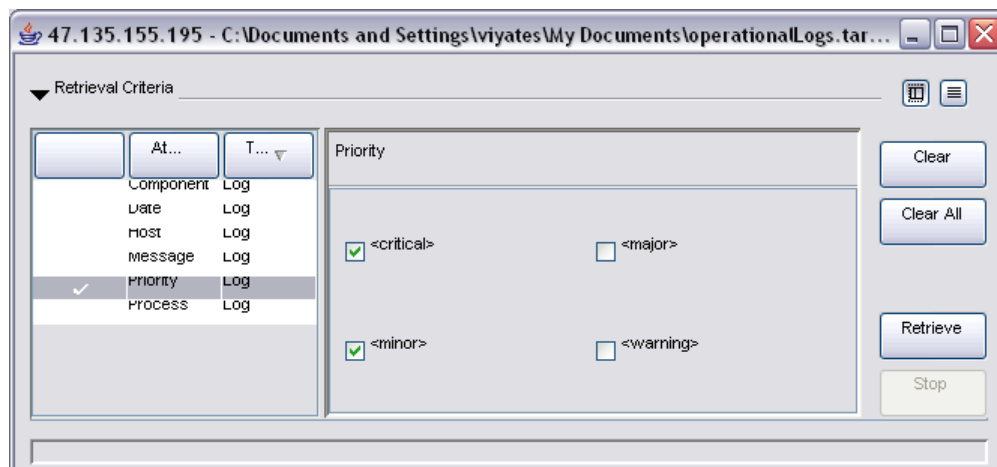
Retrieval Criteria area

The Retrieval Criteria area at the top of the Log Browser window displays a list of network element and alarm attributes that you can use to define the criteria for browsing a selected log file.

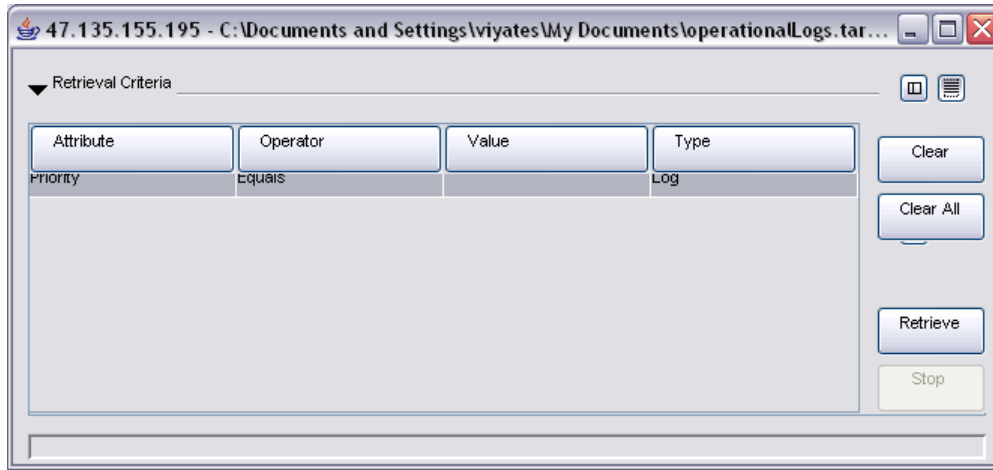
You can display or close the Retrieval Criteria area by clicking on the arrow to the right of the Retrieval Criteria field.

Retrieval criteria area specific to the log file that you are viewing. For example, .log files with four columns have four possible retrieval criteria, while .systemlog files with six columns have six possible retrieval criteria. You can define the criteria for browsing log files by selecting or deselecting criteria.

When you select an attribute from the Retrieval Criteria table, the Criteria Definition area to the right of the table displays the corresponding details for the attribute you selected. You can select or define the corresponding details.



You can click the Pane View buttons at the top right corner of the Retrieval Criteria area to display a summary view of your selected criteria. This allows you to review selected criteria before you retrieve the logs.



After you select an attribute, you can click the Clear button to remove it from the summary list, click the Clear All button to remove selected attributes, or click the Retrieve button to initiate a retrieval of log files according to the criteria you defined in the Retrieval Criteria area.

To specify retrieval criteria

- 1 In the **Retrieval Criteria** table, select an attribute.
The **Criteria Definition** area displays the corresponding details for the selected attribute.
- 2 Specify details for the selected attribute, as appropriate.
- 3 Click the **Retrieve** button.
The results of the retrieval are displayed in the **Retrieval Results** list area.

Retrieval Results area

The Retrieval Results area displays the list of log information that was retrieved according the criteria you selected in the Retrieval Criteria area. The information is displayed in a table that you can sort by clicking column headings.

While the Log Browser is retrieving records, you can monitor the progress of the retrieval by following the progress counter. This counter also displays the elapsed time and the number of records found. You can stop the retrieval by clicking the Stop button.

The Log Browser displays all the records it has found, to a set maximum display limit. The maximum display limit is 3000 records. Most log files exceed this limit; when this happens, you cannot view the remaining records in the log file. If this is the case, try using filter criteria for a specific date or dates to reduce the number of results.

You can sort the contents of the table by clicking the headings in the table. You can view details about a log record by selecting a log record or multiple log records in the Retrieval Results area.

To filter information displayed in the Retrieval Results table, you can select or clear the check boxes in the Show area below the Retrieval Results table. You can filter the results by alarm severity: Debug, Info, Warn, or Error.

To filter information in the Retrieval Results table

- 1 Retrieve log files. See the procedure [“To specify retrieval criteria” on page 365](#).
- 2 Below the Retrieval Results table, select or deselect any of the following filters:
 - Debug — displays only Debug level
 - Info — displays only Information level
 - Warn — displays only Warning level
 - Error — displays only Error level

Log Details area

The Log Details area located below the Retrieval Results list displays the details for a selected log record or multiple log records.

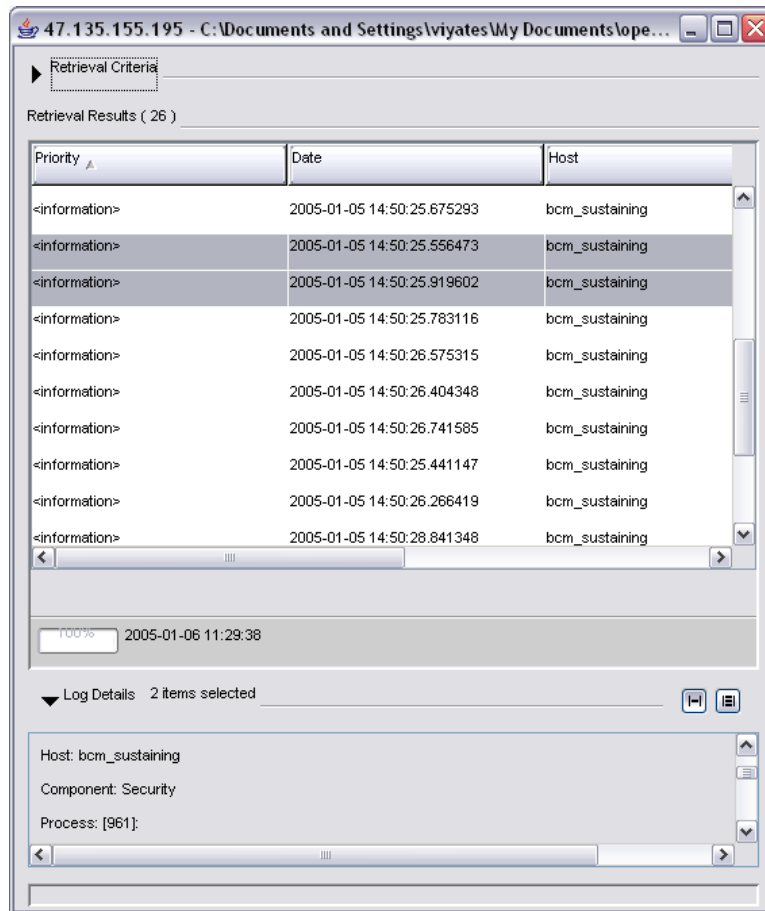
Viewing log details for a single log record

In the **Retrieval Results** list table, select a log record.

