Return
to Menu

BCM50
Administration Guide

Part No. N0016868 01
08 April 2005

Copyright © Nortel Networks Limited 2005

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.

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

Task List

Using the BCM50 Service Management System 223

Using BCM50 Metrics 227

BCM50 Utilities 249

Contents

Figures

Tables

Chapter 1
Getting started

This section contains information on the following topics:

About this guide

The *BCM50 Administration Guide* describes how to manage, maintain and sustain BCM50 network services.

Purpose

The concepts, operations, and tasks described in the guide relate to the FCAPS (fault, configuration, administration, performance, and security) management strategy for the BCM50 and BCM50 network. This guide provides task-based information on how to detect and correct faults through the interfaces and reporting system.

Use the Nortel Element Manager (EM) and Network Configuration Manager (NCM) applications to implement, monitor and administer the network level operations. Use this guide to perform equivalent network-level operations using an SNMP based network management system.

In brief, the information in this guide explains:

- Network structure and concepts
- Network management tools
- Fault management & monitoring
- Performance management
- Security administration

Audience

The *BCM50 Administration Guide* is directed to network administrators responsible for maintaining BCM50 networks. This guide is also useful for network operations center (NOC) personnel supporting a BCM50 managed services solution. To use this guide, you must:

- be an authorized BCM50 administrator within your organization
- know basic Nortel BCM50 terminology
- be knowledgeable about telephony and IP networking technology

Organization

This guide is organized for easy access to information that explains the concepts, operations and procedures associated with using the BCM50 network management applications.

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 BCM50 Management Guide organization

Chapter	Contents
Chapter 2, "Overview of BCM50 Administration"	This chapter introduces BCM50 network-level management concepts and techniques.
Chapter 3, "Business Communications Manager Management Environment"	This chapter contains information on the different tools available to manage your BCM50. It also describes the new Element Manager application in detail.
Chapter 4, "BCM 50 Security Policies and Accounts and Privileges"	This chapter describes BCM50 Security Policies and Accounts and Privileges, which allow you to establish system-wide security policies and maintain system access security using settings on the Element Manager.
Chapter 5, "Using the BCM50 Hardware Inventory"	This chapter describes how to use the BCM50 Hardware Inventory.
Chapter 6, "Managing BCM50 with SNMP"	This chapter describes the management of the BCM50 using the SNMP protocol.
Chapter 7, "Using the BCM50 Fault Management System"	This chapter contains information about managing alarms generated by the BCM50 system and administering alarm settings.
Chapter 8, "Using the BCM50 Service Management System"	This chapter describes how to use the BCM50 Element Manager to view and administer the services that run on the BCM50 system.
Chapter 9, "Using BCM50 Metrics"	This chapter describes how to use the BCM50 Element Manager to view detailed information about the performance of the BCM50 system and of system resources.
Chapter 10, "BCM50 Utilities"	This chapter contains information about the utilities that are part of the BCM50 Element Manager.
Chapter 11, "Backing Up and Restoring BCM50 Data"	This chapter provides information about how to back up and restore data from the BCM50 system.
Chapter 12, "Managing BCM50 Logs"	This chapter contains information about viewing and managing log files generated by the BCM50.
Chapter 13, "Managing BCM50 Software Updates"	This chapter contains information about managing BCM50 software updates.
Chapter 14, "Accounting Management"	This chapter describes the management of accounts in the BCM50.
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 BCM50 system.

About BCM50

The BCM50 system provides private network and telephony management capability to small and medium-sized businesses.

The BCM50 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

BCM50 key elements

BCM50 includes the following key elements:

BCM50 main units

Three types of main units are available:

- **BCM50 (with Telephony Only)**
  The BCM50 main unit provides call processing and simple data networking functions. It also provides connections for telephones, Public Switched Telephone Network (PSTN) lines, and a LAN.
- **BCM50e (with Ethernet Router)**
  The BCM50e main unit provides call processing and data routing features. It also provides connections for telephones, Public Switched Telephone Network (PSTN) lines, a LAN, and an ethernet router.
- **BCM50a (with ADSL Router)**
  The BCM50a main unit provides call processing, data routing features and an integrated ADSL modem. It also provides connections for internal telephones, Public Switched Telephone Network lines, a LAN, and an ADSL router.

BCM50 hardware

In addition to the main platform configurations, the following hardware is available:

- **Expansion unit**: This unit is designed to accommodate a media bay module (MBM). The BCM50 main unit supports up to two expansion units.
- **Small system wallmount bracket**: A bracket designed for mounting the BCM50 main unit or expansion unit to a wall. An optional wiring field card (WFC) is available with the wallmount bracket, which provides RJ-45 connectors for all BCM50 main unit trunk and station interfaces, and a terminal block to connect the auxiliary equipment.
- **Small system rackmount shelf**: A shelf designed for mounting up to four BCM50 units into a standard 19 inch equipment rack. An optional patch field is available, which provides RJ-45 connectors for all BCM50 main unit trunk and station interfaces, and a terminal block to connect the auxiliary equipment.

BCM50 features

BCM50 supports the complete range of IP telephony features offered by existing BCM products.

You enable the following features by entering the appropriate keycodes (no additional hardware is required):

- VoIP Gateway (H.323): Up to 12 VoIP trunks
- VoIP Telephony Clients: Up to 32 VoIP Telephony clients, supporting the range of Nortel IP Phones.

BCM50 applications

BCM50 also supports many of the high-value applications provided on the existing BCM platforms.

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

Symbols and conventions used in this guide

These symbols are used to highlight critical information for the BCM50 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 BCM50 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`**`}`.
italic text	Indicates book titles
`plain Courier text`	Indicates command syntax and system output (for example, prompts and system messages). Example: `Set Trap Monitor Filters`
FEATURE **HOLD** **RELEASE**	Indicates that you press the button with the coordinating icon on whichever set you are using.

Related publications

Related publications are listed below. To locate specific information, you can refer to the ***Master Index of the BCM50 Library***.

BCM50 Core Guides

BCM50 Keycode Installation Guide (N0016865)

BCM50 Administration Guide (N0016868)

BCM50 Installation & Maintenance Guide (N0027152)

BCM50 ISDN Device Installation & Configuration Guide (N0027268)

BCM50 IP Telephone Installation and Configuration Guide (N0027269)

BCM50 Device Configuration Guide (N0027146)

BCM50 First Time Installation and Configuration Guide (N0027149)

BCM50 LAN CTE Configuration Guide (N0027154)

BCM50 Networking Configuration Guide (N0027156)

BCM50 System Overview (N0027157)

BCM50 Analog Device Installation and Configuration Guide (N0035159)

BCM50 Telset Administration Guide (N0027176)

BCM50 Unified Messaging Installation and Maintenance Guide (N0027179)

BCM50a Integrated Router Configuration Guide (N0027181)

BCM50e Integrated Router Configuration Guide (N0027182)

BCM50 Call Detail Recording Guide (N0027926)

BCM50 Digital Telephone Installation and Configuration Guide (N0027330)

BCM50 Telephone Features User Guide (N0027160)

CallPilot and Call Center Guides

Call Center Agent Guide (N0027187)

Call Center Set Up and Operation Guide (N0027203)

Call Center Supervisor Guide (N0027206)

CallPilot 2.5 Unified Messaging Addendum (N0027223)

CallPilot 2.5 Unified Messaging User Guide for Internet Clients

CallPilot 2.5 Unified Messaging User Guide for Lotus Notes

CallPilot 2.5 Unified Messaging User Guide for Microsoft Outlook

CallPilot 2.5 Unified Messaging User Guide for Novell GroupWise

CallPilot Call Center Telephone Administration Guide (N0025637)

CallPilot Fax Set Up & Operation Guide (P0606017)

CallPilot Fax User Guide (N0027227)

CallPilot Manager Set Up and Operation Guide (N0027247)

CallPilot Message Networking Set Up and Operation Guide (N0027249)

CallPilot Message Networking User Guide (N0027253)

CallPilot Programming Record (N0027404)

CallPilot Quick Reference Card - CP Interface (N0027401)

CallPilot Quick Reference Card - NVM Interface (N0027379)

CallPilot Quick Reference Card - Remote Users (CP Interface) (N0027359)

CallPilot Quick Reference Card - Remote Users (NVM Interface) (N0027346)

CallPilot Reference Guide (N0027332)

CallPilot Telephone Administration Guide (N0027331)

Central Answering Position (CAP) User Guide (P0603480)

Hospitality Features Card (N0027326)

i2050 Software Phone Installation Guide (N0022555)

IP Phone 2001 User Guide (N0027313)

IP Phone 2002 User Guide (N0027300)

IP Phone 2004 User Guide (N0027284)

NCM Release Notes & Installation Guide (N0027265)

Personal Call Manager User Guide (N0027256)

System-wide Call Appearance (SWCA) Features Card (N0027186)

T24 KIM Installation Card (P0603481)

T7000 Telephone User Card (P0912061)

T7100 Telephone User Card (P0609621)

T7208 Telephone User Card (P0609622)

T7316 Telephone User Card (P0935248)

T7316E Telephone User Card (P0609623)

T7406 Cordless Handset Installation Guide (P0606142)

T7406 Cordless Telephone User Card (P0942259)

Using NCM to Manage BCM50 (N0027151)

How to get help

If you do not see an appropriate number in this list, go to www.nortel.com/cs.

USA and Canada Authorized Distributors

Technical Support - GNTS/GNPS

Telephone:
1-800-4NORTEL (1-800-466-7835)

If you already have a PIN Code, you can enter Express Routing Code (ERC) 196#. If you do not yet have a PIN Code, or for general questions and first line support, you can enter ERC 338#.

Web site:
http://www.nortel.com/cs

Presales Support (CSAN)

Telephone:
1-800-4NORTEL (1-800-466-7835)

Use Express Routing Code (ERC) 1063#

EMEA (Europe, Middle East, Africa)

Technical Support - CTAS

Telephone:
*European Free phone 00800 800 89009

European Alternative:

United Kingdom	+44 (0)870-907-9009
Africa	+27-11-808-4000
Israel	800-945-9779

Calls are not free from all countries in Europe, Middle East, or Africa.

Fax:
44-191-555-7980

e-mail:
emeahelp@nortel.com

CALA (Caribbean & Latin America)

Technical Support - CTAS

Telephone:
1-954-858-7777

e-mail:
csrmgmt@nortel.com

APAC (Asia Pacific)

Service Business Centre & Pre-Sales Help Desk:
+61-2-8870-5511 (Sydney)

Technical Support - GNTS

Telephone:
+612 8870 8800

Fax:
+612 8870 5569

e-mail:
asia_support@nortel.com

Australia	1-800-NORTEL (1-800-667-835)
China	010-6510-7770
India	011-5154-2210
Indonesia	0018-036-1004
Japan	0120-332-533
Malaysia	1800-805-380
New Zealand	0800-449-716
Philippines	1800-1611-0063
Singapore	800-616-2004
South Korea	0079-8611-2001
Taiwan	0800-810-500
Thailand	001-800-611-3007
Service Business Centre & Pre-Sales Help Desk	+61-2-8870-5511

Chapter 2
Overview of BCM50 Administration

The BCM50 Administration Guide describes the tools available with which to administer, or manage, the BCM50. This section is an introduction to the information covered in this guide about administering your BCM50 system.

The administration overview information is divided into two three categories:

- BCM50 Management Model
- BCM50 Management Interfaces
- BCM50 Administration Guide overview

BCM50 Management Model

Whether BCM50 is being installed as a standalone element, is part of a network of many BCM50s, or is part of a network encompassing both BCM50s 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 BCM50 manageability is achieved by breaking the management functions into layers.

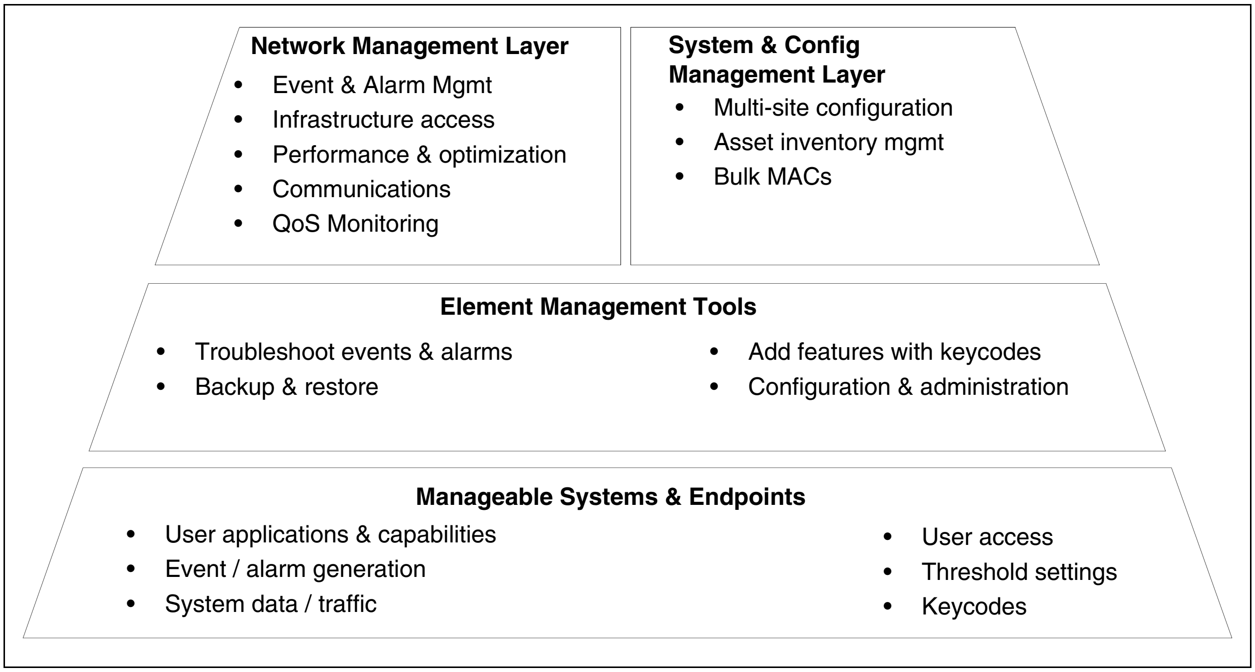
At the base of the model is the element itself. In order to be a manageable system, the element must provide not only the ability to configure services, but must also regulate access to the system by administrative users, generate alarms in the event of issues, support the easy addition of new features 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 BCM50 device. The primary BCM50 management application is the BCM50 Element Manager, complemented by other management applications as explained in the BCM50 Management Overview in section 2.

If the BCM50 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 BCM50s. For more information about NCM, please consult the NCM User documentation.

Figure 1 BCM50 network management model


Network Management Layer
• Event & Alarm Mgmt
• Infrastructure access
• Performance & optimization
• Communications
• QoS Monitoring
System & Config Management Layer
• Multi-site configuration
• Asset inventory mgmt
• Bulk MACs
Element Management Tools
• Troubleshoot events & alarms
• Backup & restore
• Add features with keycodes
• Configuration & administration
Manageable Systems & Endpoints
• User applications & capabilities
• Event / alarm generation
• System data / traffic
• User access
• Threshold settings
• Keycodes

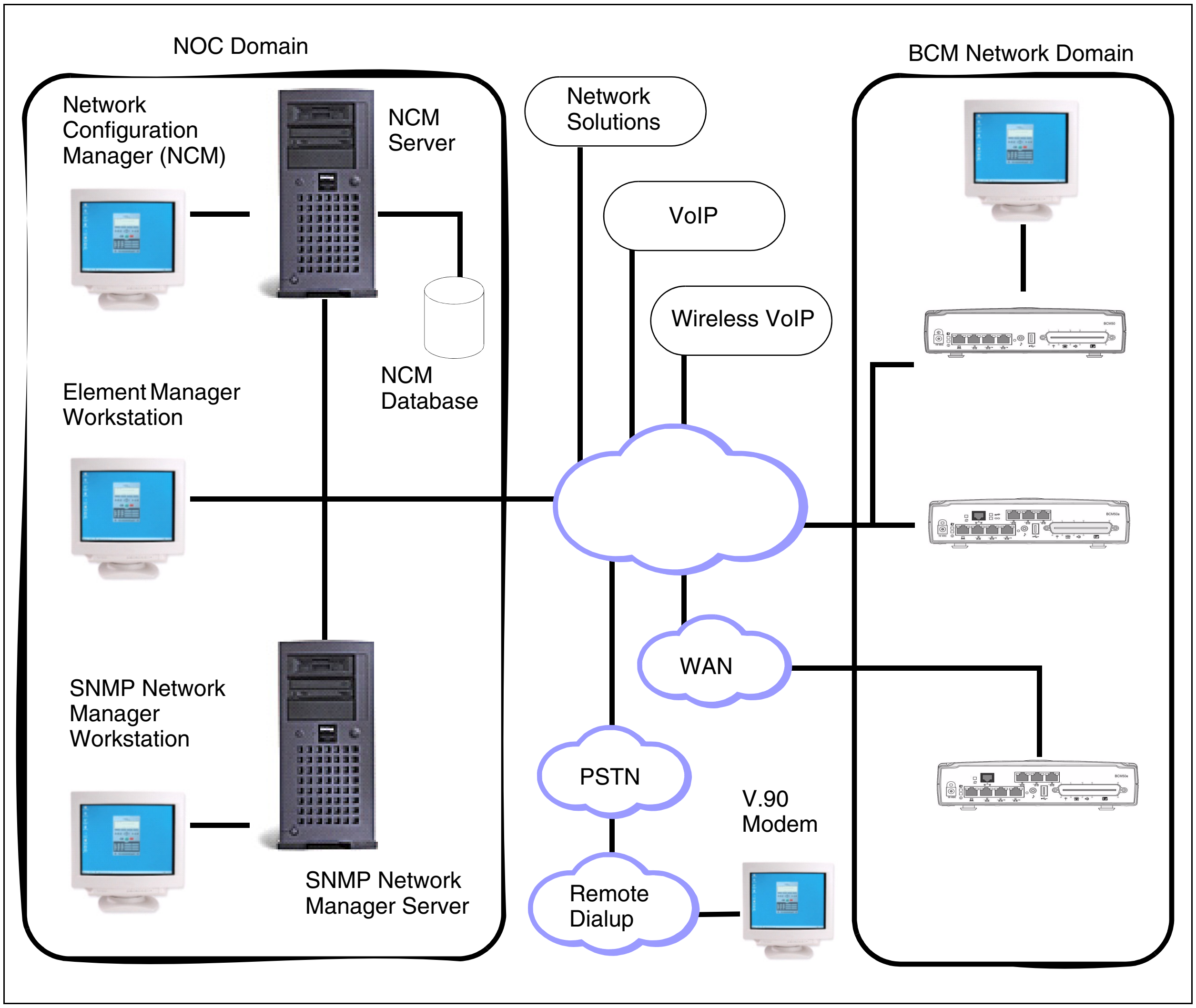
"BCM50 enterprise network model" on page 32 shows an example BCM50 enterprise network, illustrating the various communications between the BCM50 end devices and management applications managing end devices. The diagram also shows that the physical enterprise network, conceptually, is segmented into domains.

The Network Operations Center (NOC) domain represents the tools, equipment and activities used to analyze and maintain the operation of a network of BCM50 devices. Element Manager and Network Configuration Manager are the management applications which allow the network administrators working in the NOC domain to perform the administrative functions. The management application workstations can be physically distributed across different enterprise sites if they are networked via an IP network as represented by the cloud in the middle of the figure.

The BCM network domain represents one or more BCM50s located a different sites in the network connected through an enterprise LAN to one or more management application workstations. The WAN represents an adjacent network, external to the LAN.

The VoIP and Wireless VoIP domains represent terminating IP devices. Note that wireless devices are not supported in BCM50 Release 1.

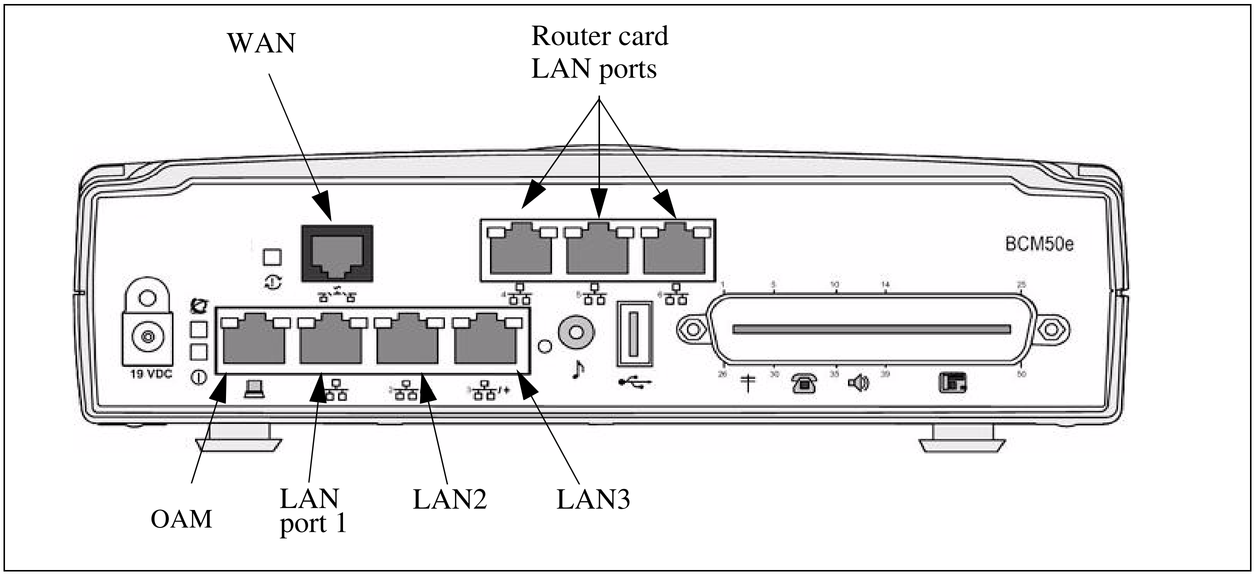
Figure 2 BCM50 enterprise network model


NOC Domain
Network Configuration Manager (NCM)
NCM Server
NCM Database
Element Manager Workstation
SNMP Network Manager Workstation
SNMP Network Manager Server
Network Solutions
VoIP
Wireless VoIP
WAN
PSTN
Remote Dialup
V.90 Modem
BCM Network Domain

BCM50 Network Management interfaces

The BCM50 network can be distributed geographically across different sites. The network administrator must be able to remotely access each BCM50 in the network. BCM50 offers alternatives for connecting to the BCM50 devices (see Figure 3 on page 33) depending on the network configuration and telephony resources available with a given system.

Figure 3 BCM50 physical interfaces



OAM Port

The administration and maintenance (OAM) port, also called Port 0, is used to connect an on-site management computer to the BCM50. Using this connection, you can access management tools, such as Element Manager, without requiring access to the main LAN.

This port is not connected to the network switch built into the BCM50 and cannot be used to connect other network devices.

BCM50 associates a DHCP server with the OAM port. Any computer attaching to this port will automatically be assigned an IP address by the BCM50 DHCP server. This means that if the administrator's computer is connected to the OAM port, there will never be a need to know the IP address of the BCM50 before being able to launch Element Manager to log into the system.

The default IP address for the BCM50 system is 192.168.1.2 with a Subnet of 255.255.255.0.

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.

Each BCM50 main unit has an integrated Ethernet switch. The LAN port entitled Port 1 is intended to be the main customer LAN port.

If the BCM50 system does not include an expansion unit, then the RJ45 ports called Port 2 and Port 3 on the BCM50 main unit (of all three BCM50) models can be used as a second and third LAN port for the integrated Ethernet switch. If an expansion unit is required, ports 2 and 3 must be used as the expansion Ports to connect the main unit and expansion unit(s). However, the expansion unit also provides a LAN port that is part of the same main unit LAN, thereby ensuring that there should always be at least 3 available LAN ports regardless of the specific system configuration. All three LAN Ethernet interfaces, Ports 1, 2 and 3 transmit at 10/100 Mbps.

A network administrator can connect to and manage a BCM50 via an IP over LAN interface. If the administrator is accessing the BCM50 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

BCM50 provides an integrated soft modem which supports the ability for the system to accept an incoming modem call on any BCM50 system line. The BCM50 system can be configured to let the modem auto-answer a specific. The remote user can also first initiate a voice call to a person or an auto-attendant, who would then transfer the call to the modem.

The soft modem also supports callback for management user access to the BCM50. 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, *BCM50 Networking Configuration guide.*

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.

The two BCM50 models with integrated routers provide the option of a direct connection to a WAN. Both an Ethernet WAN option and an ADSL WAN option are supported. With these devices, remote management can be done over a connection from the public network (WAN) side of the BCM50 device.

Section 2 of this guide explains how to configure the optional integrated router to enable Element Manager access for management from the public network. Also provided is information on how to configure the optional integrated router to enable SNMP access for remote manageability from the public network.

Several protocols are used in the day to day management of a network of BCM50s. 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").
- HTTP (Hyper Text Transfer Protocol): The Hyper Text Transfer Protocol is the protocol used between a Web browser and a server to request a document and transfer its contents. HTTP is used by BCM50 in some situations to send and receive files required by an HTTP application.
- 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 Element Manager and the BCM50.
- 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/servers.
- 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 chapt.er.

Administration Guide Overview

This section summarizes the content of the Administration Guide.

BCM50 management environment

The BCM50 management environment includes the BCM50 Web page, the BCM50 Element Manager and CallPilot Manager. Element Manager is a client-based management application that runs on a Windows computer and is used to configure, administer, and monitor BCM50 devices. For further information on the Business Communications Manager 50, refer to "Element Manager" on page 43.

BCM50 security

The BCM50 security chapter covers BCM50 security policies and user access, management, and also covers BCM50 security fundamentals. For further information on BCM50 security, refer to "BCM50 security fundamentals" on page 124

BCM50 hardware inventory

The hardware inventory task in the BCM50 Element Manager displays information about the BCM50 system such as connected expansion units, populated Media Bay Modules (MBMs) and attached telephone devices. For further information on BCM50 hardware inventory, refer to "About the BCM50 Hardware Inventory" on page 129.

BCM50 management with SNMP

SNMP (Simple Network Management Protocol) 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. The BCM50 main unit has an SNMP agent, as does the optional integrated router. For further information on BCM50 management with SNMP, refer to "Overview of BCM50 support for SNMP" on page 137.

BCM50 fault management

The Fault management chapter contains information about administering alarm settings and managing alarms generated by the BCM50 system. For further information on BCM50 fault management, refer to "Overview of BCM50 fault management" on page 151.

BCM50 service management system

The BCM50 Service management system enables you to view the services that run on the BCM50 system. For further information about the BCM50 service management system, refer to "Overview of the BCM50 service management system" on page 223

BCM50 metrics

System and telephony metrics enable you to view detailed information about the performance of the BCM50 system and of the system resources. For further information on BCM50 metrics, refer to "" on page 227.

BCM50 utilities

Several utilities are provided to allow partners and customers to monitor and analyze the system. Included are BCM Monitor, Ping, Trace Route, Ethernet Activity, Diagnostic Settings and Reset. For further information on BCM50 utilities, refer to "" on page 249.

BCM50 back up and restore

Maintaining current backups of your system configuration is essential to be able to restore a unit to an current or previous configuration level. For further information on BCM50 backup and restore, refer to "Overview of backing up and restoring data" on page 279.

BCM50 logs

Log files are collections of individual log events generated by the BCM50. An administrator can use log files to monitor and analyze system behavior, user session activities, and events. Log files can be transferred to your personal computer and viewed using the BCM50 Element Manager Log Browser. For further information on BCM50 logs, refer to "Overview of BCM50 logs" on page 315.

BCM50 software management

During the lifecycle of the BCM50, you might apply software updates to the BCM50 unit to correct known issues or to introduce new functionality. BCM50 provides a flexible patch management capability that can be run remotely, even if the software update requires a system reboot. For further information on BCM50 software management, refer to "Overview of BCM50 software updates" on page 341.

BCM50 accounting management

Account management utilizes 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 into a Call Detail Recording file. You can use this information to determine whether the telephone system is being used efficiently and to guard against abuse of the telephone system. For further information on BCM50 accounting management, refer to "Overview of accounting management" on page 359.

BCM50 troubleshooting

under development.

Chapter 3

Business Communications Manager Management Environment

This chapter contains information on the different tools available for managing your BCM50. It also describes the new Element Manager application in detail. It includes the following sections:

- "BCM50 web page" on page 39
- "BCM50 Management Environment and Applications" on page 41
- "Element Manager" on page 43
- "BCM50 feature licensing" on page 71
- "BCM50 Help system" on page 72
- "BCM50 common file input/output processes" on page 74
- "BCM50 Element Manager usage on a BCM50a or BCM50e" on page 78

BCM50 web page

The BCM50 web page facilitates the download of applications, documentation, and other information necessary for running the BCM50 and its services. You connect to the BCM50 web page by typing the IP address of your BCM50 into your browser. A valid user name and password is required in order to access the web page.

There are two default user accounts configured on the BCM50 at time of shipping: the nnadmin user account and the nnguest user account. See Chapter 4, "BCM 50 Security Policies and Accounts and Privileges," on page 81 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 BCM50 web page.

The BCM50 web page contains the following links:

- User Application - Applications listed in Table 2 on page 40 that are available to the end users of the BCM50.
- User Documentation - Documentation for the BCM50 end users to explain the end-user applications and BCM50-specific tasks.
- Administrator Applications - Applications listed in Table 2 on page 40 that are available to BCM50 administrators.

- Administrator Documentation - Documentation for the BCM50 administrators to explain the BCM50 management applications and BCM50 management tasks.
- Nortel's Contact Information - A list of Nortel contact numbers.

Table 2 Applications available on BCM50 web page

Application	User	Administrator
CallPilot Unified Messaging	Y	Y
Desktop Assistant	Y	Y
Desktop Assistant Pro	Y	Y
Desktop Assistant Pro AE	N	Y
i2050 Software Phone	Y	Y
Personal Call Manager	Y	Y
LAN CTE Client	Y	Y
BCM50 Element Manager	N	Y
NCM for BCM50	N	Y*
BCM Monitor	N	Y
CDR Clients	N	Y
BCM50 MIBs	N	Y
Startup Profile Template	N	Y
SSH Client (PuTTY)	N	Y
BCM50 Logs	N	Y

* Provides a URL that can be accessed to download the BCM50 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

BCM50 Management Environment and Applications

A number of tools are available to help manage your BCM50. This section describes the following tools:

- "Managing BCM50 with Element Manager" on page 41
- "Managing BCM50 with Telset administration" on page 41
- "Managing the BCM50 integrated router: Router WebGUI" on page 41
- "Managing BCM50 Voicemail and CallCenter: CallPilot Manager" on page 42
- "Programming telephone sets: Desktop Assistant portfolio" on page 42
- "Performing initialization: Startup Profile" on page 42
- "Monitoring BCM50: BCM Monitor" on page 43
- "Managing BCM50 remotely with SNMP" on page 43

Managing BCM50 with Element Manager

The primary management application for configuring and administering the BCM50 is the BCM50 Element Manager. The BCM50 Element Manager is a client-based management application that runs on a Windows computer. The Element Manager allows for connection to BCM50 devices over an IP network. It is used to configure, administer, and monitor BCM50 devices. See "Element Manager" on page 43 for more information about the BCM50 Element Manager.

The Element Manager application can be downloaded from the BCM50 web page or from the Nortel Networks support web site. See "BCM50 web page" on page 39 for a description of the BCM50 web page. The procedure "Installing Element Manager" on page 44 provides detailed steps for downloading and installing the BCM50 Element Manager.

Managing BCM50 with Telset administration

While Element Manager is the primary management application, BCM50 also supports the programming of telephony and applications areas of BCM50 through set-based administration. This allows installers, already familiar with this interface, to perform programming from the keypad of any telephone connected to the BCM50 device. This alleviates the need for access to a computer at the customer site. For more information about using Telset programming on the BCM50, refer to the following documents:

- *BCM50 Telset Administration Guide*
- *CallPilot Telephone Administration Guide*
- *Call Center Telephone Administration Guide*

Managing the BCM50 integrated router: Router WebGUI

The Router WebGUI is used to manage BCM50a and BCM50e systems. In addition to configuring the router, the WebGUI supports tasks such as backing up software, and performing alarm and performance monitoring. Fore more information about managing the BCM50 integrated router, refer to the following documents:

- *BCM50a Integrated Router Configuration Guide*
- *BCM50e Integrated Router Configuration Guide*

Managing BCM50 Voicemail and CallCenter: 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 call center applications for the BCM Release 3 software stream. For more information about using CallPilot Manager, refer to the CallPilot documentation on the BCM50 web page.

CallPilot Manager can be launched only by users with sufficient security privileges. BCM50 administrators must assign privileges. See Chapter 4, "BCM 50 Security Policies and Accounts and Privileges," on page 81 for more information on security privileges.

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 BCM50 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 Assisstant Pro AE. See the *BCM50 LAN CTE Configuration Guide* 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 BCM50 element to a basic operational and ready-to-customize state without using either 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 BCM50 before the initial start-up. On start-up the BCM50 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

See the *BCM50 Installation Guide* for detailed information on the Startup Profile.

Monitoring BCM50: BCM Monitor

BCM Monitor is a monitoring and diagnostics tool that can connect to and monitor BCM3.x systems and BCM50 systems. It is installed as part of the BCM50 Element Manager installation. See Chapter 10, "BCM50 Utilities," on page 249 for information about the BCM Monitor for BCM50.

Managing BCM50 remotely with SNMP

Simple Network Management Protocol is a standard for network management. BCM50 supports a number of standard MIBs, including MIB II RFC 1213, Entity MIB RFC 2737, and Host MIB RFC 2790. SNMPv1, v2c and v3 are supported, as well as SNMP traps.

If you are using the BCM50a or BCM50e, you must configure the router to enable SNMP.

See Chapter 6, "Managing BCM50 with SNMP," on page 137 for more information about using Element Manager with SNMP.

Element Manager

The Element Manager is a client-based management application that runs on a Windows computer. The Element Manager allows for connection to BCM50 devices over an IP network. It is used to configure, administer, and monitor BCM50 devices.

The BCM50 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

You can load the Element Manager client onto your computer from a BCM50 web page. See "Element Manager setup" on page 44 for details on installing Element Manager.

The Element Manager allows you to connect to the BCM50 devices to be managed either through an IP network connection, or through the craftsperson OAM port on the BCM50 main unit. See the *BCM50 Installation Guide* for information on connecting to a BCM50 through a craftperson OAM port.

If your BCM50 includes an optional Ethernet or ADSL router, you must configure the router to provide Element Manager access to the BCM50 over the WAN interface. See "BCM50 Element Manager usage on a BCM50a or BCM50e" on page 78 for a description of how to configure the router firewall and NAT to enable the router to connect to the BCM50 with Element Manager from the WAN.

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

- "Element Manager setup" on page 44
- "Element Manager window attributes" on page 48
- "Element Manager panels" on page 56
- "Effective use of BCM50 Element Manager" on page 59
- "Element Manager data features" on page 59
- "BCM50 Element Manager application logging" on page 69
- "BCM50 integrated launch of related applications" on page 69

Element Manager setup

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

- "Installing Element Manager" on page 44
- "Accessing BCM50s using Element Manager" on page 45
- "Adding a BCM50 to the Network Element tree" on page 46
- "Finding Network Elements" on page 46
- "Disconnecting from an element" on page 47
- "Closing the Element Manager" on page 48

Installing Element Manager

You can download the Element Manager application from the BCM50 web page and install it on your computer at any time. However, cannot connect to a BCM50 until the BCM50 main unit is installed and running.

To install Element Manager on your computer:

1 Connect to the BCM50 web page:

— If the BCM50 is installed on the network use a browser and type in the BCM50 IP address as the URL in the following format:

http://xxx.xxx.xxx.xxx

— If the BCM50 is installed but not yet configured, connect directly to the BCM50 through the OAM port and, using a browser, type the following:

http://192.168.1.2

2. Enter the user name and password to be authenticated on the BCM50 web page. See Chapter 4, “BCM 50 Security Policies and Accounts and Privileges,” on page 81 for information on default user and passwords.
3. Select the **Administrator Applications** link.
4. Select the **BCM50 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 BCM50 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 BCM50 Element Manager is installed, find the BCM50EM.exe icon where you installed it. The default installation location is C:\Program Files\Nortel\BCM50\bin. Double-click on the BCM50EM.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 48.
10. Next steps:

- If the BCM50 you want to connect to is installed and has been booted up (both LEDs should be solid green), connect your computer to either the craftsperson OAM port on the BCM50, or to the IP network that connects to the BCM50.
- Set up the BCM50 as a device in the Network Elements tree. See “Adding a BCM50 to the Network Element tree” on page 46 for information on how to add BCM50s to the Network Element tree.

➡ **Note:** You must install future releases of BCM50 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.

Accessing BCM50s 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 BCM50 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.

Adding a BCM50 to the Network Element tree

Before you can connect to a BCM50, you must define it in Element Manager as a Network Element.

1 Select **Network Element**s 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 BCM50 with SNMP," on page 137 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 become editable, type in the new information.

Refer to "Element Manager window attributes" on page 48 for a detailed description of the common Element Manager window elements.

Next steps: Proceed to "Connecting to a BCM50 element" on page 47.

Finding Network Elements

You can search for a group of BCM50s located on the same subnet by using F**ind Network Elements**. This function uses SNMP to search for all of the BCM50s in the specified IP address range and add them to the Element Navigation tree. Only BCM50s with SNMP enabled will be detected. This tool saves time when trying to quickly populate Element Manager with previously deployed BCM50s 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 BCM50s 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 BCM50 element

Use the following steps to connect to your BCM50 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 BCM50 to which you are trying to connect.

3 Perform one of the following tasks to connect to the BCM50:

- 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 56 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 steps 1 and 3 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 BCM50 by using one of the following:

- "Disconnecting in the Element Navigation Panel" on page 47
- "Disconnecting through the menu bar" on page 48

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 BCM50 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 panel in Figure 4 on page 49 shows the initial window of a newly-installed Element Manager. At this point, no network elements have been defined, and the Business Communications Manager 50 is not connected to any elements.

Figure 4 Element Manager Window - no defined Elements

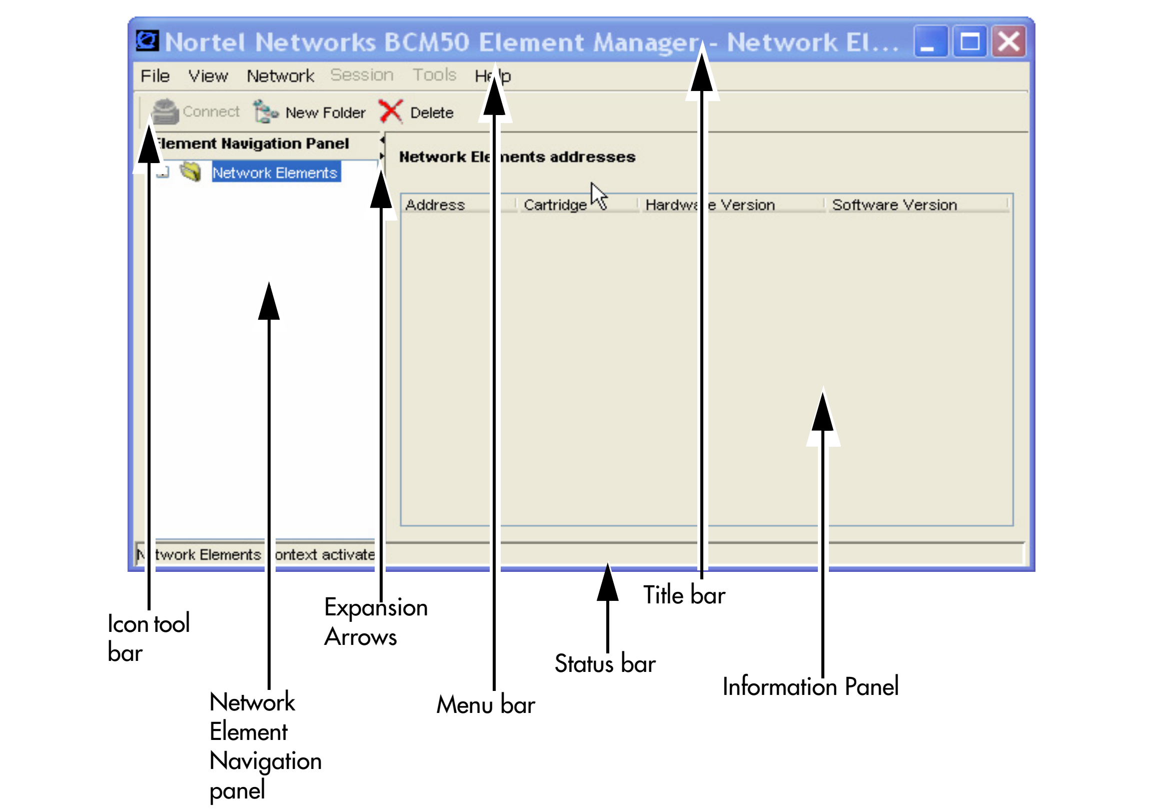

Nortel Networks BCM50 Element Manager - Network El...
File View Network Session Tools Help
Connect New Folder Delete
Element Navigation Panel
Network Elements
Network Elements addresses
Address Cartridge Hardware Version Software Version
Network Elements Context activate
Icon tool bar
Network Element Navigation panel
Expansion Arrows
Menu bar
Status bar
Title bar
Information Panel

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 BCM50 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	Provides 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	This menu provides three selections: • 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.

Table 3 Initial Element Manager window attributes (Continued)

Network	This menu is not available when a connected device is selected. When the Network Elements folder icon is selected in the Network Elements tree the following options are available: • 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 BCM50s that have SNMP turned on (by default, SNMP is turned off). When an unconnected device is selected in the network element tree, the following options are available under the Network selection: • 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 BCM50 Logs,” on page 315 for more information on viewing logs.
Session	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. • 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. • View Logs: Provides a dialog box that allows you to search for and to view logs that are available for the connected element. • Save Programming Record: Allows you to save programmed information in either Microsoft Excel format or HTML.
Tools	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. • 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.

Table 3 Initial Element Manager window attributes (Continued)

Help	Provides information to assist in using the Element Manager. • 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 BCM50 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 "BCM50 Help system" on page 72 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	Three icons are available if the Network Elements folder is at the top of Network Elements tree or if an unconnected device is selected. • 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.
Network Elements navigation panel	This panel contains the Network Element Navigation tree which displays devices and groups of devices (folders). • 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 an 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.
Information panel	The information in the Information panel changes depending on what is selected in the Network Elements tree. • 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 52. • 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 52 for an example of the presentation of the information by Element Manager.