Log details for the selected log record are displayed in the **Log Details** area.

To view log details for multiple log records

- 1 In the **Retrieval Results** list table, hold down the **Shift** key and select log records to select multiple contiguous log records.
Log details for the selected log records are displayed in the Log Details area, separated by dashed lines.
- 2 In the **Retrieval Results** list table, hold down the **Control** key and select log records to select multiple non-contiguous log records.
Log details for the selected log records are displayed in the Log Details area, separated by dashed lines.
- 3 To toggle between viewing log details for single and multiple log records separated by a dashed line, click the **View Control** buttons to the right of the **Log Details** area.



Viewing log files using other applications

Using the BCM Element Manager Log Browser to view log files enables you to control how you view log events by means of retrieval criteria and sorting tools. You can also view log files using other applications if the BCM Element Manager is not available. For example, you can use WordPad to view .systemlog and .log files (tab delimited), or you can open the files using Microsoft Word or Microsoft Excel.

Chapter 13

Managing BCM Software Updates

This chapter contains information about managing BCM software updates.

During the lifecycle of the BCM, you can apply software updates to the BCM unit to introduce new functionality. Between software upgrades, you may find it necessary to apply software updates to resolve field issues. Both software upgrades and software updates are applied in the same manner.

Using the BCM, you can:

- obtain software updates from different storage locations, such as an FTP site or USB storage device
- view the software upgrade and update history of the BCM
- apply and, in some cases, remove software updates
- view the software inventory of the BCM
- apply software updates at a scheduled time

Overview of BCM software updates

Using the Software Management task, an administrator can view and manage software updates and upgrades to the BCM.

The Software Management interface consists of three panels:

- Software Updates — used to manage the application of software updates to the BCM
- Software Update History — used to view the history of updates that have been applied to the BCM, and to remove an applied update
- Software Inventory — used to view a complete list of software components, their version, and the functional group to which they belong

Obtaining software updates

Before you can apply a software update to your BCM, you must obtain the software update and unzip the file. Authorized Nortel partners can download BCM software updates from the Nortel Technical Support web page.

To obtain updates from the Nortel Technical Support Web page

- 1 In your web browser, enter <address> and then click the **Go** button.
The Nortel Technical Support Web page opens.
- 2 Download the required updates.
- 3 Create a directory for each update and unzip the downloaded file into a directory.

Viewing software updates in progress

You can view the status of software updates that are transferring or waiting to be transferred, or waiting to be applied.

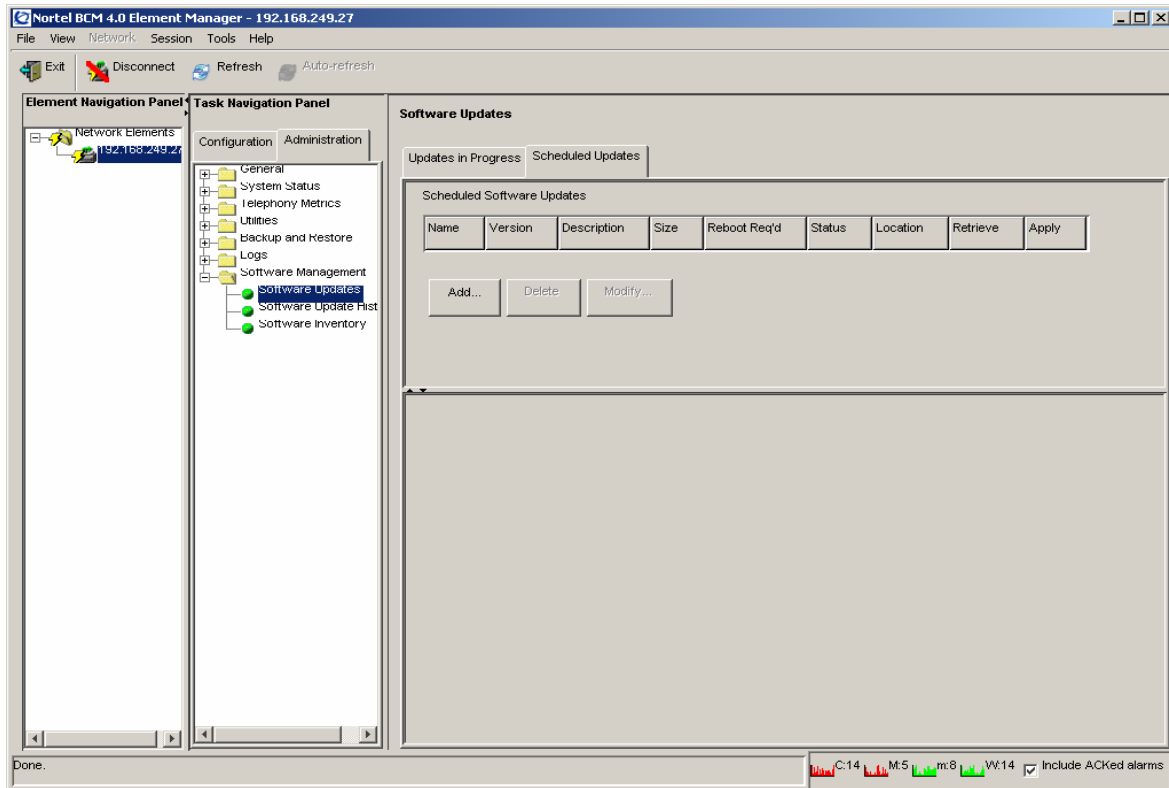


Table 112 lists the information that is available on the Updates in Progress table.

Table 112 Information about updates in progress

Detail	Description
Name	The name of the software update.
Version	The version of the software update.
Description	A brief description of the software update.
Size	The size of the software update, in KB.
Reboot Req'd	Displays whether the software update causes the BCM to reboot when the update has been applied. If a reboot is required, the check box is checked.
Location	The location from which the software update is being retrieved, for example an FTP server or a network folder.
Status	The status of the update. See Table 113 for information.

Table 113 lists the statuses of software updates.

Table 113 Software update statuses

Status	Description
Available	The software update is available to be applied to the BCM. Only an Available software update can be applied to the BCM.
Invalid	A newer version of software has been applied to the BCM, or a problem has been detected with the software update, and has rendered this software update invalid. An update will also be listed as invalid if a requirement for the update is not met; requirements may include keycodes or a related update.
Installed	The software update has been applied to the BCM.
In Progress	The software update is in the process of being applied to the BCM. An update may be In Progress for up to 15 minutes, depending on the size of the update file.
Scheduled	A download of the software update is scheduled.

You can change the order of columns in the Updates in Progress table by clicking a column heading and dragging it to a different place in the table.

To view details about software updates in progress

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task. The **Software Update** panel opens and displays the **Updates in Progress** tab.
- 3 View the details in the **Updates in Progress** table.
Once a software update is complete, the entry is removed from the **Updates in Progress** table and a new entry is added to the **Software History** table to document the installation of the software update.

Applying software updates

Once you have downloaded a software update from the Nortel Technical Support Web page, you can apply it to the BCM.

You can apply one software update at a time. For multiple software updates, repeat the following procedure until each update has been applied. When you have several updates to apply, any software updates that require the system to reboot should be applied last. Information about each update is available when you click the Show Details button.

Applying a software update is a two-part process:

- 1 You transfer a software update to the BCM, which validates the integrity of the software update and ensures that the BCM meets prerequisites for applying the software update.
- 2 You apply the software update to the BCM, which then brings the update into service.



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours. Refer to the detailed information provided with each update to understand its impact on the system.



Caution: In the case of some software updates, the BCM automatically restarts as soon as an update has been applied, without prompting or confirmation. These updates are identified as Reboot Req'd in the Find Software Updates window.



Note: Software update files may range in size from several hundred kilobytes to many megabytes, depending on the software components addressed by the software update. The amount of time required to transfer the software update to the BCM before you apply the update depends on the size of the software update file and on the type of connectivity between the location of the software update and the BCM being updated.

You can apply software updates that have a status of “Available.”

The application of software generates an information event, but does not generate an alarm condition.

You can apply updates from the following storage locations:

- a USB storage device
- your personal computer
- a shared folder
- an FTP server
- an HTTP server, with or without SSL

You can view details about a software update before you apply it. You can apply a software immediately or schedule the update for a future time.

Applied software is displayed in the Software Update History table.

Applying an update from your personal computer



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM automatically restarts as soon as the update is applied. You do not receive a reboot confirmation before the reboot occurs.

To apply an update from your personal computer

- 1 In the task panel, click the **Configuration** tab.
- 2 Select **System>Date and Time** and verify that the date, time, and time zone are correctly set.
- 3 In the task panel, click the **Administration** tab.
- 4 Open the **Software Management** folder, and then click the **Software Update** task. The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 5 Click the **Get New Updates** button. The **Get New Updates** window opens.
- 6 Select **My Computer** from the **Retrieve From** selection field.
- 7 Click the **Browse** button. The **Select** window opens.
- 8 Navigate to the directory where you unzipped the update file and click **Select**.



Note: The Select dialog displays directories only and does not show the contents of the directories.

- 9 Select the location from which you want to retrieve the update. The **Find Software Updates** window opens and displays a list of updates found in the specified location
- 10 Select an update. The update must have a status of “Available.”
- 11 To view details about the update, click the **Show Details** button. The **Details for Update** window opens and displays any details about the update. Click the **OK** button to close the details window.



Note: If the information in the **Find Software Updates** window indicates that you are applying an upgrade rather than an update, you will need to generate a keycode before proceeding.

- 12 Click the **Apply** button to apply the update.
A warning dialog box opens.
- 13 Click the **OK** button.
The **Software Update Complete** confirmation window opens.
- 14 A dialog box opens to display the options available for this update. The options available depend on the update that you are applying. Select the appropriate options and click the **OK** button. If no options are available, click the **OK** button to continue.
- 15 The **Updates in Progress** table lists the update as In Progress. Click the **OK** button.
A software update that has the **Reboot Required** field checked automatically restarts the BCM once the update has been applied.

Applying a software update from a USB storage device

Before you apply an update from a USB storage device, make sure that:

- the USB storage device is formatted as a FAT32 device
- you know the path to the location of the updates on the device
- the device is connected to the BCM
- the size of the software update is not greater than the capacity of the storage device



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.



Caution: Do not remove the USB storage device until the update is applied. Removing the device before the update has been applied may seriously harm the integrity of your system.

To apply a software update from a USB storage device

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task.
The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Get New Updates** button.
The **Get New Updates** window opens.
- 4 Select **USB Storage Device** from the **Retrieve From** selection field.
- 5 Enter the path to the location of the update in the **Directory** field.

- 6 Click the **OK** button.
The **Find Software Updates** window opens and displays a list of updates found in the specified location.
- 7 Select an update. The update must have a status of “Available”.
- 8 Click the **Apply** button.
A confirmation window opens.
- 9 Click the **Yes** button.
The **Software Update Complete** confirmation window opens.
- 10 Click the **OK** button.
The **Updates in Progress** table lists the update as “In Progress”. A software update that has the **Reboot Required** field checked will automatically reboot the BCM once the update has been applied.

Applying an update from a shared folder



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM will automatically reboot as soon as the patch has been applied. You will not receive a reboot confirmation before the reboot occurs.

To apply an update from a shared folder

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task.
The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Get New Updates** button.
The **Get New Updates** window opens.
- 4 Select **Network Folder** from the **Retrieve From** selection field.
- 5 Configure the network folder attributes.

Table 114 Configure Network Folder attributes

Attribute	Action
Network Folder	Enter the IP address or host name of the remote computer.
User Name	Enter the user name associated with the shared folder.
Password	Enter the user name associated with the shared folder.
Directory	Enter the name of the shared folder, as well as the path to update if it is a subdirectory of the shared folder.

- 6 Click the **OK** button.
The **Find Software Updates** window opens and displays a list of updates found in the specified location.
- 7 Select an update. The update must have a status of “Available”.
- 8 Click the **Apply** button.
A confirmation window opens.
- 9 Click the **Yes** button.
The **Software Update Complete** confirmation window opens.
- 10 Click the **OK** button.
The **Updates in Progress** table lists the update as “In Progress”. A software update that has the **Reboot Required** field checked will automatically reboot the BCM once the update has been applied.

Applying an update from an FTP server



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

To apply an update from an FTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task.
The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Get New Updates** button.
The **Get New Updates** window opens.
- 4 Select **FTP Server** from the **Retrieve From** selection field.
- 5 Configure the FTP Server attributes.

Table 115 Configure FTP Server attributes

Attribute	Action
FTP Server	Enter the IP address or host name of the remote computer, and the port number if required.
User Name	Enter the user name associated with the FTP server.

Table 115 Configure FTP Server attributes

Attribute	Action
Password	Enter the user name associated with the FTP server.
Directory	Enter the path to the location of the update. The path is relative to the root of the FTP server you are logging into. For example, if the root of the FTP server you have logged into is /public and your patches are located under /public/patches , you would enter patches as the directory.

- 6 Click the **OK** button.
The **Find Software Updates** window opens and displays a list of updates found in the specified location.
- 7 Select an update. The update must have a status of “Available”.
- 8 Click the **Apply** button.
A confirmation window opens.
- 9 Click the **Yes** button.
The **Software Update Complete** confirmation window opens.
- 10 Click the **OK** button.
The **Updates in Progress** table lists the update as “In Progress”. A software update that has the **Reboot Required** field checked will automatically reboot the BCM once the update has been applied.

Applying an update from an HTTP server



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Required column of the Find Software Updates window, the BCM will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

To apply an update from an HTTP server

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task.
The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Get New Updates** button.
The **Get New Updates** window opens.
- 4 Select **HTTP Server** from the **Retrieve From** selection field.

5 Configure the HTTP Server attributes.

Table 116 Configure HTTP Server attributes

Attribute	Action
HTTP Server	Enter the IP address or host name of the remote computer, and the port number if required.
Use HTTPS	Check this box if the HTTP server requires SSL.
User Name	Enter the user name associated with the HTTP server.
Password	Enter the user name associated with the HTTP server.
Directory	Enter the path to the location of the update. The path is relative to the root of the HTTP server you are logging into. For example, if the root of the HTTP server you have logged into is /public and your patches are located under /public/patches , you enter patches as the directory.

6 Click the **OK** button.

The **Find Software Updates** window opens and displays a list of updates found in the specified location.