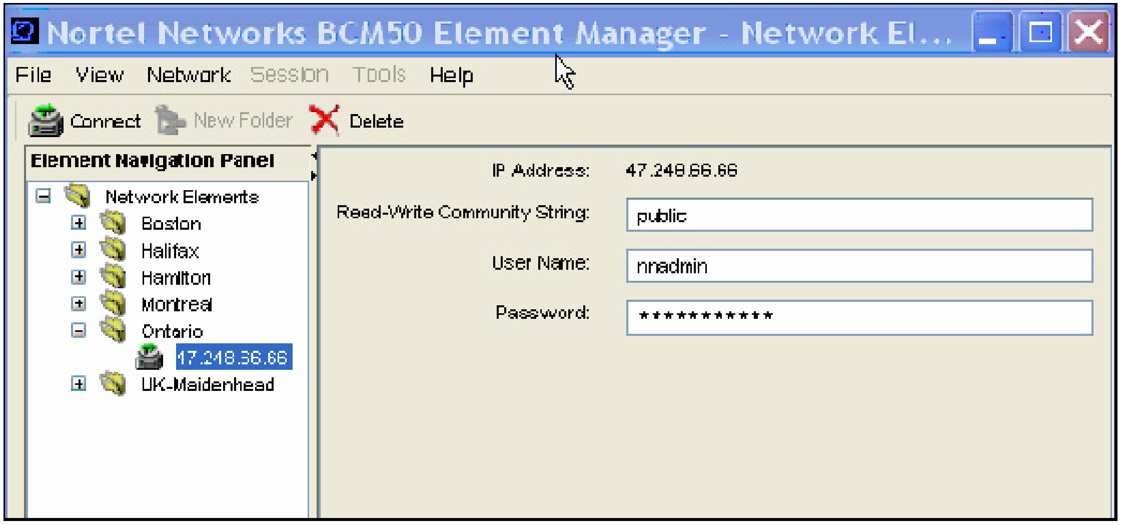
Table 3 Initial Element Manager window attributes (Continued)

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 52 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 on page 52.

Figure 5 Information display for unconnected network element



IP Address: 47.248.66.66

Read-Write Community String: public

User Name: nnadmin

Password: ************

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.
User Name	Name of an authorized BCM50 user account.
Password	A valid password associated to the User Name.

Information displayed for connected elements

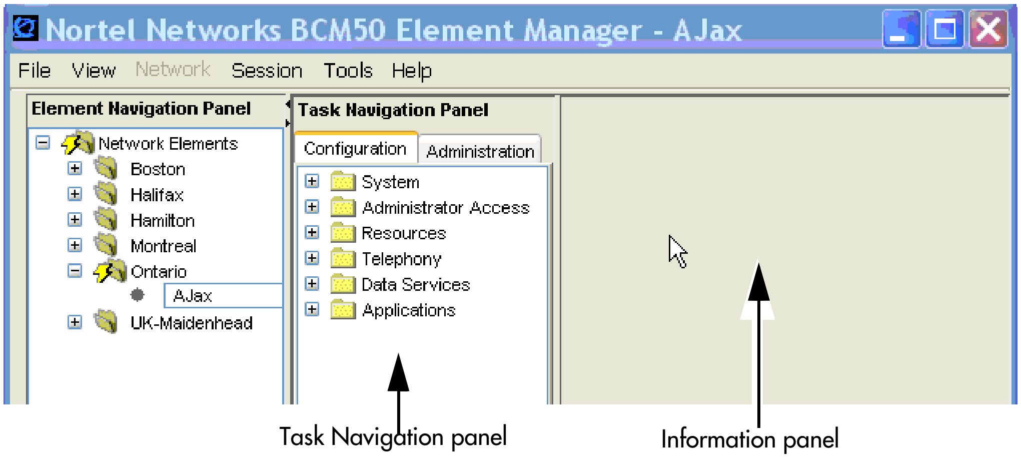
Element Manager displays two panels to the right of the Network Elements navigation panel once a BCM50 element has been connected:

- Task Navigation panel

- Information panel

Figure 6 shows the panels displayed in the Element Manager when it is connected to a BCM50. The Task Navigation panel contains the Configuration tab and the Administration tab. See "Configuration task navigation panel details" on page 53 for information contained in the Configuration navigation tree. See "Administration task navigation panel details" on page 55 for information contained in the Administration navigation tree.

Figure 6 Element Manager window when connected to a BCM50



Configuration task navigation panel details

The Configuration task navigation panel contains the Configuration task tree that allows you to set up and configure your BCM50 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
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
IP Subsystem	View and modify settings governing BCM50 IP networking capabilities
Administrator Access	
Accounts and Privileges	Manage users, groups, and privileges
Security policies	Manage passwords and other security policies
SNMP	Manage SNMP settings, and trap destinations

Table 5 Configuration task navigation panel headings (Continued)

Modem	Manage modem parameters
Resources	
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
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
Ring Groups	Manage group membership and line settings

Table 5 Configuration task navigation panel headings (Continued)

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
Router	Launch BCM50 Integrated Router WebGUI management application
Applications	
Voice Messaging/Call 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

Administration task navigation panel details

The Administration task navigation panel contains the Administration task tree that provides access to the BCM50 that allows you to monitor and maintain your BCM50.

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)
Hardware Inventory	Manage general information for attached BCM50 systems and devices
System Metrics	
QoS Monitor	Manage Quality of Service monitor modes, logging and mean opinion scores
UPS Metrics	Manage uninterrupted power supply status, events and metrics
NTP Metrics	Manage network time protocol metrics synchronization details
Telephony Metrics	

Table 6 Administration task navigation panel headings (Continued)

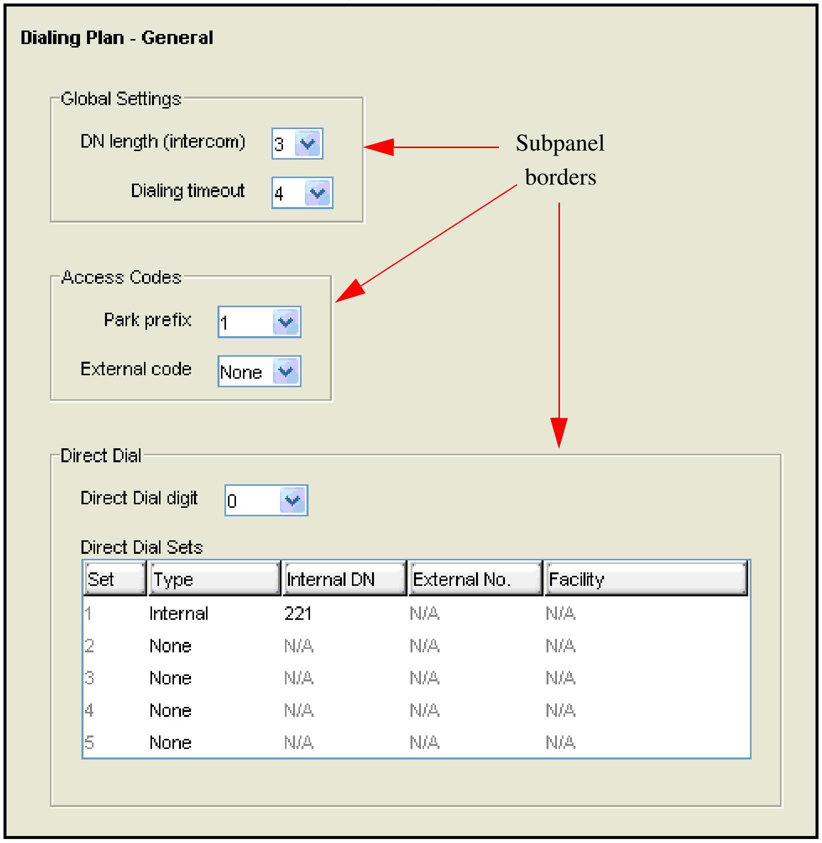
Trunk Module Metrics	Run loopback test on trunk modules
CbC Limit Metrics	View (Call by Call) logs of denied calls
Hunt Group Metrics	Reset metrics by hunt group
PSTN Fallback Metrics	Reset PSTN fallback metrics
Utilities	
BCM Monitor	Launch BCM Monitor
Ping	Send an ICMP packet to the selected switch 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 BCM50 or either a warm or cold reset of telephony services or router
Diagnostic Settings	Set release reasons for ISDN or VoIP calls
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 BCM50 Element Manager Configuration and Administration trees group the various tasks and functions required to configure the BCM50 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. Figure 7 on page 57 shows a information panel with related information groupings

Figure 7 Information panel groupings



Dialing Plan - General

Global Settings

DN length (intercom) 3

Dialing timeout 4

Access Codes

Park prefix 1

External code None

Direct Dial

Direct Dial digit 0

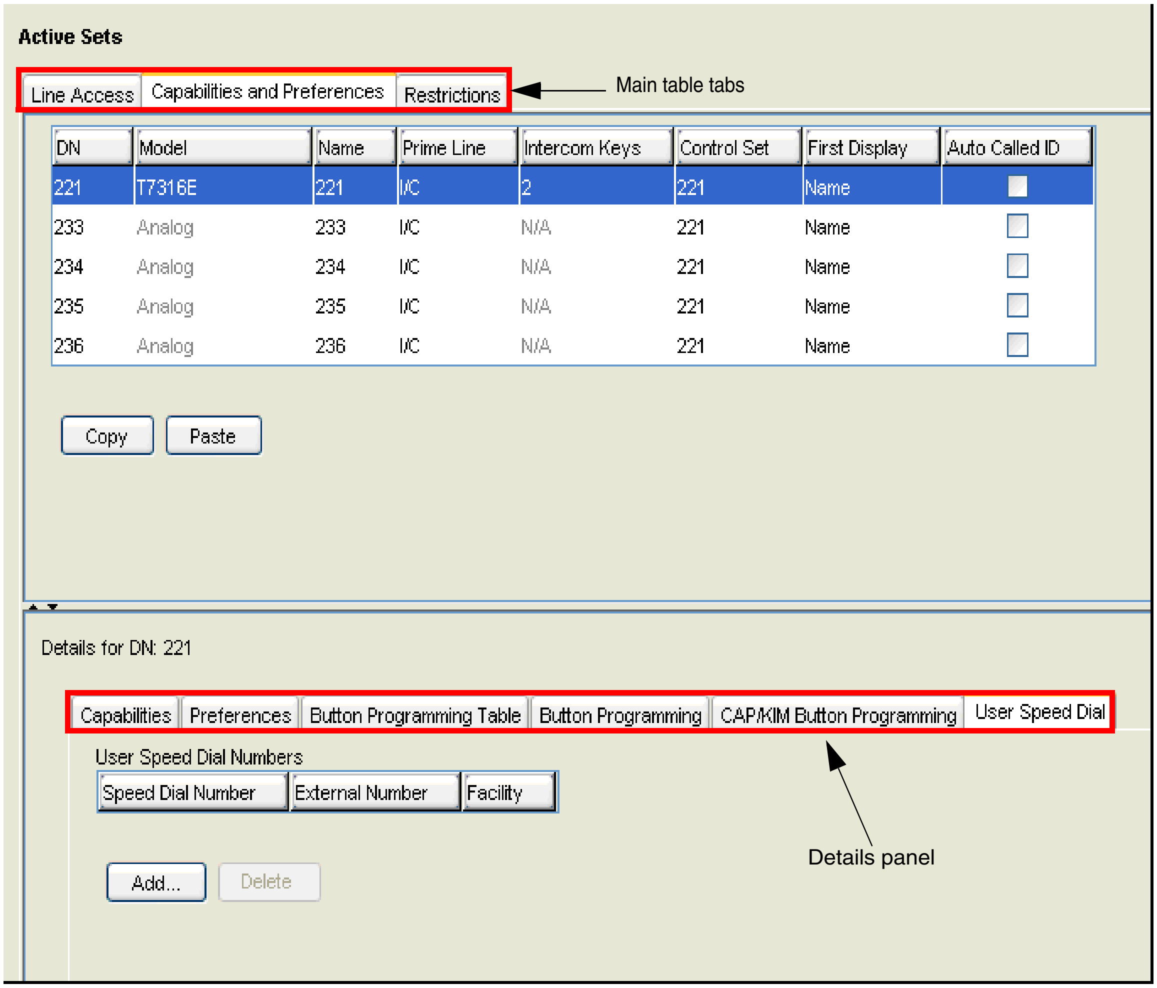
Direct Dial Sets

Set	Type	Internal DN	External No.	Facility
1	Internal	221	N/A	N/A
2	None	N/A	N/A	N/A
3	None	N/A	N/A	N/A
4	None	N/A	N/A	N/A
5	None	N/A	N/A	N/A

Subpanel borders

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. Figure 8 on page 58 shows an example of a table with an associated panel.

Figure 8 Main table and detail table



Main table tabs

DN	Model	Name	Prime Line	Intercom Keys	Control Set	First Display	Auto Called ID
221	T7316E	221	I/C	2	221	Name	□
233	Analog	233	I/C	N/A	221	Name	□
234	Analog	234	I/C	N/A	221	Name	□
235	Analog	235	I/C	N/A	221	Name	□
236	Analog	236	I/C	N/A	221	Name	□

Details for DN: 221

User Speed Dial Numbers

Speed Dial Number	External Number	Facility

Details panel

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 59 for details about navigating and changing information.

Effective use of BCM50 Element Manager

This section describes how Element Manager interacts with data to help the BCM50 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 nnadmin group will have administrator privileges and can view all panels and trees available through Element Manager. See the Chapter 4, "BCM 50 Security Policies and Accounts and Privileges," on page 81 for more information on grouping users and assigning privileges.

The BCM50 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 50 Security Policies and Accounts and Privileges," on page 81 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" on page 60
- "Copying table information" on page 60
- "Copying table information" on page 60
- "Rearranging table information" on page 62
- "Using your keyboard to move around a table" on page 65

Adding, deleting, and modifying table information

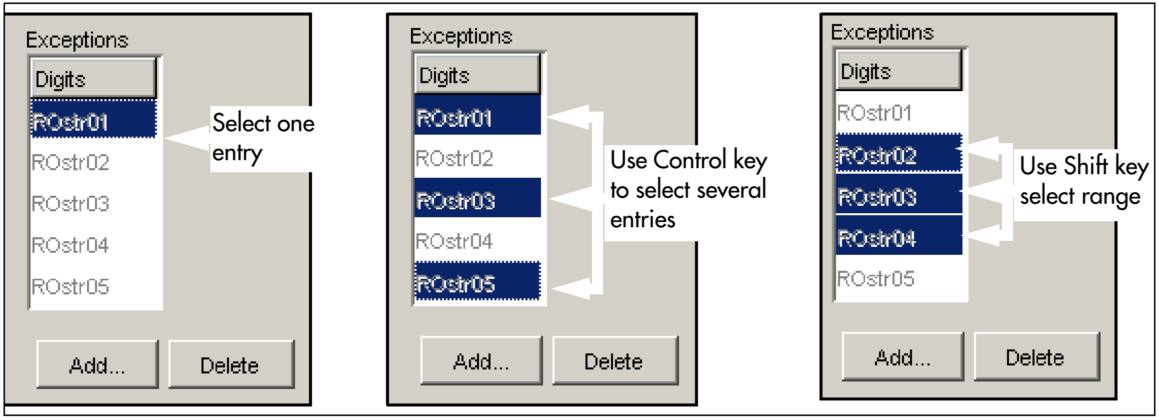
Some tables automatically list all available records, such as the restriction filters. These are tables where the number of entries is restricted by the BCM50. Other tables allow you to add or delete entries. These tables have an Add and Delete button under the table.

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 9 shows examples of how to select table entries for deletion.

Figure 9 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)	• Control set from the copied source into the selected row	
Restrictions (Lines, Sets)	• Set restrictions • Set lock • Allow Last Number Redial • Allow Saved Number Redial • Allow Link • Line/set restrictions	• 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)	• Data in common between the copied and pasted trunks.	• Data can be copied between two different trunk cartridge types
Telco data (Lines, Sets)	• Call Log set (Logging set) • 1stDisplay	• Log password • Log space
Buttons (Sets)	• All programmable set buttons from the copied set into the selected row's programmable buttons.	
Line access (Sets)	• Line assignment • Line pool access • Prime line designation • Number of intercom keys • Answer DNs (unless Answer button DN is same as telephone to which is being copied)	• Private line appearances

Table 7 Paste Data (Continued)

Check box title	Settings copied	Settings not copied
Capabilities (Sets)	• 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)	• Set name • Use ringback setting under ATA settings • SM Supervisor
User Preferences (Sets)	• Language choice • Ring type • Calls log options *(Auto logging)* • Display contrast • Dialing options (automatic, pre-dial, standard)	• 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:

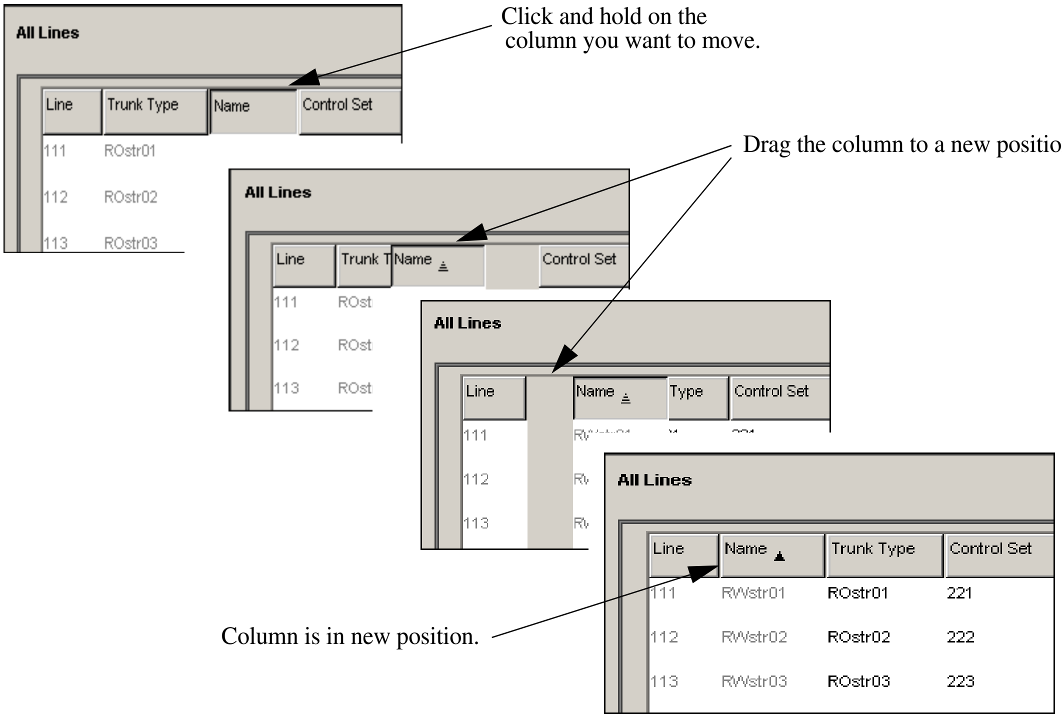
- “Rearranging columns” on page 63
- “Rearranging lines” on page 63

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

Figure 10 Changing the order of columns in a table



Click and hold on the column you want to move.

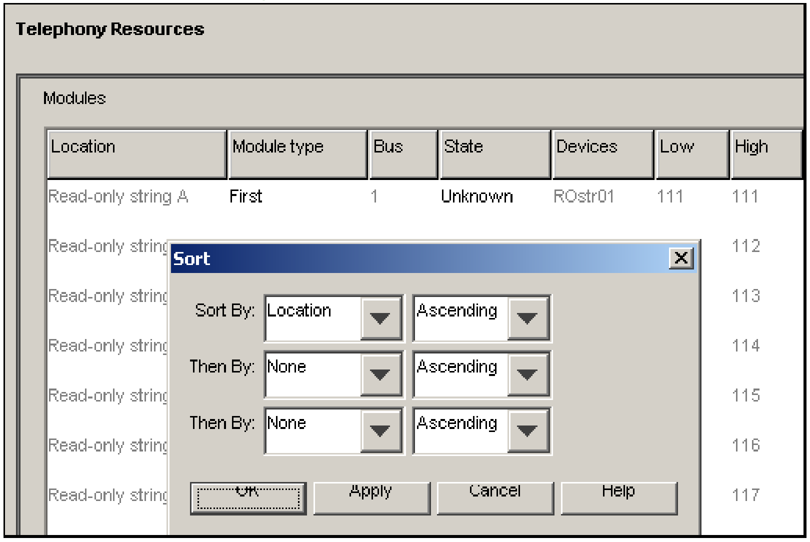
Drag the column to a new position

Column is in new position.

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 11 on page 64 shows the Sort dialog box. Table 8 on page 64 lists and describes the fields and buttons in the Sort dialog box.

Figure 11 Sort dialog box



Location	Module type	Bus	State	Devices	Low	High
Read-only string A	First	1	Unknown	ROstr01	111	111
Read-only string						112
Read-only string						113
Read-only string						114
Read-only string						115
Read-only string						116
Read-only string						117

Sort By: Location Ascending

Then By: None Ascending

Then By: None Ascending

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

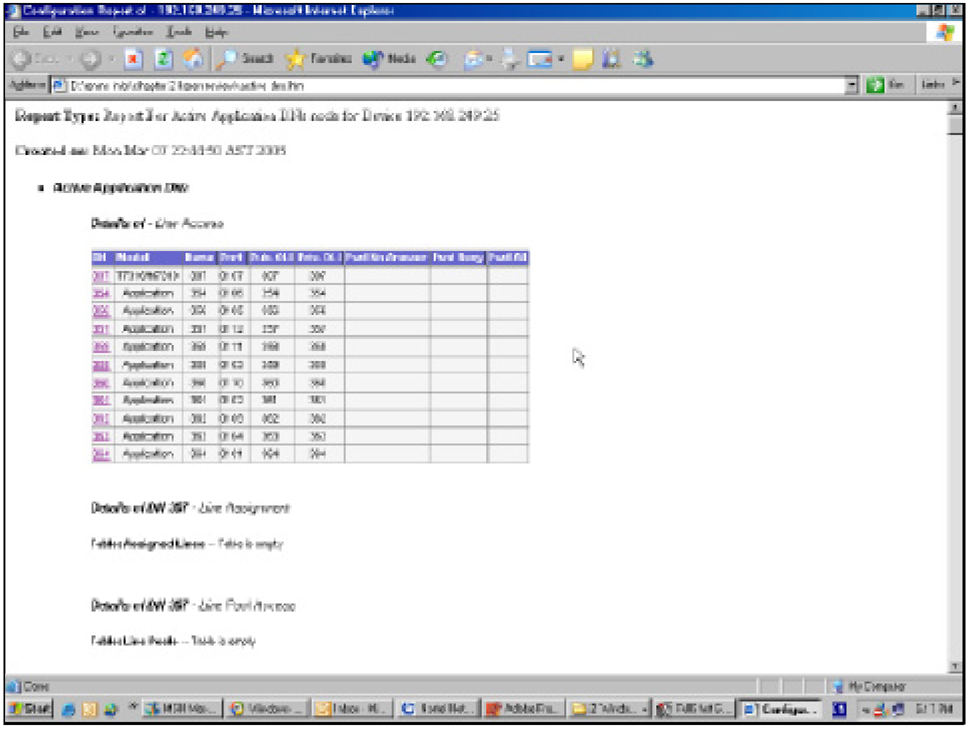
Use the <Tab> key or the directional arrow keys on your keyboard to move around a table.

<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. Figure 12 shows an example of a programming record saved in HTML format and Figure 13 on page 67 shows an example of a programming record saved in Excel spreadsheet format.

Figure 12 Programming record in HTML format



Report Type: Report For Active Application DNs node for Device 192.168.249.25

Created on: Mon Mar 07 22:44:50 AST 2005

- Active Application DNs

Details of - Line Access

DN	Model	Name	Port	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			
[illegible]	Application	[illegible]	[illegible]	[illegible]	[illegible]			

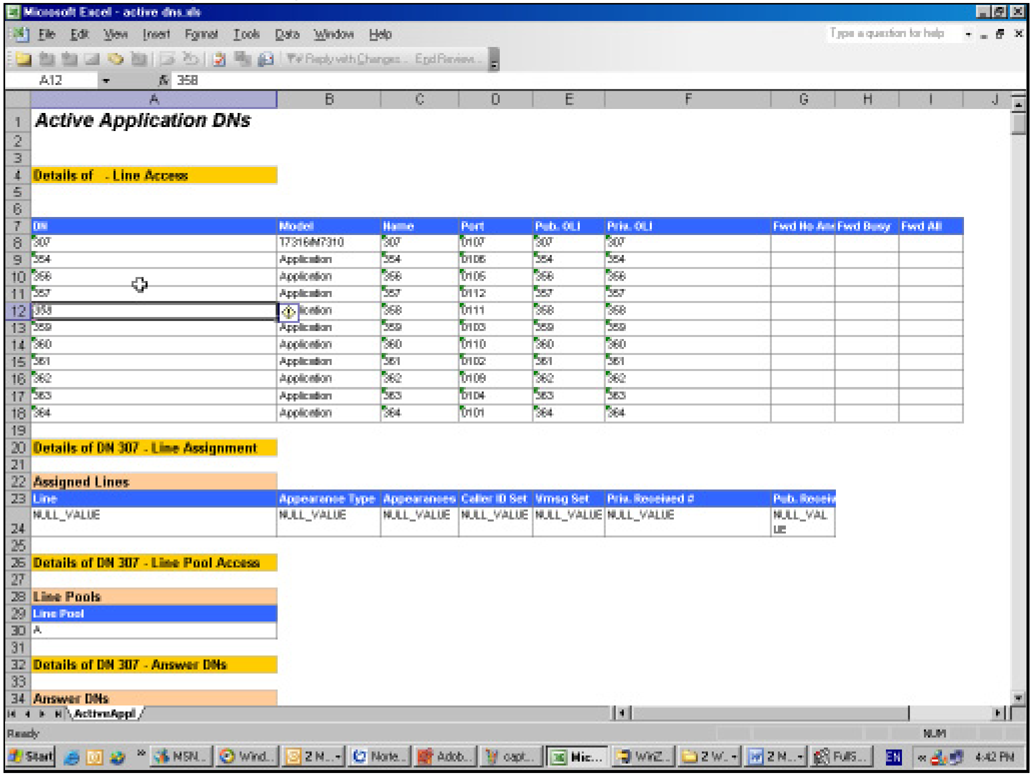
Details of DN [illegible] - Line Assignment

Table Assigned Lines -- Table is empty

Details of DN [illegible] - Line Pool Access

Table Line Pools -- Table is empty

Figure 13 Programming record in an Excel spreadsheet



Microsoft Excel - active dns.xls
File Edit View Insert Format Tools Data Window Help
Type a question for help
Reply with Changes... End Review...
A12
358
ActiveAppl
Ready
NUM
Start
4:42 PM

Active Application DNs

Details of - Line Access

DN	Model	Name	Port	Pub. OLI	Priv. OLI	Fwd No Ans	Fwd Busy	Fwd All
307	T7316/M7310	307	0107	307	307			
354	Application	354	0106	354	354			
356	Application	356	0105	356	356			
357	Application	357	0112	357	357			
358	lication	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			

Details of DN 307 - Line Assignment

Assigned Lines

Line	Appearance Type	Appearances	Caller ID Set	Vmsg Set	Priv. Received #	Pub. Receiv
NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VALUE	NULL_VAL UE

Details of DN 307 - Line Pool Access

Line Pools

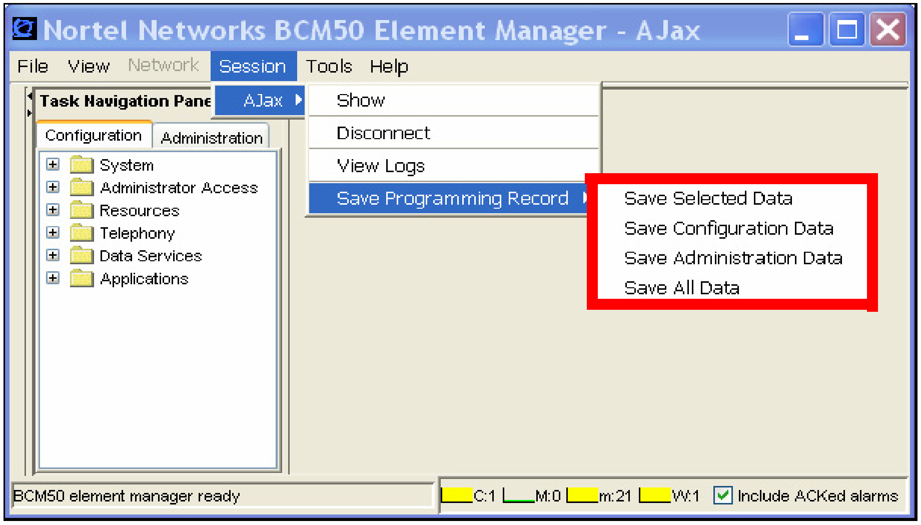
Line Pool
A

Details of DN 307 - Answer DNs

Answer DNs

To create this file, you use the **Save Programming Record** command on the Session menu. The Save Programming Record provides four menu options. Figure 14 shows the menu options available.

Figure 14 Session selections for saving programming records



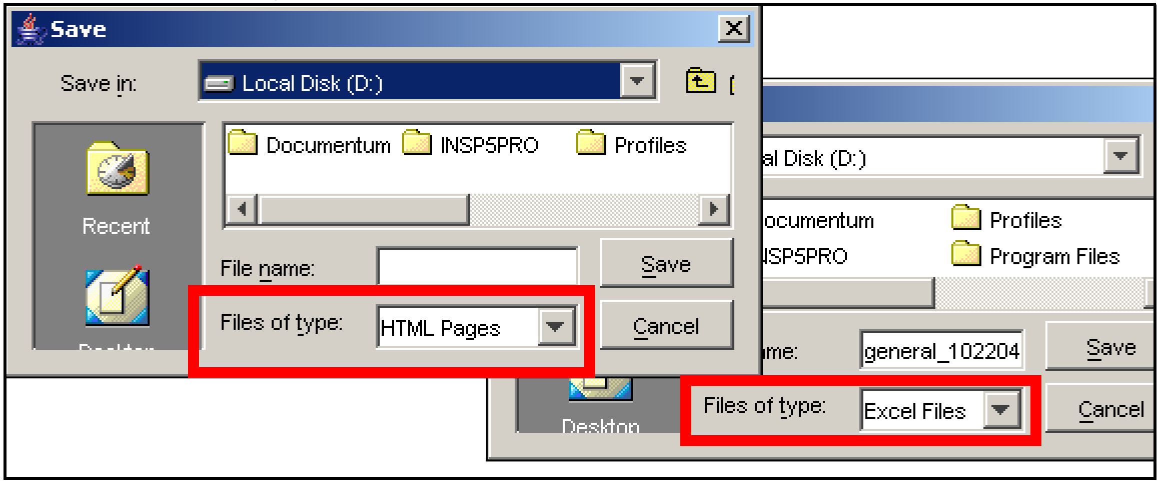
BCM50 element manager ready

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 15 for an example of a **Save** dialog box.

Figure 15 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 Networks 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 in step 5 until the function is complete.

BCM50 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.

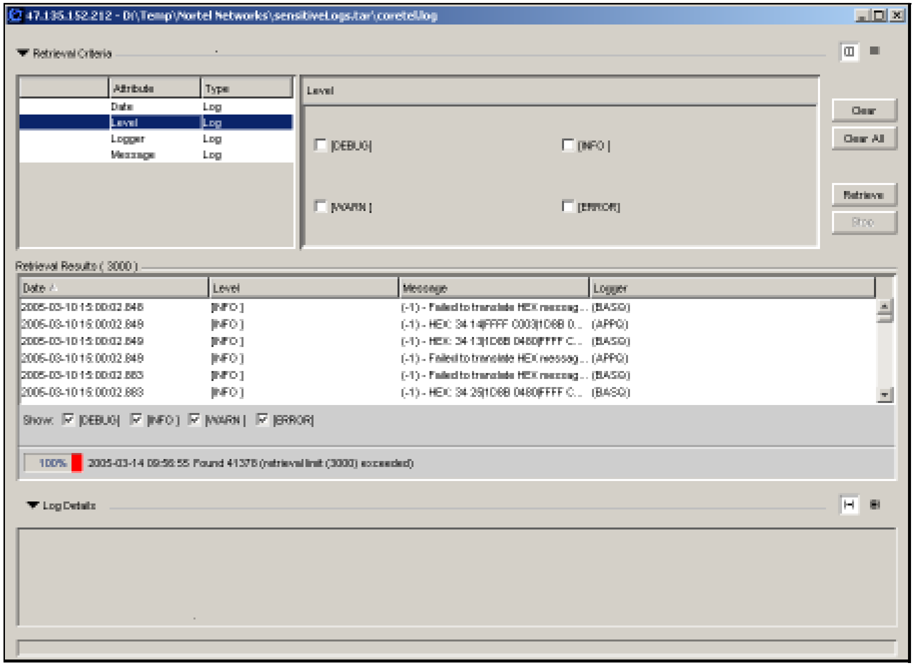
When you select Application Log from the menu bar Help command, the Element Manager Log Browser opens. You can use the Log Browser to sort the events in the Application Log.

The BCM50 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 16 on page 69 for the Application log panel.

Figure 16 Application log panel



47.135.152.212 - D:\Temp\Nortel Networks\sensitiveLogs.tar\coretel.log

Retrieval Criteria

	Attribute	Type
	Date	Log
	Level	Log
	Logger	Log
	Message	Log

Level

□ [DEBUG] □ [INFO]

□ [WARN] □ [ERROR]

Retrieval Results (3000)

Date	Level	Message	Logger
2005-03-10 15:00:02.848	[INFO]	(-1) - Failed to translate HEX messag...	(BASG)
2005-03-10 15:00:02.849	[INFO]	(-1) - HEX: 34 14[FFFF 0003]1D8B 0...	(APPG)
2005-03-10 15:00:02.849	[INFO]	(-1) - HEX: 34 13[1D8B 0480]FFFF C...	(BASG)
2005-03-10 15:00:02.849	[INFO]	(-1) - Failed to translate HEX messag...	(APPG)
2005-03-10 15:00:02.883	[INFO]	(-1) - Failed to translate HEX messag...	(BASG)
2005-03-10 15:00:02.883	[INFO]	(-1) - HEX: 34 25[1D8B 0480]FFFF C...	(BASG)

Show: ☑ [DEBUG] ☑ [INFO] ☑ [WARN] ☑ [ERROR]

100% 2005-03-14 09:56:55 Found 41378 (retrieval limit (3000) exceeded)

Log Details

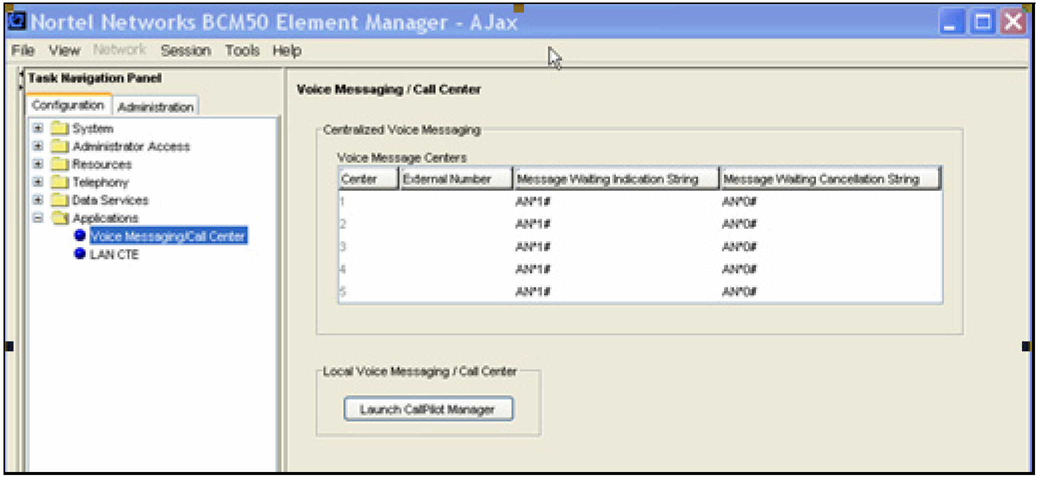
BCM50 integrated launch of related applications

BCM50 Voicemail and CallCenter applications are managed by CallPilot Manager, Integrated routers are managed by the BCM50 Integrated Router WebGUI management application, and real-time system activity is monitored with the BCM Monitor. All of these applications can be launched through buttons provided at an appropriate location in the Element Manager. 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/Call Center**. Figure 17 on page 70 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 17 Launch CallPilot Manager button



Voice Messaging / Call Center

Centralized Voice Messaging

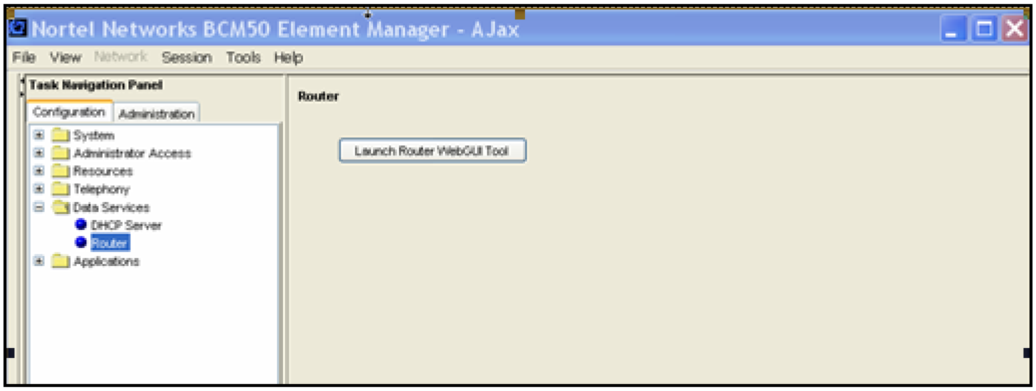
Voice Message Centers

Center	External Number	Message Waiting Indication String	Message Waiting Cancellation String
1		AN*1#	AN*0#
2		AN*1#	AN*0#
3		AN*1#	AN*0#
4		AN*1#	AN*0#
5		AN*1#	AN*0#

Local Voice Messaging / Call Center

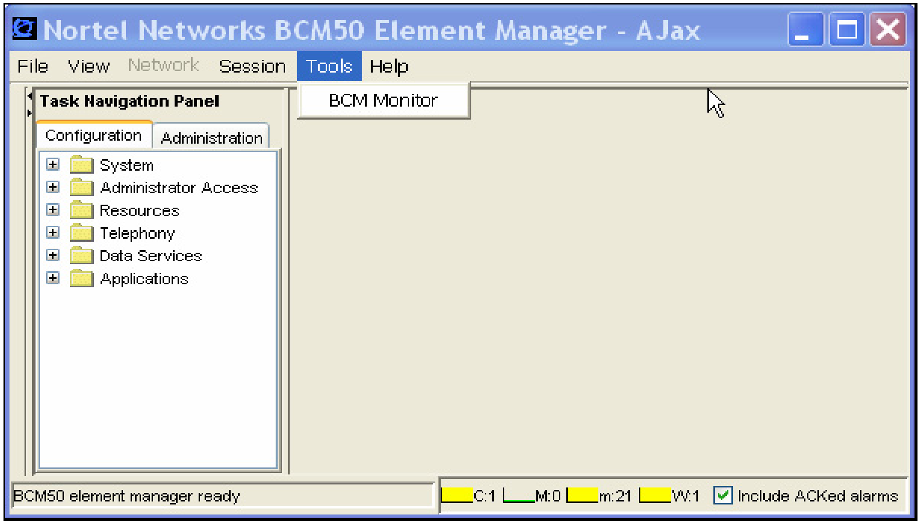
You can access the BCM50 Integrated Router WebGUI management application through the **Launch Router Configuration Tool** button under **Configuration Task > Data > Services > Router**. Figure 18 shows the location of the **Launch Router Configuration Tool** button. See the *BCM50a Integrated Router Configuration Guide* and the *BCM50e Integrated Router Configuration Guide* for more information on the Router Configuration tool.

Figure 18 Launch Router Configuration Tool button



You can access the BCM Monitor through the **Launch BCM Monitor** button under **Administration Task > Utilities > BCM Monitor**. Figure 19 on page 71 shows the location of the **Launch BCM Monitor** button.

Figure 19 Launch BCM Monitor button



BCM50 feature licensing

You require a keycode to enable software features on the BCM50. The keycode is a 24-digit code that authenticates the feature or bundle of features you purchased for your BCM50.

To obtain and load a keycode you require the following:

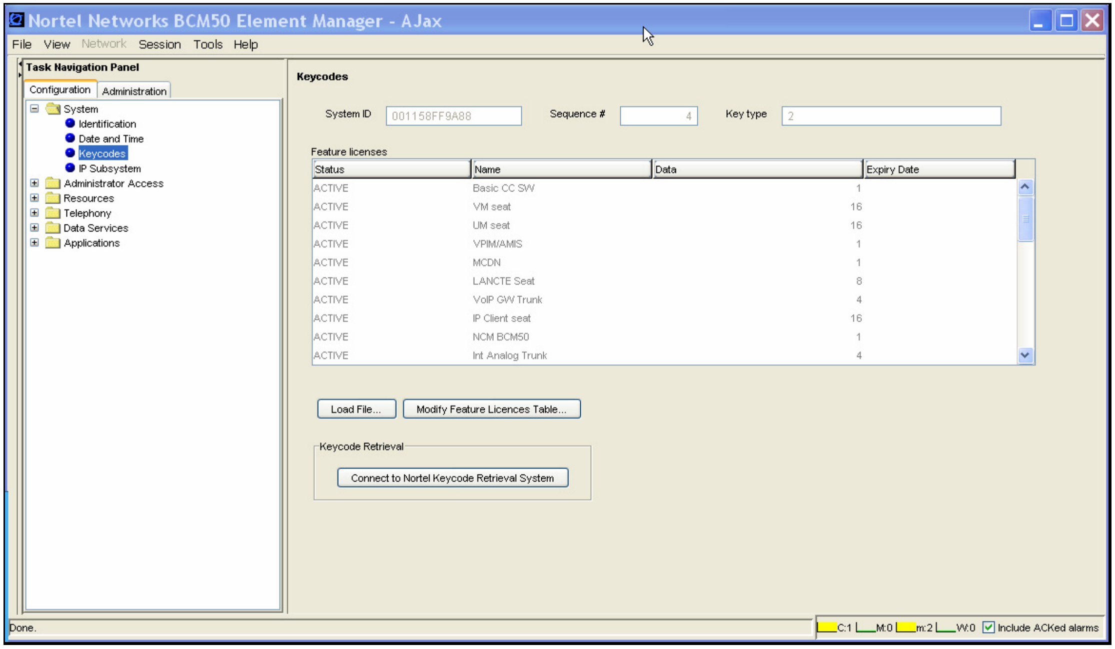
- authorization code for the desired feature to demonstrate proof of ownership
- system ID of the system to which you want to apply the new feature

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 *BCM50 Keycode Installation Guide*.