7 Select an update. The update must have a status of “Available”.

8 Click the **Apply** button.

A confirmation window opens.

9 Click the **Yes** button.

The **Software Update Complete** confirmation window opens.

10 Click the **OK** button.

The **Updates in Progress** table lists the update as In Progress. A software update that has the **Reboot Required** field checked will automatically reboot the BCM once the update has been applied.

Creating and modifying scheduled software updates

You can apply a software update to the BCM at a future date by creating a schedule. A scheduled software update is displayed in the **Scheduled Updates** tab. You can schedule only one update at a time.

You can view, modify, or delete a scheduled software update. When you schedule a software update, the device where the update is stored (such as a USB device) must be connected to the BCM when you create the schedule.

Table 117 lists the information that is displayed about scheduled software updates in the Scheduled Software Updates table.

Table 117 Information about scheduled software updates

Columns	Description
Name	The name of the update.
Version	The version of the update.

Table 117 Information about scheduled software updates

Columns	Description
Description	A brief description of the update.
Size	The size of the software update, in kilobytes.
Reboot Req'd	Displays whether the software update causes the BCM to reboot when the update has been applied. If a reboot is required, the check box is checked.
Location	The storage location of the update. For example, FTP server.
Status	The status of the update. See Table 118 for information.
Retrieve	The date and time at which the update will be retrieved.
Apply	The date and time at which the update will be applied.

Table 118 lists the statuses of scheduled software updates.

Table 118 Statuses of scheduled software updates

Status	Description
Scheduled	The software update has been scheduled.
Removed	The scheduled software update has been deleted.
Modified	The scheduled software update has been modified.
Applied	The scheduled software update has been applied to the BCM.

Creating a scheduled software update



Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.

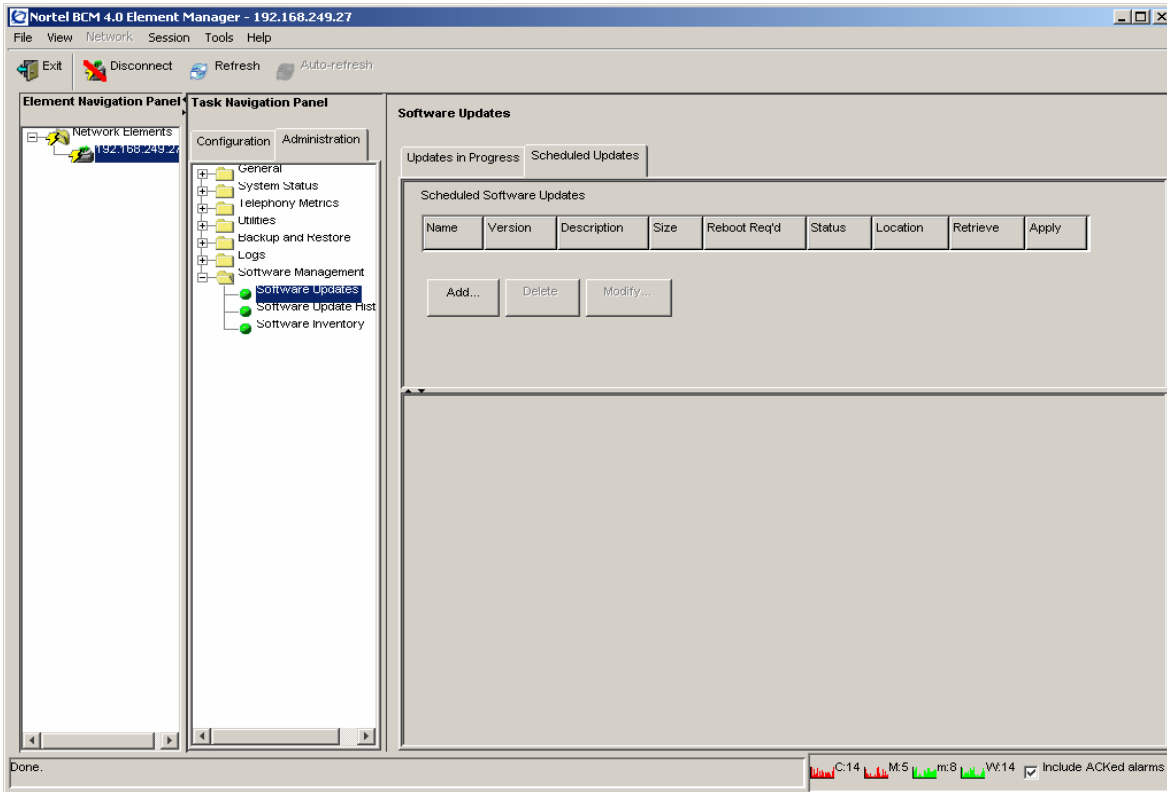


Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the New Updates Found window, the system will automatically reboot as soon as the patch has been applied. You will not receive a reboot confirmation before the reboot occurs.

To create a scheduled software update

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task. The **Software Update** panel opens. The **Updates in Progress** tab is open.

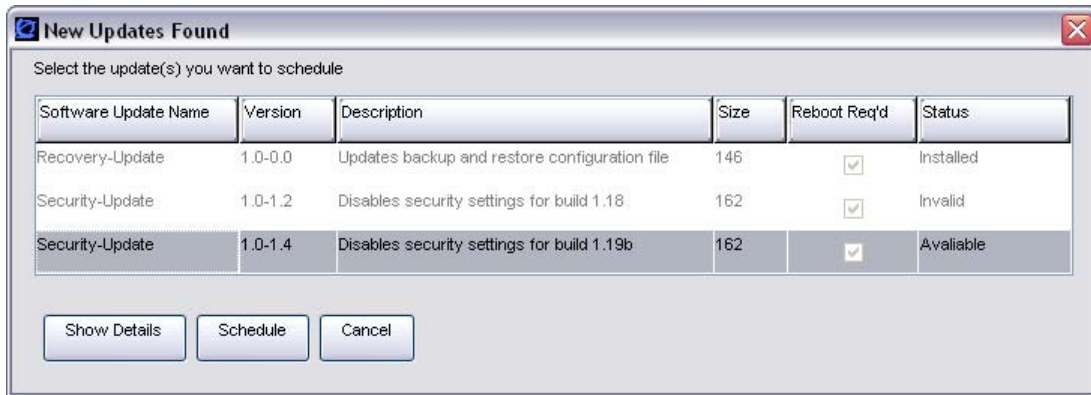
- 3 Click the **Scheduled Updates** tab.
The **Scheduled Software Updates** panel opens.



- 4 Click the **Add** button.
The **Get New Updates** window opens.
- 5 In the **Retrieve From** selection field, select the location where the software update is stored:
 - USB Storage Device
 - My Computer
 - Network Folder
 - FTP Server
 - HTTP Server
- 6 Select an update location and/or complete the appropriate access information. For more information, see the procedures in [“Applying software updates”](#).

- 7 Click the **OK** button.

The **New Updates Found** window opens and displays a list of updates found in the specified location.



- 8 Select an update. The update must have a status of “Available”.
- 9 To view the details for an update, click the **Show Details** button.
The **Details for Update** window opens and displays any details about the update. Click the **OK** button to close the details window.
- 10 Click the **Schedule** button to create a schedule.
The **Schedule Software Updates** window opens.
- 11 Click the **Retrieve** field to select a date and time at which to retrieve the update. A calendar window opens.
- 12 Select a retrieve date and time, and then close the window.
- 13 Click the **Apply** field to select a date and time at which to apply the update. A calendar window opens.
- 14 Select an apply date and time, and then close the window.
- 15 Click the **OK** button.
The software update is added to the **Scheduled Software Updates** table. The status of the update is “Schedule”.

Modifying a scheduled software update



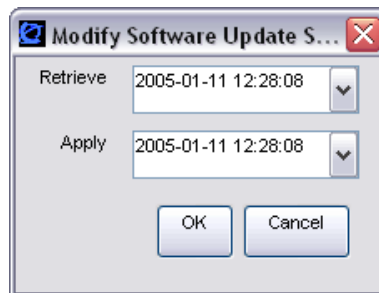
Caution: Applying a software update to the BCM is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the New Updates Found window, the BCM will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

To modify a scheduled software update

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task. The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Scheduled Updates** tab.
- 4 In the **Scheduled Software Updates** table, select a scheduled update.
- 5 Click the **Modify** button.
The **Modify Scheduled Software Update** window opens.



- 6 Click the **Retrieve** field to select a date and time at which to retrieve the update. A calendar window opens.
- 7 Select a retrieve date and time, and then close the window.
- 8 Click the **Apply** field to select a date and time at which to apply the update. A calendar window opens.
- 9 Select an apply date and time, and then close the window.
- 10 Click the **OK** button.
The modified software update is displayed in the **Scheduled Software Updates** table. The modification may take a few minutes to appear in the table.

To delete a scheduled software update

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update** task. The **Software Update** panel opens. The **Updates in Progress** tab is open.
- 3 Click the **Scheduled Updates** tab.
- 4 In the **Scheduled Software Updates** table, select a scheduled update.
- 5 Click the **Delete** button. The **Confirm Delete** window opens.
- 6 Click the **Yes** button to delete the update. The scheduled update is removed from the **Scheduled Software Update** table.

Viewing a history of software updates

Using the Software Update History panel, you can view the history of all software updates, including software upgrades, that have been applied to the BCM since the it was shipped.

You can:

- view the current software release level of the BCM
- view a history of all software updates (including upgrades) applied to the BCM
- view release notes that apply to a particular software update
- remove certain software updates from the BCM

Table 119 lists the information displayed in the Software Update History table.

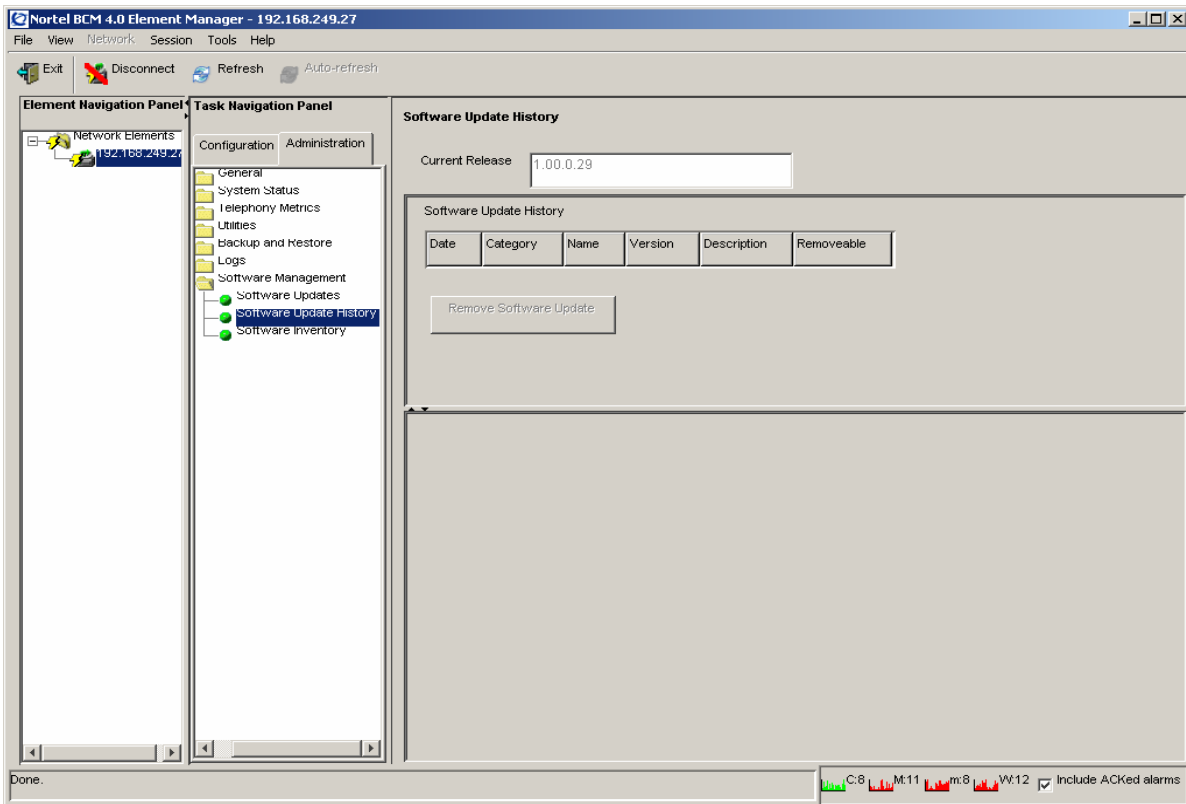
Table 119 Information displayed in the Software Update History table

Columns	Description
Date	The date and time that the software update was applied.
Category	The software update category (Scheduled, Removed, Modified, Applied).
Name	The name of the software update.
Version	The version of the software update.
Description	A brief description of the software update.
Removeable	Indicates whether the software update can be removed from the BCM. If it can be removed, the check box is checked.

To view the software update history

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update History** task. The **Software Update History** panel opens.

- View the updates in the **Software Update History** table. If software updates have not been applied to your BCM, the table is empty.



- To view release notes about a particular software update, select the update in the table. Release notes containing details about the software update are displayed in the **Release Notes** panel below the table.

Removing software updates

You may find that you need to remove a software update that has been applied to the BCM. Not all software updates can be removed; whether a software update can be removed depends on the particular software update.

Removing a software update does not remove the software itself from the BCM; it only returns the software components of the software update to a previous software version. You must have administrator privileges to remove a software update from the BCM.

Removing a software patch or upgrade from the BCM is a service-affecting operation. All services running on the system will be stopped. Consequently, Nortel recommends that you schedule removal of updates for low-traffic periods.

If a software update is applied to a BCM and then removed, this information is displayed in the Software Update History table. A removal operation is logged by the BCM, but does not generate an alarm condition.

You can remove a software update if the update has a checkmark in the Removeable column of the Software Update History table.

Removing a software update



Caution: Removing a software patch or upgrade from the BCM is a service-affecting operation. All services running on the system will be stopped. Consequently, Nortel recommends that you schedule removal of updates during low-traffic hours.

To remove a software update

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Update History** task. The **Software Update History** panel opens.
- 3 Select an update in the **Software Update History** table. The update must have a checkmark against it in the **Removeable** column.
- 4 Click the **Remove Software Update** button. A confirmation window opens.
- 5 Click **Yes**. The **Category** column in the **Software Update History** table displays “Patch Removed” for the removed software update.

Viewing the inventory of BCM software

BCM software is organized into software components that you can individually update as required. The version of each software component is tracked so that you can determine the exact software release level of a BCM to the component level.

You can view the complete inventory of software installed on the BCM. The Software Inventory table displays all the software components installed on the system, the functional group and the software version of each component.

Table 120 lists the information displayed in the Software Component Version Information table.