The System ID is unique for your BCM50. It is located on the label on the bottom of the BCM50 chassis and on the product packaging label. Figure 20 on page 72 shows the Element Manager keycode panel. See the *BCM50 Keycode Installation Guide* for details on BCM50 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 20 BCM50 Keycode panel



Keycodes

System ID: 001158FF9A88 Sequence #: 4 Key type: 2

Feature licenses

Status	Name	Data	Expiry Date
ACTIVE	Basic CC SW	1	
ACTIVE	VM seat	16	
ACTIVE	UM seat	16	
ACTIVE	VPIM/AMIS	1	
ACTIVE	MCDN	1	
ACTIVE	LANCTE Seat	8	
ACTIVE	VoIP GW Trunk	4	
ACTIVE	IP Client seat	16	
ACTIVE	NCM BCM50	1	
ACTIVE	Int Analog Trunk	4	

> **Note:** The system ID on the label has colons which the KRS requires you to input when creating a keycode (for example, xx:xx:xx:xx:xx:xx). The system ID is displayed in Element Manager without any colons.

BCM50 Help system

The following types of help information are available to you in Element Manager to help you understand how to program your BCM50:

- "Menu bar Help" on page 72
- "Field-level Help" on page 73
- "Context-sensitive Help" on page 74

Menu bar Help

The menu bar help provides access to the entire Help system and the documentation interface. Table 10 on page 72 shows the help elements available from menu bar Help. Figure 21 on page 73 shows the pull-down menu from the Help on the menu bar.

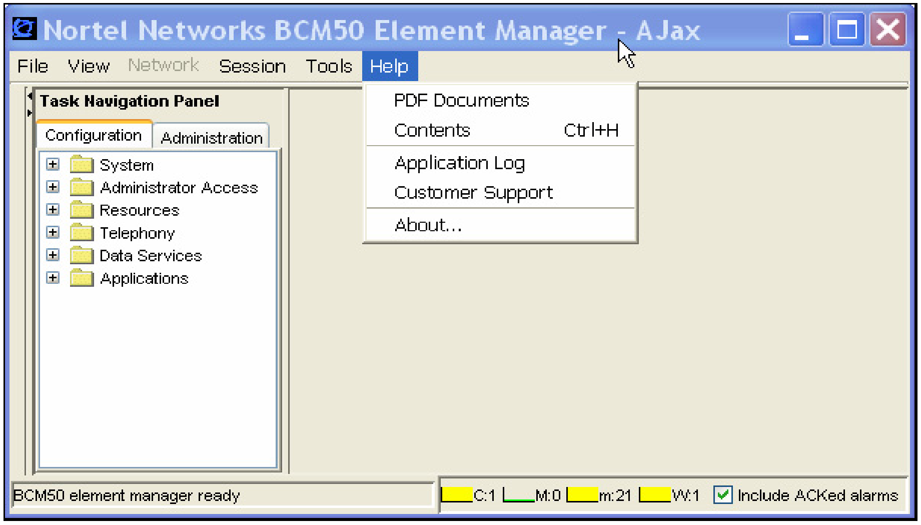
Table 10 Element Manager help elements

Help menu option	Description
PDF Documents	Link to PDF documents located on the BCM50 web page.

Table 10 Element Manager help elements (Continued)

Contents	Opens a browser window that shows the help information by contents or index and allows a search.
Application Log	Opens an interface to the BCM50 Element Manager logs.
Customer Support	Opens a browser to a Nortel Networks customer support web site
About	Provides information about the BCM50 Element Manager software.

Figure 21 BCM50 Element Manager menu bar help



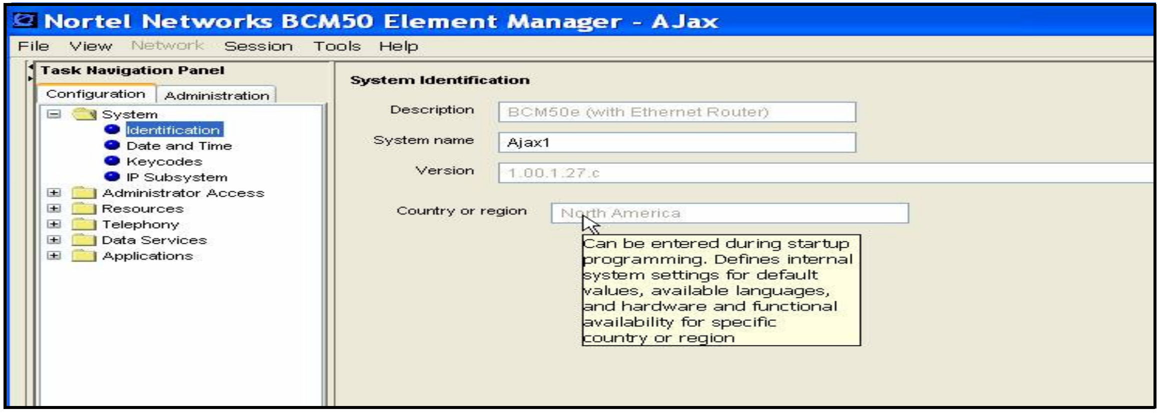
BCM50 element manager ready

☑ Include ACKed alarms

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

Figure 22 Field-level Help



Description: BCM50e (with Ethernet Router)

System name: Ajax1

Version: 1.00.1.27.c

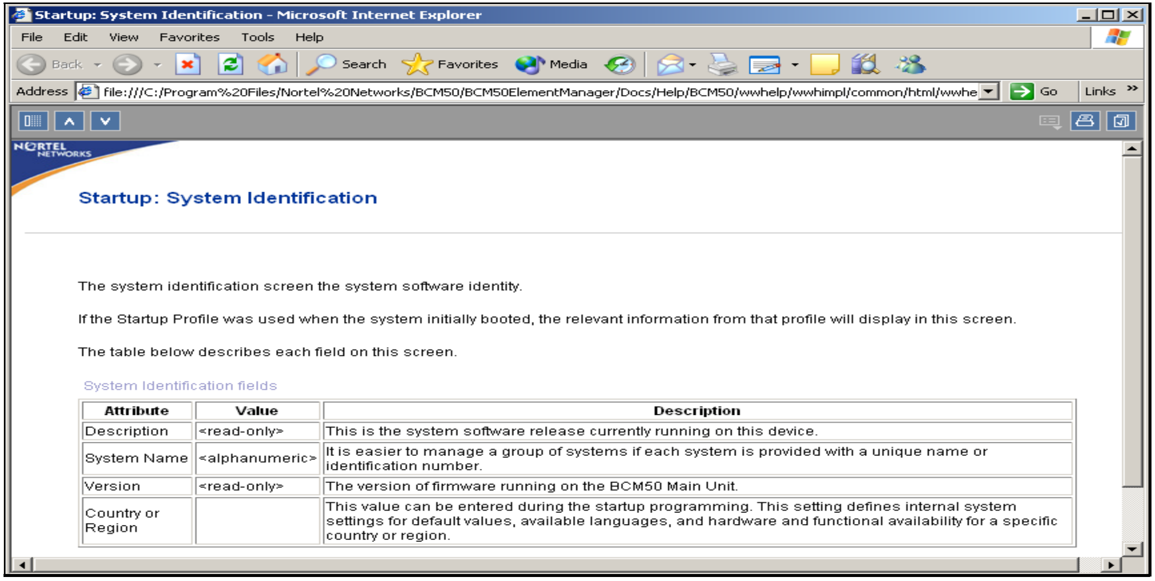
Country or region: North America

Can be entered during startup programming. Defines internal system settings for default values, available languages, and hardware and functional availability for specific country or region

Context-sensitive Help

You can view context-sensitive Help by clicking on a navigation tree heading, tab heading, or field heading of a connected BCM50 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 provide links to tasks and other features related to the panel function. Figure 23 on page 74 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 23 Context-sensitive HTML page


Startup: System Identification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address file:///C:/Program%20Files/Nortel%20Networks/BCM50/BCM50ElementManager/Docs/Help/BCM50/wwhelp/wwhimpl/common/html/wwhe
Go Links
NORTEL NETWORKS

Startup: System Identification

The system identification screen the system software identity.

If the Startup Profile was used when the system initially booted, the relevant information from that profile will display in this screen.

The table below describes each field on this screen.

System Identification fields

Attribute	Value	Description
Description	<read-only>	This is the system software release currently running on this device.
System Name	<alphanumeric>	It is easier to manage a group of systems if each system is provided with a unique name or identification number.
Version	<read-only>	The version of firmware running on the BCM50 Main Unit.
Country or Region		This value can be entered during the startup programming. This setting defines internal system settings for default values, available languages, and hardware and functional availability for a specific country or region.

BCM50 common file input/output processes

Many BCM50 tasks require task data to be transferred, to or retrieved from, different destinations or sources. BCM50 can use the following data repositories when transferring or retrieving task data:

- BCM50
- 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 BCM50 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 BCM50	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 BCM50, 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
BCM50	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 BCM50

Transferring information on the BCM50 is quick and easy, but does not protect your data in the event of damage to the BCM50. It makes an ideal solution in small environments where the BCM50 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 BCM50 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 BCM50 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 BCM50 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 50 Security Policies and Accounts and Privileges," on page 81.

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 BCM50. The backup and log information can be saved only to the top level of the USB storage drive file hierarchy. Transfers from the BCM50 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

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 BCM50s 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

BCM50 Element Manager usage on a BCM50a or BCM50e

If you have a BCM50a or a BCM50e, Element Manager cannot be used from the WAN until the router is configured properly. This section explains the necessary settings for enabling Element Manager operation from the WAN side of the integrated router.

Consult the BCM50a or BCM50e documentation for information on how to modify these settings.

Configuring firewall settings

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: BCM50 LAN IP address. This is the IP address listed in Element Manager under System/IP Subsystem/General Settings.
- Service Type: TCP:5989, 443 and 80 (port number for OpenWbem, https and http)
- Action: forward

Adding NAT rules

You must configure these three services for NAT: OpenWbem, HTTPs, and HTTP. Configure them using the following three rules:

- Name: OpenWbem
- Start Port: 5989
- End Port: 5989
- Server IP address: The BCM50 LAN IP address

- Name: HTTPs

- Start Port: 443
- End Port: 443
- Server IP address: The BCM50 LAN IP address

- Name: HTTP
- Start Port: 80
- End Port: 80
- Server IP address: The BCM50 LAN IP address

After these rules are configured, the BCM50 Element Manager can be accessed from the WAN.

Chapter 4

BCM 50 Security Policies and Accounts and Privileges

BCM50 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 BCM50 Element Manager. Some security capabilities are available on the BCM50 router models, for example, security related to firewalls, NAT, VPN, DoS alert, data communication, DHCP, VLAN, PPP, SNMP, and logging. You can configure the router security policies through the router web page; see the *BCM50 Integrated Router Configuration Guide* for more information.

➡ **Note:** If you do not have an integrated router you should ensure that your firewall and NAT are configured properly in your network.

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.

Navigation

Security Policies

- "Configuring system security policies" on page 82
- "Configuring user accounts, user groups and privileges" on page 91

Accounts and Privileges

- "Configuring user accounts, user groups and privileges" on page 91
- "Accounts and Privileges GUI description" on page 114
- "BCM50 security fundamentals" on page 124

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.

The default security settings assume a medium level of security.

Prerequisites

- To access the Securities Policies panel, you must have Security level privileges to modify these settings.

Navigation

- "Configuring user accounts, user groups and privileges" on page 91
- "Setting system access control policies" on page 86
- "Setting credential complexity" on page 87
- "Setting lockout on failed login" on page 88
- "Uploading a Web Server Certificate" on page 89
- "Transferring an SSH Key-Pair" on page 90

Job Aid

These links provide navigation to the sections of the panel for each security policy item:

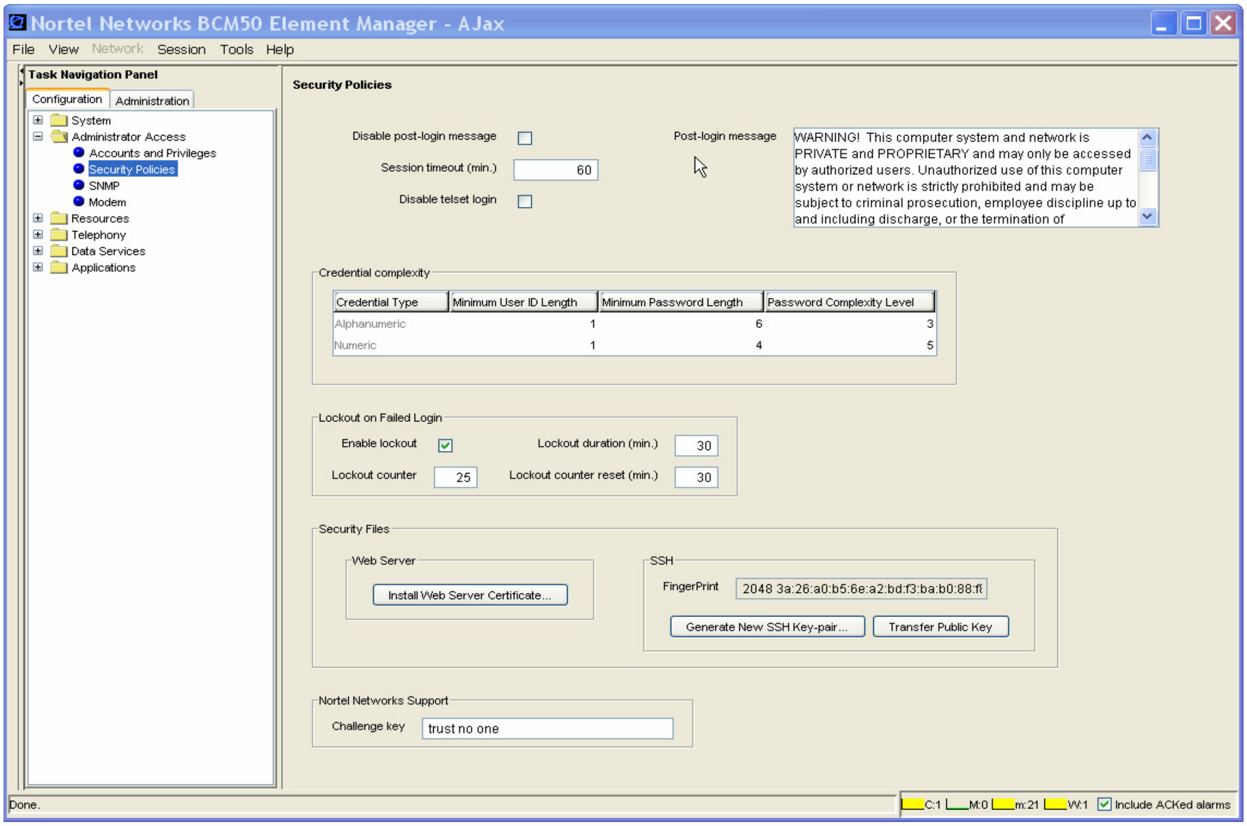
Panel section	Tasks
• System Access Rules	• "Setting system access control policies" on page 86
• Credential Complexity	• "Setting credential complexity" on page 87
• Lockout on Failed Login	• "Setting lockout on failed login" on page 88
• Security Files	
— Web Server	• "Uploading a Web Server Certificate" on page 89
— SSH	• "Transferring an SSH Key-Pair" on page 90

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

Security Policies GUI description

The fields that make up the Security Policies panel are described in this section.

Figure 24 Security Policies panel



Security Policies

Disable post-login message □

Session timeout (min.) 60

Disable telset login □

Post-login message: WARNING! This computer system and network is PRIVATE and PROPRIETARY and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of

Credential complexity

Credential Type	Minimum User ID Length	Minimum Password Length	Password Complexity Level
Alphanumeric	1	6	3
Numeric	1	4	5

Lockout on Failed Login

Enable lockout ☑ Lockout duration (min.) 30

Lockout counter 25 Lockout counter reset (min.) 30

Security Files

Web Server

SSH

FingerPrint 2048 3a:26:a0:b5:6e:a2:bd:f3:ba:b0:88:f(

Nortel Networks Support

Challenge key trust no one

The following table describes the fields on this panel:

Note: If you are using Network Configuration Manager, password policies are applied, regardless of the Element Manager settings.

Table 17 Security Policies fields

Attribute	Value	Description
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.
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

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Post login message	text	Displays the post-login security warning. The warning can be edited to customize the message for your system.
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)	1 2 3 4	Defines the number of character types required for an alphanumeric password. Default: 3 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:** Check minimum length setting to ensure that it is equal to or greater than the complexity level. Password complexity consists of the following types: • upper case alphabet (English) • lower case alphabet (English) • westernized Arabic numbers • non-alphanumeric characters ($, !, %, ^, period, comma)
Password Complexity Level (telset interface)	1 2 3 4 5	Specifies the number of unique digits that must be part of a telset password: 1: one unique digit 2: two unique digits 3: three unique digits 4: four unique digits 5: prevent consecutive numbering **Note:** Check the minimum length setting to ensure that it is equal to or greater than the complexity level.

Table 17 Security Policies fields (Continued)

Attribute	Value	Description
Lockout on Failed Logon		
Enable lockout	check box	When checked, specifies that enable lockout rules apply 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 116 (Locked Out box) and "View by Account: General" on page 118 (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.
Web Server		
Upload Security Certificate (button) SSL certificate download		Opens the file system browser to allow a system-specific security certificate and the accompanying Private key to be selected. 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.
Nortel Support		
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.

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**.
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. Enter the number of minutes to wait after a period of inactivity before logging a user off in the Session timeout (min.) box.
5. Click in the **Disable telset login** box to prevent users from having administrating the system through any telset interface.

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**.
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. For an alphanumeric password, the level is from 1 to 4. For a numeric password, the level is from 1 to 5.

Variable Table

Variable	Value
Complexity Level (Element Manager)	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 The four character types are: • lowercase letters • uppercase letters • numbers • !^,.@#$%& and spaces
Complexity Level (Telset)	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 on failed login

Setting Lockout on Failed Login allows the administrator to set lockout rules.

To set Lockout on Failed Login

1. Select **Configuration**, **Administrator Access**, **Security Policies**.
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.

Uploading a Web Server Certificate

This procedure allows you to upload a private security certificate to replace the generic web certificate provided with BCM50. Using a custom site-specific certificate, you can have site validation which will eliminate the security warnings.

To upload a Web Server Certificate

1. Select **Configuration**, **Administrator Access**, **Security Policies**.
2. In the Security Files, Web Server 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 BCM50 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**.
2. In the **Security Files**, **SSH** section, click the **Generate New SSH Key-pair** button.
   The new key is put on the computer running BCM50.
3. Click the **Save** button.
4. For SSH Key-pair, in the **Transfer Public Key** dialog box, read the information provided and note the FingerPrint text. Click the **OK** button.
5. On the **Transfer Public Key** dialog box, locate and select the public key file.
6. Click **Transfer** 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

Navigation

- “Adding a new user account” on page 93
- “Modifying a user account” on page 93
- “Adding callback for a dial-up user” on page 94
- “Adding Telset access for a user” on page 94
- “Deleting a user account” on page 95
- “Changing a user’s password” on page 96
- “Changing the current user’s password” on page 96
- “Creating a group” on page 97
- “Deleting a group” on page 97
- “Adding a user account to a group” on page 98
- “Deleting a user account from a group” on page 99
- “Rel-enable a locked-out user” on page 99
- “Enabling and disabling an account” on page 100
- “Enabling and disabling exclusive access” on page 101
- “User account and user group management fundamentals” on page 102
- “Accounts and Privileges GUI description” on page 114

Job Aid

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

Panel tabs	Tasks
"Current Account" on page 114	"Enabling and disabling exclusive access" on page 101
"View by Accounts" on page 116	• "Adding a new user account" on page 93 • "Modifying a user account" on page 93 • "Deleting a user account" on page 95 • "Changing a user's password" on page 96 • "Changing the current user's password" on page 96 • "Adding callback for a dial-up user" on page 94 • "Rel-enable a locked-out user" on page 99
"View by Account: General" on page 118	• "Enabling and disabling an account" on page 100
"View by Account: Group Membership" on page 119	• "Adding a user account to a group" on page 98 • "Deleting a user account from a group" on page 99
"View by Accounts" on page 120	• "Creating a group" on page 97 • "Deleting a group" on page 97
"View by Groups: General" on page 121	• "Modifying group privileges" on page 98
"View by Groups: Members" on page 123	• "Adding a user account to a group" on page 98 • "Deleting a user account from a group" on page 99

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

As an administrator, you can create user accounts.

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 the user's identifier in the **User ID** field.
4. In the **User password** field, enter the user's password.
5. In the **Confirm password** dialog box, enter the user's password again.
6. If call back for dial-up users is required, enter the number the system dials to contact the client modem in the **Callback Number** field..
7. In the **Callback Passcode** field, enter the call back passcode.
8. If telset access is required, enter the user's identifier in the **Telset User ID** field.
9. In the **Telset Password** field, enter the user's telset password.
10. 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 96.

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 94.
5. If telset access is required, see "Adding Telset access for a user" on page 94.
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 V.90 modem, you can enhance your access security by assigning that person a specific user account that prompts the system to acknowledge the user, then hang up and dial back the user at a designated telephone number, before allowing the person to have access to the system.

To add callback for a dial-up 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 **Callback Number** field, enter the number the system dials to contact the client modem. Ensure you include the correct routing codes.
4. In the **Callback Passcode** field, enter the call back passcode.
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. 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 V**iew by Account** tab.
2. Select a user on the Users table.
3. Click the **Delete** button.
4. In the confirmation box, click **OK** 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.

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.
5. 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 114).

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 Accounts** 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. From the **Group Privileges** box, click the **Add** button and select one or more group privileges to assign to the group and click **Add**.
7. In the **Add Privilege** dialog box, select one privilege at a time to assign to the group and click **Add**. Repeat as necessary to add the set of privileges required. See "Default groups" on page 103 and "Default access privileges excluding set-based privileges" on page 105 for more information.
8. Populate the group using "Adding a user account to a group" on page 98.

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 **OK** on the confirmation box to remove the groups from the list.

Modifying group privileges

Prerequisites

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. On the **Group Privileges** tab, select one or more group privileges to delete from the existing group, or click the **Add** button to add privileges to the group. To delete a privilege, see Step 6.
4. To add a privilege, click **Add**.
5. In the **Add Privilege** dialog box, select one privilege at a time to assign to the group and click **Add**. Repeat as necessary to add the set of privileges required. See "Default groups" on page 103 and "Default access privileges excluding set-based privileges" on page 105 for more information.
6. To delete a privilege, click **Delete**.
7. Click **OK** 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.

Rel-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.

Prerequisites

- 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 ou**t 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 and interfaces, such as the **nnguest** account and the modem.

To 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 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 On the General panel, ensure that **Enable account expiry** is selected.

4 Click in the **Account will be disabled** field, and choose the date the account is to be disabled.

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

Navigation

User accounts

User accounts are defined by:

- a unique numerical user ID that is visible only to authenticating services
- 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

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 and the user ID that created the account
- modify date and the user ID that modified the account
- expiry date, if enabled
- login history, including failed attempts and the date 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 BCM50 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 teleset administration menu (F9*8), tonly he 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 18 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 BCM50 comes with a number of default read-only groups that provide a predetermined set of access privileges. Also included in Table 19 are the default privilege levels for each default group, which are described in “Default access privileges excluding set-based privileges” on page 105 and “Telset access security” on page 111.

Table 19 Default user account groups

Group Name	Privileges	Notes
SBA Installer	SBAInstaller IP Set Registration	See “SBA - Installer group access privileges” on page 112 See “IP Set Registration group access privileges” on page 106

Table 19 Default user account groups (Continued)

Group Name	Privileges	Notes
SBA Coord+ Group	SBASystemCoordBasic	See “SBA - System Coordinator+ group access privileges” on page 112
SBA Coord Group	SBASystemCoord	See “SBA - System Coordinator group access privileges” on page 112
SBA Basic Group	SBABasic	See “SBA - Basic group access privileges” on page 113
Voice & Callcenter Group	VoiceMailAdmin	Only access to voicemail/call center administration if this is the only group assigned to a user account. See “Voice Mail & Callcenter group access privileges” on page 105.
Call Center	Voice Mail & CallCenter	Only access to the Callcenter application is available if this is the only group assigned to a user account. See “Call Center group access privileges” on page 105
CDR Application	CDRApp	Only access to the call detail record functions is available if this is the only group assigned to a user account. See “CDR Appl group access privileges” on page 107
CTE Application	CTEAppl	See “CTE Appl group access privileges” on page 106
BCM Monitor Application	BCMMonitorAppl	See “BCMMonitor Appl group access privileges” on page 106
Administrator	All privileges	The group contains all available privileges, including the installer-level access to the set based configuration menus (F9*8, **CONFIG, and *983).
Data Admin	DATAAdmins	See “DATA Admins group access privileges” on page 108
Remote Access	PPP RemoteAccess	See “PPP Access group access privileges” on page 107 See “Remote Access group access privileges” on page 108
Guest	Guests	See “Guests group access privileges” on page 109
Voice Admin	VoiceMail&Callcenter IP Set Registration VoiceAdmins Alarm Monitor	See “Voice Mail & Callcenter group access privileges” on page 105 See “IP Set Registration group access privileges” on page 106 See “Voice Admins group access privileges” on page 109 See “Alarm Viewer group access privileges” on page 110
Power Users	VoiceMail&Callcenter IP Set Registration DATAAdmins VoiceAdmins Alarm Monitor	See “Voice Mail & Callcenter group access privileges” on page 105 See “IP Set Registration group access privileges” on page 106 See “DATA Admins group access privileges” on page 108 See “Voice Admins group access privileges” on page 109 See “Alarm Viewer group access privileges” on page 110
Backup Operators	Security BackupOperators	See “Security group access privileges” on page 105 See “Backup Operators group access privileges” on page 109
Security	Security AdminDownload Operational Logs Diagnostic Logs	See “Security group access privileges” on page 105 See “Admin Download group access privileges” on page 107 See “Operational Logs group access privileges” on page 111 See “Diagnostic Logs group access privileges” on page 111
Admin Download	AdminDownload	See “Admin Download group access privileges” on page 107

Table 19 Default user account groups (Continued)

Group Name	Privileges	Notes
Guest Download	GuestDownload	Can access the BCM50 web page for application downloads and user documentation. See "Guest Download group access privileges" on page 107
Remote Monitoring	Remote Monitor Operational Logs	See "Remote Monitoring group access privileges" on page 110 See "Operational Logs group access privileges" on page 111

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 & Callcenter group access privileges

- SBA -Voice Mail
- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Applications - Voice Messaging
  EM - CONFIG - Applications - Callcenter
- Web Documentation - User Documentation
- BCM50 Applications - Applications - CallPilot Manager
- Web - User Applications

Call Center group access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM50 Applications - Applications - CallPilot Manager
- Web - User Applications

Security group 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 - Reboot
- 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 group access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM50 Applications - Applications - CTE DA Pro AE
- Web - User Applications

IP Set Registration group access privileges

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

BCMMonitor Appl group access privileges

- EM - CONFIG - Administrator Access - Current User
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- BCM50 Applications - Applications - BCM Monitor
- Web - User Applications

CDR Appl group access privileges

- EM - CONFIG - Administrator Access - Current User
- Web Documentation - User Documentation
- BCM50 Applications - Applications - Call Detail Recording
- Web - User Applications

PPP Access group access privileges

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

Guest Download group 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 group access privileges

- Web Documentation - User Documentation
- Web Documentation - Admin Documentation
- Web Application Download - Web Download - Element Manager
- Web Application Download - Web Download - NCM for BCM50
- 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 group access privileges

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

Admin group 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 group 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 Setting
- Web Documentation - User Documentation

Guests group 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 group 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 - Callcenter
- 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 Metrics - Qos Monitor
- EM - ADMIN - System Metrics - 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 group 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 group 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 Setting
- EM - ADMIN - General - Service Manager as read only
- EM - ADMIN - General - Inventory as read only
- EM - ADMIN - System Metrics - Qos Monitor
- EM - ADMIN - System Metrics - UPS Metrics as read only
- EM - ADMIN - System Metrics - NTP Metrics as read only
- EM - ADMIN - Telephone Metrics - all
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- Web - User Applications

Software Upgrade group 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 group 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 group access privileges

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

Diagnostic Logs group access privileges

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

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 20 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	
	Dfltgwy	
License	FILE Keycode data	Uses Keycodes that can be entered one at a time through Feature 9*8 .

Table 20 Default Telset access

Configuration Heading	Parameters	Comments
TelephonyStartup	Template	Uses Feature ** STARTUP on telset within 15 minutes of a bootup of m50. See Norstar documentation.
	StartDN	Uses Feature ** STARTUP on telset within 15 minutes of a bootup of m50. 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 passowrk setting is used)
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM50 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
- BCM50 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

- BCM50 Applications - User Applications

SBA - Basic group access privileges

- SBA - Basic Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM50 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.

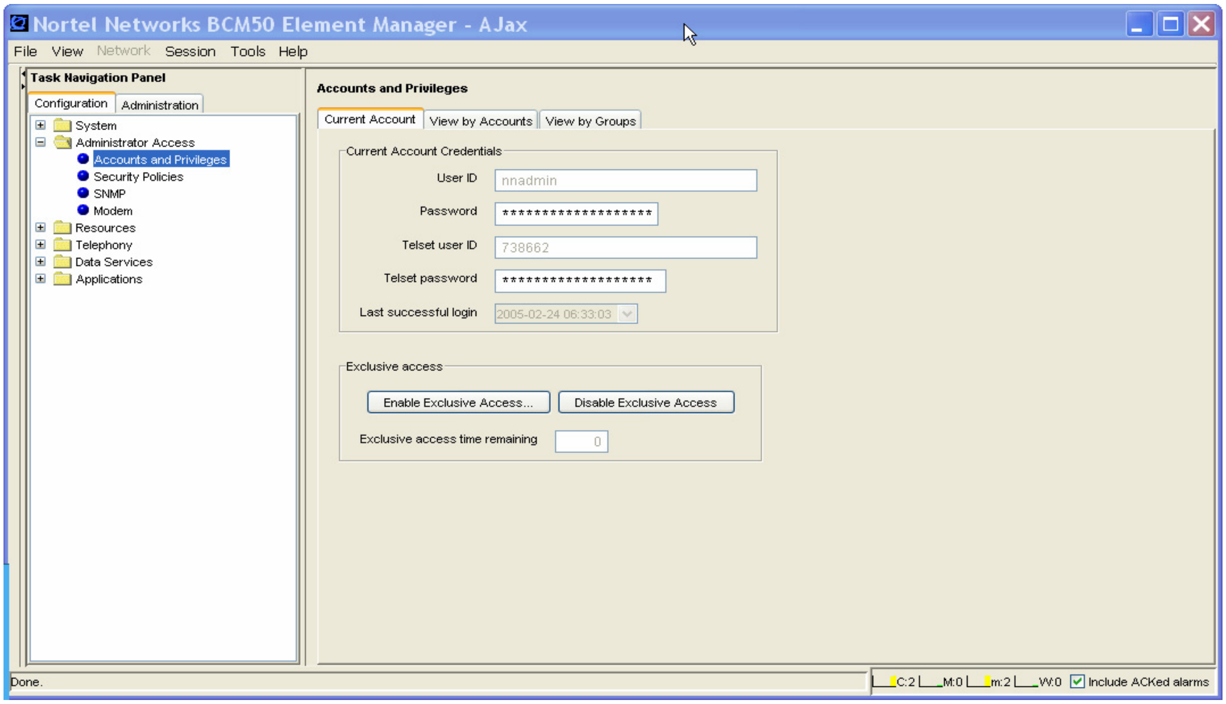
Accounts and Privileges GUI description

Current Account

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

This panel allows the user to change either the Element Manager password or the telset interface password. Users cannot change user IDs from this panel.

Figure 25 Accounts and Privileges: Current Account context panel



User ID: nnadmin
Password: *******************
Telset user ID: 738662
Telset password: *******************
Last successful login: 2005-02-24 06:33:03
Exclusive access time remaining: 0

Refer to the next section, “View by Accounts” on page 120, for details about changing user IDs.

Table 21 describes each field on the Current Account context panel.

Table 21 Current Account fields

Attribute	Value	Description
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 87. **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 21 Current Account fields (Continued)

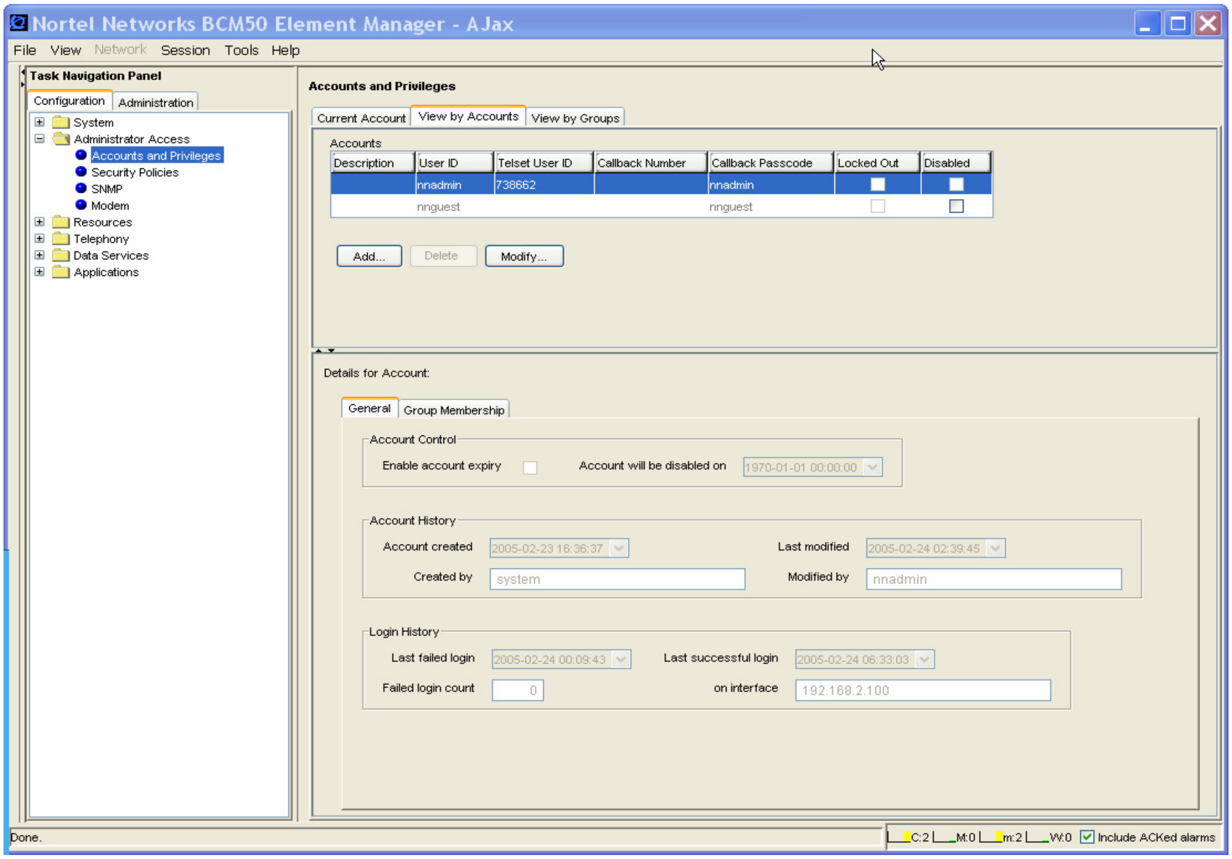
Attribute	**Value**	**Description**
Telset password	numeric	Requires a numeric password entry that is unique for each user. These strings must satisfy the security requirements. Refer to "Complexity Level (Telset)" on page 87. **Note:** This password takes effect at the next login.
Last Successful log-in	read-only	Aread-only field that indicates the last date and time the user account was used to log on to the system.
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 26 Accounts and Privileges, View by Accounts context panel



Accounts

Description	User ID	Telset User ID	Callback Number	Callback Passcode	Locked Out	Disabled
	nnadmin	738662		nnadmin	□	□
	nnguest			nnguest	□	□

Details for Account:

Account Control

Enable account expiry □ Account will be disabled on 1970-01-01 00:00:00

Account History

Account created 2005-02-23 16:36:37 Last modified 2005-02-24 02:39:45

Created by system Modified by nnadmin

Login History

Last failed login 2005-02-24 00:09:43 Last successful login 2005-02-24 06:33:03

Failed login count 0 on interface 192.168.2.100

Table 22 describes each field on the View by Accounts panel.

Table 22 View by Accounts fields

Attribute	Value	Description
Description	alphanumeric	Displays the descriptive name for the user or the user function. This field can be blank.
User ID	alphanumeric	Displays the accounts by User ID
Telset User ID	numeric	Displays the accounts by Telset User ID
Callback Number	telephone #	Specifies the number the system will call to verify the dial-up user access

Table 22 View by Accounts fields

Attribute	**Value**	**Description**
Callback Passcode	User ID	Specifies the passcode the system uses to confirm the callback is legitimate
Locked Out	true/false	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 "Rel-enable a locked-out user" on page 99.
Disabled	true/false	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 100.
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 nnadmin 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.

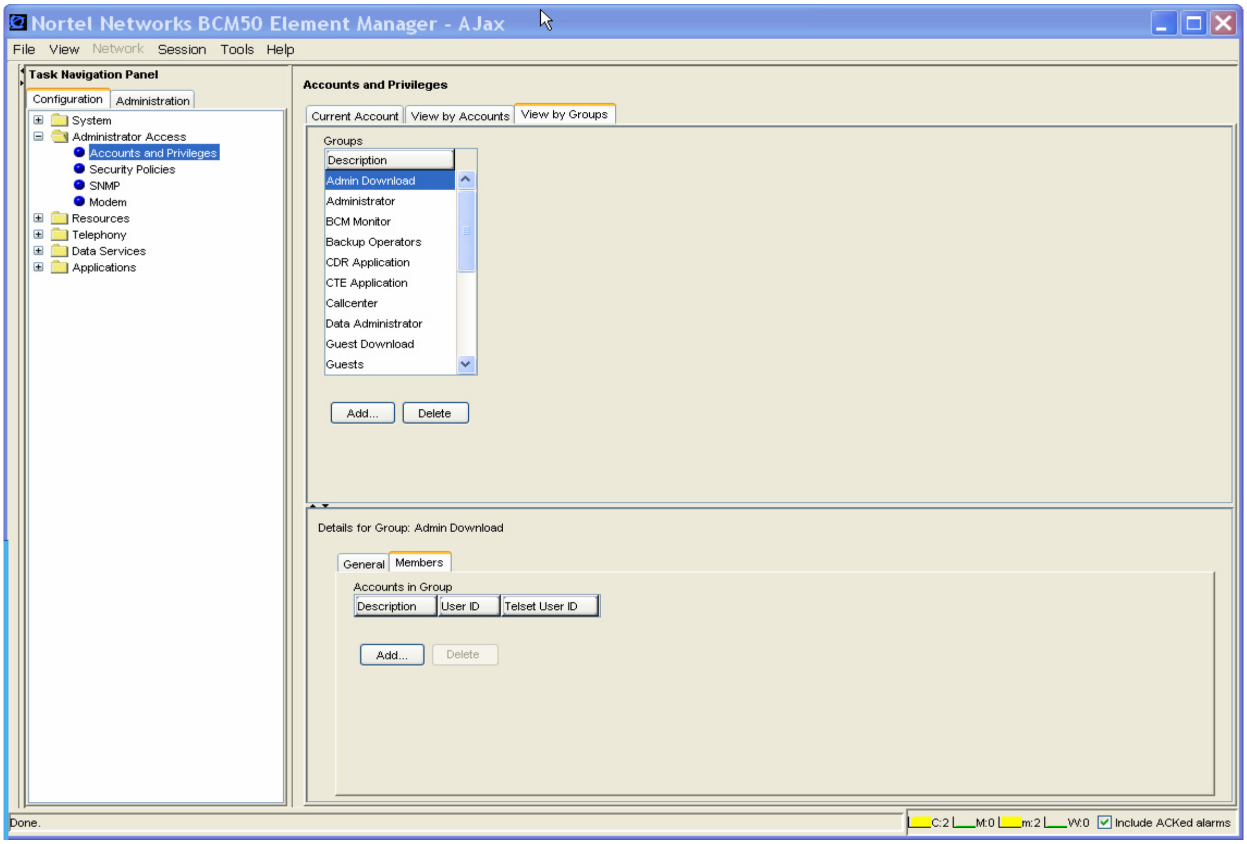
If you select a user on the Users list, two more panels appear in the lower frame:

- The General panel allows you to see the current status of the account. See to "View by Account: General" on page 118
- The Group Membership panel allows you to associate the account to group profiles, which determines what type of access the user has. See to "View by Account: Group Membership" on page 119.

View by Account: General

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

Figure 27 Users: General user settings



[Table 23](#) describes each field on this panel.

Table 23 View by Accounts: General fields

Attribute	Value	Description
Account Control		
Enable account expiry	check box	When selected, specifies that the user account is scheduled to automatically expire at the specified date.
Account will be disabled on	date	Specifies the date when the user account will expire. The pull-down menu opens a calendar.
Account history		
Account created Created by	read-only	Specifies the date that the user record was added. Specifies the userID of the person who added the user account.
Last Modified Modified by	read-only	Specifies the date the user record was last modified. Specifies the userID of the person who last modified the account.