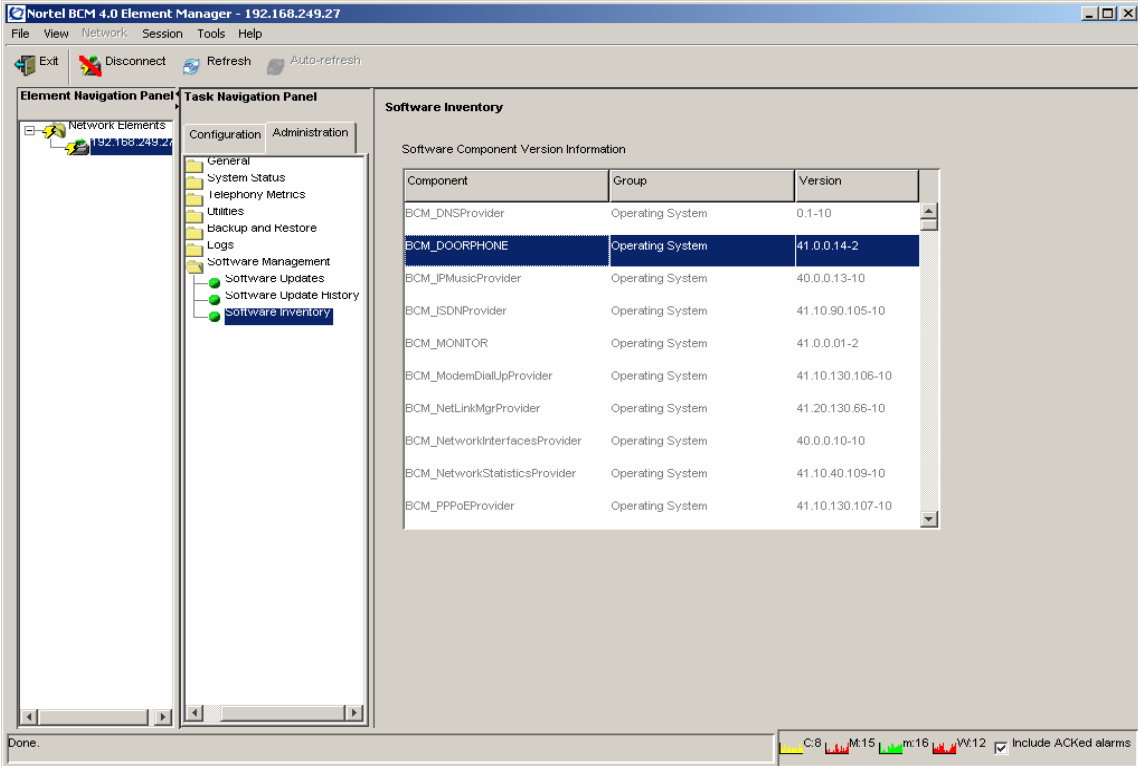
Table 120 Information displayed in the Software Component Version Information table

Column	Description
Component	The name of the software component installed on the BCM. For example, backup-recovery.
Group	The functional group to which the software component belongs. For example, Operating System.
Version	The version of the software component.

You can change the order of the information displayed in the table by clicking a column heading and dragging it to a new place in the table. You can also sort the information in a column by descending or ascending order, by clicking the column heading.

To view the BCM software inventory

- 1 In the task panel, click the **Administration** tab.
- 2 Open the **Software Management** folder, and then click the **Software Inventory** task. The **Software Inventory** panel opens.
- 3 View the details in the **Software Component Version Information** table.



The screenshot shows the Nortel BCM 4.0 Element Manager interface. The main window displays the **Software Inventory** panel, which contains a table titled **Software Component Version Information**. The table has three columns: **Component**, **Group**, and **Version**. The **BCM_DOORPHONE** component is highlighted in blue. The status bar at the bottom shows "Done." and a set of alarm indicators for C:8, M:15, m:16, and W:12, along with a checkbox for "Include ACKed alarms".

Component	Group	Version
BCM_DNSProvider	Operating System	0.1-10
BCM_DOORPHONE	Operating System	41.0.0.14-2
BCM_IPMusicProvider	Operating System	40.0.0.13-10
BCM_JSDNProvider	Operating System	41.10.90.105-10
BCM_MONITOR	Operating System	41.0.0.01-2
BCM_ModemDialUpProvider	Operating System	41.10.130.106-10
BCM_NetLinkMgrProvider	Operating System	41.20.130.66-10
BCM_NetworkInterfacesProvider	Operating System	40.0.0.10-10
BCM_NetworkStatisticsProvider	Operating System	41.10.40.109-10
BCM_PPPEProvider	Operating System	41.10.130.107-10

Chapter 14

Accounting Management

This chapter describes how to manage accounts in a BCM system.

Overview of accounting management

BCM Call Detail Recording (CDR) is an application that records call activity. Each time a telephone call is made to or from a BCM, detailed information about the call can be captured into a Call Detail Recording file. You can use this information to:

- create billing records using third party software
- monitor call activity and therefore infer information about system utilization and other indicators of system and services activity



Note: CDR monitors only incoming and outgoing calls. It does not monitor calls within the BCM system.

About Call Detail Recording

You can use information collected by Call Detail Recording to determine whether the telephone system is being used efficiently and to guard against abuse of the telephone system.

Call Detail Recording provides information about:

- the date and time of a call, and digits dialed
- the originating and the terminating line or station set
- whether an incoming call was answered
- elapsed time between origin of a call and when it was answered
- whether a call was transferred or put on hold
- call duration
- call charges
- calls associated with Account codes
- incoming call Calling Line Identification (CLID) information
- bearer Capability of the line in the call
- hospitality records for room occupancy status
- real Time records for ringing, DNIS, answered, unanswered, transferred, and released events
- for incoming calls with CLID information and Hospitality room occupancy status

CDR information can be collected for all calls, outgoing calls only, specific long distance prefix strings only, or calls associated with an account code only (to track calls for client billing purposes). You can set parameters to specify whether additional information should be recorded, such as hospitality information, including room occupancy status and room number information.

Using Call Detail Recording

BCM Call Detail Recording is covered in detail in the *Call Detail Recording System Administration Guide* (N0060599). The Call Detail Recording System Administration Guide covers the following topics:

- setting up the system so that the information you want to collect is written to the Call Detail Record
- configuring CDR data file management and transfer
- installing and using the CDR Client for real-time monitoring of CDR records

You can configure the BCM to create a new CDR file on a daily, weekly, or monthly basis, or when the file reaches a specified size. You can retrieve CDR files by configuring the BCM to send (“push”) the files to a remote system or by using a toolkit application to retrieve (“pull”) the files from a remote system.



Note: Two CallPilot reports are included in the data transfer when CDR data files are “pulled” or “pushed” from the BCM system. These are the Call Pilot Mailbox activity report and the All Mailbox Activity Report.

CDR Toolkit

A CDR Toolkit is provided with the BCM to enable third-party developers to retrieve BCM Call Detail Record data files and integrate them into their applications.

Appendix A

Management Information Bases

This appendix describes the Management Information Bases (MIBs) supported by the BCM.

A MIB is a virtual information store that contains a collection of objects that are managed using Simple Network Management Protocol (SNMP). The MIB is software that defines the data reported by a computing or network device and the extent of control over that device.

About SNMP MIBs

A MIB enables access to the managed objects of a system. MIBs are managed using a network management protocol, such as Simple Network Management Protocol (SNMP).

BCM supports the following MIBs:

- MIB-II (RFC1213)
- SNMP-FRAMEWORK-MIB (RFC2261)
- ENTITY-MIB (RFC273)
- HOST-MIB (RFC2790)
- IF-MIB (RFC2863)
- BCM Small Site MIB
- BCM Small Site Events MIB
- OSPFv2 (RFC1850)
- RIPv2 (RFC1724)

BCM supports read-only SNMP requests, even for SNMP variables that display as read-write. BCM does not support configuration through SNMP. Variables that are not supported are displayed as “0.”

MIB file descriptions

BCM MIBs belong to two categories:

- Standard MIBs — include MIB-II (RFC1213), SNMP-FRAMEWORK-MIB (RFC2261), ENTITY-MIB (RFC273), HOST-MIB (RFC2790), and IF-MIB (RFC2863)
- Nortel MIBs — include BCM Small Site MIB and BCM Small Site Events MIB

Table 121 lists the file names and file descriptions of each supported standard MIB.

Table 121 MIB file descriptions for standard MIBs

MIB	File Name	Notes
MIB-II	rfc1213.mib	This MIB defines the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets.
SNMP-FRAMEWORK-MIB	rfc2261.mib	This is the SNMP Management Architecture MIB. This standard MIB displays parameters related to the SNMP agent on the BCM.
ENTITY-MIB	rfc2737.mib	This MIB defines physical and logical system components on the BCM and associations between these components.
HOST-MIB	rfc2790.mib	This MIB is used to manage host systems. It is useful for monitoring resource usage and system performance.
IF-MIB	rfc2863.mib	This MIB describes generic objects for network interface sub-layers.
OSPFv2 MIB	rfc1850.mib	This MIB describes objects for monitoring the Open Shortest Path First routing protocol.
RIPv2 MIB	rfc1724.mib	This MIB describes objects for monitoring the Routing Information Protocol.

Table 122 lists the file names and file descriptions of each supported Nortel MIB.

Table 122 MIB file descriptions for Nortel MIBs

MIB	File Name	Notes
Small Site MIB	Smallsite.mib	This MIB defines the upper-level hierarchy of an enterprise(1).nortel(562) sub-branch called smallsite. This Nortel MIB is the basis for several Nortel smallsite products. In the BCM, this MIB is a prerequisite for the Small Site Events MIB.
Small Site Events MIB	Smallsiteevents.mib	This MIB defines the events (traps) that the Small Site product or component can use. This MIB describes the events generated by the BCM. This MIB contains fields such as eventId, eventSource, eventTime, and EventDescr.

Accessing, compiling, and installing MIB files

You access MIB files from the BCM Web Page. You can also access BCM MIB files as a zipped file from the Nortel Customer Service Site.



Note: You can use a MIB browser to load MIB information so that you can browse the structure of a MIB. An example of a MIB browser is Microsoft Operations Manager (MOM). Each MIB browser has its own MIB compilation tool.

To access MIB files from the BCM Web Page

- 1 Go to the BCM Web Page.
- 2 Click the **Administration Applications** link.
- 3 Click **Download MIBs**.
- 4 Click **Download Device MIBs**.
A File Download dialog box displays.
- 5 Click **Save** to download the file.

To access MIB files from the Nortel Customer Service Site

- 1 In your browser, go to <http://www.nortel.com>.
The Nortel Customer Service Site home page opens.
If you used the direct link, the Technical Support page opens. Go to step 5.
- 2 Select the **Support & Training** navigation menu, and then select **Technical Support, Software Downloads**.
The **Technical Support** page opens. The **Browse Product Support** tab displays **Product Finder** fields.
- 3 In area **1**, select **Product Families** from the selection field, and then select **BCM** from the selection box.
- 4 In area **2**, select **Business Communications Manager (BCM)**.
- 5 In area **3**, select **Software**.
- 6 Click the **Go** link.
The **Software** tab opens.
- 7 In the **by Title/Number Keyword** field, enter **mib**, and then press the **Enter** key.
A list of MIBs is displayed.
- 8 In the **Title** column, click the **BCM MIB** link.
The **Software Detail Information** page opens.
- 9 Right-click the **BCM MIB** link, and select **Save Target As**.
The **File Download** dialog box opens.

- 10** In the **Save As** dialog box, select the file or folder in which you want to save the MIB zip file, and then click the **Save** button.

The MIB zip file is saved to your personal computer.

Compiling and installing Nortel MIB files



Note: Small Site MIBs have definitions for the binding values of the BCM SNMP traps. For more information, see [Table 125](#) in this section.

Complete the compilation procedure, in the following order:

- a SmallSite.mib
- b SmallSiteEvents.mib

Compiling and installing standard MIB files

Complete the compilation procedure, in the following order:

- a rfc1213.mib
- b rfc2261.mib
- c rfc2737.mib
- d rfc2790.mib
- e rfc2863.mib



Note: BCM files are created and released in a MicroSoft Windows environment so that when these files are copied and transferred to a UNIX environment the last carriage return can be deleted. In this case, you can get an “END is not found” error message during the compilation. Open the MIB file with a UNIX text editor and add a carriage return at the end of the word “END”.

Small Site MIB

The device sysObjectIDs are defined in the BCM Small Site MIB. The sysObjectIDs are defined for the BCM main unit. Table 123 summarizes the sysObjectID assignments.

Table 123 sysObjectID assignments

Model	Main Unit sysObjectID
BCM	1.3.6.1.4.1.562.37.1.7

Small Site Event MIB

The Small Site Events MIB defines events (SNMP traps) that can be used by any Small Site product or component. BCM traps can be captured and viewed using a standard SNMP fault monitoring framework or trap watcher.

SNMP traps are generated by the BCM if you have enabled SNMP for specific BCM alarms. You configure SNMP settings using the Alarm Settings task in the Element Manager. For information about how to configure SNMP traps, see [Chapter 6, “Managing BCM with SNMP,”](#) on page 135.

Table 124 lists the BCM-specific SNMP trap fields for Small Site Event MIBs.

Table 124 BCM-specific SNMP trap fields for the Small Site Event MIB

Trap Field	Description
Enterprise	OID identifies the product (iso.org.dod.internet.private.enterprises.nortel.smallsite.common.events[1.3.6.1.4.1.562.37.3.1])
Agent address	IP address of one of the BCM interfaces
Generic trap type	6 for Enterprise-specific traps
Specific trap type	1 = eventInfo trap type 2 = eventWarning trap type 3 = eventError trap type
Time stamp	the system up time

Table 125 lists the BCM-specific SNMP variable bindings.

Table 125 BCM-specific variable bindings

Trap Field	Description
Binding #1	Contains the corresponding alarm ID. OID: 1.3.6.1.4.1.562.37.3.1.1.0
Binding #2	Contains the name of the software component that generated the alarm (trap). This is in the 3-part DN format defined in the Nortel Common Alarm Framework. The 3-part DN is in the format: systemId=BCM, entityId=System Name, subEntityId=Component Name OID: 1.3.6.1.4.1.562.37.3.1.2.0
Binding #3	Contains the alarm (trap) Date and Time OID: 1.3.6.1.4.1.562.37.3.1.3.0
Binding #4	Contains the alarm (trap) problem description OID: 1.3.6.1.4.1.562.37.3.1.4.0

Index

A

account created, users 116
 account expiry, users 115
 account failed login 116
 account modified, users 116
 account successful login 116
 Application backups, about 316
 applications
 callback numbers, users 115

B

Backing up and restoring, overview 315
 Backup and Restore Data
 Backup
 Backup destinations 318
 Creating a scheduled backup 327, 328, 330, 331, 332
 Overview 315
 Restore 335
 Options 335
 Backup schedule, creating 326
 Backup schedule, creating or modifying 334
 Backup schedule, deleting 334
 Backup schedule, modifying 334
 Backup, destinations 318
 Backup. See Backup and Restore Log Data
 BCM Monitor 285
 BCM Monitor, Installing 286
 BCM Monitor, Removing 286
 BCM Monitor, Starting 287
 BCM system, Connecting to 287
 blocking interface
 access time remaining 112
 BMC Monitor, installing 286
 Business Communications Manager
 Overview 23