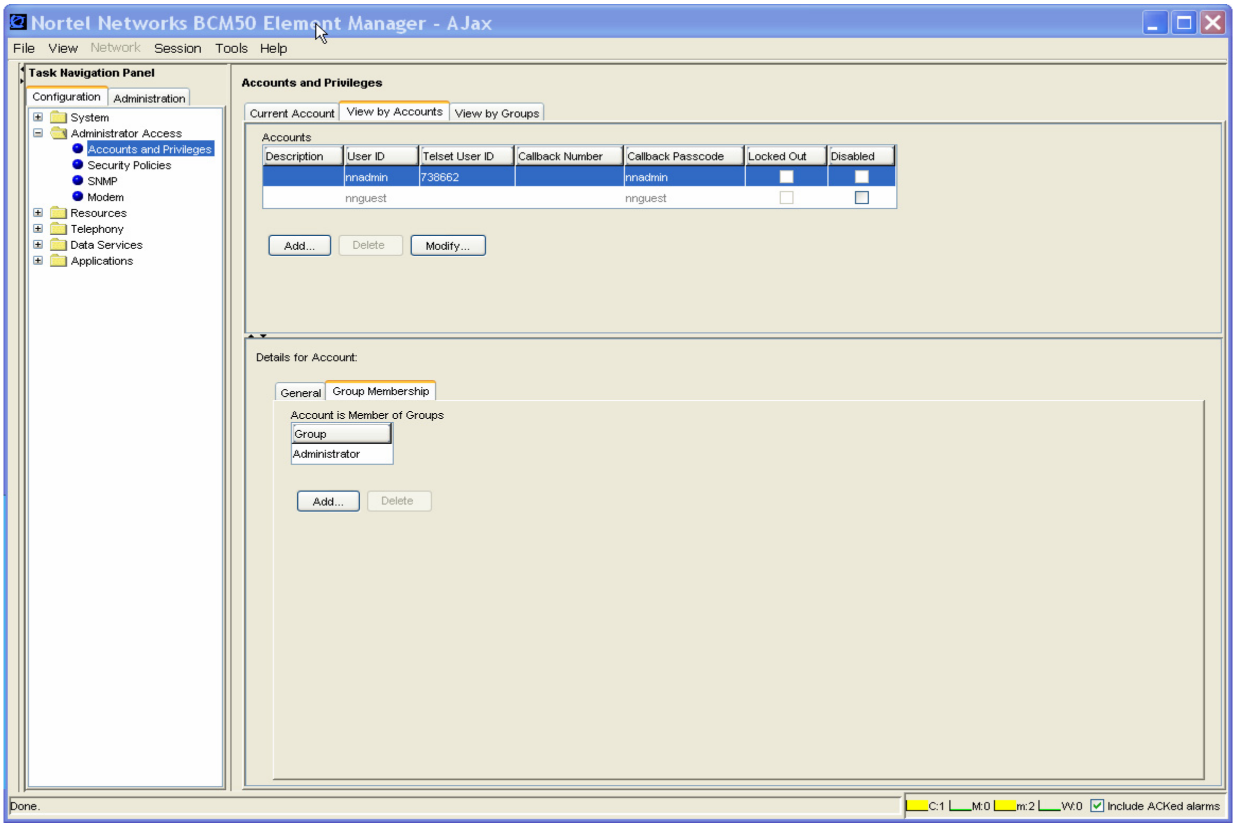
Table 23 View by Accounts: General fields (Continued)

Attribute	Value	Description
Login history		
Last failed login	read-only	Specifies the date that the user last tried and failed to logon.
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 successful login	read-only	Specifies the date the user last successfully logged on to either the Element Manager or the telset interface.
On interface	read-only	Element Manager: Displays the IP address of the Element Manager 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.

Figure 28 Group Membership tab panel



Accounts

Description	User ID	Telset User ID	Callback Number	Callback Passcode	Locked Out	Disabled
	nnadmin	738662		nnadmin	□	□
	nnguest			nnguest	□	□

Account is Member of Groups

Group
Administrator

Table 24 describes each field on this panel.

Table 24 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 103 for a list of the default groups and the privileges associated with each. Note: Groups are added, modified or deleted from the "View by Accounts" on page 120 panel.
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 Accounts

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

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

Figure 29 View by Groups tab, Groups panel

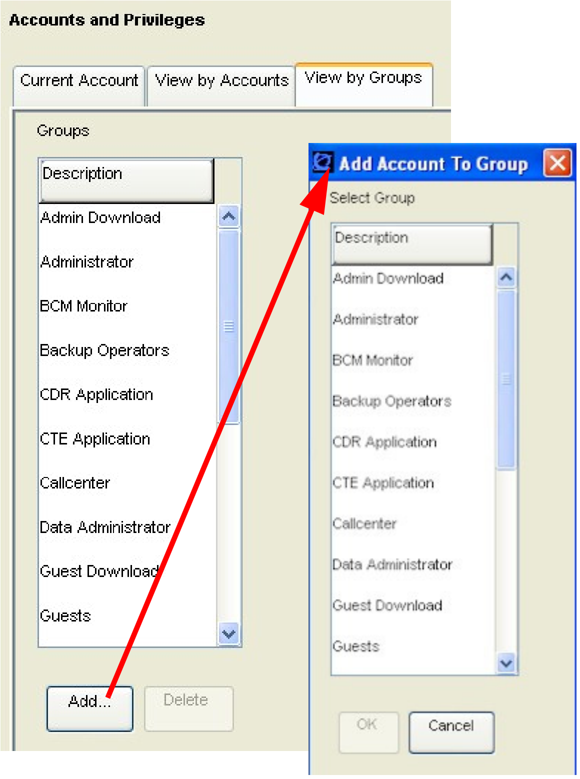


Table 25 describes each field on this panel.

Table 25 View by Groups fields

Attribute	Description
Groups	Lists all the defined groups. Refer to "Default groups" on page 103 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.

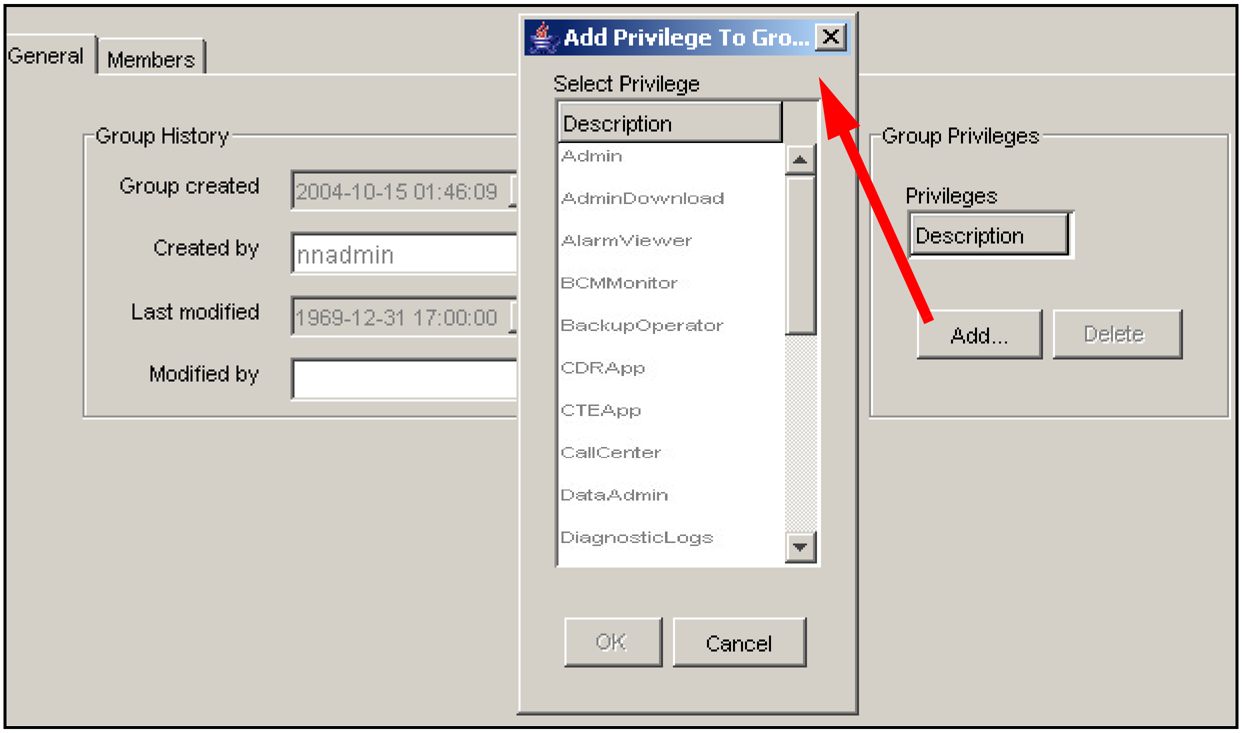
For more details about groups, refer to the panels described in "View by Groups: General" on page 121.

View by Groups: General

For a selected entry in the Groups table ("View by Accounts" on page 120), 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.

Figure 30 Adding privileges to groups



Group History
Group created: 2004-10-15 01:46:09
Created by: nnadmin
Last modified: 1969-12-31 17:00:00
Modified by:

Table 26 describes each field on this panel.

Table 26 View by Groups: General panel fields

Attribute	Value	Description
Group History		
Group created Created by	read-only	Specifies the date the group account was created Specifies the user who created the account
Last modified Modified by	read-only	Specifies the last date the group account was changed 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 Accounts" on page 120), you can use the Members panel to assign the group to existing user accounts and to view which accounts have the selected group assigned.

Figure 31 Adding user accounts to a group

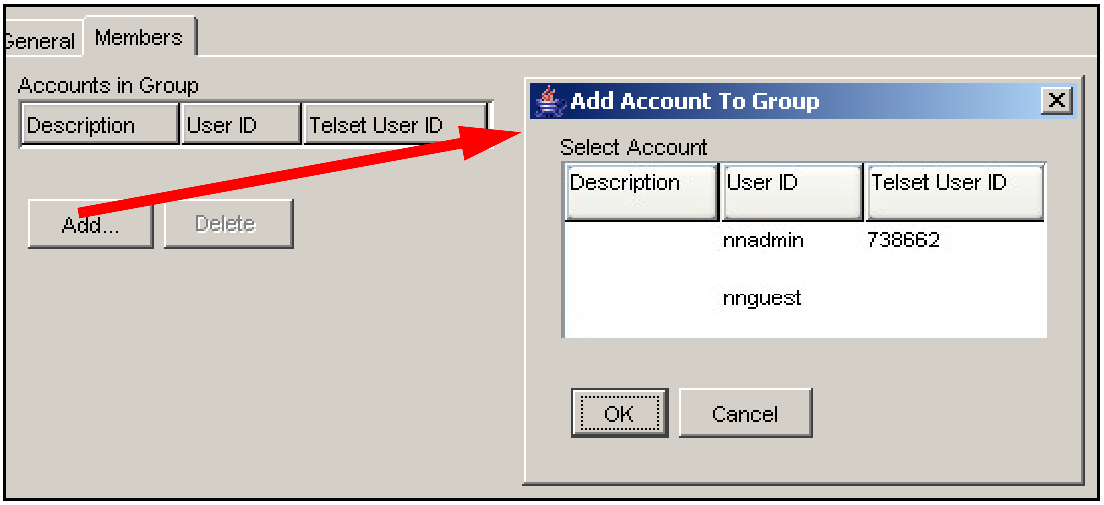


Table 27 describes each field on this panel.

Table 27 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.

BCM50 security fundamentals

This section provides an overview of BCM50 security policies and user access and a reference to other panels that provided topic-specific security.

Navigation

Security Policies and User Access

- "Secure network protocols and encryption" on page 125
- "Security audits" on page 125
- "System security considerations" on page 126
- "Security certificate" on page 127
- "Site authentication" on page 128
- "Firewalls" on page 127

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 BCM50 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 BCM50 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 BCM50 Logs,” on page 315.

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, *nnadmin.* 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. Firewalls are enabled by default by BCM router security software. The default rule prevents incoming communication from the WAN side but allows out-going communication.

Depending on the hardware being used and the type of security being employed, specific firewall rules must be set to enable communication between the BCM50 and the Element Manager. See the *BCM50 Integrated Router Configuration Guide* for more information.

Security certificate

The BCM50 is delivered with a generic SSL security certificate. The self-signed certificate that is included in BCM50 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 BCM50 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 BCM50.

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 BCM50 generic SSL certificate is used, the user is prompted to accept an unsigned certificate when accessing the SSLweb interface in their web browser.

Chapter 5
Using the BCM50 Hardware Inventory

This chapter describes how to use the BCM50 Hardware Inventory. The Hardware Inventory task in the BCM50 Element Manager displays information about the BCM50 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 BCM50 Hardware Inventory

The BCM50 Hardware Inventory panel provides information about the BCM50 physical system. There are three tabs on the main Hardware Inventory panel:

Table 1 Hardware Inventory panel

Tab	Description
BCM50 system	Provides information about the key components of the BCM50. For more information, see "Viewing and updating information about the BCM50 system" on page 130.
Devices	Provides information about any non-BCM50 components connected to the system. For more information, see "Viewing information about BCM50 devices" on page 133.
Additional information	Provides manufacturer details about the BCM50. For more information, see "Viewing additional information about the BCM50 main unit" on page 135.

➡ **Note:** You can also add information about certain devices, such as an asset ID and location information, to facilitate tracking of the BCM50 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 66 for information about how to generate this record.

Viewing and updating information about the BCM50 system

You can view and update certain information about the BCM50 main unit using the BCM50 System tab in the BCM50 Element Manager. The BCM50 System tab is divided into three areas:

- BCM50 main unit
- BCM50 expansion unit
- Other Information

You can save inventory information to a file using the Programming Record. See "Saving programming records" on page 66.

Viewing and updating information about the BCM50 main unit

You can view information about the BCM50 main unit, such as the Nortel part number, the System ID, and other information. See Table 28.

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

Table 28 BCM50 main unit 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 BCM50 Communications Server	Read
Type*	The type of the physical entity	Chassis	Read
Serial number	The serial number to the BCM50 unit	Nortel System Serial Number	Read
Nortel part number*	The Nortel part number used to order the system	NT <xxxxxx>	Read
Model*	A textual description of the object	example 'BCM50 Telephony Only'	Read
System ID	A unique string that identifies this specific instance of the element	System ID which is Mac #1	Read
System name*	A user-friendly name for the object	System name of the BCM50	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 BCM50 main unit.

To view or update information about the BCM50 main unit

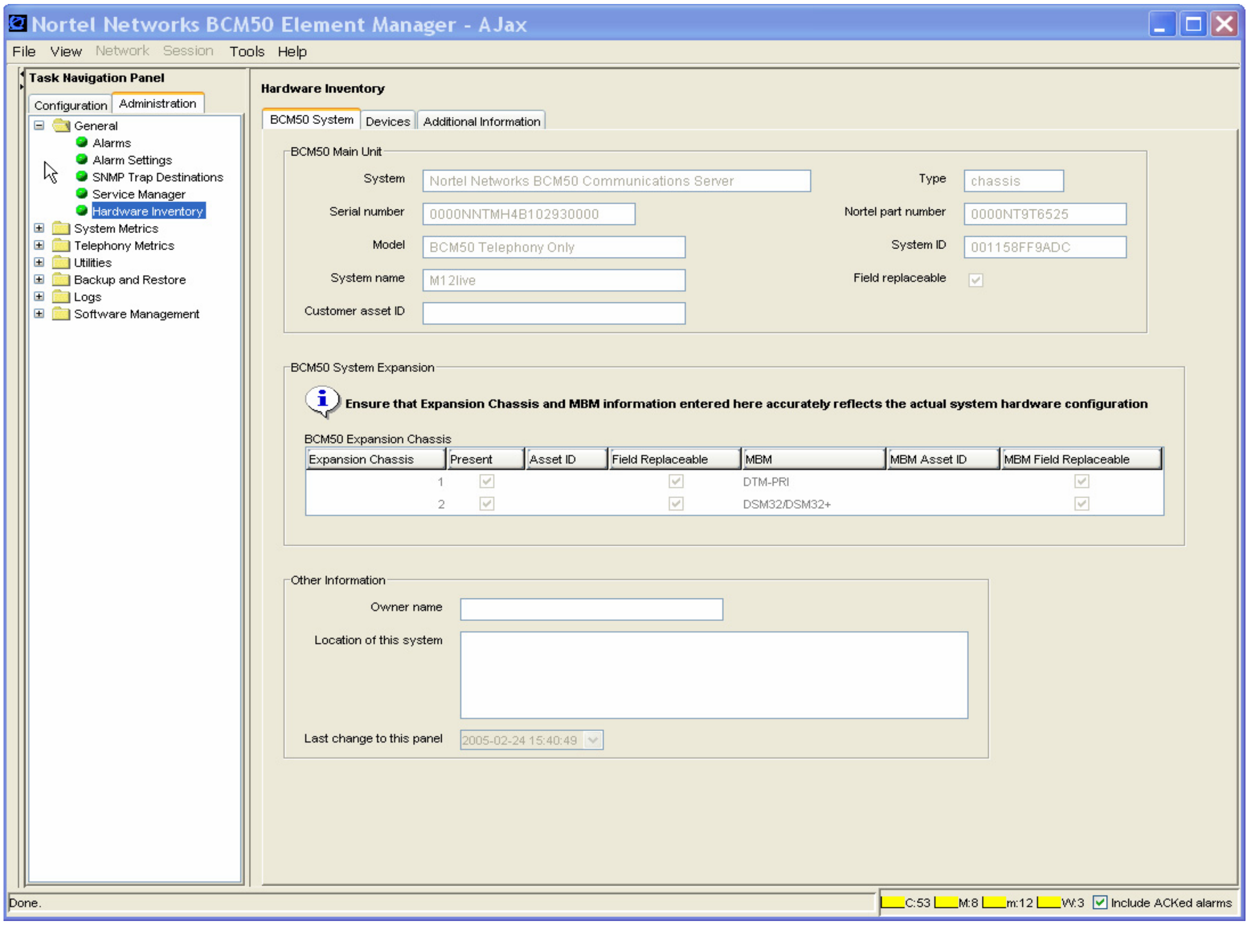
1 In the BCM50 Element Manager, connect to a BCM50 device.

2 Select **Administration**, **General**, **Hardware Inventory**.
The **Hardware Inventory** panel opens and displays the **BCM50 System** tab.

3 View the information displayed in the **BCM50 main unit** area.

4 If you want to add or update the asset ID for the BCM50 main unit, enter an asset ID in the **Customer Asset ID** field.

Figure 32 Hardware Inventory


Nortel Networks BCM50 Element Manager - AJax
File View Network Session Tools Help
Task Navigation Panel
Configuration Administration
General
Alarms
Alarm Settings
SNMP Trap Destinations
Service Manager
Hardware Inventory
System Metrics
Telephony Metrics
Utilities
Backup and Restore
Logs
Software Management
BCM50 System Devices Additional Information
Done.
C:53 M:8 m:12 W:3 ☑ Include ACKed alarms

Hardware Inventory

BCM50 Main Unit

System: Nortel Networks BCM50 Communications Server

Serial number: 0000NNTMH4B102930000

Model: BCM50 Telephony Only

System name: M12live

Customer asset ID:

Type: chassis

Nortel part number: 0000NT9T6525

System ID: 001158FF9ADC

Field replaceable: ☑

BCM50 System Expansion

Ensure that Expansion Chassis and MBM information entered here accurately reflects the actual system hardware configuration

BCM50 Expansion Chassis

Expansion Chassis	Present	Asset ID	Field Replaceable	MBM	MBM Asset ID	MBM Field Replaceable
1	☑		☑	DTM-PRI		☑
2	☑		☑	DSM32/DSM32+		☑

Other Information

Owner name:

Location of this system:

Last change to this panel: 2005-02-24 15:40:49

Viewing and updating BCM expansion unit information

The BCM50 expansion unit area in the BCM50 System tab provides information about the expansion unit connected to the BCM50 main unit, if any. If an expansion unit is present and populated with an MBM, this information is also provided.

Table 29 provides information about the fields in the BM50 expansion unit area.

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

Table 29 BCM50 expansion unit area

Column Name	Column Description	Column Value	Read/Write
Expansion Unit*	Index for the expansion unit	1 or 2	Read
Present	Indicates if an expansion unit to main unit is present	Yes (if checked)	Read
Asset ID*	Customer defined tracking number	Initially zero	Write
Field Replaceable*	Indicates if the entity is considered a Field Replaceable Unit by the supplier	Always True (checked)	Read
MBM*	MBM associated with that unit	example 'BRIM' or ‘DTM-T1’. As configured in the Configuartion>Resources>Telephony Resources panel	Read
MBM Asset ID*	The asset identifier assigned to the entity instance by its owner	Initially zero	Write
MBM Field Replaceable*	Indicates if the entity is considered a Field Replaceable Unit by the supplier	Always True (checked)	Read

You can add or update the following expansion unit information:

- the customer asset ID
- the MBM asset ID

To view or update expansion unit information

1. In the BCM50 Element Manager, connect to a BCM50 device.
2. Select **Administration**, **General**, **Hardware Inventory**.
   The Hardware Inventory panel opens, and displays the **BCM50 System** tab.
3. View the information displayed in the **BCM50 expansion unit** area.
4. If you want to add or update the asset ID for the BCM50 main unit, enter an asset ID in the **Customer Asset ID** field.
5. If you want to add or update the asset ID for the MBM, enter an asset ID in the **MBM Asset ID** field.

Viewing and updating other information about the BCM50 system

The Other Information area in the BCM50 System tab displays other information associated with this particular BCM50 system, such as:

- the name of the administrator and their contact information
- the location of the BCM50 system

You can add or update this information. The date on which this information is updated is displayed BCM50 area, in accordance with "LastChangeTime" of the Entity MIB.

Table 30 lists the fields displayed in the Other Information area.

Table 30 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 BCM50 main unit

1. In the BCM50 Element Manager, connect to a BCM50 device.
2. Select **Administration**, **General**, **Hardware Inventory**.
   The Hardware Inventory panel opens. The **BCM50 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 BCM50 system, enter information in the **Owner Name** field.
5. If you want to add or update information about the location of BCM50 system, enter information in the **Location of the System** field.

Viewing information about BCM50 devices

The Devices tab displays information about all devices attached to the BCM50. These devices may include:

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

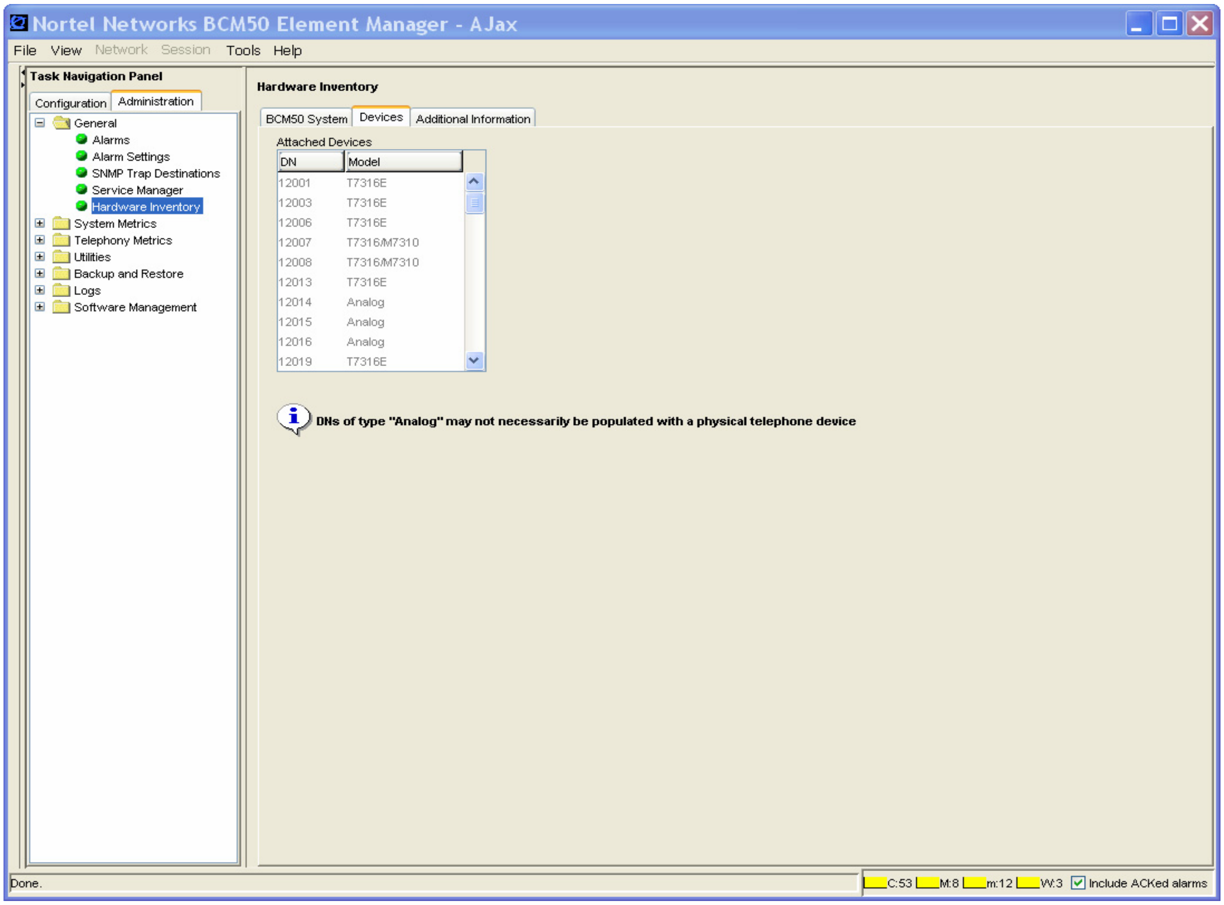
You can view all Directory Numbers (DNs) and the type of set associated with the DN. Table 31 lists the fields in the Attached Devices table.

Note: DNs of type "Analog" are not necessarily be populated with a physical telephone device.

Table 31 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 33 Hardware Inventory Devices tab



Attached Devices

DN	Model
12001	T7316E
12003	T7316E
12006	T7316E
12007	T7316/M7310
12008	T7316/M7310
12013	T7316E
12014	Analog
12015	Analog
12016	Analog
12019	T7316E

DNs of type "Analog" may not necessarily be populated with a physical telephone device

To view information about attached devices

1 In the BCM50 Element Manager, connect to a BCM50 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 BCM50 main unit

The Additional Information tab displays additional information about the BCM50 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.

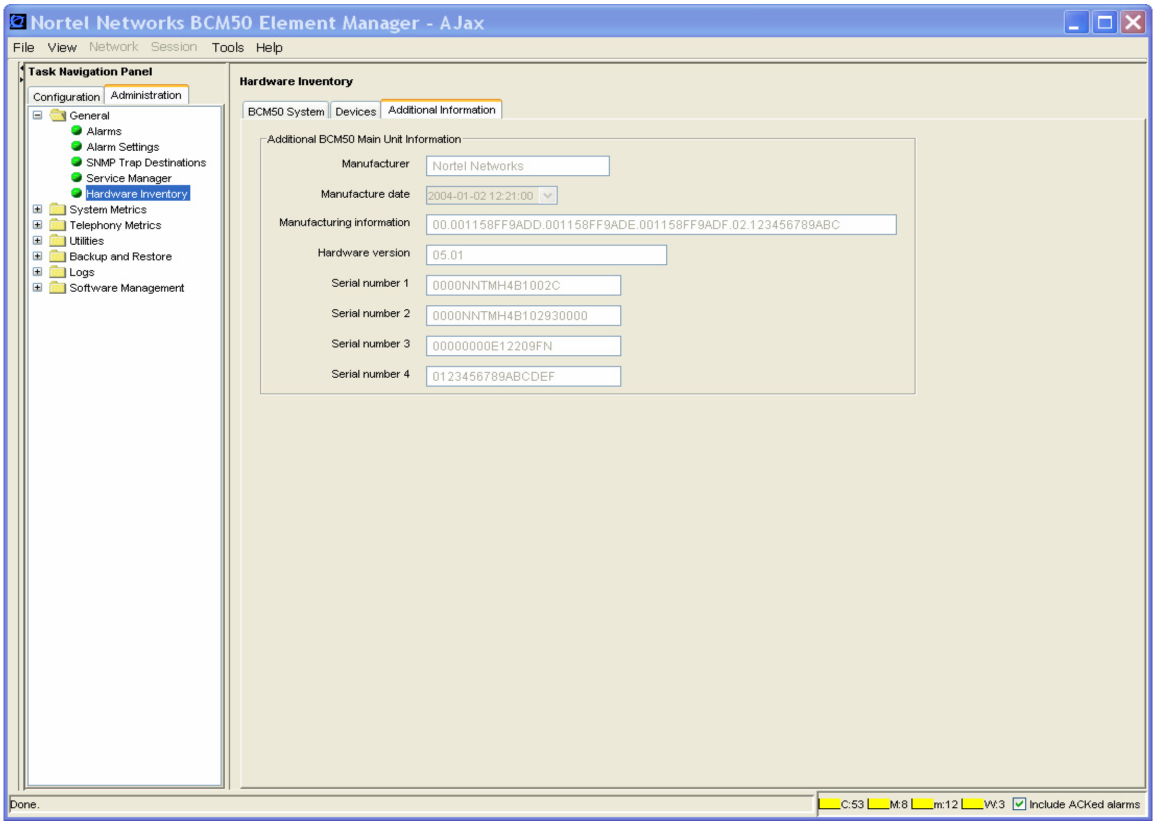
Table 32 lists the fields displayed in the Additional Information tab.

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

Table 32 Additional BCM50 main unit Information fields

Field Name	**Read/Write**
Manufacturer*	Read
Manufacture date	Read
Manufacturing information	Read
Hardware version*	Read
Serial number 1	Read
Serial number 2	Read
Serial number 3	Read
Serial number 4	Read

Figure 34 Hardware Inventory Additional Information tab



Additional BCM50 Main Unit Information

Manufacturer	Nortel Networks
Manufacture date	2004-01-02 12:21:00
Manufacturing information	00.001158FF9ADD.001158FF9ADE.001158FF9ADF.02.123456789ABC
Hardware version	05.01
Serial number 1	0000NNTMH4B1002C
Serial number 2	0000NNTMH4B102930000
Serial number 3	00000000E12209FN
Serial number 4	0123456789ABCDEF

To view additional information about the BCM50 main unit

1. In the BCM50 Element Manager, connect to a BCM50 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 BCM50 main unit Information** area.

Chapter 6
Managing BCM50 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. The BCM50 main unit has an SNMP agent, as does the optional integrated router.

You can use external clients, such as HP OpenView, to monitor the BCM50 system by means of read-only SNMP requests.

This chapter provides information about:

- BCM50 support for SNMP
- configuring the router to enable SNMP management
- configuring BCM50 SNMP settings
- using SNMP to send traps

Overview of BCM50 support for SNMP

This chapter provides information about SNMP support provided by the BCM50 main unit.

➡ **Note:** The optional integrated router supports MIB II as defined in RFC-1213 and RFC-1215. For information about using SNMP with the router, see the *BCM50a Integrated Router Configuration Guide* or the *BCM50e Integrated Router Configuration Guide*.

The BCM50 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 BCM50 Element Manager, you can select which versions of SNMP you want the BCM50 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. BCM50 supports the following MIBs:

- RFC-1213 — MIB II
- RFC 2863 — Interface MIB
- RFC 2737 — Entity MIB
- RFC 2790 — Host MIB
- SmallSiteEvent MIB for traps

For information about supported MIBs, how to install MIBs, and how to view SNMP traps, see "Management Information Bases" on page 361.

BCM50 supports read-only SNMP requests, even for SNMP variables that display as read-write; BCM50 does not support configuration operations through SNMP. Variables that are not supported are displayed as "0".

Configuring routers to use Element Manager with SNMP

Before you use the BCM50 for SNMP management, you must ensure that the BCM50 and the optional integrated router are configured to allow SNMP queries to be received and responded to. You will need to correctly configure NAT and Firewall settings for the router. For information on using the router web-based interface to modify these settings, see the *BCM50 Installation Guid*e and the *BCM50 Networking Guide*. The sections below provide an overview of configuring the router to enable SNMP management.

Connecting through the WAN

In this scenario, the LAN is configured as a private network with no public access. Before beginning configuration, ensure that both the BCM50 and the SNMP Management Station are working correctly. If you are using the BCM50a or BCM50e, only SNMPv1 is supported. If you are using an external router, you can those versions of SNMP supported by that router. To enable SNMP, you must configure firewall settings, add NAT rules, and configure the SNMP port.

Configuring firewall settings

If the firewall is enabled on the router, several rules must be added so that the SNMP Management Station and the BCM50 can communicate. If you are using a BCM50a or BCM50e, these settings are configured in the Router manager. The first rule allows WAN to WAN communication:

- Source address: Management station's IP Address, or "any"
- Destination address: Router's WAN IP Address
- Service Type: SNMP (TCP/UDP: 163)
- Action: forward

The second rule allow WAN to LAN communication:

- Source address: Management station's IP Address, or "any"
- Destination address: BCM50 LAN IP Address. This is the IP Address listed in Element Manager under System/IP Subsystem/General Settings.
- Service Type: SNMP (TCP/UDP: 161)
- Action: forward

Adding NAT rules

In the NAT section of the router configuration, create a rule with the following settings:

- Start port: 161
- End port: 161
- Server IP address: The BCM50 LAN IP address.

This rule means that all TCP/IP traffic to port 161, which is the BCM50's SNMP agent port, will be forwarded to the BCM50 for processing.

Configuring the SNMP router port

By default, both the BCM50 and the BCM50 router attempt to use port 161 for SNMP. This causes a conflict. In the router configuration, access the Remote Management section, and the SNMP tab to change this.

Change the communities to *public*, and set the SNMP Service Port to163. If the trap needs to be enabled, set it to the SNMP management station IP address. Otherwise, set it to *public*.

The SNMP management station can now connect to the BCM50 LAN through port 161 and to the router through port 163.

Connecting through the LAN

An SNMP management station that is configured on the LAN can access the BCM50 and Router SNMP directly by using the LAN addresses of the BCM50 and BCM50 router.

An SNMP management station that is connected to the OAM LAN cannot access the router SNMP, as there is no relay on the BCM50.

Configuring SNMP settings

You can use the BCM50 Element Manager to configure the BCM50 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 66.

To configure the SNMP agent on the router, see the *BCM50 Integrated Router Configuration Guide*.

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 BCM50 system by specifying their IP addresses. If you have specified SNMP managers, the BCM50 SNMP agent will respond only to SNMP requests from those IP devices.

To configure the BCM50 SNMP agent

1. Start the BCM50 Element Manager.
2. In the **Network Element** navigation panel, select a BCM50 element.
3. Log on to the BCM50 by clicking the **Connect** button.
4. When the BCM50 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 33 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 BCM50 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 34 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 BCM50 can interact with any SNMP agent manager.

6 Click the **OK** button.

Adding an SNMP manager to the BCM50 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 BCM50 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 35 SNMP Manager Attributes

Attribute	Action
Manager IP Address	Enter the IP address of the SNMP manager that you want to authorize to query the BCM50 system. The IP address must correspond to the PC where the trap collector software is installed. Do not use the dynamic IP address that the PC receives when the dial-up link activates (when the BCM50 initiates dialing). Using the dynamic IP address causes the removal of the required static route. The format for the IP address is X.X.X.X:P, where P is the port. Setting the IP address to 0.0.0.0 authorizes all SNMP managers to query the system.

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 BCM50 responds with the requested information. If the community string is incorrect, the BCM50 discards the request and does not respond.

Community strings are used for SNMP v1 and v2C only.

BCM50 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 36 SNMP Community String Attributes

Attribute	Action
Community String	Enter the entry name used as 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 37 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 hexidecimal 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 38 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 39 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 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 BCM50 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 154.

BCM50 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 BCM50 if you have enabled SNMP for specific BCM50 alarms. You configure SNMP settings using the Alarm Settings task in the BCM50 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 "Administering SNMP trap destinations".

➡ **Note:** You can configure and administer SNMP trap destinations in both the Configuration tab and the Administration tab of the BCM50 Element Manager. This allows operators who manage BCM50 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 40 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.

Administering 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 BCM50 Element Manager. This allows operators who manage BCM50 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 41 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 a modem to deliver alarms to a specified destination.

You can access the auto-SNMP dial-out on the Modem panel under the Dial-out tab.

To configure auto-SNMP dialout

1. Click the **Configuration** tab.
2. Open the **Administrator Access** folder, and then click **Modem**.
3. Click the **Dial-out Parameters** tab.
   The **Dial-out Parameters** panel is displayed.
4. In the **Dial-out Number** field, enter a phone number for the modem to use.
5. In the **Dial-out Routes** area, click the **Add** button and enter a route and subnet mask..
6. In the **Static IP Address Pool** area, enter a static IP address.
7. Select the **SNMP** page and select the **SNMP Trap Destination** tab.
8. Click the **Add** button and enter a destination IP address for the alarms to be delivered to.
9. Click **OK**.

Note: If the line is busy or if the modem cannot connect for any reason, the alarm will not be delivered to the destination. If you are using SNMP v3, the modem will re-attempt the connection three times.

Alarm severity levels

The terminology used for alarm severity levels in the Alarms panel and in SNMP traps is not the same. Table 42 lists Alarms panel terminology and the equivalent SNMP trap type.

Table 42 Terminology used for alarm severity levels

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

While the BCM50 fault management system denotes the source of a BCM50 alarm as “ComponentID”, the SNMP system denotes the sources of this information as a trap of source “eventSource”.

Chapter 7
Using the BCM50 Fault Management System

This chapter contains information about managing alarms generated by the BCM50 system and administering alarm settings.

The chapter provides information about the following:

- an overview of BCM50 fault management tools
- an overview of BCM50 alarms
- alarms and log files
- administering alarms
- configuring alarm settings
- BCM50 alarm list
- alarm severities

Overview of BCM50 fault management

This chapter provides information about managing faults for the BCM50; faults generated by the optional router are not covered.

For information about traps and events generated by the optional integrated router, see cthe *BCM50a/e Integrated Router Configuration Guide*.

You can view and manage real-time alarms generated by the BCM50 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 BCM50 has been stopped by an administrator

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

- the Alarms Panel in the BCM50 Element Manager
- the Alarm Banner in the BCM50 Element Manager
- all alarms shown on the alarm set
- Simple Network Management Protocol (SNMP) traps for remote management of faults
- LEDs on the BCM50 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 BCM50 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 selected alarms using the programming record. For information about using the programming record, see "Saving programming records" on page 66.

About BCM50 alarms

Alarms are generated by software components that are running on the BCM50 system, and cover BCM50 services and applications.

Each component has a range of alarm IDs, so that each BCM50 alarm has a unique alarm ID. Table 43 lists the components and the alarm ID ranges.

Table 43 BCM50 components and Alarm ID ranges

BCM50 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
Unistim Terminal Proxy Server	50000—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

Alarms and log files

All alarms that appear in the BCM50 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 BCM50 keeps the current file as well as three previous files. The file is also capped and a new file is started when the BCM50 system is rebooted.

You can retrieve the alarms.systemlog files (the current file plus the three previous files) from the BCM50 system using the Log Management task in the BCM50 Element Manager. You can view the files using the BCM50 Log Browser. For more information, see “Managing BCM50 Logs,” on page 315.

Alarm severities

Alarm severities are as follows:

Table 44 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 BCM50 sends SNMP traps and alerts the alarm set for alarms with a severity of Major and Critical.

Table 45 provides the default mapping of each severity level against the Alarms Panel, alarms set, LEDs, and SNMP.

Table 45 Default mapping of severity levels

Alarm Severity	Alarms Panel	Alarm Set	LEDs	SNMP
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 BCM50 Element Manager
- the Alarm Banner in the BCM50 Element Manager
- the alarm set
- Simple Network Management Protocol (SNMP) traps for remote management of faults
- LEDs on the BCM50 main unit

Using the Alarms Panel

You can view real-time alarm information using the Alarms Panel in the BCM50 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 BCM50 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 156.

To view an alarm

When you view an alarm in the Alarm table, 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.

Clearing the alarm log

Caution: Clearing the alarm log clears the alarms in the Alarms Panel, as well as from BCM50 memory. Therefore, alarms will no longer be available for viewing by any other BCM50 Element Manager clients connected to the BCM50. To view alarms, access the Alarm log.

To clear the alarm log

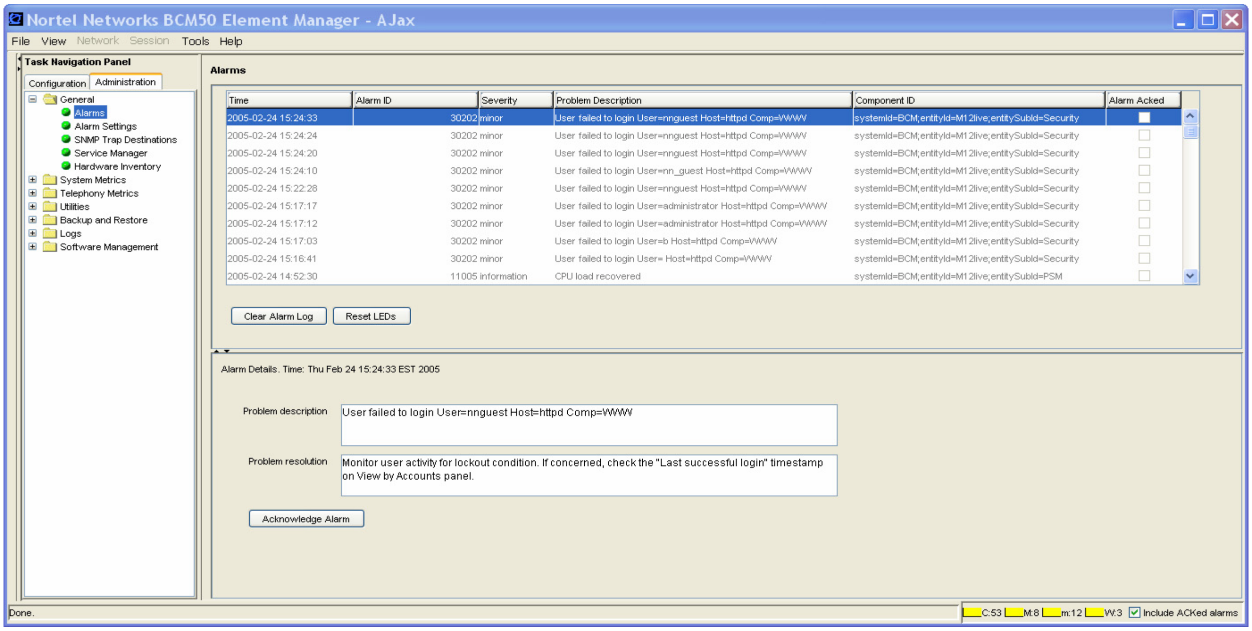
1 Click the **Administration** tab.

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 BCM50 Element Manager to view current alarm counts and recent alarm activity on the BCM50 system. The Alarm Banner appears on the bottom-right corner of the BCM50 Element Manager window. The Alarm Banner is visible at all times, so you do nothave 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.



Alarms

Time	Alarm ID	Severity	Problem Description	Component ID	Alarm Acked
2005-02-24 15:24:33	30202	minor	User failed to login User=nnguest Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:24:24	30202	minor	User failed to login User=nnguest Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:24:20	30202	minor	User failed to login User=nnguest Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:24:10	30202	minor	User failed to login User=nn_guest Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:22:28	30202	minor	User failed to login User=nnguest Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:17:17	30202	minor	User failed to login User=administrator Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:17:12	30202	minor	User failed to login User=administrator Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:17:03	30202	minor	User failed to login User=b Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 15:16:41	30202	minor	User failed to login User= Host=httpd Comp=WWW	systemId=BCM;entityId=M12live;entitySubId=Security	□
2005-02-24 14:52:30	11005	information	CPU load recovered	systemId=BCM;entityId=M12live;entitySubId=PSM	□

Alarm Details. Time: Thu Feb 24 15:24:33 EST 2005

Problem description: User failed to login User=nnguest Host=httpd Comp=WWW

Problem resolution: Monitor user activity for lockout condition. If concerned, check the "Last successful login" timestamp on View by Accounts panel.

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 46 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.

Table 46 Alarm graph colors

Color	Indicates
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 BCM50 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 alarms on a telephone set on the BCM50 system. This allows a system administrator to monitor alarm activity without having a BCM50 Element Manager and a personal computer. The alarm set shows alarms with a severity level of Critical and Major.

If an alarm is displayed on the alarm set, it remains visible until you clear the alarm using a softkey on the alarm set. More recent alarms will not be displayed until the current alarm is cleared on the alarm set.

You can specify the telephone to serve as the alarm set in the BCM50 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 blank for all alarms except Core Telephony.

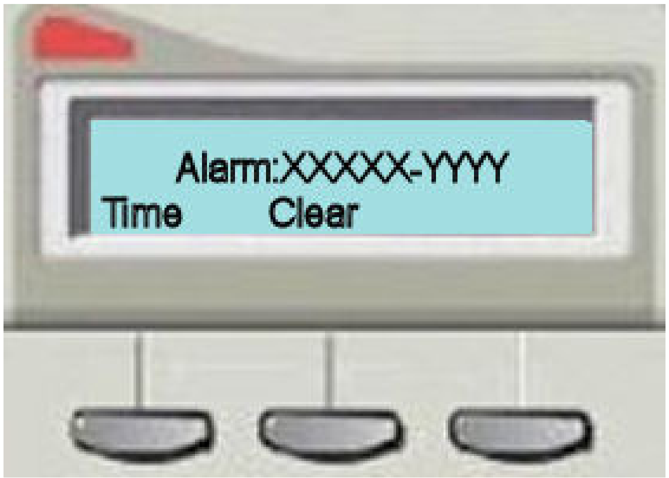
The following options are available when an alarm is generated to the alarm set:

- 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 BCM50 Element Manager or reset the LEDs on the front panel of the unit.

Figure 35 shows an example of an alarm on the alarm set.

Figure 35 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 BCM50 Element Manager or reset the LEDs on the front panel of the unit.

➡ **Note:** If an alarm is displayed on the alarm set, it remains visible until you clear the alarm using a softkey on the alarm set. More recent alarms will not be displayed until the current alarm is cleared on the alarm set.

Alarms and LEDs

When an alarm condition occurs on the system, the Status LED on the front of the BCM50 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 BCM50 front panel, except in the event of a Failed Startup Profile, which is indicated by a flashing red LED. The Status LED is the top LED.

Using the BCM50 Element Manager, you can reset the Status LEDs on the front panel of the BCM50 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 BCM50 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 BCM50 is reset from red to normal operation green.

Using SNMP traps

You can use an SNMP trap manager to remotely monitor BCM50 alarms via SNMP traps. A trap is an indication from the BCM50 system to configured trap managers that an alarm has occurred in the BCM50 system. Any BCM50 alarm can generate an SNMP trap but by default, only critical and major alarms generate an SNMP trap.

If you want the BCM50 to send SNMP traps, you must first configure the SNMP agent using the BCM50 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 139.

The BCM50 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 361.

By default, the BCM50 sends SNMP traps for alarms with a severity of Major and Critical. 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 160.

Configuring alarm settings

Although the BCM50 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, call Critical and Major alarms are sent to this set

You can also test a selected alarm. This allows you to test whether the alarm set, 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 BCM50 system, see “Managing BCM50 with SNMP,” on page 139.

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 enable or disable alarm set for selected 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 Alarm Set** column, select or clear the check box to enable or disable the alarm from being sent to the alarm set. If you clear the check box for a selected alarm, the alarm will not be displayed on the alarms set 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.

List of BCM50 alarms

Table 47 lists BCM50 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 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	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 unit connections. If problem persists replace the DTM or expansion unit 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
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 unit 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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
7	36	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failure.	Power down the system and check the expansion unit 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
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. Ask your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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. Ask 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. Ask your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
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. Ask 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. Ask your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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. Ask 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. Ask your network provider to check the circuit during problem conditions.	Yes	Yes	Yes	Yes
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 unit 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 unit containing the digital or analog trunk module. If the problem persists, replace the module.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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 unit 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 unit.	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
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
26	67	critical	Core Telephony	Core Telephony - Invalid trunk media bay module connected to an expansion unit.	Power down the system and check all connections to the expansion unit 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
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
33	79	critical	Core Telephony	Core Telephony - ASM firmware download error.	Power down the system and check the ASM hardware and the expansion unit connections. If problem persists replace the ASM or expansion unit 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
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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
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

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
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	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
57	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
58	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
59	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
60	799	minor	Core Telephony	Core Telephony - ISDN call processing error.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
61	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 unit and try to get the circuit back online. If problem persists contact your local support group.	Yes	No	No	No
62	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
63	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
64	999	warning	Core Telephony	Core Telephony - Unknown alarm.	Contact your local support group.	Yes	No	No	No
65	1001	major	Operating System	Operating System - Major operating system error (Kernel Oops).	Contact your local support group.	Yes	Yes	Yes	Yes
66	1002	critical	Operating System	Operating System - Critical operating system error (Kernel panic).	Contact your local support group.	Yes	Yes	Yes	Yes
67	2100	information	Software Updates	Software Update - Software update applied successfully.	No Action Required.	Yes	No	No	No
68	2101	information	Software Updates	Software Update - Software upgrade applied successfully.	No Action Required.	Yes	No	No	No
69	2102	information	Software Updates	Software Update - Software update started.	No Action Required.	Yes	No	No	No
70	2103	information	Software Updates	Software Update - Software upgrade started.	No Action Required.	Yes	No	No	No
71	2104	information	Software Updates	Software Update - Software update scheduled.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
72	2105	information	Software Updates	Software Update - Scheduled software update completed.	No Action Required.	Yes	No	No	No
73	2106	information	Software Updates	Software Update - Software update removed.	No Action Required.	Yes	No	No	No
74	2300	critical	Software Updates	Software Update - Software update failed to apply.	Contact your local support group.	Yes	Yes	Yes	Yes
75	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	Yes
76	2302	critical	Software Updates	Software Update - Software upgrade	Contact your local support group.	Yes	Yes	Yes	Yes
77	2303	major	Software Updates	Software Update - Failed to remove software update.	Retry removal of software update and if problem	Yes	Yes	Yes	Yes
78	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	Yes
79	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	Yes
80	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
81	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	Yes
82	6000	minor	Date and Time	Date and Time - Time has been updated by CoreTel.	No Action Required.	Yes	No	No	No
83	6003	minor	Date and Time	Date and Time - Time service syncing hardware clock.	No Action Required.	Yes	No	No	No
84	6004	critical	Date and Time	Date and Time - Time service initialization failed.	Contact your local support group.	Yes	Yes	Yes	Yes
85	6007	minor	Date and Time	Date and Time - The NTP server changed the time to a value larger than the configured alarm condition in Element manager.	Confrim the date/ time is correct on the system.	Yes	No	No	No
86	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	No
87	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	Yes
88	8001	critical	Modem Call Control	Modem Call Control - MCC Stopped Unexpectedly. Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
89	8002	critical	Modem Call Control	Modem Call Control - MCC Failed to Register with Voice CTI. CTI Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
90	8003	Warning	Modem Call Control	Modem Call Control - MCC Modem DSP Task Cannot be Loaded. Disabling the Modem. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
91	8004	critical	Modem Call Control	Modem Call Control - MCC Failed to Start an Emulator for the Modem. Voice CTI Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
92	8005	critical	Modem Call Control	Modem Call Control - MCC Failed to Get a Modem DN. Voice CTI Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
93	8008	critical	Modem Call Control	Modem Call Control - MCC Failed to Create a State Machine to Receive Call Progress Information. OSA Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
94	8009	critical	Modem Call Control	Modem Call Control - MCC Failed to Create the Internal State Machine Queue. OSA Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
95	8010	critical	Modem Call Control	Modem Call Control - MCC Failed to Read the Internal State Machine Queue. OSA Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
96	8011	critical	Modem Call Control	Modem Call Control - MCC Failed to Send to the Internal State Machine Queue. OSA Return Code = %ld.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
97	8012	Warning	Modem Call Control	Modem Call Control - MCC Failed to Transfer the call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
98	8013	Warning	Modem Call Control	Modem Call Control - MCC Cannot Monitor Incoming Line. CTI Return Code = %ld.	Reboot system and contact your local support group.	Yes	No	No	No
99	8014	Warning	Modem Call Control	Modem Call Control - MCC Can only Transfer to Modem DN Manually. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
100	8015	Warning	Modem Call Control	Modem Call Control - MCC Cannot Stop to Monitor the Line Number. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
101	8016	Warning	Modem Call Control	Modem Call Control - MCC Cannot Unload the Modem DSP Task. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
102	8017	Warning	Modem Call Control	Modem Call Control - MCC Failed to Answer Incoming Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
103	8018	information	Modem Call Control	Modem Call Control - MCC Incoming Call on Busy Modem [%s].	No Action Required.	Yes	No	No	No
104	8019	information	Modem Call Control	Modem Call Control - MCC Attempt to Connect to a Disabled Modem [%s].	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
105	8020	Warning	Modem Call Control	Modem Call Control - MCC Failed to Register for CLID/ANI Service. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
106	8021	information	Modem Call Control	Modem Call Control - MCC Modem Connected [%s].	No Action Required.	Yes	No	No	No
107	8022	information	Modem Call Control	Modem Call Control - MCC Modem is Disconnected.	No Action Required.	Yes	No	No	No
108	8023	information	Modem Call Control	Modem Call Control - MCC Modem Enabled.	No Action Required.	Yes	No	No	No
109	8024	information	Modem Call Control	Modem Call Control - MCC Modem Disabled.	No Action Required.	Yes	No	No	No
110	8025	Warning	Modem Call Control	Modem Call Control - MCC Failed to Get Switch Information. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
111	8029	Warning	Modem Call Control	Modem Call Control - MCC Failed to Answer Modem Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
112	8030	Warning	Modem Call Control	Modem Call Control - MCC Failed to Acknowledge Modem Request. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
113	8031	Warning	Modem Call Control	Modem Call Control - MCC Failed to Originate a Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No
114	8032	Warning	Modem Call Control	Modem Call Control - MCC Failed to Disconnect a Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
115	8033	Warning	Modem Call Control	Modem Call Control - MCC Received Unknown Request from Modem. Request = %ld.	Contact your local support group.	Yes	No	No	No
116	8035	information	Modem Call Control	Modem Call Control - MCC Modem Auto Disabled.	No Action Required.	Yes	No	No	No
117	8038	information	Modem Call Control	Modem Call Control - MCC Modem Call Put on Hold. Disconnecting…	No Action Required.	Yes	No	No	No
118	8040	Warning	Modem Call Control	Modem Call Control - MCC Failed to Open Prompts Library. NNU Return Code = %ld.	Contact your local support group.	Yes	No	No	No
119	8041	information	Modem Call Control	Modem Call Control - MCC Modem DN changed in admin.	No Action Required.	Yes	No	No	No
120	8042	Warning	Modem Call Control	Modem Call Control - MCC Failed to Open the Communication Path to RAS. Disabling the Modem.	Contact your local support group.	Yes	No	No	No
121	10001	critical	Service Manager	Core Telephony has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10101 or 10301. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	Yes
122	10002	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
123	10003	critical	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	Yes
124	10004	critical	Service Manager	Hot Desking for IP Terminals (HotDesking) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10104 or 10304. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	Yes
125	10005	critical	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	Yes
126	10006	critical	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	Yes
127	10007	critical	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	Yes
128	10008	critical	Service Manager	Voice Application Interface Service (ctiserver) has stopped unexpectedly. This will affect CallPilot, System Set Based Admin and the modem. 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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
129	10009	critical	Service Manager	Modem Call Control (modemcc) has stopped unexpectedly. This will affect Dial-In and Dial-Out using the integrated modem. Service Manager is attempting to restart the service.	Check for corresponding alarm 10109 or 10309. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	Yes
130	10010	critical	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	Yes
131	10011	critical	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	Yes
132	10012	critical	Service Manager	Line Monitor Service (lms) has stopped unexpectedly. This will affect the Line 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	Yes
133	10013	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
134	10014	critical	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	Yes
135	10015	critical	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	Yes
136	10016	critical	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	Yes
137	10017	critical	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	Yes
138	10018	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
139	10019	critical	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	Yes
140	10020	critical	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	Yes
141	10021	critical	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	Yes
142	10101	critical	Service Manager	Core Telephony has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
143	10102	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
144	10103	critical	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	Yes
145	10104	critical	Service Manager	Hot Desking for IP Terminals (HotDesking) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
146	10105	critical	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	Yes
147	10106	critical	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	Yes
148	10107	critical	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	Yes
149	10108	critical	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 the modem.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
150	10109	critical	Service Manager	Modem Call Control (modemcc) has stopped unexpectedly and could not be restarted by service manager. This will affect Dial-In and Dial-Out using the integrated modem.	Reboot system and contact your local support group.	Yes	Yes	Yes	Yes
151	10110	critical	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	Yes
152	10111	critical	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	Yes
153	10112	critical	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	Yes
154	10113	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
155	10114	critical	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	Yes
156	10115	critical	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	Yes
157	10116	critical	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	Yes
158	10117	critical	Service Manager	Keycode Service (cfsserver) 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	Yes
159	10118	critical	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
160	10119	critical	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	Yes
161	10120	critical	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	Yes
162	10121	critical	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	Yes
163	10122	critical	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	Yes
164	10200	critical	Service Manager	Service Manager - (service name) stopped unexpectedly, restarting (service name) tree	Check for corresponding alarm 101XX or 103XX. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
165	10201	Warning	Service Manager	Core Telephony 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	No
166	10202	Warning	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	No
167	10203	Warning	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	No
168	10204	Warning	Service Manager	Hot Desking for IP Terminals (HotDesking) 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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
169	10205	Warning	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	No
170	10206	Warning	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	No
171	10207	Warning	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	No
172	10208	Warning	Service Manager	Voice Application Interface Service (ctiserver) 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 CallPilot, System Set Based Admin and the modem.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
173	10209	Warning	Service Manager	Modem Call Control (modemcc) 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 Dial-In and Dial-Out using the integrated modem.	No Action Required.	Yes	No	No	No
174	10210	Warning	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	No
175	10211	Warning	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
176	10212	Warning	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	No
177	10213	Warning	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	No
178	10214	Warning	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
179	10215	Warning	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	No
180	10216	Warning	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	No
181	10217	Warning	Service Manager	Keycode Service (cfsserver) 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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
182	10218	Warning	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	No
183	10219	Warning	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	No
184	10220	Warning	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
185	10221	Warning	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	No
186	10300	Information	Service Manager	Service Manager - (service name) started succesfully.	No Action Required.	Yes	No	No	No
187	10301	Information	Service Manager	Core Telephony has been successfully restarted.	No Action Required.	Yes	No	No	No
188	10302	Information	Service Manager	CallPilot has been successfully restarted.	No Action Required.	Yes	No	No	No
189	10303	Information	Service Manager	IP Terminal Service (UTPS) has been successfully restarted.	No Action Required.	Yes	No	No	No
190	10304	Information	Service Manager	Hot Desking for IP Terminals (HotDesking) has been successfully restarted.	No Action Required.	Yes	No	No	No
191	10305	Information	Service Manager	Voice over IP Gateway (feps) has been successfully restarted.	No Action Required.	Yes	No	No	No
192	10306	Information	Service Manager	Quality of Service Monitor (qmond) has been successfully restarted.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
193	10307	Information	Service Manager	Call Detail Recording Service (CDRService) has been successfully restarted.	No Action Required.	Yes	No	No	No
194	10308	Information	Service Manager	Voice Application Interface Service (ctiserver) has been successfully restarted.	No Action Required.	Yes	No	No	No
195	10309	Information	Service Manager	Modem Call Control (modemcc) has been successfully restarted.	No Action Required.	Yes	No	No	No
196	10310	Information	Service Manager	System Set Based Admin Feature9*8 (ssba) has been successfully restarted.	No Action Required.	Yes	No	No	No
197	10311	Information	Service Manager	Computer Telephony Service (Cte) has been successfully restarted.	No Action Required.	Yes	No	No	No
198	10312	Information	Service Manager	Line Monitor Service (lms) has been successfully restarted.	No Action Required.	Yes	No	No	No
199	10313	Information	Service Manager	Media Services Manager (Msm) has been successfully restarted.	No Action Required.	Yes	No	No	No
200	10314	Information	Service Manager	Media Path Server (mps) has been successfully restarted.	No Action Required.	Yes	No	No	No
201	10315	Information	Service Manager	Media Gateway Server (mgs) has been successfully restarted.	No Action Required.	Yes	No	No	No
202	10316	Information	Service Manager	Persistent Data Repository (Pdrd) has been successfully restarted.	No Action Required.	Yes	No	No	No
203	10317	Information	Service Manager	Keycode Service (cfsserver) has been successfully restarted.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
204	10318	Information	Service Manager	Time Service (tmwservice) has been successfully restarted.	No Action Required.	Yes	No	No	No
205	10319	Information	Service Manager	Platform Status Monitor (psm) has been successfully restarted.	No Action Required.	Yes	No	No	No
206	10320	Information	Service Manager	Web Server (httpd) has been successfully restarted.	No Action Required.	Yes	No	No	No
207	10321	Information	Service Manager	On Box Management Framework (owcimomd) has been successfully restarted.	No Action Required.	Yes	No	No	No
208	10322	Information	Service Manager	Service Manager (monit) has been successfully restarted.	No Action Required.	Yes	No	No	No
209	10906	Information	Startup Sequence	System Startup - Operating system and alarm subsystem available. Power LED = flashing green; Status LED = flashing yellow.	No Action Required.	Yes	No	No	No
210	10907	Information	Startup Sequence	System Startup - Telephony and Voicemail active. Power LED = flashing green; Status LED = flashing green	No Action Required.	Yes	No	No	No
211	10908	Information	Startup Sequence	System Startup - Element Manager is available. Power LED = solid green; Status LED = flashing green	No Action Required.	Yes	No	No	No
212	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
213	11002	Information	Platform Status Monitor	Platform Status Monitor - Power Recovered.	No Action Required. Recovery alarm for corresponding alarms 11200 and 11400.	Yes	No	No	No
214	11003	Information	Platform Status Monitor	Platform Status Monitor - Hard drive space recovered	No Action Required. Recovery alarm for corresponding alarms 11201.	Yes	No	No	No
215	11004	Information	Platform Status Monitor	Platform Status Monitor - Memory recovered	No Action Required. Recovery alarm for corresponding alarm 11202	Yes	No	No	No
216	11005	Information	Platform Status Monitor	Platform Status Monitor - CPU load Recovered.	No Action Required. Recovery alarm for corresponding alarm 11203.	Yes	No	No	No
217	11006	Information	Platform Status Monitor	Platform Status Monitor - LAN Recovered.	No Action Required. Recovery alarm for corresponding alarm 11204.	Yes	No	No	No
218	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	No
219	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	No
220	11014	Information	Platform Status Monitor	Platform Status Monitor - Fan recovered.	No Action Required. Recovery alarm for corresponding alarms 11212 and 11408.	Yes	No	No	No
221	11015	Information	Platform Status Monitor	Platform Status Monitor - Router Recovered.	No Action Required. Recovery alarm for corresponding alarm 11409.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
222	11016	Information	Platform Status Monitor	Platform Status Monitor - OAM Port Link Up	No Action Required. Recovery alarm for corresponding alarm 11214.	Yes	No	No	No
223	11017	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 1 Link Up	No Action Required. Recovery alarm for corresponding alarm 11215.	Yes	No	No	No
224	11018	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 2 Link Up	No Action Required. Recovery alarm for corresponding alarm 11216.	Yes	No	No	No
225	11019	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 3 Link Up	No Action Required. Recovery alarm for corresponding alarm 11217.	Yes	No	No	No
226	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	No
227	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	Yes
228	11202	major	Platform Status Monitor	Platform Status Monitor - Memory near capacity	Contact local support group for assistance in analyzing memory usage.	Yes	Yes	Yes	Yes
229	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
230	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	Yes
231	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	Yes
232	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	Yes
233	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	Yes
234	11213	major	Platform Status Monitor	Platform Status Monitor - Failed to get Router status.	Check the router and if needed replace it.	Yes	Yes	Yes	Yes
235	11214	warning	Platform Status Monitor	Platform Status Monitor - OAM Port Link Down	Check the OAM Port physical LAN connection	Yes	No	No	No
236	11215	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 1 Link Down	Check the Customer LAN Port 1 physical LAN connection	Yes	No	No	No
237	11216	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 2 Link Down	Check the Customer LAN Port 2 physical LAN connection	Yes	No	No	No
238	11217	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 3 Link Down	Check the Customer LAN Port 3 physical LAN connection	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
239	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	Yes
240	11400	critical	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	Yes
241	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	Yes
242	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	Yes
243	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	Yes
244	11409	critical	Platform Status Monitor	Platform Status Monitor - Router does not Exist.	Check Router operation as it is apparently malfunctioning. If alarm persists, replace router.	Yes	Yes	Yes	Yes
245	12001	major	Backup and Restore	Backup and Restore - Backup file could no be renamed.	Contact your local support group.	Yes	Yes	Yes	Yes
246	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
247	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	Yes
248	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	Yes
249	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	Yes
250	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	Yes
251	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	Yes
252	12008	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Try a different backup file.	Yes	No	No	No
253	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	Yes
254	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	No
255	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	No
256	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
257	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	Yes
258	12014	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes	Yes
259	12015	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes	Yes
260	12016	warning	Backup and Restore	Backup and Restore - Backup is busy serving another request.	No Action Required.	Yes	No	No	No
261	12017	warning	Backup and Restore	Backup and Restore - File integrity error. Contents altered since creation.	Use a different backup file	Yes	No	No	No
262	12018	major	Backup and Restore	Backup and Restore - Internal error. Database could not be backed-up.	Attempt another backup and if problem perists contact your local support group	Yes	Yes	Yes	Yes
263	12019	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No	No
264	12020	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No	No
265	12021	major	Backup and Restore	Backup and Restore - Internal error. Could not shadow data.	Attempt another backup and if problem perists contact your local support group	Yes	Yes	Yes	Yes
266	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	Yes
267	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
268	12024	major	Backup and Restore	Backup and Restore - Internal error. Compression incorrectly specified in configuration file.	Attempt another backup and if problem perists contact your local support group	Yes	Yes	Yes	Yes
269	12025	major	Backup and Restore	Backup and Restore - Internal error. Component in configuration file not recognized.	Attempt another backup and if problem perists contact your local support group	Yes	Yes	Yes	Yes
270	12026	major	Backup and Restore	Backup and Restore - Internal error. Unrecognized transfer mechanism.	Attempt another backup and if problem perists contact your local support group	Yes	Yes	Yes	Yes
271	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	Yes
272	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	No
273	12029	major	Backup and Restore	Backup and Restore - Internal error. Could not restore the database.	Attempt another restore and if problem perists contact your local support group	Yes	Yes	Yes	Yes
274	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	No
275	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	No
276	12032	major	Backup and Restore	Backup and Restore - Could not use the USB device.	Check the USB connection and flash device	Yes	Yes	Yes	Yes
277	12033	minor	Backup and Restore	Backup and Restore - Could not detach the USB device.	Check the USB connection and flash device	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
278	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	No
279	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	No
280	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	No
281	12037	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem perists contact your local support group	Yes	No	No	No
282	12038	minor	Backup and Restore	Backup and Restore - A backup file does not exist.	Attempt another backup or restore and if problem perists contact your local support group	Yes	No	No	No
283	12041	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem perists contact your local support group	Yes	No	No	No
284	12202	Information	Backup and Restore	Backup and Restore - Onbox Backup/Log collection has completed.	No Action Required.	Yes	No	No	No
285	12203	Information	Backup and Restore	Backup and Restore - Backup/ Log files have been successfully transferred off box.	No Action Required.	Yes	No	No	No
286	12204	Information	Backup and Restore	Backup and Restore - Restore has started.	No Action Required.	Yes	No	No	No
287	12205	Information	Backup and Restore	Backup and Restore - Restore has completed successfully.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
288	12206	Information	Backup and Restore	Backup and Restore - Restore has rebooted the system to complete its operation.	No Action Required.	Yes	No	No	No
289	13002	Information	UPS	UPS - Power failure.	Check local power connected to the system.	Yes	No	No	No
290	13003	Information	UPS	UPS - Running on UPS batteries.	Check local power connected to the system.	Yes	No	No	No
291	13004	warning	UPS	UPS - Battery power exhausted.	Check local power connected to the system.	Yes	No	No	No
292	13005	warning	UPS	UPS - Reached run time limit on batteries.	Check local power connected to the system.	Yes	No	No	No
293	13006	warning	UPS	UPS - Battery charge below low limit.	Check batteries in UPS and replace if needed.	Yes	No	No	No
294	13007	warning	UPS	UPS - Reached remaining time percentage limit on batteries.	No Action Required.	Yes	No	No	No
295	13008	warning	UPS	UPS - Failed to kill the power! Attempting a REBOOT!.	Check USB connection to UPS.	Yes	No	No	No
296	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	No
297	13010	Information	UPS	UPS - Power is back. UPS running on mains.	No Action Required.	Yes	No	No	No
298	13011	Information	UPS	UPS - Users requested to logoff.	No Action Required.	Yes	No	No	No
299	13012	major	UPS	UPS - Battery failure. Emergency.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes	Yes
300	13013	major	UPS	UPS - UPS battery must be replaced.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
301	13014	Information	UPS	UPS - Remote shutdown requested.	No Action Required.	Yes	No	No	No
302	13015	major	UPS	UPS - Communications with UPS lost.	Check USB connection to UPS.	Yes	Yes	Yes	Yes
303	13016	Information	UPS	UPS - Communications with UPS restored.	No Action Required.	Yes	No	No	No
304	13017	Information	UPS	UPS - Self Test switch to battery.	No Action Required.	Yes	No	No	No
305	13018	Information	UPS	UPS - Self Test completed.	No Action Required.	Yes	No	No	No
306	13019	warning	UPS	UPS - Master not responding.	No Action Required.	Yes	No	No	No
307	13020	Information	UPS	UPS - Connect from master.	No Action Required.	Yes	No	No	No
308	13021	Information	UPS	UPS - Mains returned. No longer on UPS batteries.	No Action Required.	Yes	No	No	No
309	16001	Information	Configuration Change	Configuration Change - Configuration Change has occurred.	No Action Required.	No	No	No	No
310	17002	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn=Y, login success.	No Action Required.	No	No	No	No
311	17003	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn Y logged off.	No Action Required.	No	No	No	No
312	17004	Information	System Set Based Admin	System Set Based Admin - UserId=X, user account created successfully, Dn=Y.	No Action Required.	Yes	No	No	No
313	17005	Information	System Set Based Admin	System Set Based Admin - UserId=X, user account deleted successfully, Dn=Y.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
314	17006	Information	System Set Based Admin	System Set Based Admin - UserId=X, password changed successfully, Dn=Y.	No Action Required.	Yes	No	No	No
315	17007	Information	System Set Based Admin	System Set Based Admin - DHCP client enabled for eth1.	No Action Required.	Yes	No	No	No
316	17008	Information	System Set Based Admin	System Set Based Admin - DHCP client disabled for eth1.	No Action Required.	Yes	No	No	No
317	17009	Information	System Set Based Admin	System Set Based Admin - IP=%s, ip address changed successfully.	No Action Required.	Yes	No	No	No
318	17010	Information	System Set Based Admin	System Set Based Admin - MASK=%s, subnet mask changed successfully.	No Action Required.	Yes	No	No	No
319	17011	Information	System Set Based Admin	System Set Based Admin - Gateway=X, ip gateway changed successfully.	No Action Required.	Yes	No	No	No
320	17012	Information	System Set Based Admin	System Set Based Admin - Keycode validated.	No Action Required.	Yes	No	No	No
321	17013	Information	System Set Based Admin	System Set Based Admin - Reboot required.	No Action Required.	Yes	No	No	No
322	17014	Information	System Set Based Admin	System Set Based Admin - Modem disabled.	No Action Required.	Yes	No	No	No
323	17015	Information	System Set Based Admin	System Set Based Admin - Modem enabled.	No Action Required.	Yes	No	No	No
324	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
325	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	No
326	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	No
327	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	No
328	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	No
329	17121	warning	System Set Based Admin	System Set Based Admin - Key code set failed	Log back into System Set based admin to verify keyccode. If problem persists contact your local support group.	Yes	No	No	No
330	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	No
331	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	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
332	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	No
333	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	No
334	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	No
335	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	Yes
336	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	Yes
337	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	No
338	30100	major	System Authentication	System Authentication - User Locked out.	Check user account for potential security issues.	Yes	Yes	Yes	Yes
339	30101	information	System Authentication	System Authentication - User Lockout ended.	No Action Required.	Yes	No	No	No
340	30200	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=Z	No Action Required.	No	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
341	30201	information	System Authentication	System Authentication - User logged out of SSBA.	No Action Required.	No	No	No	No
342	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	No
343	30203	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=WWW	No Action Required.	Yes	No	No	No
344	30300	information	System Authentication	System Authentication - Account created.	No Action Required.	Yes	No	No	No
345	30301	information	System Authentication	System Authentication - Account updated.	No Action Required.	Yes	No	No	No
346	30302	information	System Authentication	System Authentication - Account password changed.	No Action Required.	Yes	No	No	No
347	30303	information	System Authentication	System Authentication - Account enabled.	No Action Required.	Yes	No	No	No
348	30304	information	System Authentication	System Authentication - Account deleted.	No Action Required.	Yes	No	No	No
349	30400	information	System Authentication	System Authentication - Group Created.	No Action Required.	Yes	No	No	No
350	30401	information	System Authentication	System Authentication - Group member added.	No Action Required.	Yes	No	No	No
351	30402	information	System Authentication	System Authentication - Group member removed.	No Action Required.	Yes	No	No	No
352	30403	information	System Authentication	System Authentication - Group Deleted.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
353	30404	information	System Authentication	System Authentication - Group permissions modified.	No Action Required.	Yes	No	No	No
354	31006	critical	Keycodes	Keycodes - invalid license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
355	31007	critical	Keycodes	Keycodes - unknown license file status.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
356	31019	warning	Keycodes	Keycodes - failed to find component (<component handle>).	Ensure component is running properly and if problem perists contact your local support group.	Yes	No	No	No
357	31045	critical	Keycodes	Keycodes - failed to open file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
358	31052	critical	Keycodes	Keycodes - failed to open license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
359	31055	critical	Keycodes	Keycodes - failed to read system id.	Reboot the system and if problem persists contact your local support group.	Yes	Yes	Yes	Yes
360	31056	critical	Keycodes	Keycodes - cannot find system id tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
361	31057	critical	Keycodes	Keycodes - failed to read sequence number.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
362	31058	critical	Keycodes	Keycodes - cannot find sequence tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
363	31059	critical	Keycodes	Keycodes - failed to read key type.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
364	31060	critical	Keycodes	Keycodes - cannot find key type tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
365	31062	critical	Keycodes	Keycodes - failed to read key code <keycode size>.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes
366	31063	critical	Keycodes	Keycodes - failed to find key code.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
367	31067	critical	Keycodes	Keycodes - failed to find comp for feature (<feature code> <feature data>).	Ensure component is running properly and if problem persists contact your local support group.	Yes	Yes	Yes	Yes
368	31068	critical	Keycodes	Keycodes - invalid data range for feature (<feature code> <feature data>).	Contact your local support group.	Yes	Yes	Yes	Yes
369	31079	critical	Keycodes	Keycodes - wrong system id.	Check the system ID in your licensing configuration.	Yes	Yes	Yes	Yes
370	31089	critical	Keycodes	Keycodes - wrong sequence number.	Check the sequence number in your licensing configuration.	Yes	Yes	Yes	Yes
371	40002	information	Media Services Manager	MSM - DSP initialized.	No Action Required.	Yes	No	No	No
372	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	Yes
373	40004	warning	Media Services Manager	MSM - DSP audit failed.	Contact your local support group.	Yes	No	No	No
374	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	Yes
375	41001	major	CTE	CTE - Cte table corruption.	Contact your local support group.	Yes	Yes	Yes	Yes
376	41002	major	CTE	CTE - Unsupported KSU.	Restart system and if problem persists contact your local support group.	Yes	Yes	Yes	Yes
377	41003	major	CTE	CTE - Incorrect state index in the state machine.	Contact your local support group.	Yes	Yes	Yes	Yes
378	41004	warning	CTE	CTE - Error replying to licensing process.	Check your licensing information.	Yes	No	No	No
379	41005	minor	CTE	CTE - Error getting feature from list in licensing process.	Check your licensing information.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
380	41006	warning	CTE	CTE - Error processing Data Status in licesning process.	Check your licensing information.	Yes	No	No	No
381	42200	warning	Call Detail Recording Transfer	CDR Transfer minor error.	Check your configuration parameters.	Yes	No	No	No
382	42500	critical	Call Detail Recording Transfer	CDR Transfer initialization error.	Contact your local support group.	Yes	Yes	Yes	Yes
383	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	Yes
384	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	Yes
385	43002	warning	Voice CTI	Voice CTI no voice channels allocated.	Contact your local support group.	Yes	No	No	No
386	43003	critical	Voice CTI	Voice CTI unable to regsigter with MSM.	Contact your local support group.	Yes	Yes	Yes	Yes
387	43004	critical	Voice CTI	Voice CTI subcomponent failure.	Contact your local support group.	Yes	Yes	Yes	Yes
388	43005	critical	Voice CTI	Voice CTI software error.	Contact your local support group.	Yes	Yes	Yes	Yes
389	43006	warning	Voice CTI	Voice CTI application did not register properly.	Contact your local support group.	Yes	No	No	No
390	50000	critical	Unistim Terminal Proxy Server	UTPS fatal error.	Contact your local support group.	Yes	Yes	Yes	Yes
391	50100	warning	Unistim Terminal Proxy Server	UTPS packet loss on IP terminals.	Check the IP Network in between the system and IP terminal for any issues.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
392	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	No
393	51014	information	VoIP Gateway	VoIP Gateway succeeded to ping gatekeeper address.	No Action Required.	Yes	No	No	No
394	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	No
395	51016	warning	VoIP Gateway	VoIP Gateway remote gateway mismatch.	Verify the remote gateway is supported for interopability with BCM50.	Yes	No	No	No
396	51020	critical	VoIP Gateway	VoIP Gateway failed to initialize h.323 stack.	Contact your local support group.	Yes	Yes	Yes	Yes
397	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	Yes
398	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	Yes
399	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
400	51901	critical	VoIP Gateway	VoIP Gateway serious system error.	Contact your local support group.	Yes	Yes	Yes	Yes
401	51902	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes	Yes
402	51903	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes	Yes
403	51904	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes	Yes
404	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	Yes
405	52001	critical	Media Path Server	MPS unable to initialize MPSMI. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	Yes
406	52002	critical	Media Path Server	MPS unable to connect to MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	Yes
407	52003	critical	Media Path Server	MPS unable to open FUMP channels. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	Yes
408	52004	critical	Media Path Server	MPS FUMP channel not ready. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	Yes
409	52005	critical	Media Path Server	MPS reset by network manager.	Contact your local support group.	Yes	Yes	Yes	Yes
410	52006	critical	Media Path Server	MPS received connection lost from MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes	Yes
411	52007	critical	Media Path Server	MPS unable to create event. MPS service failed to start.	Contact your local support group.	Yes	Yes	Yes	Yes
412	52008	critical	Media Path Server	MPS unable to initialize NNU messaging framework.	Contact your local support group.	Yes	Yes	Yes	Yes
413	52009	critical	Media Path Server	MPS unable to initialize message loop thread.	Contact your local support group.	Yes	Yes	Yes	Yes
414	52013	warning	Media Path Server	MPS codec incompatible, call dropped.	Contact your local support group.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
415	52014	warning	Media Path Server	MPS endpoint registration failed.	Contact your local support group.	Yes	No	No	No
416	53000	critical	Media Gateway Server	MGS Exception software error.	Contact your local support group.	Yes	Yes	Yes	Yes
417	53001	critical	Media Gateway Server	MGS shutting down due to gateway creation failure.	Contact your local support group.	Yes	Yes	Yes	Yes
418	53002	critical	Media Gateway Server	MGS shutting down due to gateway initialization error.	Contact your local support group.	Yes	Yes	Yes	Yes
419	53003	critical	Media Gateway Server	MGS shutting down due to a fatal error.	Contact your local support group.	Yes	Yes	Yes	Yes
420	53004	critical	Media Gateway Server	MGS shutting down due to MSM communication failure.	Contact your local support group.	Yes	Yes	Yes	Yes
421	53005	critical	Media Gateway Server	MGS shutting down due to MPS communication failure.	Contact your local support group.	Yes	Yes	Yes	Yes
422	53006	critical	Media Gateway Server	MGS shutting down due to resource limits query failure.	Contact your local support group.	Yes	Yes	Yes	Yes
423	53007	critical	Media Gateway Server	MGS shutting down due to configuration query failure.	Contact your local support group.	Yes	Yes	Yes	Yes
424	53008	critical	Media Gateway Server	MGS MediaTransport Received bad ports: <port1> <port2>.	Contact your local support group.	Yes	Yes	Yes	Yes
425	53009	critical	Media Gateway Server	MGS MediaTransport Codec and/or frames per packet mismatch <details>.	Contact your local support group.	Yes	Yes	Yes	Yes
426	53010	critical	Media Gateway Server	MGS MediaTransport: Transport mismatch <details>.	Contact your local support group.	Yes	Yes	Yes	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
427	53011	critical	Media Gateway Server	MGS MsmProxy::<interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes	Yes
428	53012	critical	Media Gateway Server	MGS <entity>::<interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes	Yes
429	53018	critical	Media Gateway Server	MGS ResourceMediaController::(OID=<oid>) DSP Task Lost.	Contact your local support group.	Yes	Yes	Yes	Yes
430	53019	information	Media Gateway Server	MGS Shutting down due to IP address change.	No Action Required as service manager will restart.	Yes	No	No	No
431	56003	major	IP Telephony Provider	IP Telphony Provider fatal error was detected.	Contact your local support group.	Yes	Yes	Yes	Yes
432	56004	minor	IP Telephony Provider	IP Telphony Provider error was detected.	Contact your local support group.	Yes	No	No	No
433	56005	major	IP Telephony Provider	IP Telphony Provider software exception.	Contact your local support group.	Yes	Yes	Yes	Yes
434	56006	major	IP Telephony Provider	IP Telphony Provider shutting down due to fatal error.	Contact your local support group.	Yes	Yes	Yes	Yes
435	57002	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Test Local Mode.	No Action Required.	Yes	No	No	No
436	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	No
437	57004	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Set Firmware Upgrade in Progress.	No Action Required.	Yes	No	No	No

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
438	57005	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Normal Mode – Set Redirected to Main Office.	No Action Required.	Yes	No	No	No
439	57006	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Redirection Pending (Set on call).	No Action Required.	Yes	No	No	No
440	57007	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware Upgrade Pending (Set on call).	No Action Required.	Yes	No	No	No
441	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	No
442	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	No
443	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	No
444	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	No
445	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	Yes

Table 47 BCM50 Alarm List

No.	Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm Banner	SNMP	LED	Alarm Set
446	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	Yes
447	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	Yes
448	57750	critical	Survivable Remote Gateway	Survivable Remote Gateway - SRG terminated unexpectedly.	Contact your local support group.	Yes	Yes	Yes	Yes
449	60005	critical	LAN Driver	LAN Driver - Duplicate IP address detected on startup of LAN interface.	Check in diagnostics logs for messages log for futher information. Also Check your network to ensure no other devices are using the same IP address as the system.	Yes	Yes	Yes	Yes

Chapter 8
Using the BCM50 Service Management System

You can use the BCM50 Element Manager to view and administer the services that run on the BCM50 system.

This chapter provides:

- an overview the BCM50 service management system
- a list of BCM50 services
- information about how to start, stop, and restart BCM50 services

Overview of the BCM50 service management system

You can view details about the services that run on the BCM50 system, including:

- the name of a service
- whether a service is enabled to automatically start up
- the status of the service running on the BCM50

You can also administer services by starting, stopping, and restarting certain services.

Caution: Use the BCM50 Services Manager only as directed by Nortel Technical Support. Improper use of the BCM50 Services Manager may adversely affect system operation.

You can keep a record of BCM50 services using the programming record. For more information, see "Saving programming records" on page 66.

BCM50 services

Table 48 lists BCM50 services.

Table 48 BCM50 Services

Service Name	Description
BackupRestoreProviderAgent	Cimom Provider
BCM_DCMProviderAgent	Cimom Provider
BCM_HostProviderAgent	Cimom Provider
BCM_LicenseProviderAgent	Cimom Provider
BCM_LogProviderAgent	Cimom Provider
BCM_MIB2ProviderAgent	Cimom Provider

Table 48 BCM50 Services

Service Name	**Description**
BCM_RASProviderAgent	Cimom Provider
BCM_SecurityProviderAgent	Cimom Provider
BCM_SNMPProviderAgent	Cimom Provider
BCM_TimeServiceProviderAgent	Cimom Provider
BCM_TimeZoneSettingProviderAgent	Cimom Provider
BCMInventoryProviderAgent	Cimom Provider
BCMPerfMonProviderAgent	Cimom Provider
BCMSystemProviderAgent	Cimom Provider
BCMUPSProviderAgent	Cimom Provider
BCMWebProviderAgent	Cimom Provider
btraceserver	Plug-in for Authentication and Routing Management for BT
CallPilotProviderAgent	Cimom Provider
CDRProviderAgent	Cimom Provider
CDRService	Call Detail Recording Service
cfsserver	Component Feature Service
CoreTel	Main Telephony Process
CoreTelProviderAgent	Cimom Provider
crond	Cron Scheduler
Cte	Computer Telephony Engine
ctiserver	Computer Telephony Integration
dhcpd	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
IpTelProviderAgent	Cimom Provider
LanCteProviderAgent	Cimom Provider
LANProviderAgent	Cimom Provider
lms	Line Monitor Server
mgs	Media Gateway Server
modemcc	Modem Call Control
monit	Process Monitoring Daemon
mps	IP Telephony—Media Path
Msm	Media Services Manager

Table 48 BCM50 Services

Service Name	Description
MsmProviderAgent	Cimom Provider
NnuScheduler	System Scheduler
owcimomd	Open Wbem Cimom Server Daemon
Pdrd	Persistence Data Repository Service
psm	Process Status Monitor Service
qmond	QoS Monitor
securityservice	Authentication and Authorization
snmpd	SNMP Server Daemon
SoftwareUpdateProviderAgent	Cimom Provider
ssba	System Set Based Admin Service (Feature 9*8)
sshd	Secure Shell Daemon
SyslogListener	Syslog Receiver
tmwservice	Time Service
utps	UniSTIM Terminal Proxy Server (IP Sets)
voicemail	Voicemail Process

To view details about services

1. Start the BCM50 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 BCM50 system.

Caution: Use the BCM50 Services Manager only as directed by Nortel Technical Support. Improper use of the BCM50 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

Using BCM50 Metrics

You can use the BCM50 Element Manager to view detailed information about the performance of the BCM50 and about the performance of system resources.