C

Call Detail Recording
 CDR Toolkit 388
 Overview 387
 Using CDR 388

callback 90
 user accounts 115
 CbC Limit Metrics. See Metrics
 certificate
 private security key 123
 uploading a security certificate 123
 challenge key 75
 Community string values, configuring 139
 Community string, adding 139
 Community string, deleting 140
 complexity, password 75
 Configuring, dynamic snapshots 292
 Configuring, static snapshot settings 289
 Conventions, guide 19
 button options 19
 buttons 19
 command line 19
 copyright 2
 counter, rest lockout counter 76
 current user 111
 current user, change password 111
 current user, telset password 112
 current user, telset user ID 111

D

Diagnostic Settings 313
 Diagnostic Settings. See Metrics
 dialback 90
 dial-in
 setting up callback 90
 disable telset interface 74
 disable user accounts 114
 Disconnecting, from a BCM 288
 Display 19
 Dynamic snapshot, Starting 293
 Dynamic snapshot, Stopping 294
 Dynamic snapshots 291
 Dynamic snapshots, configuring 292
 Dynamic snapshots, starting 293
 Dynamic snapshots, stopping 294

E

Element Manager

- last successful log-in 112
- minimum password length 75
- minimum user ID length 75
- password complexity 75
- user session timeout 77

enable lockout 76

enable telset interface 74

exclusive access time remaining 112

F

failed login 116

H

Hard reset, telephony services 310

Hunt Group Metrics. See Metrics

I

Immediate backups, performing 320, 321, 322, 323, 324, 325

Info tab 294

IP Devices tab 296

ISDN

- modem link, setting up callback 90

K

key

- private security key 123

L

last failed login 116

Line Monitor tab 301

Lines, viewing 302

locked out 114

lockout counter reset 76

Lockout duration 76

lockout policy

- lockout duration 76

Log files, extracting 361

Log files, retrieving 347

Log files, transferring with the BCM Web page 357

Log files, using the BCM Element Manager 347

Log files, viewing with the Log Browser 363

Log Management

- Diagnostic logs 346

Operational Logs 346

Sensitive logs 346

System information logs 347

Logging, UIP data 299

log-in

last successful 112

security message, disable 74

M

maintenance

exclusive access time 112

Mean Opinion Scores. See QoS Monitor

Media Card tab 295

Metrics

Overview 245

System Metrics 245

CbC Limit Metrics 272

Accessing 273

Diagnostic Settings 277

Hunt Group Metrics 274

Accessing 275

NTP Metrics 253

Accessing 254

PSTN Fallback Metrics 276

Accessing 276

QoS Monitor 247

Refreshing 251

Viewing 250

Trunk Module Metrics 266

B-Channel 268, 269

CSU Alarm History 272

CSU Alarms 271

CSU statistics 269

Disabling or enabling a port channel setting 268

Viewing D-Channel information 268

Viewing Performance History information 268

Viewing Trunk Module status 266

UPS Monitor

Accessing 251

Telephony Metrics

Overview 265

Minimum and maximum values, resetting 305

Minimum and maximum values, viewing 304

Minimum and maximum values, viewing the date and time 304

minimum password length 75

minimum user ID length 75

modem

callback number, users 115

N

Nortel service

challenge key 75

NTP Metrics. See Metrics

P

password

complexity 75

current user 111

current user, terset 112

last successful log-in 112

lockout duration 76

minimum length 75

Ping 305

Ping, to ping a device 306

post log-in message, enable/disable 74

private security key 123

Q

QoS Monitor. See Metrics

R

Rebooting, the BCM system 309

regulatory information 2

related publications 20

Reset 308

reset, lockout counter 76

Restore, options 335

Restores, performing 337, 338, 339, 340, 341, 342, 343

Restoring Logs, See Backup and Restore Logs

Restoring, about 335

Restoring, data from the BCM 337, 338, 339, 340, 341, 342

RTP Sessions tab 297

S

security

callback number, user accounts 115

challenge key 75

change password 91

disable user accounts 114

locking out users 114

lockout duration 76

minimum password length 75

minimum user ID length 75

password complexity 75

post log-in message 74

private security key 123

system lockout counter 76

terset user ID 114, 119

Unified Manager considerations 121

uploading a certificate 123

user ID 114, 119

Service access points, adding 140

Service access points, deleting 142

Service access points, details 142

Service access points, modifying 142

Services access points, configuring 140

session timeout 77

Shutting down the BCM 309

Snapshots, dynamic 291

Snapshots, static 289

SNMP trap destinations, deleting 145

SNMP, adding community strings 139

SNMP, adding management stations 138

SNMP, adding trap destinations 143

SNMP, configuring community strings 139

SNMP, configuring general settings 136

SNMP, configuring service access points 140

SNMP, configuring settings 137

SNMP, configuring the agent 136

SNMP, configuring trap destinations 143

SNMP, deleting community strings 140

SNMP, deleting management stations 138

SNMP, management stations 136

SNMP, modifying trap destinations 144

SNMP, support for 135

SNMP, supported MIBs 135, 389

SNMP, supported versions 135

Software inventory, viewing 385

Software Update

Overview 369

Scheduled Update

Adding a new update 379

Modifying a new update 382

- Update History
 - Removing an update from Software History 383
- Software updates, applying 371
- Software updates, deleting a schedule 383
- Software updates, history 383
- Software updates, obtaining 369
- Software updates, removing 384
- Starting, BCM Monitor 287
- Static snapshot settings, Configuring 289
- Static snapshot, Saving 291
- Static snapshots, About 289
- Static snapshots, configuring 289
- Statistical values, using 304
- Symbols 19
- System status, analyzing 289
- system timeout 77

T

- telset
 - current user ID 111
 - current user password 112
 - disable login 74
 - minimum password length 75
 - minimum user ID length 75
 - password complexity 75
 - user ID 114, 119
- Timeout settings, configuring 300
- Timeout, enabling or disabling 300
- timeout, user session 77
- Trace Route 307
- Trace Route, performing 307
- trademarks 2
- Trap destinations, adding 143
- Trap destinations, configuring 143
- Trap destinations, deleting 145
- Trap destinations, modifying 144
- Trunk Modules Metrics. See Metrics

U

- UIP Message details, clearing 301
- UIP messages, disabling monitoring 299
- UIP messages, enabling monitoring 299
- UIP messages, expanding 301
- UIP tab 298
- UIP, logging data 299

- UIP, viewing log files 300
- Unified Manager
 - security considerations 121
- UPS Metrics. See Metrics
- Usage Indicators tab 302
- user
 - lockout duration 76
- user account
 - telset user ID 114, 119
 - user ID 114, 119
- user accounts
 - callback number 115
- user ID
 - current user 111
 - current user, telset 111
 - last successful log-in 112
 - user account 114, 119
- users
 - account created 116
 - account modified 116
 - disable account 114
 - disable telset interface 74
 - enabled account expiry 115
 - failed login 116
 - locked out 114
 - lockout counter 76
 - minimum password length 75
 - session time out 77
 - setting up callback 90
 - successful login 116
- Utilities, BCM Monitor 285
- Utilities, ping 305
- Utilities, Reset 308
- Utilities, Trace Route 307

V

- V.90
 - setting up callback 90
- Voice Ports tab 296

W

- Warm reset, telephony services 309