This chapter provides information about the following:

- system metrics
- telephony metrics

About system metrics

Using the BCM50 Element Manager, you can monitor overall system performance and other performance-related information.

You monitor system metrics using the following tools:

- QoS Monitor
- UPS Metrics
- NTP Metrics

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 *BCM50 Network Guide*. You can set the threshold in the BCM50 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

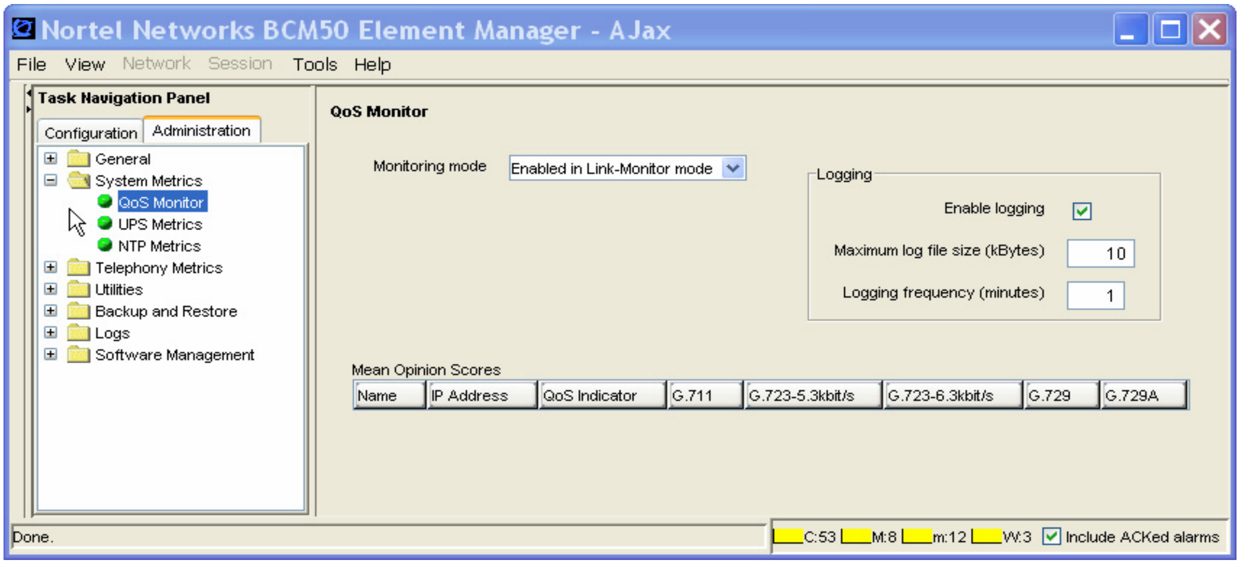
1 On the Navigation tree, click the **Administration** tab, **System Metrics**, and **QoS Monitor.**

2 Configure the monitoring mode attributes.

Table 49 Monitoring Mode attributes

Attribute	Action
Disabled	—
Link-Monitor Mode	Test the connection between the BCM50 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 36 QoS Monitoring mode



Monitoring mode: Enabled in Link-Monitor mode

Logging

Enable logging ☑

Maximum log file size (kBytes) 10

Logging frequency (minutes) 1

Mean Opinion Scores

Name	IP Address	QoS Indicator	G.711	G.723-5.3kbit/s	G.723-6.3kbit/s	G.729	G.729A

To configure logging attributes

1 On the Navigation tree, click the **Administration** tab, **System Metrics**, and **QoS Monitor.**

2 Configure logging attributes.

Table 50 Logging attributes

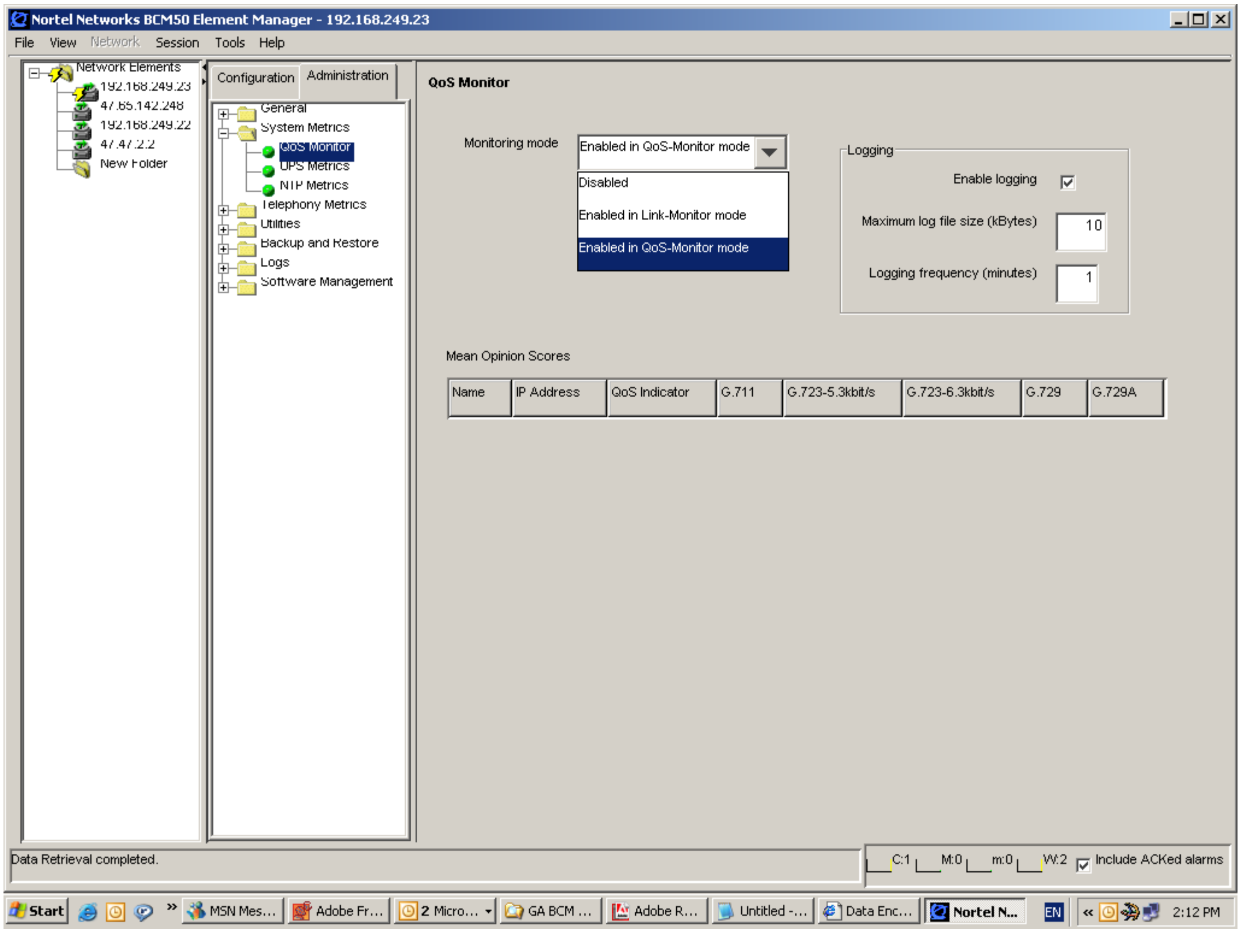
Attribute	Action
Enable Logging	Enable the check box if you want to enable the logging of MOS scores.

Table 50 Logging attributes

Attribute	Action
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 37 QoS Logging attributes



Nortel Networks BCM50 Element Manager - 192.168.249.23

QoS Monitor

Monitoring mode: Enabled in QoS-Monitor mode

Logging

Enable logging ☑

Maximum log file size (kBytes): 10

Logging frequency (minutes): 1

Mean Opinion Scores

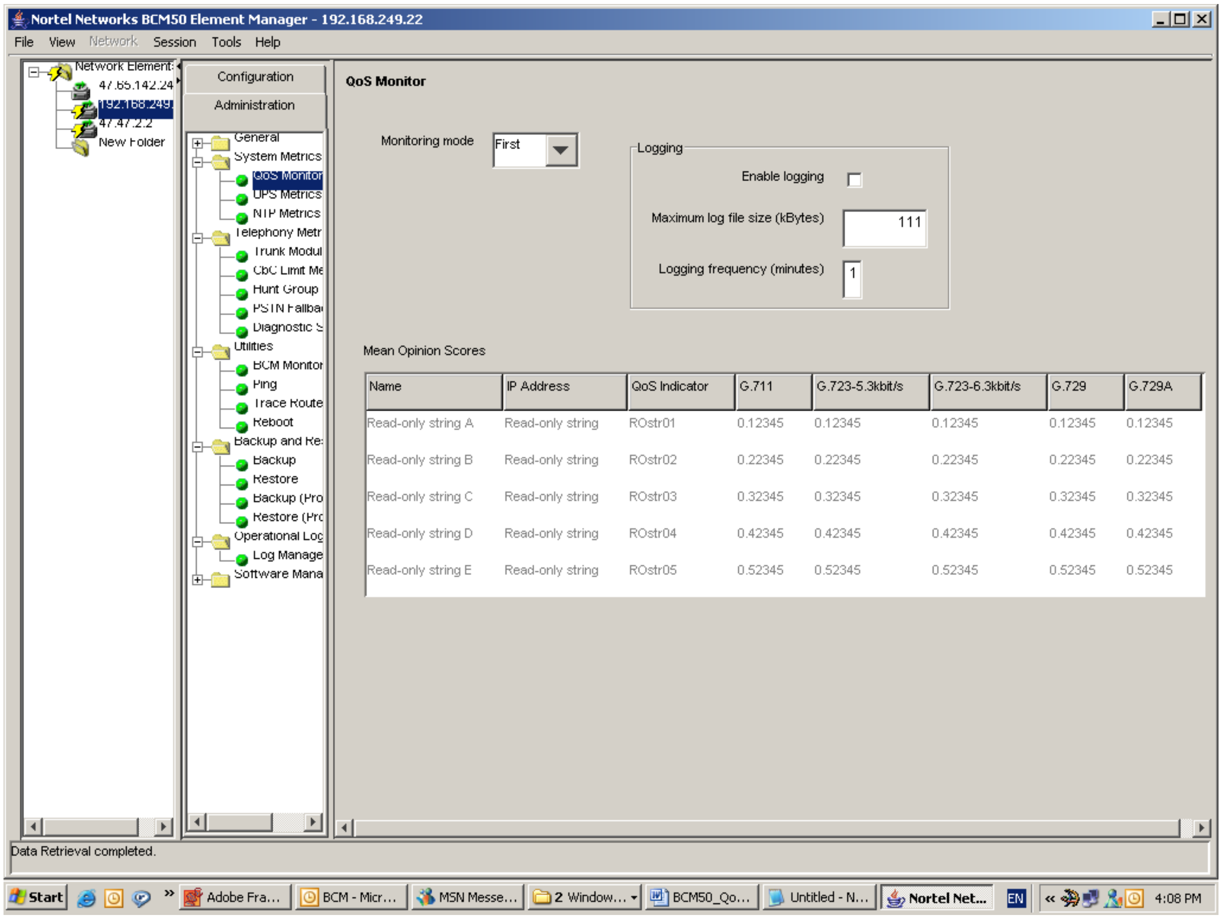
Name	IP Address	QoS Indicator	G.711	G.723-5.3kbit/s	G.723-6.3kbit/s	G.729	G.729A

Data Retrieval completed.

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 BCM50 QoS Monitor collects only the transmit values.

Figure 38 QoS Monitor Panel



QoS Monitor

Monitoring mode: First

Logging

Enable logging ☐

Maximum log file size (kBytes): 111

Logging frequency (minutes): 1

Mean Opinion Scores

Name	IP Address	QoS Indicator	G.711	G.723-5.3kbit/s	G.723-6.3kbit/s	G.729	G.729A
Read-only string A	Read-only string	ROstr01	0.12345	0.12345	0.12345	0.12345	0.12345
Read-only string B	Read-only string	ROstr02	0.22345	0.22345	0.22345	0.22345	0.22345
Read-only string C	Read-only string	ROstr03	0.32345	0.32345	0.32345	0.32345	0.32345
Read-only string D	Read-only string	ROstr04	0.42345	0.42345	0.42345	0.42345	0.42345
Read-only string E	Read-only string	ROstr05	0.52345	0.52345	0.52345	0.52345	0.52345

Data Retrieval completed.

Note: For the QoS monitor and PSTN fallback to function, both BCM50s must list each other as a Remote Gateway and QoS Monitor must be enabled on both systems.

Table 51 lists the fields displayed in the Mean Opinion Score table.

Table 51 Mean Opinion Score descriptions

Attribute	Description
Name	Displays the name of the Remote Gateway
Destination IP	Displays the IP address of the Remote Gateway
QoS Monitor	Displays the status of QoS Monitor for this Remote Gateway If Enabled is displayed, QoS Monitor is currently collecting QoS information for this Remote Gateway. If Disabled is displayed, QoS Monitor is not collecting QoS information.
QoS Indicator	Displays a text description of the current MOS value. The MOS values can be Poor, Fair, Good or Excellent.

Table 51 Mean Opinion Score descriptions (Continued)

Attribute	Description
Name	Displays the name of the Remote Gateway
G.711-aLaw	Displays the current MOS value calculated when using a G.711 aLaw codec to transmit VoIP packets to this Remote Gateway. The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.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, in the **View** menu, select **Refresh** or press F5.

UPS Metrics

The BCM50 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 *BCM50 Installation Guide*, *BCM50 Initial Configuration Guide*, and *BCM50 Maintenance Guide*.

The UPS connects and communicates with the BCM50 through USB. Enabling the UPS feature requires plugging the UPS USB cable to the BCM50 USB connector and before powering up the BCM50. The UPS must be present during the boot up process for the BCM50 to function.

This section provides the procedure the describes how “To access UPS Metrics”.

To access UPS Metrics

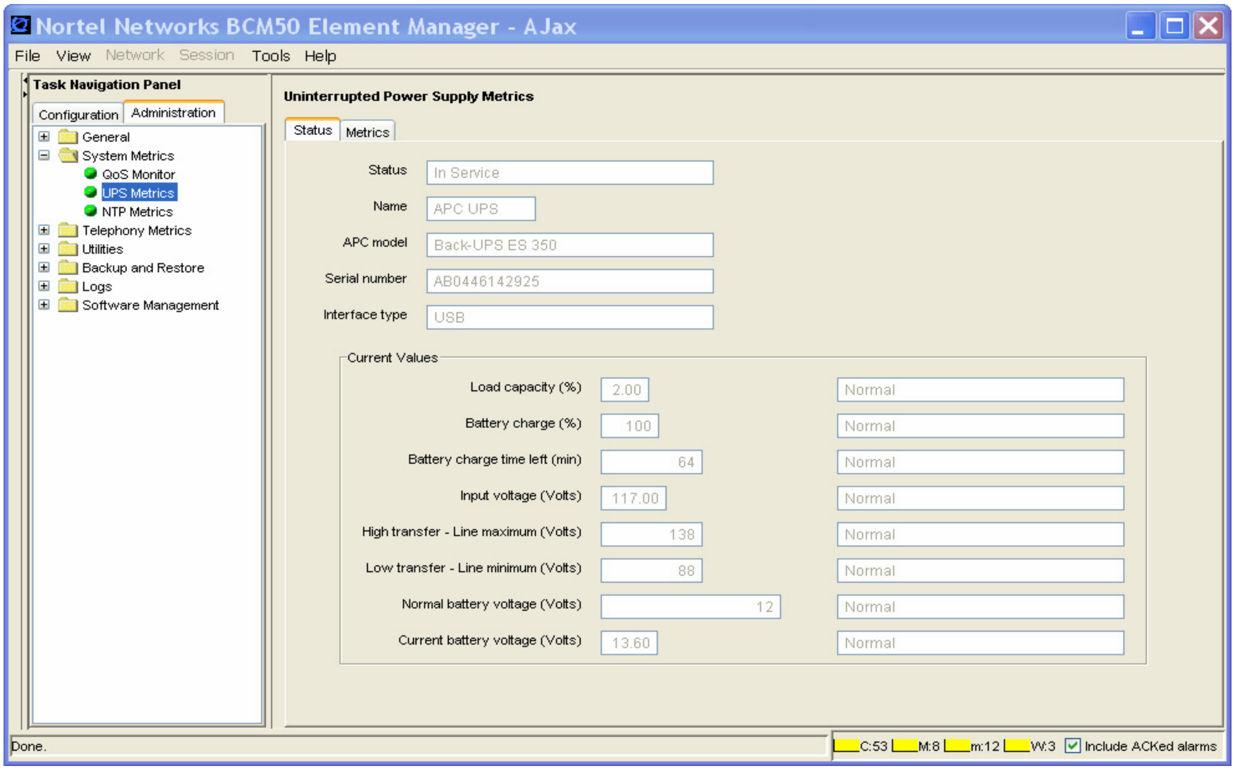
1 To access the UPS Metrics, open the BCM50 Element Manager, click the **Administration** tab, click **System Metrics** in the directory tree, and then click **UPS Metrics**.

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 Metrics panel tracks occurrences of alarms pertaining to UPS operation. These alarms are also sequentially viewable in the Alarm Viewer. The metrics correspond to alarms in the BCM50 and appear in the alarm viewer as well. See Figure 39.

Figure 39 UPS Status Monitor



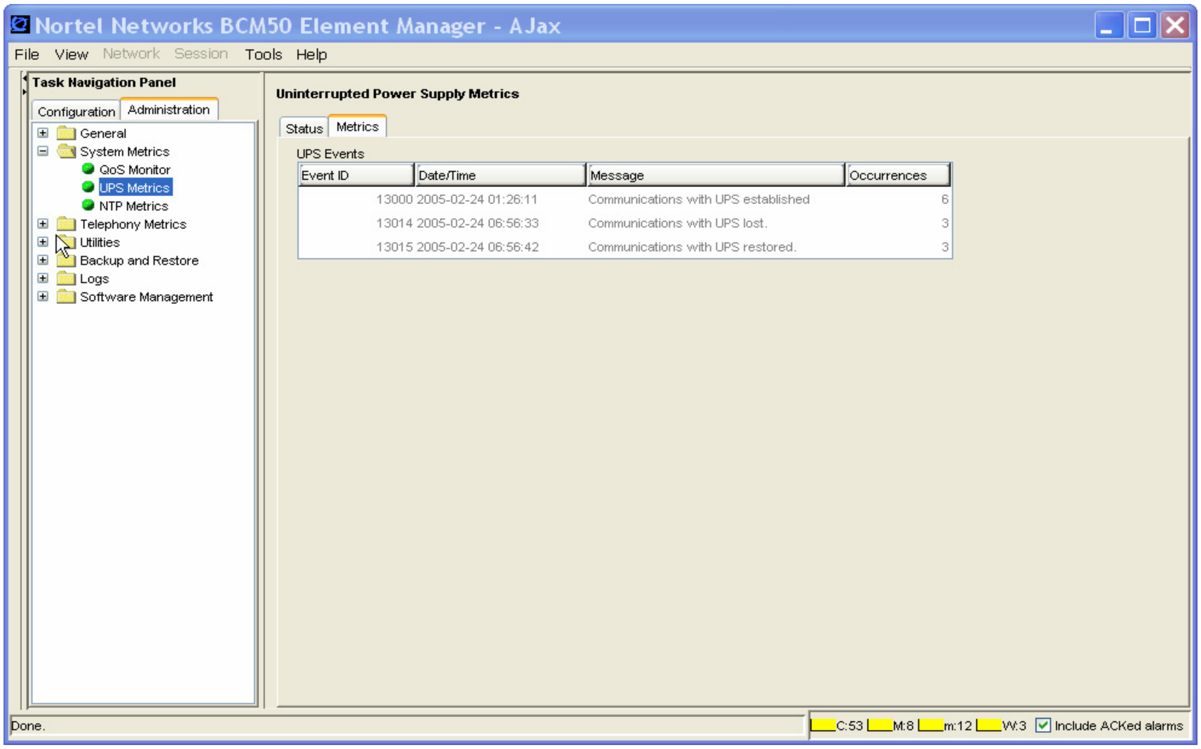
Status	In Service
Name	APC UPS
APC model	Back-UPS ES 350
Serial number	AB0446142925
Interface type	USB

Current Values

Load capacity (%)	2.00	Normal
Battery charge (%)	100	Normal
Battery charge time left (min)	64	Normal
Input voltage (Volts)	117.00	Normal
High transfer - Line maximum (Volts)	138	Normal
Low transfer - Line minimum (Volts)	88	Normal
Normal battery voltage (Volts)	12	Normal
Current battery voltage (Volts)	13.60	Normal

2 To check the metrics of the UPS, click the **Metrics** tab. It displays the information on the panel, as shown in Figure 40 on page 233.

Figure 40 UPS Metrics page



Uninterrupted Power Supply Metrics

UPS Events

Event ID	Date/Time	Message	Occurrences
13000	2005-02-24 01:26:11	Communications with UPS established	6
13014	2005-02-24 06:56:33	Communications with UPS lost.	3
13015	2005-02-24 06:56:42	Communications with UPS restored.	3

NTP Metrics

Using Network Time Protocol (NTP), you can configure the time on the BCM50 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.

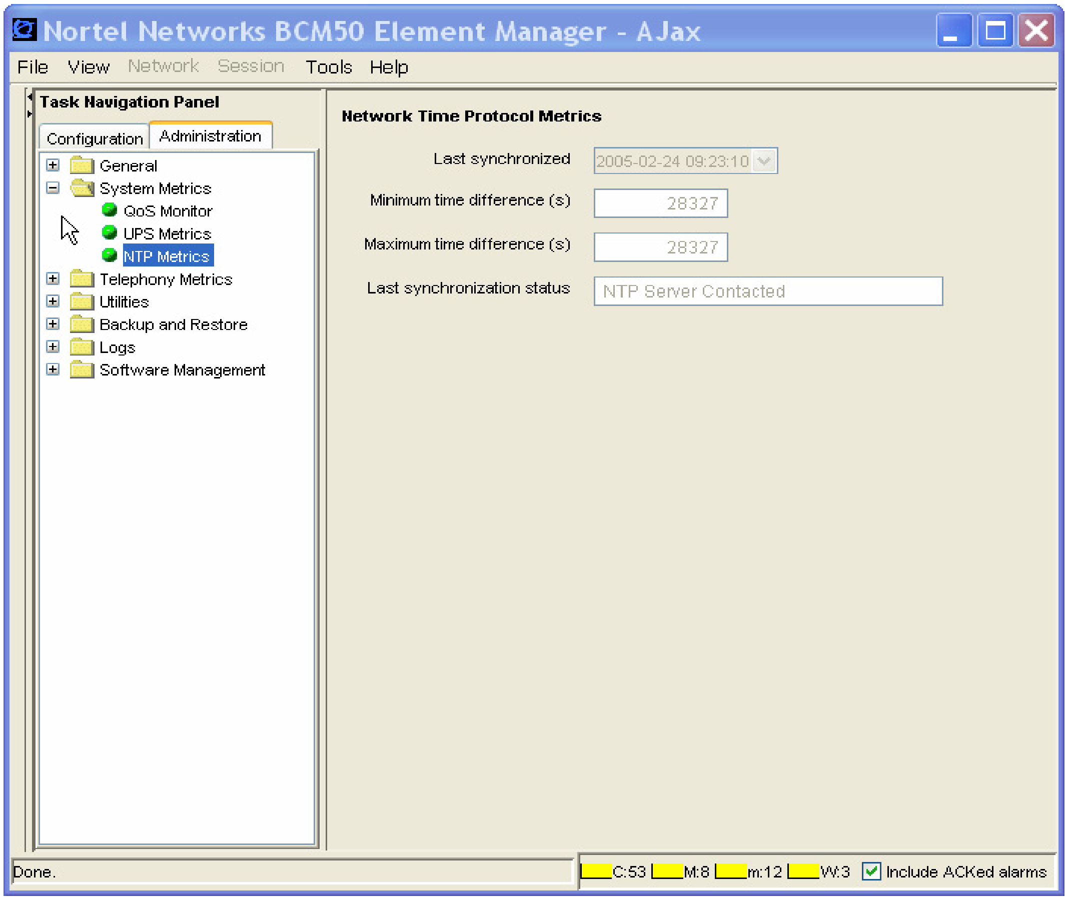
Note: If the BCM50 clock control has not been configured to use NTP (Configuration>System>Date & Time), then the NTP Metrics panel displays no data.

This section provides the procedure "To access the NTP Metrics".

To access the NTP Metrics

1 Open the BCM50 Element Manager, click the **Administration** tab, click **System Metrics** and then select **NTP Metrics** in the navigation tree. See Figure 41.

Figure 41 NTP Metrics



Network Time Protocol Metrics

Last synchronized 2005-02-24 09:23:10

Minimum time difference (s) 28327

Maximum time difference (s) 28327

Last synchronization status NTP Server Contacted

Done.

C:53 M:8 m:12 W:3 ☑ Include ACKed alarms

The **NTP Metrics** panel displays information contained in Table 52.

Table 52 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.

Telephony Metrics

The following sections provide a general overview of the BCM50 Element Manager Telephony Metrics headings.

The Telephony Metrics folder groups together a number of BCM50 system metrics tracking different aspects of Telephony services.

This overview describes the following general process information:

- "Trunk Module Metrics" on page 235.
- "CbC limit metrics" on page 242.
- "Hunt Group Metrics" on page 244.
- "PSTN Fallback Metrics" on page 246.

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 235
- "Disabling or enabling a B channel setting" on page 237
- "Provisioning a PRI B-channel" on page 238
- "Trunk Module CSU statistics" on page 239

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.

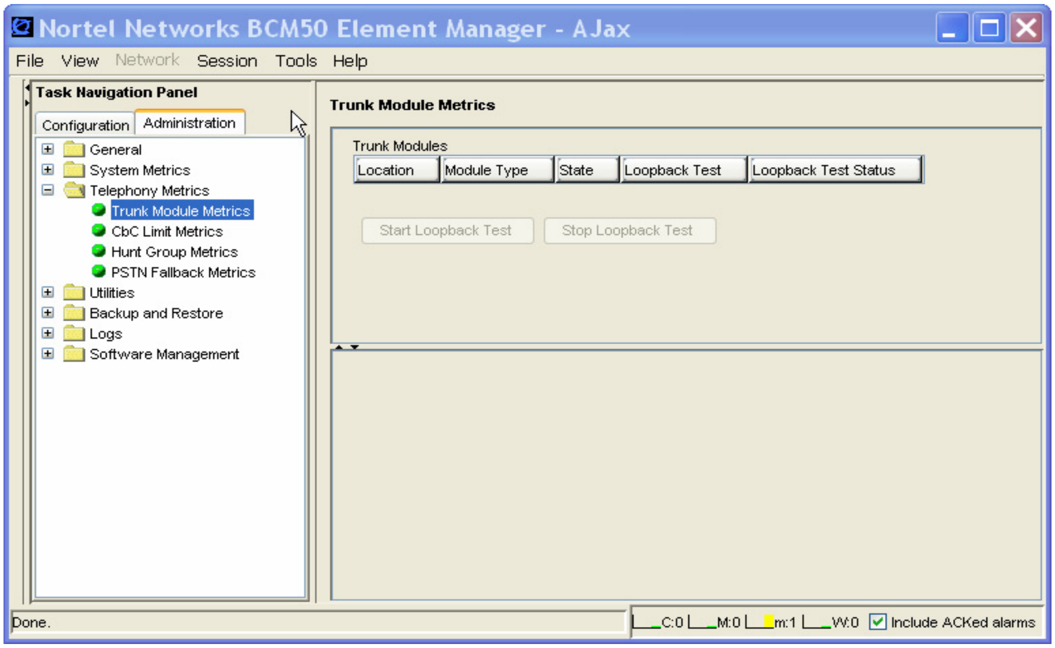
Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module state:

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 42.

Figure 42 Viewing Trunk Module metrics



3 Click **Start Loopback Test** button to start the network test without having to remove the BCM50.

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

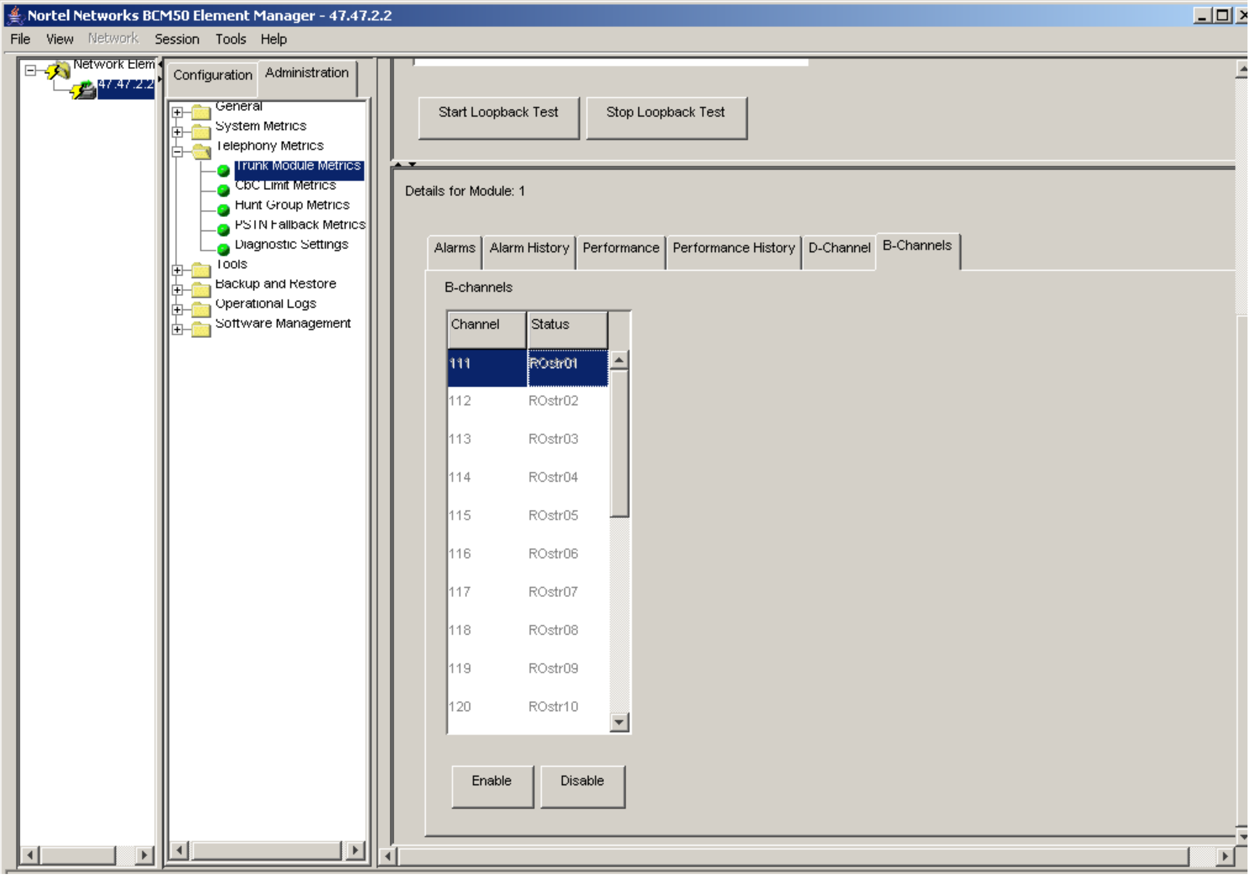
If you need to isolate a problem, you may need to turn off individual port channels, rather than the entire module.

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**; see Figure 43.

Figure 43 B-Channel Enabling/Disabling



Channel	Status
111	ROstr01
112	ROstr02
113	ROstr03
114	ROstr04
115	ROstr05
116	ROstr06
117	ROstr07
118	ROstr08
119	ROstr09
120	ROstr10

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. See Figure 43. 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. See Figure 43 on page 238.

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 239
- "Enabling the internal CSU" on page 240
- "To check the performance statistics" on page 240
- "To check the CSU alarms" on page 241
- "To check carrier failure alarms" on page 241
- "To check bipolar violations" on page 241
- "To check short -term alarms" on page 241
- "To check defects" on page 242
- "CbC limit metrics" on page 242

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 53.

Table 53 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.

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 239.

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 239.

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.

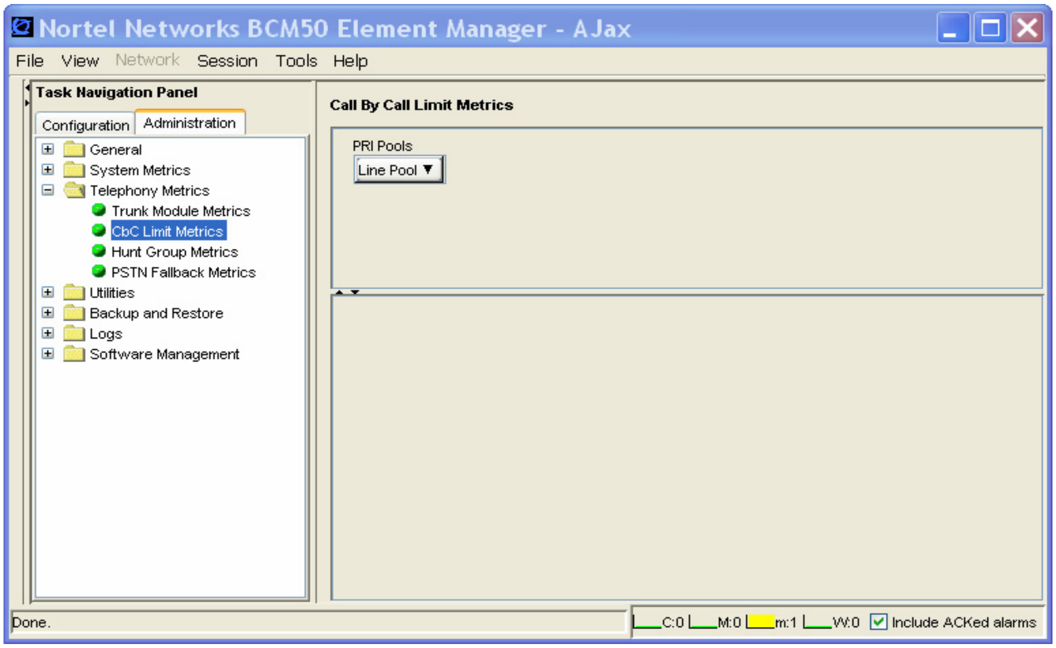
PRI lines that support call-by-call services have maximum and minimum call limits for each service. Use this panel to view reports for the services. These limits are set as part of the numbering plan programming.

This section provides the “To access the CbC limit metrics” procedure.

To access the CbC limit metrics

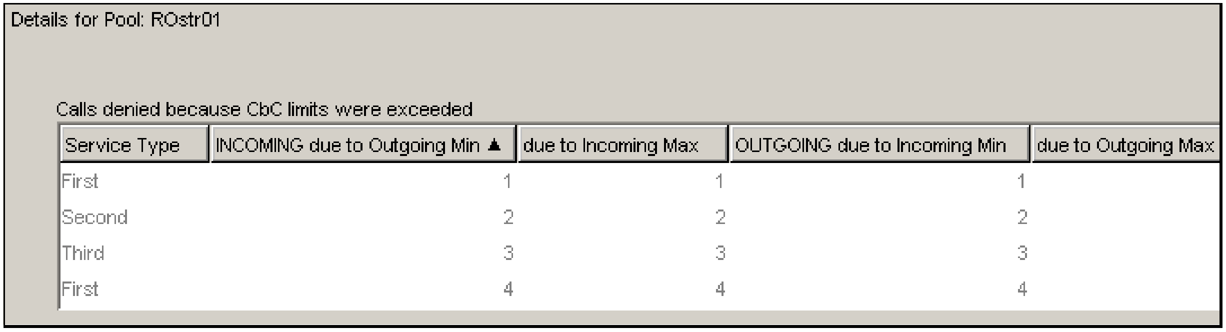
1. To access the CbC metrics, in the BCM50 Element Manager, click the **Administration** tab, click the **Telephony Metrics** and then **CbC Limit Metrics** in the navigation tree.
2. To assess the capacity of the PRI call services on your system, on the **Call by Call Metrics** table, select the line pool for which you want to view CbC traffic. See Figure 44.

Figure 44 Call By Call limit metrics



The denied call details for each type of service supported by the line pool is displayed. See Figure 45 on page 244.

Figure 45 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	
Second	2	2	2	
Third	3	3	3	
First	4	4	4	

Table 54 describes each field on the two CbC metrics panels.

Table 54 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: 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

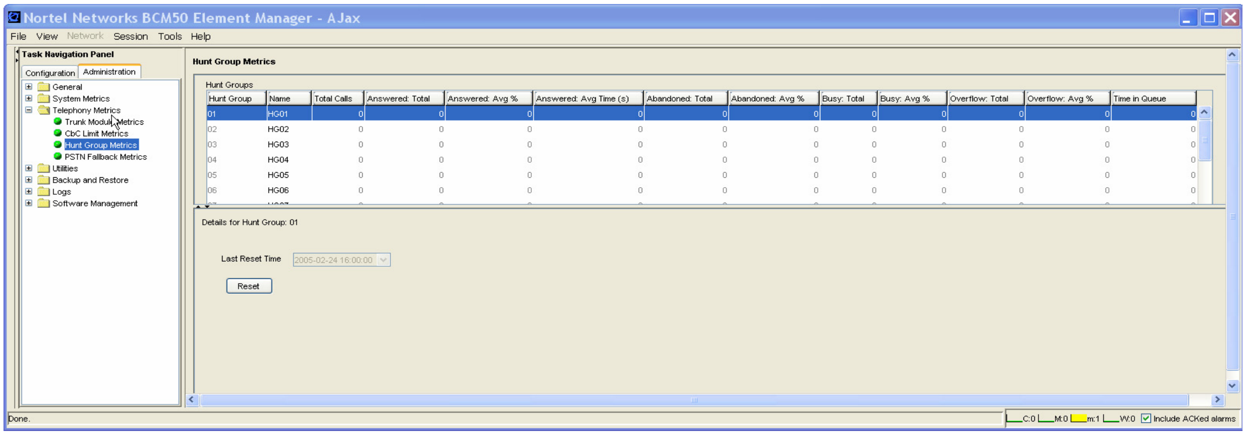
Hunt groups provide a service where incoming calls ring on a targeted group of telephones called a Hunt group. When you designate a Hunt group, you define the group as a unique Directory Number (DN). This DN receives and distributes calls to the telephones assigned to the group. This section provides the procedure for "To access the Hunt Group metrics".

To access the Hunt Group metrics

To access the Hunt Group metrics to evaluate total call processing by hunt group member:

1 In the BCM50 Element Manager, select the **Administration** tab, then the **Telephony Metrics** and **Hunt Group Metrics** in the navigation tree. See Figure 46 on page 245.

Figure 46 Hunt Group Metrics Table



Hunt Group Metrics

Hunt Groups

Hunt Group	Name	Total Calls	Answered: Total	Answered: Avg %	Answered: Avg Time (s)	Abandoned: Total	Abandoned: Avg %	Busy: Total	Busy: Avg %	Overflow: Total	Overflow: Avg %	Time in Queue
01	HG01	0	0	0	0	0	0	0	0	0	0	0
02	HG02	0	0	0	0	0	0	0	0	0	0	0
03	HG03	0	0	0	0	0	0	0	0	0	0	0
04	HG04	0	0	0	0	0	0	0	0	0	0	0
05	HG05	0	0	0	0	0	0	0	0	0	0	0
06	HG06	0	0	0	0	0	0	0	0	0	0	0

Details for Hunt Group: 01

Last Reset Time: 2005-02-24 16:00:00

Table 55 describes each field on the panel.

Table 55 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
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		

Table 55 Hunt Group Metrics fields (Continued)

Attribute	Value	
Last Reset time	Read-only	Time and date format depends country profile of system.
Reset	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.

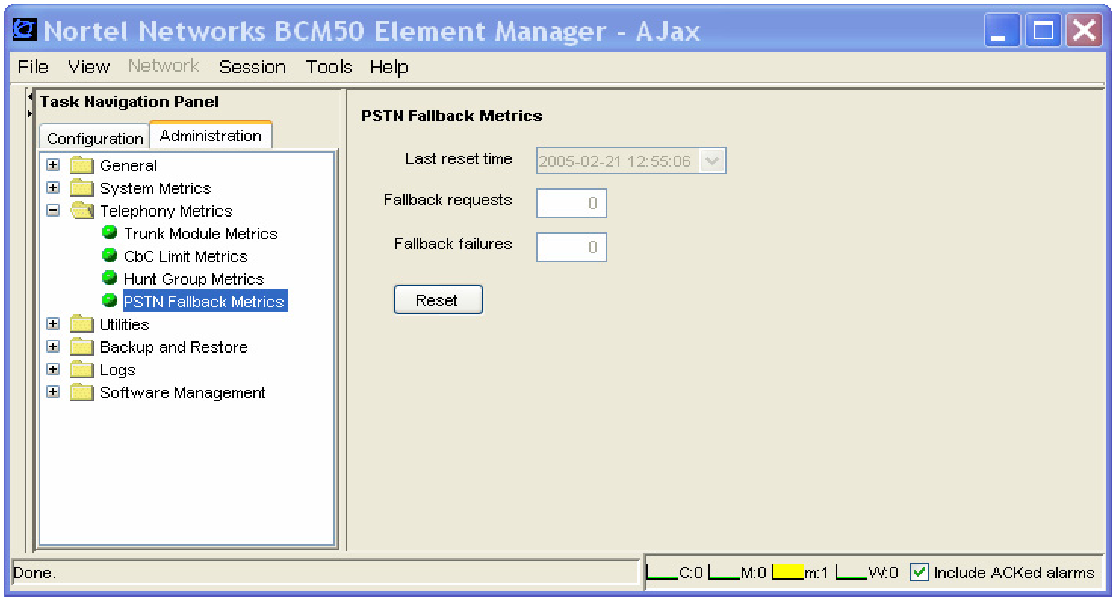
This section provides the procedure for "To access PSTN Fallback metrics".

To access PSTN Fallback metrics

1 In the BCM50 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 47 on page 247.

Figure 47 Fallback Metrics panel



PSTN Fallback Metrics

Last reset time: 2005-02-21 12:55:06

Fallback requests: 0

Fallback failures: 0

Table 56 describes each field on the panel.

Table 56 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.	

Chapter 10
BCM50 Utilities

This chapter contains information about the utilities that are part of the BCM50 Element Manager. These utilities provide information about the BCM50 system, so that you can monitor and analyze system status and performance.

BCM50 utilities are:

- BCM Monitor
- Ping
- Trace Route
- Ethernet Activity
- Reset
- Diagnostic Settings

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, BCM1000, and BCM50 systems.

BCM Monitor is included with the installation of the BCM50 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 BCM50 Element Manager.

Using BCM Monitor, you can monitor the following:

- overall system status
- IP telephony functions of the BCM50 system, including IP device activity and VoIP session information
- utilization of resources
- operation of telephony applications (for example, Voice Mail and Call 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 BCM50, BCM100, BCM200, and BCM1000 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 BCM50 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

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 BCM50 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 BCM50 Element Manager. If you do require BCM Monitor separately from the BCM50 Element Manager, you install the application from the BCM50 Web page.

Note: If BCM Monitor is already installed on your personal computer or on the personal computers of BCM50 users for the purpose of monitoring BCM200, BCM400, or BCM1000 systems, you must uninstall the client or clients and install the BCM Monitor supplied with BCM50.

To remove an earlier version of the BCM Monitor, see "To remove BCM Monitor" on page 251 or see the client documentation.

The BCM Monitor provided with BCM50 monitors both BCM50 and BCM200, BCM400 and BCM1000 systems.

To install BCM Monitor separately from BCM50 Element Manager

1. On the BCM50 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 BCM50 system

For security reasons, the user on the computer on which the BCM Monitor runs must be authenticated by the BCM50 system. Once you are connected to a BCM50 system, you are not required to re-enter a user name and password each time you connect to a different BCM50 system.

To start BCM Monitor without the BCM50 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 BCM50 you want to monitor.

3 In the **Connect As** field, enter your BCM50 user name.

4 In the **Password** field, enter the password associated with your BCM50 user name.

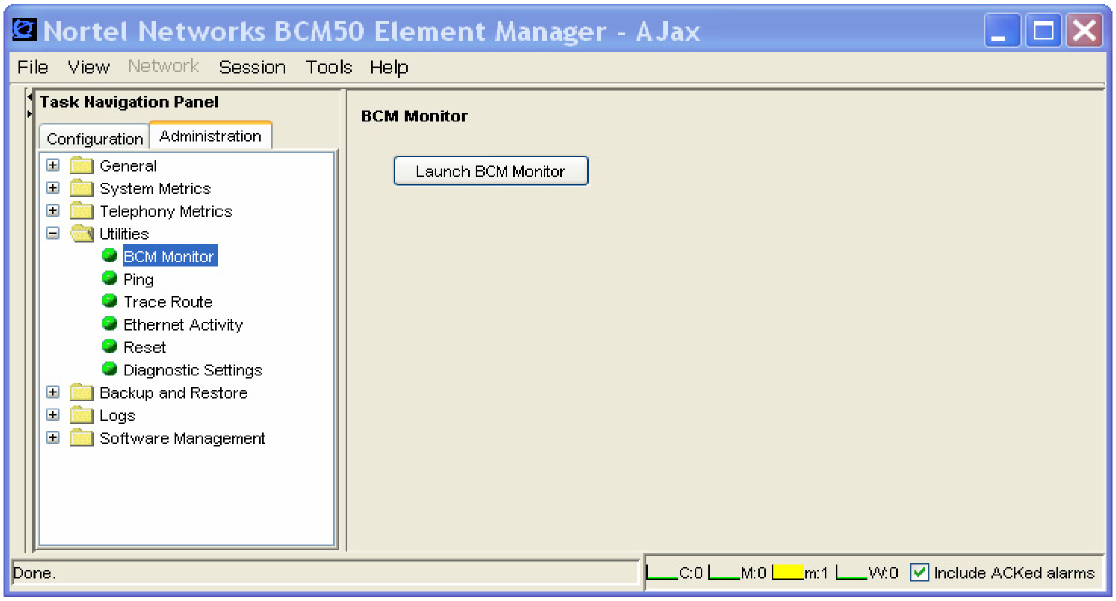
5 Click the **Connect** button.
The **BCM Monitor** panel opens.

To start BCM Monitor from the BCM50 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 BCM50 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 BCM50

On the **File** menu of the BCM Monitor, select **Disconnect from BCM**.
BCM Monitor disconnects from the BCM50 system and clears all the fields.

Note: If you do not want to connect to another BCM50 system, close the BCM Monitor application. This terminates the application and disconnects BCM Monitor from the BCM50 system.

To connect to a different BCM50

1 On the **File** menu of the BCM Monitor, select **Disconnect from BCM**.
BCM Monitor disconnects from the BCM50 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 BCM50 you want to monitor.

4 In the **Connect As** field, enter your BCM50 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 BCM50 system and to save data to generate system utilization and traffic reports.

BCM Monitor tabs provide information about the following:

- the overall BCM50 system
- utilization of resources
- operation of telephony applications (for example, Voice Mail, and Call Center)
- lines
- PRI, BRI, and IP trunks

You can capture information about the BCM50 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 BCM50 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.

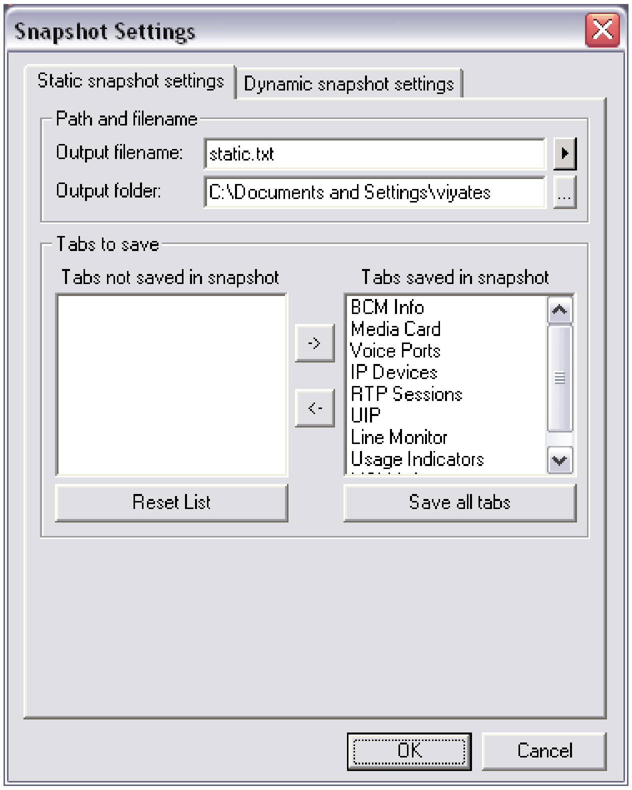
Table 57 Output filename attributes

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 snaphots to include information about voice ports, make sure that Voice Ports is included in the **Tabs Saved in Snapshot** box**.**



Snapshot Settings

Static snapshot settings | Dynamic snapshot settings

Path and filename

Output filename: static.txt

Output folder: C:\Documents and Settings\viyates

Tabs to save

Tabs not saved in snapshot

Tabs saved in snapshot:
BCM Info
Media Card
Voice Ports
IP Devices
RTP Sessions
UIP
Line Monitor
Usage Indicators

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

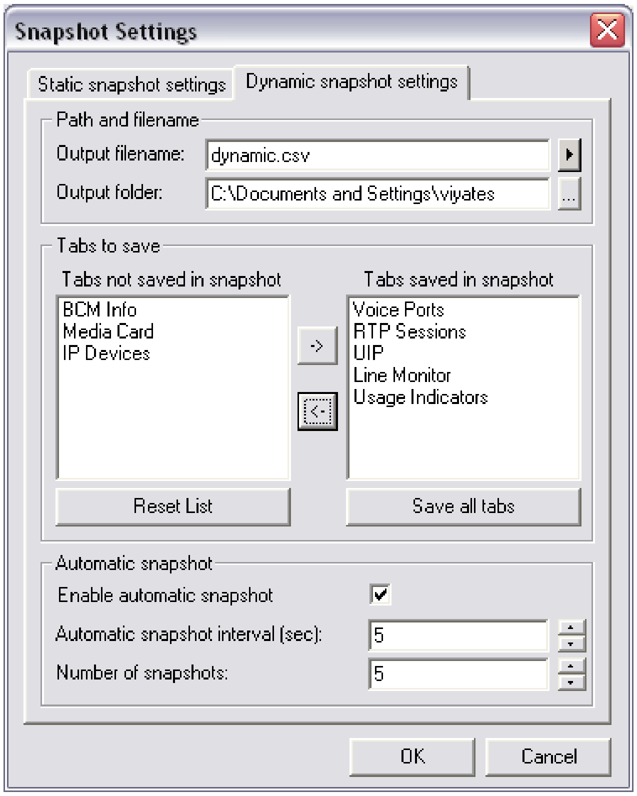
1. On the **File** menu, select **Snapshot Settings**.
   The **Snapshot Settings** panel opens.
2. Click the **Dynamic Snapshot Settings** tab.
3. In the **Path and Filename** area, enter the filename for the dynamic snapshot in the **Output Filename** field. For additional options, click the Arrow button to the right of the **Output Filename** field.
4. Configure the Output Filename attributes.

Table 58 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.**



Output filename: dynamic.csv

Output folder: C:\Documents and Settings\viyates

Tabs not saved in snapshot: BCM Info, Media Card, IP Devices

Tabs saved in snapshot: Voice Ports, RTP Sessions, UIP, Line Monitor, Usage Indicators

Enable automatic snapshot ☑

Automatic snapshot interval (sec): 5

Number of snapshots: 5

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.

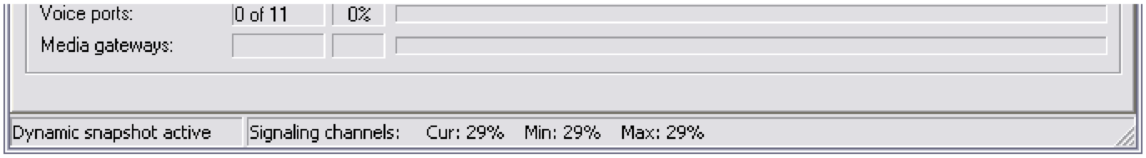
11 In the **Number of Snapshots** field, enter the number of snapshots from 1 to Infinite.

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.



Voice ports: 0 of 11 0%
Media gateways:
Dynamic snapshot active
Signaling channels: Cur: 29% Min: 29% Max: 29%

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

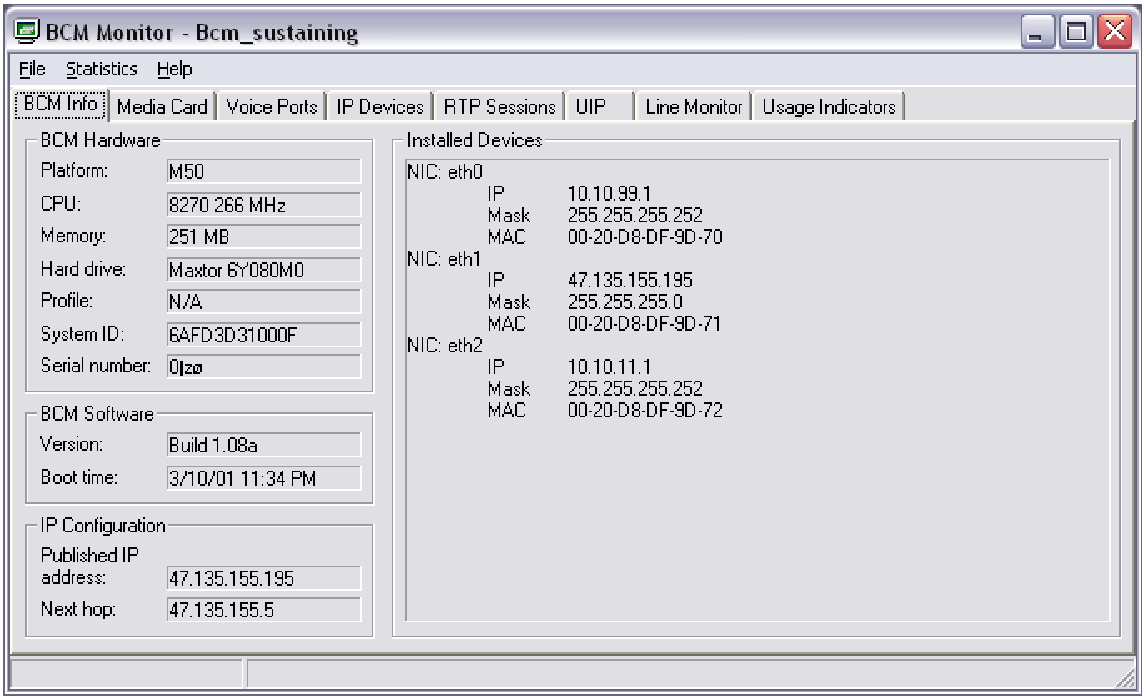
On the **File** menu, select **Dynamic Snapshot**, **Stop**.

BCM50 Info tab

The BCM50 Info tab displays static information about the BCM50 system, such as:

- information about the main hardware components of the BCM50 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 BCM50, the published IP address and default gateway of the BCM50 main unit, the last time the BCM50 was rebooted, as well as IP address information about other Ethernet interfaces on the BCM50 main unit.



BCM Hardware
Platform: M50
CPU: 8270 266 MHz
Memory: 251 MB
Hard drive: Maxtor 6Y080M0
Profile: N/A
System ID: 6AFD3D31000F
Serial number: 0|zø

BCM Software
Version: Build 1.08a
Boot time: 3/10/01 11:34 PM

IP Configuration
Published IP address: 47.135.155.195
Next hop: 47.135.155.5

Installed Devices
```
NIC: eth0
          IP      10.10.99.1
          Mask    255.255.255.252
          MAC     00-20-D8-DF-9D-70
NIC: eth1
          IP      47.135.155.195
          Mask    255.255.255.0
          MAC     00-20-D8-DF-9D-71
NIC: eth2
          IP      10.10.11.1
          Mask    255.255.255.252
          MAC     00-20-D8-DF-9D-72
```

The installed devices on the BCM50 Info tab are displayed as follows:

- Eth0 — indicates a LAN internal to the BCM50 system.
- Eth1 — indicates a customer LAN. This is the LAN accessible to the customer through ports 1, 2 and 3 on the front panel of the BCM50 main unit.
- Eth2 — OAM LAN. This is a dedicated OAM port accessible as port 0, the left-most Ethernet port on the front panel of the BCM50 main unit.

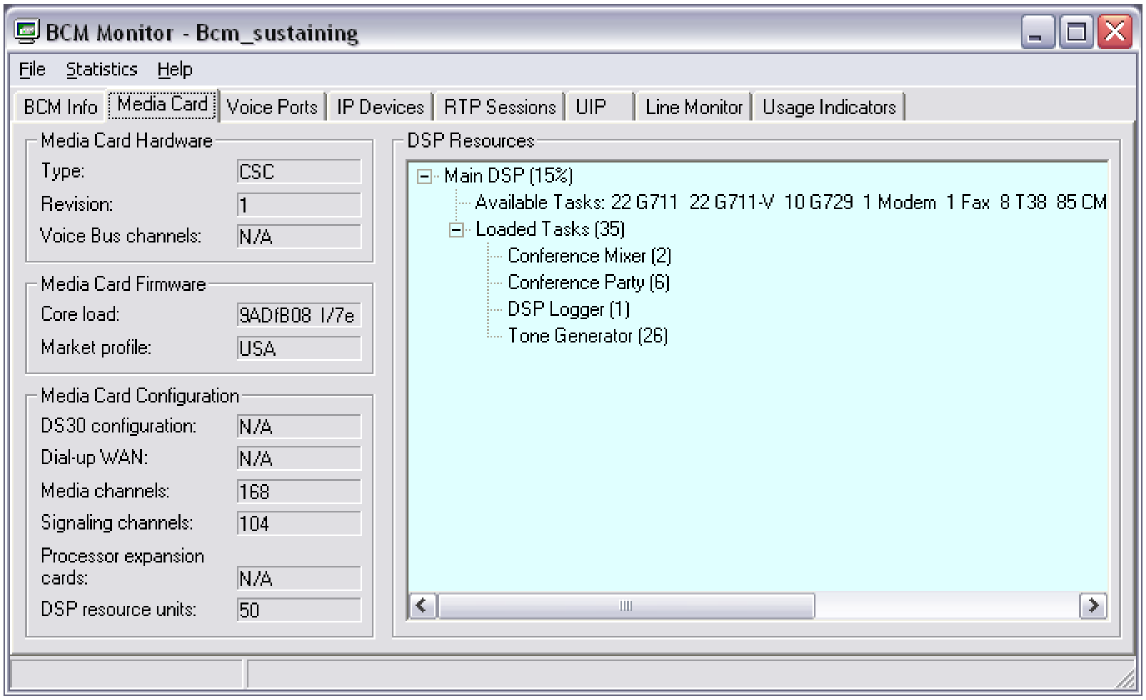
Media Card tab

The Media Card tab provides information about the telephony system of the BCM50. This tab provides the following information for a BCM50:

- the hardware of the BCM50 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), signaling channels (D 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 3.x 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



Media Card Hardware

Type: CSC

Revision: 1

Voice Bus channels: N/A

Media Card Firmware

Core load: 9ADfB08 I/7e

Market profile: USA

Media Card Configuration

DS30 configuration: N/A

Dial-up WAN: N/A

Media channels: 168

Signaling channels: 104

Processor expansion cards: N/A

DSP resource units: 50

DSP Resources

```
Main DSP (15%)
    Available Tasks: 22 G711  22 G711-V  10 G729  1 Modem  1 Fax  8 T38  85 CM
    Loaded Tasks (35)
        Conference Mixer (2)
        Conference Party (6)
        DSP Logger (1)
        Tone Generator (26)
```

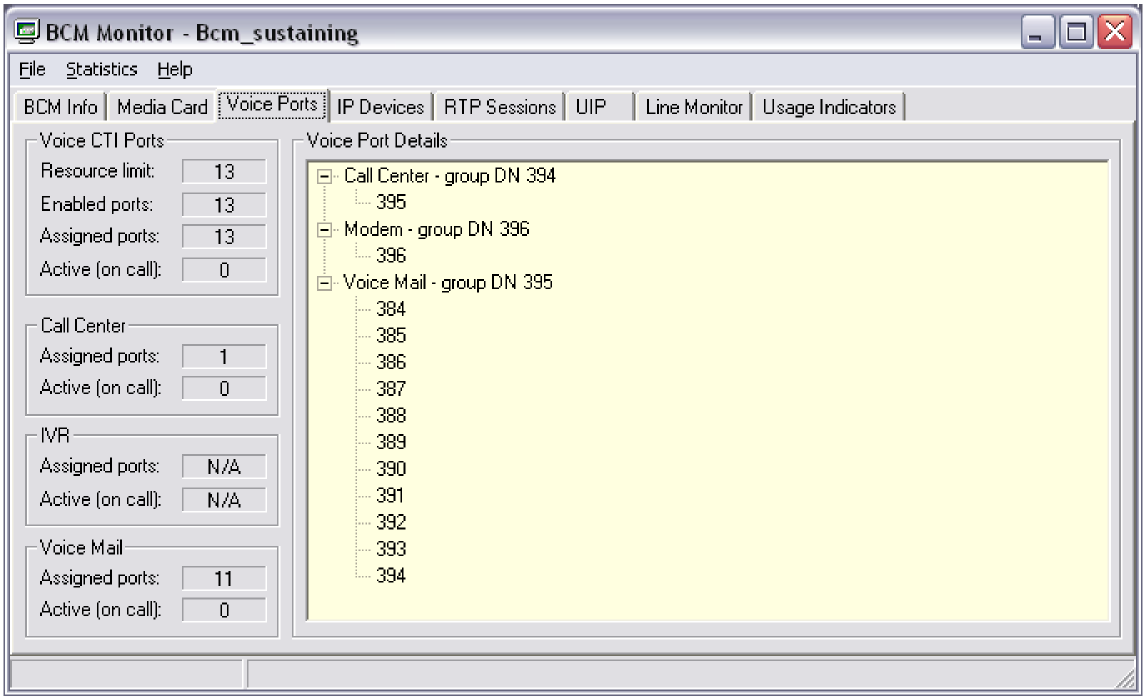
Voice Ports tab

The Voice Ports tab displays real-time information about configured voice ports. A configured voice port is a logical device used for Voice Mail, Call 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.

Note: IVR is supported on the BCM3.x release level for BCM200, BCM400, and BCM1000, but it is not supported on the BCM50.

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 Call 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



Voice CTI Ports

Resource limit: 13

Enabled ports: 13

Assigned ports: 13

Active (on call): 0

Call Center

Assigned ports: 1

Active (on call): 0

IVR

Assigned ports: N/A

Active (on call): N/A

Voice Mail

Assigned ports: 11

Active (on call): 0

Voice Port Details

```
Call Center - group DN 394
    395
Modem - group DN 396
    396
Voice Mail - group DN 395
    384
    385
    386
    387
    388
    389
    390
    391
    392
    393
    394
```

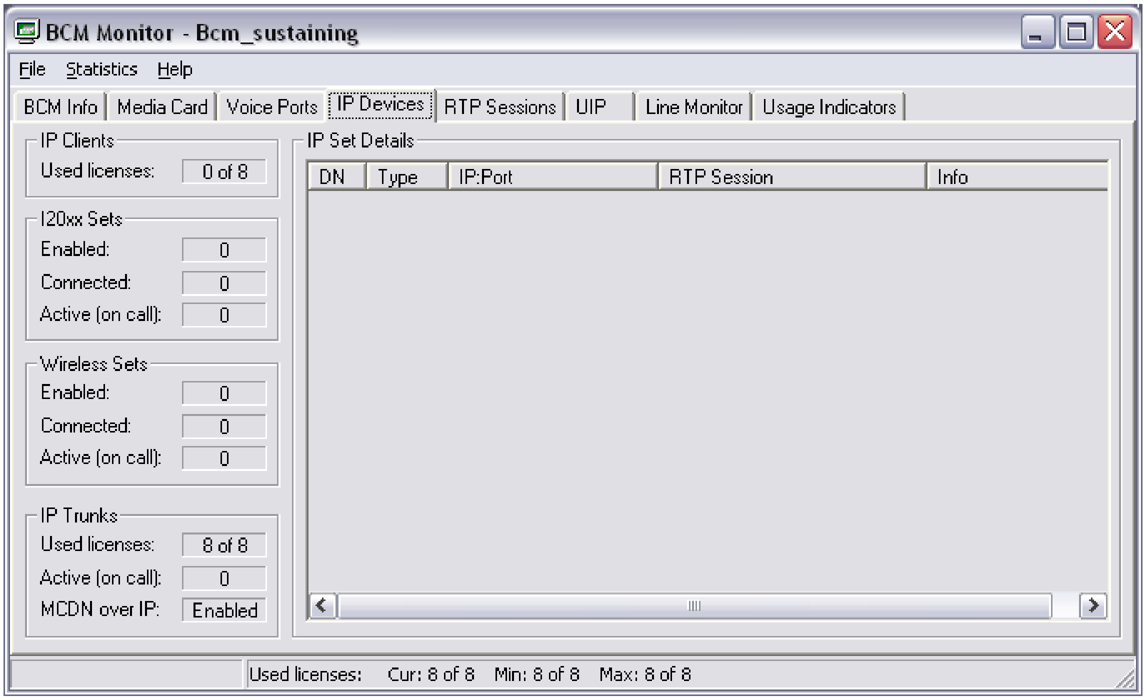
IP Devices tab

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: BCM50 release 1.0 does not support wireless sets.

Note: IVR is supported on the BCM3.x release level for BCM200, BCM400, and BCM1000, but it is not supported on the BCM50.

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.



IP Clients

Used licenses: 0 of 8

I20xx Sets

Enabled: 0

Connected: 0

Active (on call): 0

Wireless Sets

Enabled: 0

Connected: 0

Active (on call): 0

IP Trunks

Used licenses: 8 of 8

Active (on call): 0

MCDN over IP: Enabled

IP Set Details

DN	Type	IP:Port	RTP Session	Info

Used licenses: Cur: 8 of 8 Min: 8 of 8 Max: 8 of 8

RTP Sessions tab

The RTP Sessions tab shows details about RTP (Real Time Protocol over UDP) sessions, which involve either the BCM50 system or an IP set controlled by the BCM50 system.

You can use the information in this tab to monitor the direct path between two IP sets.

The tab displays information about:

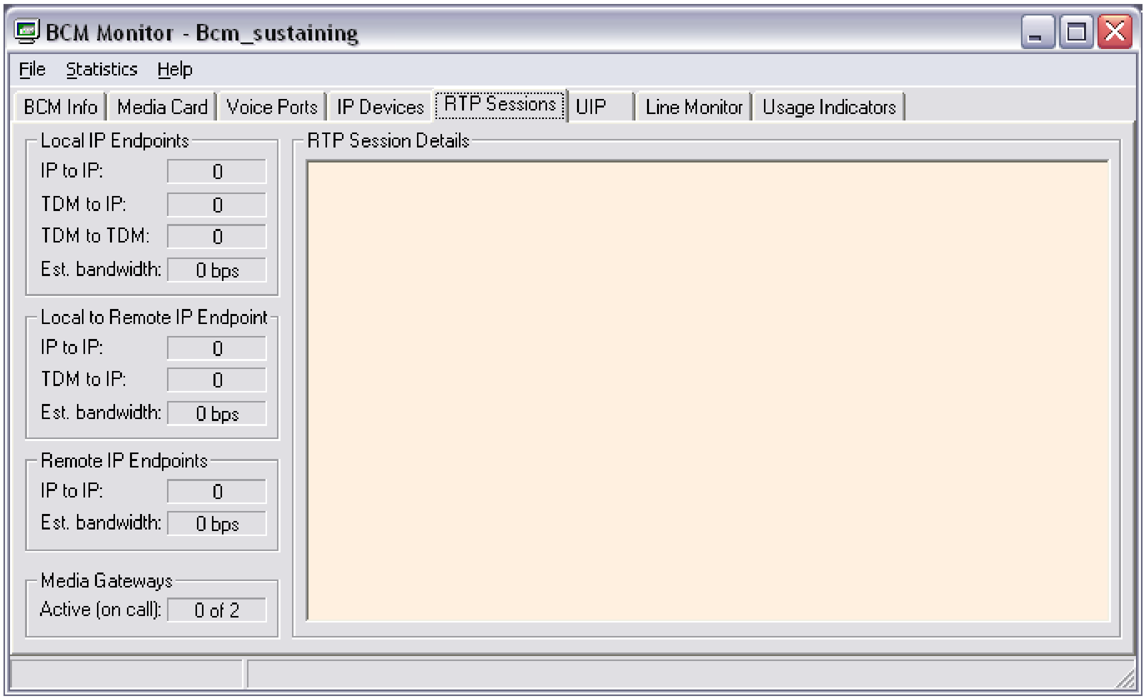
- local IP endpoints (two sets both connected to the BCM50)
  - combinations of IP to IP, TDM to IP, and TDM to TDM
  - an estimate of network traffic generated by RTP sessions between TDM devices or local IP devices
- local to remote IP endpoints
  - combinations of IP to IP, TDM to IP
  - an estimate 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 269.



Local IP Endpoints
IP to IP: 0
TDM to IP: 0
TDM to TDM: 0
Est. bandwidth: 0 bps

Local to Remote IP Endpoint
IP to IP: 0
TDM to IP: 0
Est. bandwidth: 0 bps

Remote IP Endpoints
IP to IP: 0
Est. bandwidth: 0 bps

Media Gateways
Active (on call): 0 of 2

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 BCM50.

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 BCM50 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
- Select the type of ISDN module or modules connected to the expansion module that you selected in step 3.
- PRI — enables monitoring of a DTI module that is connected to the expansion 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 BRI - Bus 5, then select Module 1 - Loop 1
- Select BRI - Bus 5, then select Module 1 - Loop 2
- Select PRI 6

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 deselet 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 BCM50 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 BCM50 (> 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

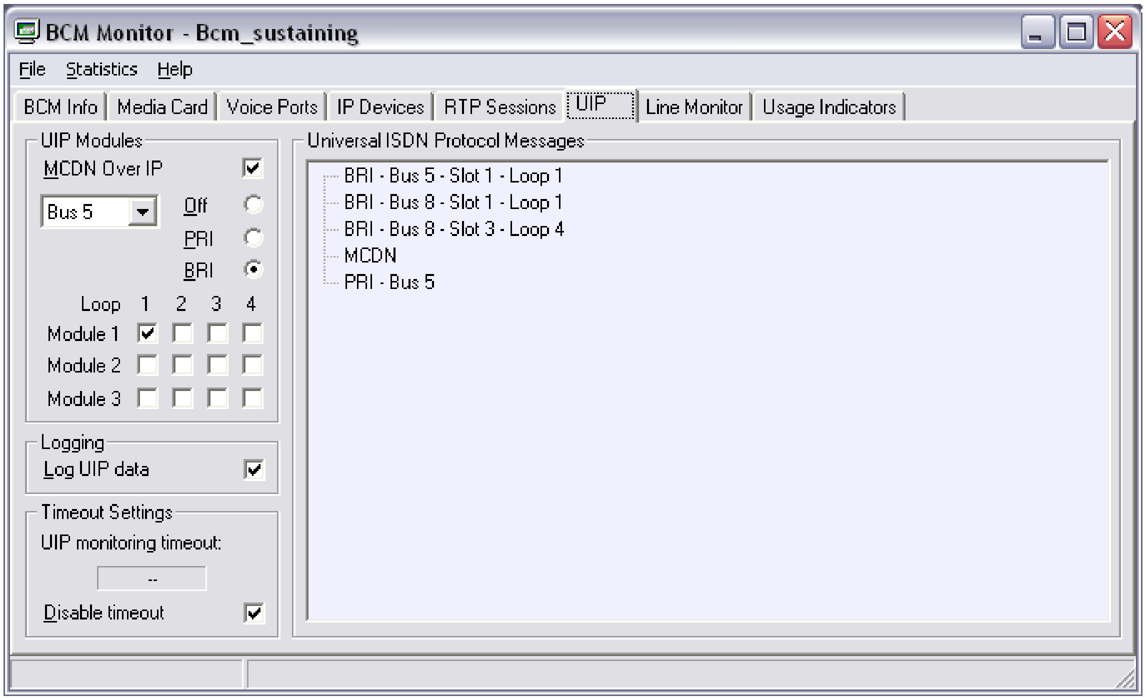
1 Click the **UIP** tab.
The **Universal ISDN Protocol Messages** area displays detailed information about monitored UIP modules.

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.



UIP Modules
MCDN Over IP ☑
Bus 5
Off ○
PRI ○
BRI ●

Loop	1	2	3	4
Module 1	☑	□	□	□
Module 2	□	□	□	□
Module 3	□	□	□	□

Logging
Log UIP data ☑

Timeout Settings
UIP monitoring timeout:
--
Disable timeout ☑

Universal ISDN Protocol Messages
BRI - Bus 5 - Slot 1 - Loop 1
BRI - Bus 8 - Slot 1 - Loop 1
BRI - Bus 8 - Slot 3 - Loop 4
MCDN
PRI - Bus 5

Line Monitor tab

The Line Monitor tab shows the status of lines on the BCM50 system. You can view the number of active lines, and view all lines on the BCM50 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 BCM50; “Incoming” indicates that the call originated from outside and is directed at the BCM50
- start time — displays the time and date on which the call started
- user — displays the DN and name of the BCM50 user
- state — displays Idle if there is no active call on the line; displays Dialing if the BCM50 user is in the process of dialing digits to place a call; dispalys Alerting if a call has been received on the line and a BCM50 user’s phone is ringing; displays Connected if the line has a connected call; displays Held if the line has a call on hold.

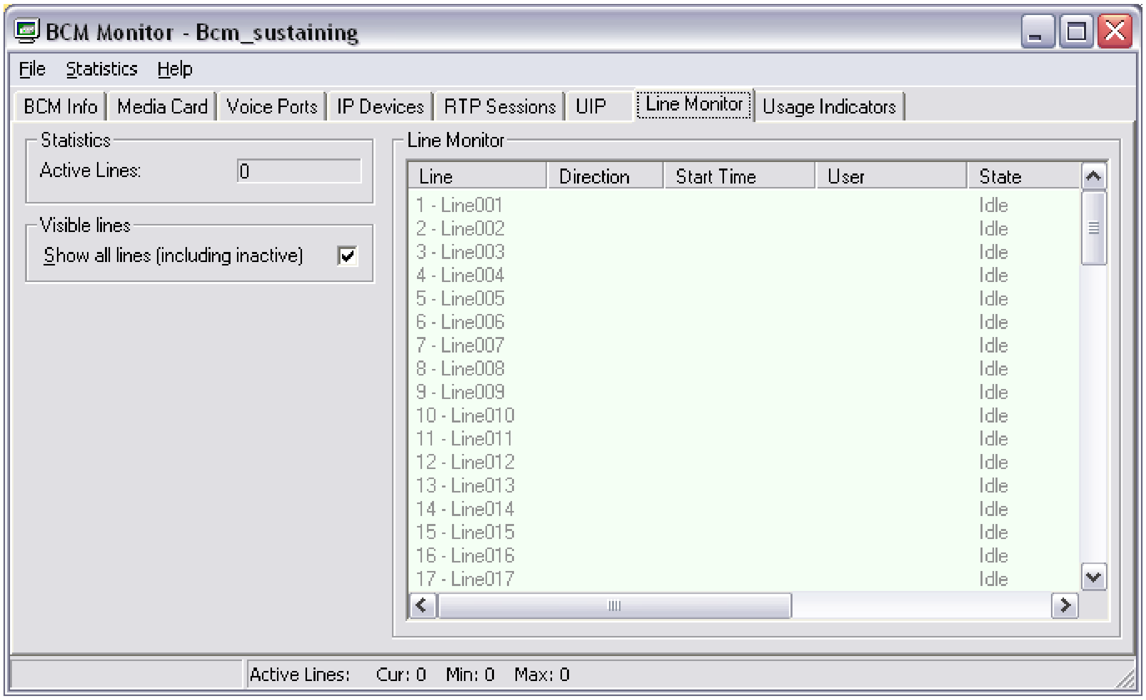
In the line monitor area, colours are used to indicate the state of each line:

- 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 BCM50 system. For lines displayed in light gray, previous calls are shown until a new call is placed or received on that line.



Statistics
Active Lines: 0

Visible lines
Show all lines (including inactive) ☑

Line Monitor

Line	Direction	Start Time	User	State
1 - Line001				Idle
2 - Line002				Idle
3 - Line003				Idle
4 - Line004				Idle
5 - Line005				Idle
6 - Line006				Idle
7 - Line007				Idle
8 - Line008				Idle
9 - Line009				Idle
10 - Line010				Idle
11 - Line011				Idle
12 - Line012				Idle
13 - Line013				Idle
14 - Line014				Idle
15 - Line015				Idle
16 - Line016				Idle
17 - Line017				Idle

Active Lines: Cur: 0 Min: 0 Max: 0

Usage Indicators tab

The Usage Indicators tab displays real time information about the BCM50 system.

The tab displays the following information:

- BCM50 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

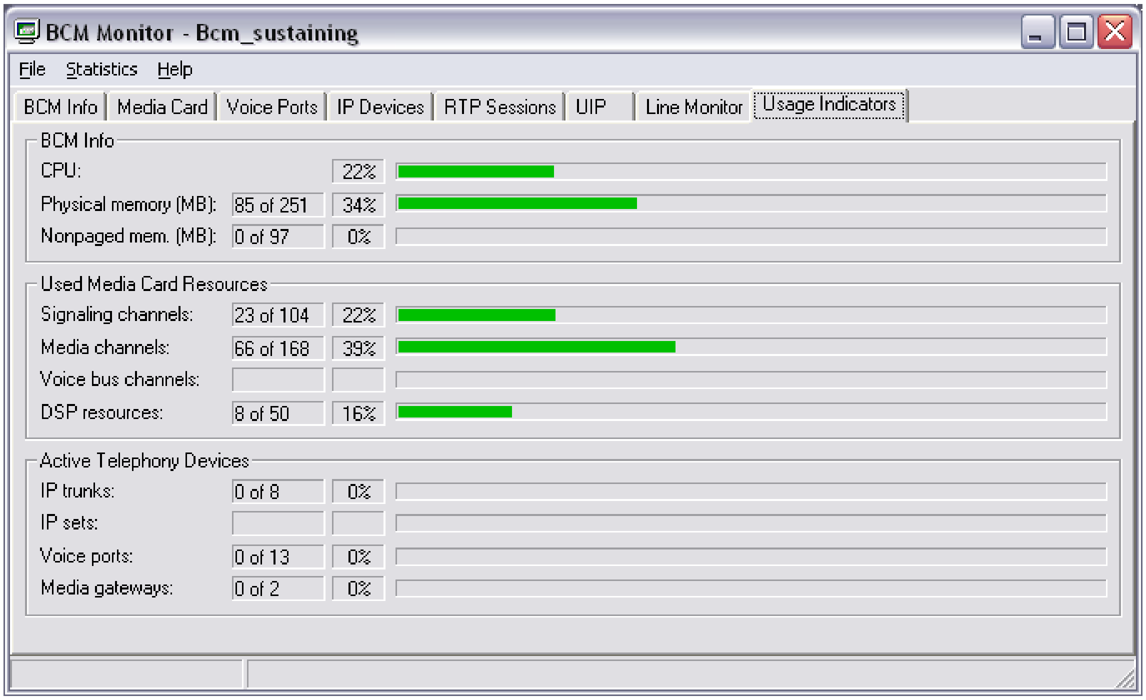
The information is displayed as an absolute figure and as a percentage of the resource used. You can capture a static snapshot of this information or log it dynamically. For more information about snapshots, see "Using BCM Monitor to analyze system status" on page 253.

Usage values

Usage values are accompanied by a colored bar. Table 59 describes the usage value indicators and recommended actions.

Table 59 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.



BCM Info

CPU:		22%
Physical memory (MB):	85 of 251	34%
Nonpaged mem. (MB):	0 of 97	0%

Used Media Card Resources

Signaling channels:	23 of 104	22%
Media channels:	66 of 168	39%
Voice bus channels:		
DSP resources:	8 of 50	16%

Active Telephony Devices

IP trunks:	0 of 8	0%
IP sets:		
Voice ports:	0 of 13	0%
Media gateways:	0 of 2	0%

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.

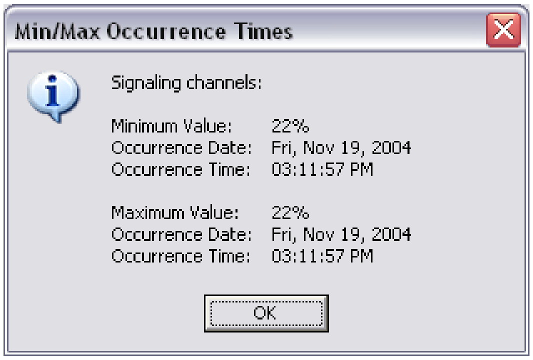
Viewing the date and time of minimum and maximum values

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.



Signaling channels:

Minimum Value:	22%
Occurrence Date:	Fri, Nov 19, 2004
Occurrence Time:	03:11:57 PM
Maximum Value:	22%
Occurrence Date:	Fri, Nov 19, 2004
Occurrence Time:	03:11:57 PM

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.

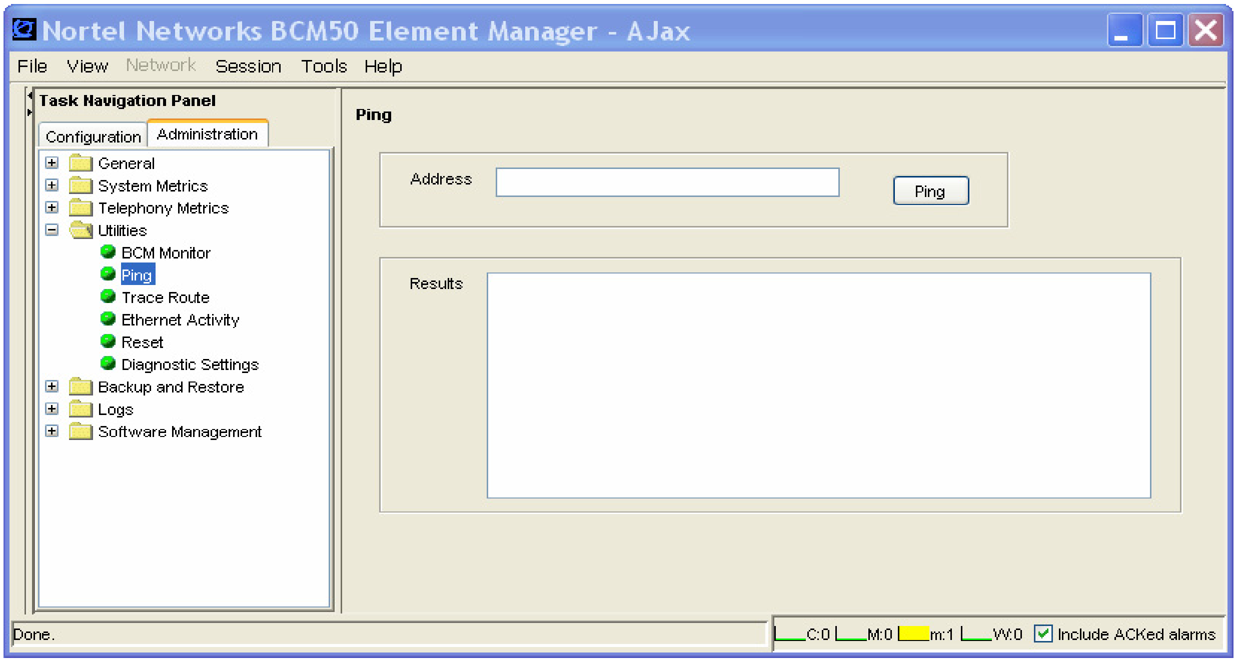
2 Do one of the following:

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 BCM50 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.

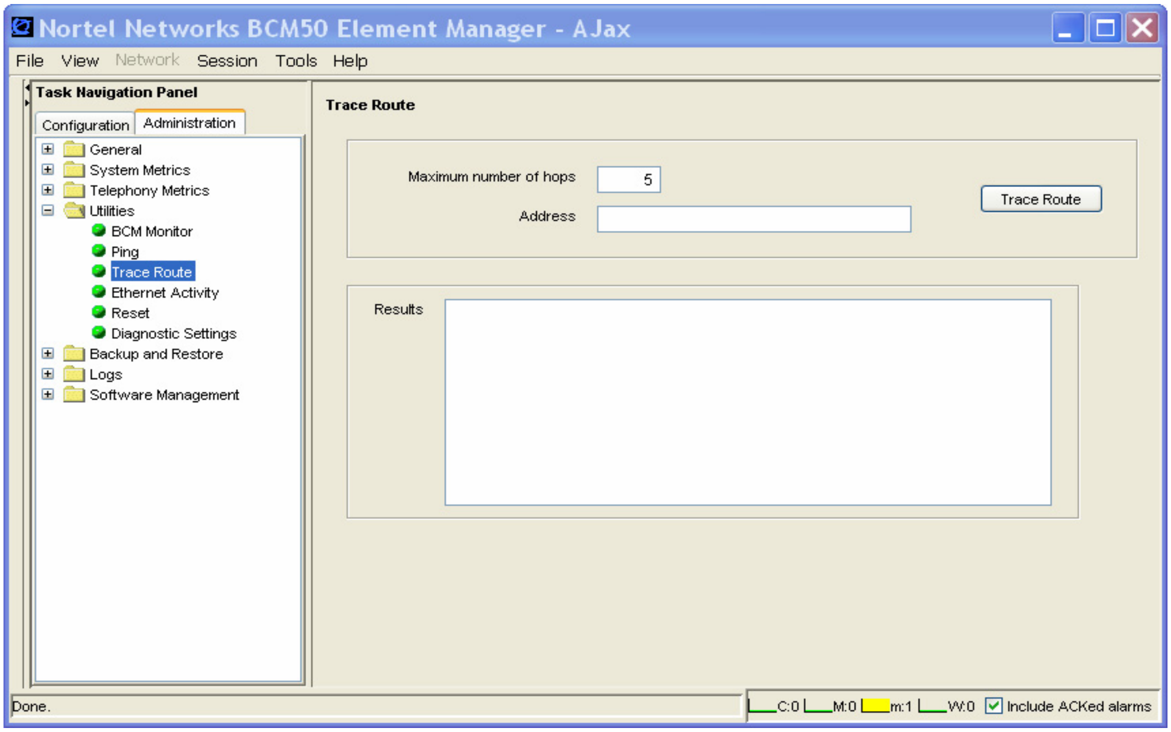
Trace Route

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:



Maximum number of hops 5

Address

☑ Include ACKed alarms

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.

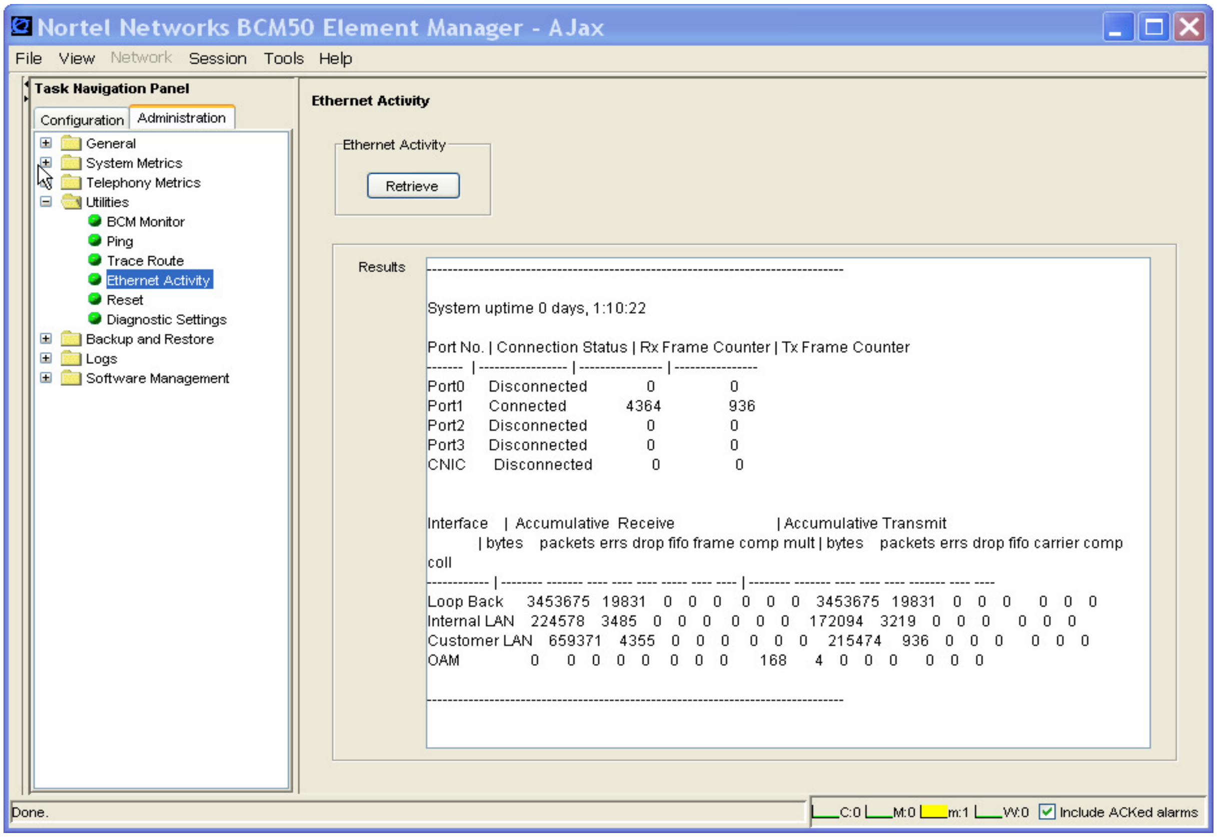
3 In the **Maximum Number of Hops** field, enter the maximum number of hops on the route.
The default is 5 hops.

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.

Ethernet Activity

The Ethernet Activity panel, shown below, is a utility that you can use to view ethernet activity in the BCM50 system.



```
--------------------------------------------------------------------------------


System uptime 0 days, 1:10:22

Port No. | Connection Status | Rx Frame Counter | Tx Frame Counter
-------  | ----------------- | ---------------- | ----------------
Port0     Disconnected          0              0
Port1     Connected           4364            936
Port2     Disconnected          0              0
Port3     Disconnected          0              0
CNIC       Disconnected          0              0



Interface    | Accumulative  Receive                    | Accumulative Transmit
          | bytes    packets errs drop fifo frame comp mult | bytes    packets errs drop fifo carrier comp
coll
------------ | -------- ------- ---- ---- ---- ----- ---- ---- | -------- ------- ---- ---- ---- ------- ---- ----
Loop Back     3453675  19831   0   0   0    0   0   0   3453675  19831   0   0   0     0   0   0
Internal LAN   224578   3485   0   0   0    0   0   0   172094   3219   0   0   0     0   0   0
Customer LAN   659371   4355   0   0   0    0   0   0   215474    936   0   0   0     0   0   0
OAM             0      0   0   0   0    0   0   0     168     4   0   0   0     0   0   0


--------------------------------------------------------------------------------
```

To view Ethernet activity

1 Click the **Administration** tab.

2 Open the **Utilities** folder, and then click **Ethernet Activity**.
The **Ethernet Activity** panel opens.

3 In the Ethernet Activity area, click the **Retrieve** button.
Details are displayed in the **Results** area.

Reset

You can use the Reset utility to:

- reboot the BCM50 system
- perform a warm reset of telephony services
- perform a cold reset of telephony services
- perform a cold reset of the optional integrated router

Table 60 lists the Reset functions.

Table 60 Reset functions

Function	Description	Impact
Reboot BCM50 System	Restarts the operating system of the BCM50 system	Temporarily stops all services on the system. Restarts all services. This operation does not affect configuration parameters or programming.
Warm Reset Telephony Services	Restarts telephony services running on the BCM50 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 BCM50 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.
Cold Reset Router	Resets router programming to the factory default for that software level	Affects BCM50 services that rely on the WAN.

Rebooting the BCM50 system

Caution: Rebooting the BCM50 system temporarily stops all services running on the system.

To reboot the BCM50

1. Click the **Administration** tab.
2. Open the **Utilities** folder, and then click **Reset**.
   The **Reset** panel opens.
3. Click the **Reboot BCM50 System** button.
   A confirmation dialog box opens.

4 Click the **OK** button.
The operating system of the BCM50 restarts.

Performing a warm reset of BCM50 telephony services

⛔ **Caution:** All active calls on the BCM50 system will be dropped.

To perform a warm reset of BCM50 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 BCM50 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 BCM50 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 61 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.

5 Click the **OK** button.
All telephony services are reset, including LAN CTE, Voicemail, and IP telephony.

Performing a cold reset of the BCM50 router

Caution: Performing a hard reset of the optional integrated router affects all services relying on the WAN.

To perform a cold reset of the BCM50 route

1 Click the **Administration** tab.

2 Open the **Utilities** folder, and then click **Reset**.
The **Reset** panel opens.

3 Click the **Cold Reset Router** button.
A confirmation dialog box opens.

4 Click the **OK** button.
The router programming is reset to the factory default values for that software level.

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

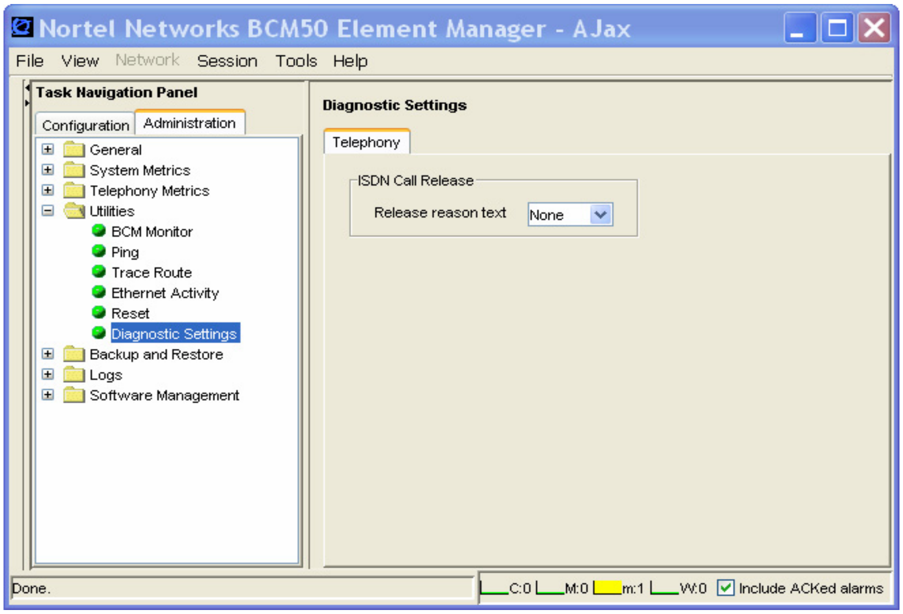
To set Release reasons, follow these steps:

1 Click **Administration**, **Utilities**, **Diagnostic settings**.

2 Click the **Telephony** tab.

The **Release Reasons** panel appears. See Figure 48.

Figure 48 Telephony diagnostic settings



Release reason text: None

☑ Include ACKed alarms

3 From the Release Reason drop-down menu, select the level of reporting that you require. Table 62 lists the possible values for Release reasons.

Table 62 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.
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.

Chapter 11
Backing Up and Restoring BCM50 Data

This chapter provides information about how to back up and restore data from the BCM50 system.

Overview of backing up and restoring data

A system administrator programs the BCM50 to support required services. Programming the BCM50 results in configuration data. As end users use the system, additional data is generated. This type of data is application data.

Before you make administrative changes or as your BCM50 system accumulates information, you can backup to another location on the network. At a later time, you can restore the data to the BCM50.

Note: Nortel recommends that you back up BCM50 data, including router configuration data, on a regular basis. In particular, you should perform a backup of the BCM50 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 BCM50 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 schedule backup operations to occur at specified times, and save a record of the backup schedule that you set. For information about the programming record, see “Saving programming records” on page 66.

Backing up and restoring router configuration data

If the BCM50 unit includes an integrated router, you can back up the router configuration data using the BCM50 integrated router WebGUI.

For information about backing up router configuration data, see the *BCM50 Integrated Router Configuration Guide*. If you have a BCM50e or BCM50a model, see the *BCM50e/a Integrated Router Configuration Guide*.

Note: The rest of this module contains information about using the BCM50 Element Manager to perform backup and restore operations on the BCM50 main unit, exclusive of the integrated router.

Backup and restore options

You can back up and restore configuration data or application data. If you select application data, both configuration data and application data is backed up or restored.

You can exclude Voicemail and Call Center from a backup operation if you want to perform a backup that does not affect the system, or include them and perform a backup at a time when the system is typically not in use.

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. A restore operation can be performed on demand only.

You can back up data to different locations, including:

- the BCM50 hard drive
- remote resources
- a USB storage device

Whichever destination you choose, a copy of the most recent backup always remains on the BCM50. You can use this to restore your BCM50 without transferring a backup from an external device or server.

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 "Managing BCM50 Logs," on page 315.

About configuration backups

A configuration backup backs up the configuration of the BCM50 system. This includes the configuration of relevant embedded third-party software, but does not include configuration of the optional integrated router.

Caution: A backup operation will interrupt BCM50 services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them and perform a backup at a time when the system is typically not in use.

Examples of configuration data include:

- IP configuration details
- telephony programming
- SNMP settings
- Call Detail Recording settings
- BCM50 schedules (for example, the backup schedule, and the log retrieval schedule)
- greetings
- prompts

The backup task collects the BCM50 system configuration information quickly.

Configuration backups can be performed to a location that you specify, on demand or according to a schedule.

About application backups

An application backup collects all the configuration data that is collected in a configuration backup, as well as data generated during the normal operation of the BCM50 system.

Examples of application data include:

- voicemail messages
- Call Detail Records
- faxes
- email text-to-speech
- envelope information

Caution: A backup operation interrupts voicemail services if Voicemail and Call Center services are included in the backup. The interruption period varies with the amount of voicemail that your BCM50 has accumulated. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them and perform a backup at a time when the system is typically not in use.

Caution: If the system has many users with many saved voicemails, the Application backup task can take 30 minutes or more to collect the BCM50 system configuration and application data. The resulting data file may be quite large.

The BCM50 can accommodate an application backup file that is greater than 500 MB. To minimize the size of the backup file, exclude Voicemail and Call Center from the backup operation. The BCM50 will compress some files 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 BCM50 Element Manager.

BCM50 backup file

When you perform a backup operation, the BCM50 creates an archive file that is stored at a location that you specify. The archive file includes embedded archive files, each of which represent a different part of the BCM50 system:

- backup.sig — ensures the integrity of the file
- backup.md5sum — uses a checksum algorithm to ensure the integrity of each file in the archive file
- various archive files — various archive files that contain the configuration and application 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 are named according to the backup type performed and the system name of the BCM50. An application backup file is prefixed with App_. A configuration backup archive is prefixed with Cfg_.

Backup destinations

Table 63 lists the destinations to which you can back up configuration and application data. Each backup operation, regardless of destination, replaces the BCM50's own copy of the backup.

Table 63 Backup destinations

Destination	Description
BCM50	For an immediate backup, saves data to the hard drive of the BCM50. You cannot specify a path. Each backup rewrites any pre-existing backup of the same type.
My Computer	For an immediate backup, saves data to any accessible location on the client PC on which the BCM50 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 files 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.
FTP Server	Saves backup data 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 BCM50 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 data to an SFTP server. This method sends encrypted login credentials and backup data. You must set up the remote SFTP server to allow the BCM50 to communicate with the SFTP server. The BCM50 system can generate a public SSH key, which you must install on the remote SFTP server. For information about SSH keys, see the chapter BCM50 Security.

For more information about how to access and use the storage locations, see "BCM50 common file input/output processes" on page 74.

Before you back up BCM50 data, make sure that the BCM50 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 BCM50 and the network folder are on different networks, configure the BCM50 to use a DNS server. The Windows 98 SE computer name must be identical to the DNS hostname entry for that computer.

If the BCM50 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 Configuration or Application backups to the following storage locations:

- BCM50
- client PC
- network folder
- USB storage device
- FTP server
- SFTP sever

Performing an immediate backup to the BCM50

Caution: A backup operation will interrupt voicemail services if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or include them and perform a backup at a time when the system is typically not in use.

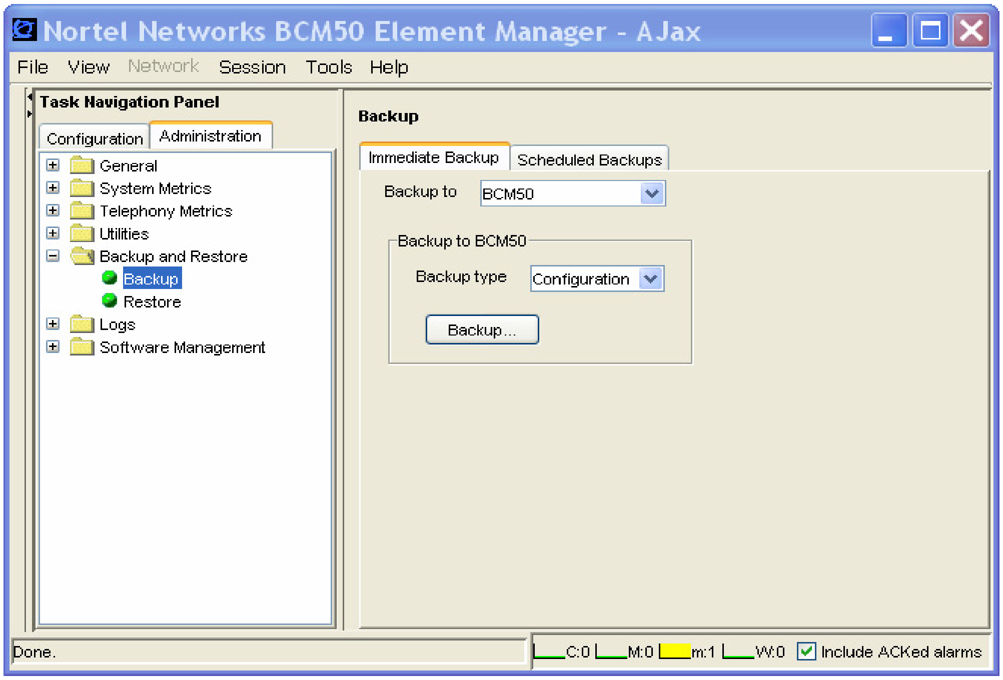
To perform an immediate backup to the BCM50

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 **BCM50**.
3. In the Backup Type selection field, select one of the following:

- **Configuration**
- **Application**

4 Click the **Backup** button.
The **Backup** window opens.

5 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.



Backup to: BCM50

Backup type: Configuration

Done.

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 appears.

8 Click the **OK** button.

Performing an immediate backup to your personal computer

Caution: A backup operation interrupts voicemail service if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or include them 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.**

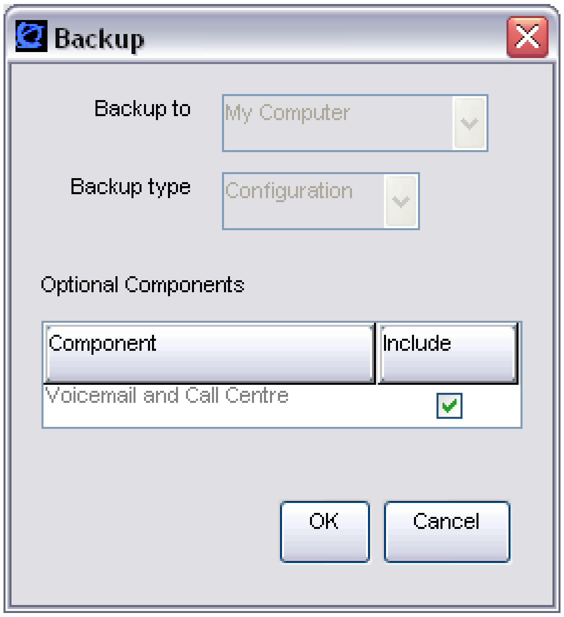
4 In the Backup Type selection field, select one of the following:

   a **Configuration**

   b **Application**

5 Click the **Backup** button.
The **Backup** window opens.

6 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.



Backup to: My Computer

Backup type: Configuration

Optional Components

Component	Include
Voicemail and Call Centre	☑

7 Click the **OK** button.
A warning message appears.

8 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Save** window opens.

9 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.

10 Click the **Save** button.
When the backup is complete the **Backup Complete** window opens.

11 Click the **OK** button.

Performing an immediate backup to a network folder

⛔ **Caution:** A backup operation interrupts voicemail services if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the Backup Type selection field, select one of the following:

   a **Configuration**

   b **Application**

Configure the Network Folder attributes.

Table 64 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).

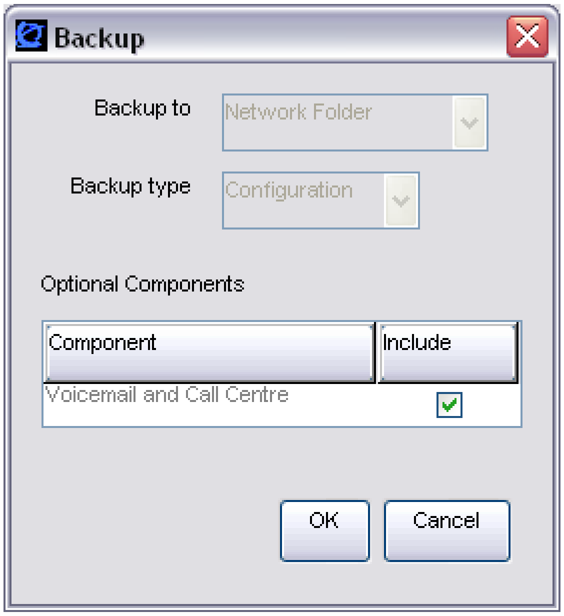
Note: When you backup to a network folder hosted in a computer running Windows 98 SE, you cannot specify an IP address in the folder name. You must specify the computer name in the network folder name. For example, enter \\<computer>\<resource>.

If the BCM50 and the network folder are on different networks, configure the BCM50 to use a DNS server. The Windows 98 SE computer name must be identical to the DNS hostname entry for that computer.

If the BCM50 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 **Voicemail and Call Center** to include or exclude these components from the backup operation.



Backup to: Network Folder

Backup type: Configuration

Optional Components

Component	Include
Voicemail and Call Centre	☑

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** window opens.

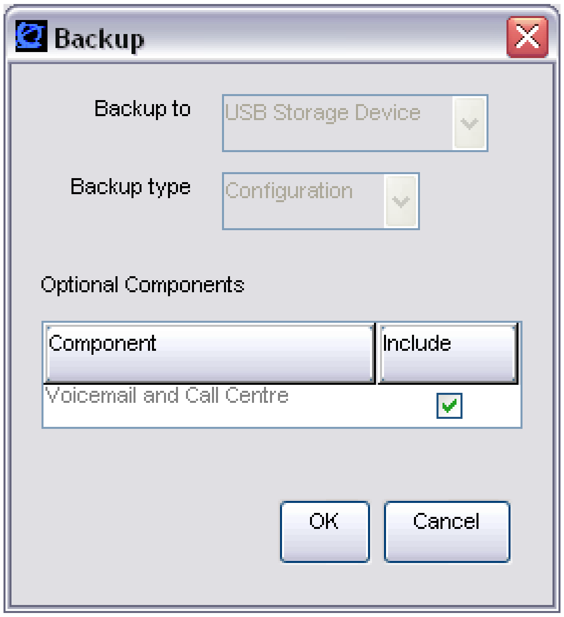
9 Click the **OK** button.

Performing an immediate backup to a USB storage device

Caution: A backup operation interrupts voicemail services if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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. In the **Backup Type** selection field, select one of the following:
   - a **Configuration**
   - b **Application**
5. Click the **Backup** button.
   The **Backup** window opens.



Backup to: USB Storage Device

Backup type: Configuration

Optional Components

Component	Include
Voicemail and Call Centre	☑

6. In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** 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 is complete, the **Backup Complete** window opens.

9 Click the **OK** button.

Performing an immediate backup to an FTP server

Caution: A backup operation interrupts voicemail services if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the Backup Type selection field, select one of the following:

- **Configuration**
- **Application**

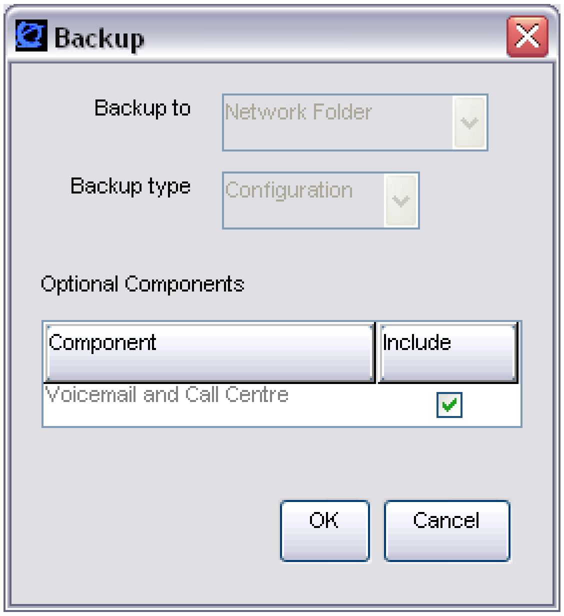
5 Configure the FTP Server attributes.

Table 65 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).

6 Click the **Backup** button.
The **Backup** window opens.

7 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.



Backup to: Network Folder

Backup type: Configuration

Optional Components

Component	Include
Voicemail and Call Centre	☑

8 Click the **OK** button.
A warning window opens.

9 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Backup Complete** window opens.

10 Click the **OK** button.

Performing an immediate backup to an SFTP server

Caution: A backup operation interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the Backup Type selection field, select one of the following:

- **Configuration**

- **Application**

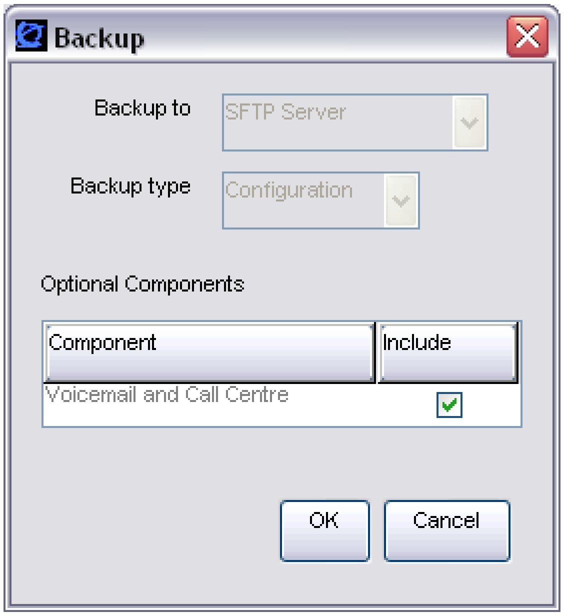
5 Configure the SFTP Server attributes.

Table 66 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.

6 Click the **Backup** button.
The **Backup** window opens.

7 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.



Backup to: SFTP Server

Backup type: Configuration

Optional Components

Component	Include
Voicemail and Call Centre	☑

8 Click the **OK** button.
A warning window opens.

9 Click the **Yes** button to proceed.
A progress window opens. When the backup preparation is complete, the **Backup Complete** window opens.

10 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 interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them and perform a backup at a time when the system is typically not in use.

Table 67 lists the information that is displayed in the Scheduled Backups table.

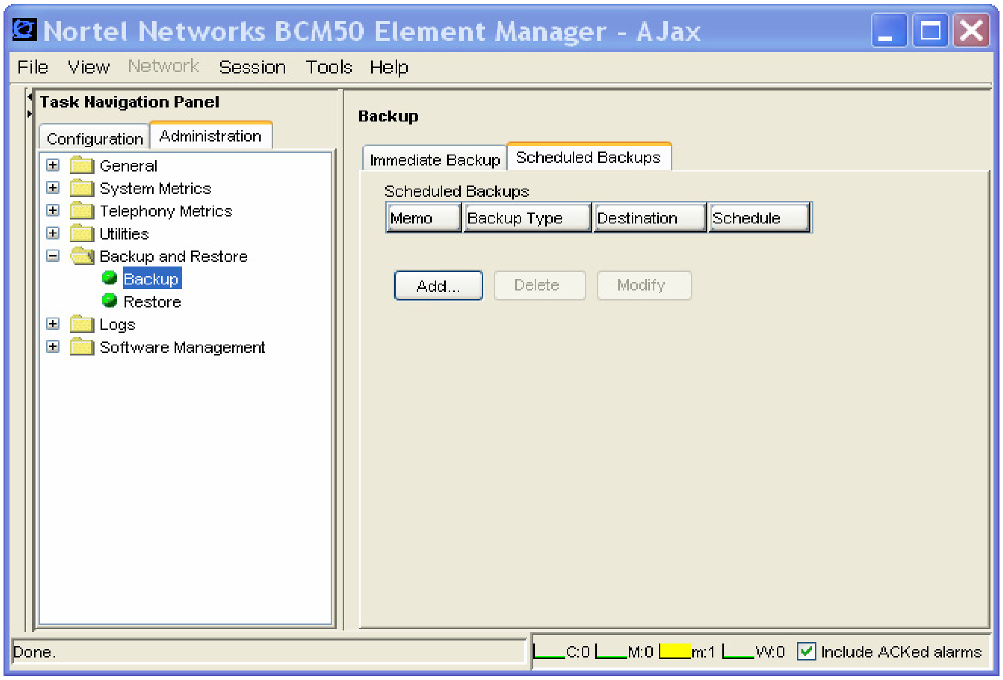
Table 67 Information displayed in the Scheduled Backups table

Column	Description
Memo	Displays the memo for the scheduled backup.
Backup Type	Displays the type of scheduled backup that will be performed: Application or Configuration.
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 BCM50

Caution: A backup operation interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them and perform a backup at a time when the system is typically not in use.

To perform a scheduled backup to the BCM50

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 **BCM50**.
5. In the **Backup Type** selection field, select one of the following:
   a. **Configuration**
   b. **Application**

6 Click the **OK** button.
The **Add Scheduled Backup** window opens.

7 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.Click the **OK** button.

8 Configure the schedule attributes.

Table 68 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 a network folder

Caution: A backup operation interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the **Backup Type** selection field, select one of the following:

   a **Configuration**

   b **Application**

7 Configure the Network Folder attributes.

Table 69 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).

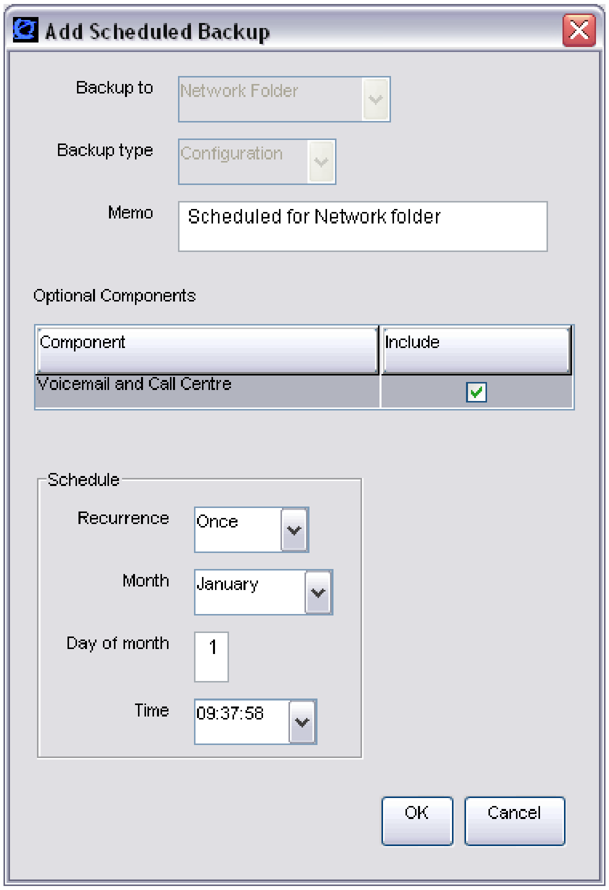
8 Click the **OK** button.
The **Add Scheduled Backup** window opens

9 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.

10 Configure the schedule attributes.

Table 70 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.



Backup to: Network Folder

Backup type: Configuration

Memo: Scheduled for Network folder

Optional Components

Component	Include
Voicemail and Call Centre	☑

Schedule

Recurrence: Once

Month: January

Day of month: 1

Time: 09:37:58

11 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 interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the **Backup Type** selection field, select one of the following:

   a **Configuration**

   b **Application**

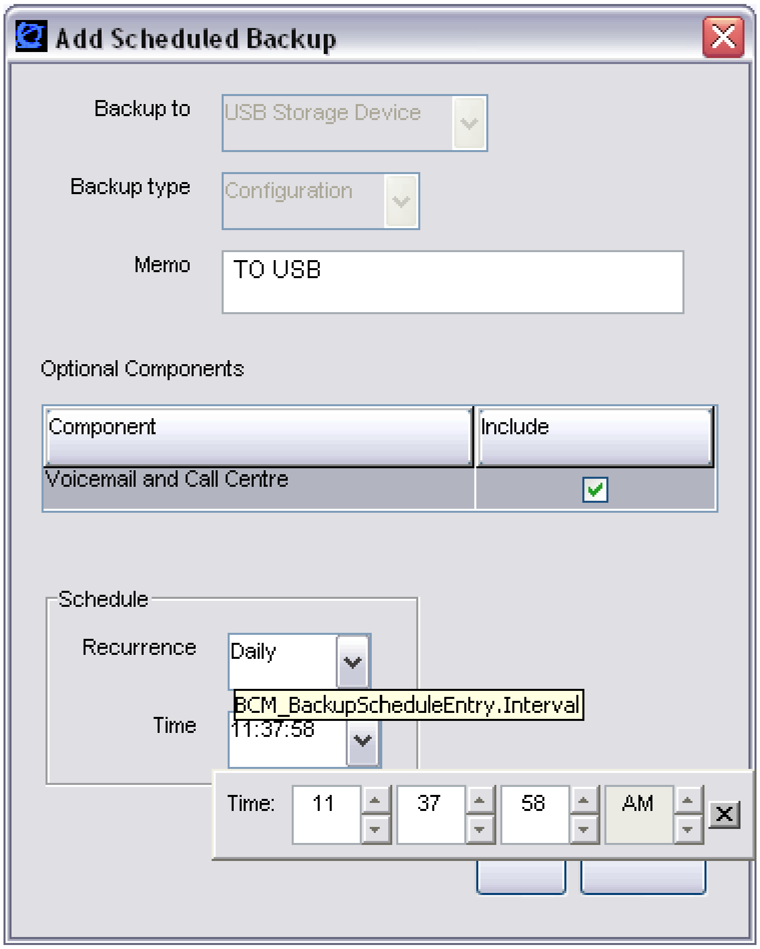
7 Click the **OK** button.
The **Add Scheduled Backup** window opens

8 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.

9 Configure the schedule attributes.

Table 71 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.



Backup to: USB Storage Device

Backup type: Configuration

Memo: TO USB

Optional Components

Component	Include
Voicemail and Call Centre	☑

Schedule

Recurrence: Daily

Time: 11:37:58

BCM_BackupScheduleEntry.Interval

Time: 11 37 58 AM

10 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 interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the **Backup Type** selection field, select one of the following:

a **Configuration**

b **Application**

7 Configure the FTP Server attributes.

Table 72 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).

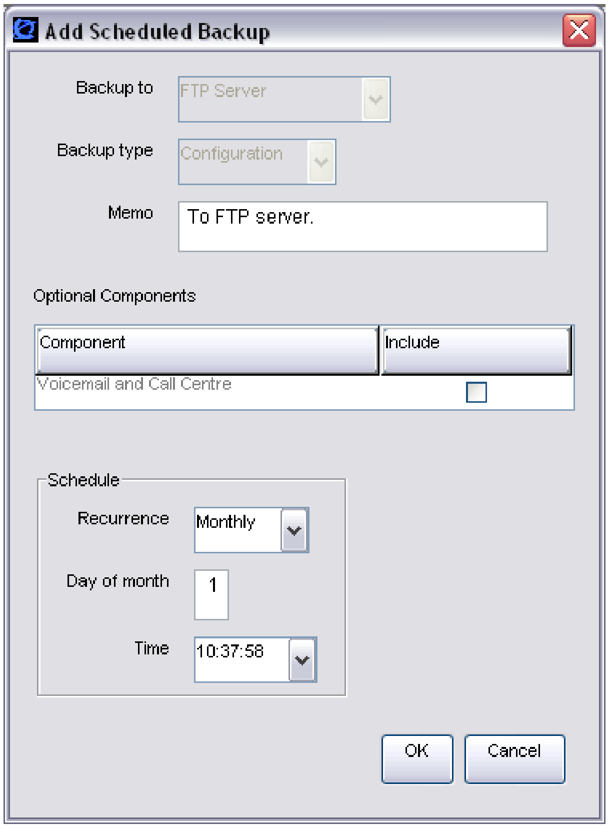
8 Click the **OK** button.
The **Add Scheduled Backup** window opens.

9 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.

10 Configure the schedule attributes.

Table 73 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.


Add Scheduled Backup

Backup to: FTP Server

Backup type: Configuration

Memo: To FTP server.

Optional Components

Component	Include
Voicemail and Call Centre	□

Schedule

Recurrence: Monthly

Day of month: 1

Time: 10:37:58

11 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 interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them 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 In the **Backup Type** selection field, select one of the following:

  a **Configuration**

  b **Application**

7 Configure the SFTP Server attributes.

Table 74 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).

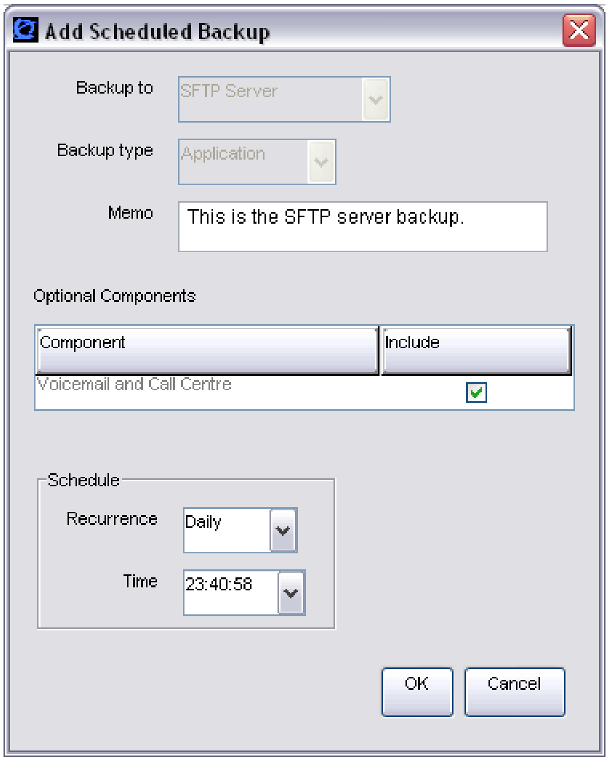
8 Click the **OK** button.
The **Add Scheduled Backup** window opens.

9 In the **Optional Components** table, select or clear the check box for **Voicemail and Call Center** to include or exclude these components from the backup operation.

10 Configure the schedule attributes.

Table 75 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.



Backup to: SFTP Server

Backup type: Application

Memo: This is the SFTP server backup.

Optional Components

Component	Include
Voicemail and Call Centre	☑

Schedule

Recurrence: Daily

Time: 23:40:58

11 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 interrupts voicemail services for several minutes if Voicemail and Call Center services are included in the backup. You can exclude these components from the backup if you want to perform a backup that does not affect the system, or you can include them and perform a backup at a time when the system is typically not in use.

To modify a scheduled backup

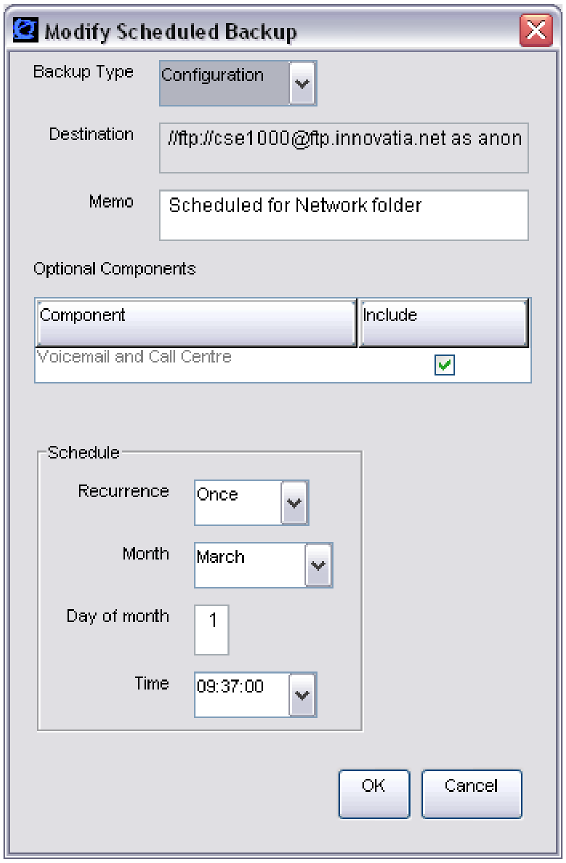
1 In the task panel, click the **Administration** tab.

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.



Modify Scheduled Backup

Backup Type: Configuration

Destination: //ftp://cse1000@ftp.innovatia.net as anon

Memo: Scheduled for Network folder

Optional Components

Component	Include
Voicemail and Call Centre	☑

Schedule

Recurrence: Once

Month: March

Day of month: 1

Time: 09:37:00

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 293.
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 BCM50 system data

You can restore BCM50 configuration and application data using the BCM50 Element Manager.

The restore software determines compatibility with the backup file. 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 BCM50 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 BCM50 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 BCM50 or from an external storage location. For information about storage locations, see "Backup destinations" on page 283.

When you restore data, the following details are available to you:

- the type of backup you have chosen (Configuration or Application)
- 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.

Backup information can be restored only to another unit that has an older software release level. If the second unit has an older software release level, you can use the Reset button on the BCM50 front panel to reset the BCM50 unit to the factory default software level and default configuration settings. You can then apply software updates to bring the unit to the same software release level as that of the unit from which the backup was taken.

For information about applying software updates to the BCM50, see "Managing BCM50 Software Updates," on page 341.

The BCM50 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 BCM50 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
- Core Telephony
- Resources
- Date and Time
- Dial-In/Dial-Out
- IP Telephony
- Keycodes (available when the restore device is the originating device)
- Network
- SNMP
- Scheduling
- Security
- LAN CTE
- QoS Monitor
- Voicemail and Call Centre

Effects on the system

A restore operation is a service-affecting operation. A number of services running on the BCM50 system are stopped and then restarted using the restored configuration or application data. A reboot is required if you choose to restore the Keycodes component. It takes several minutes before Voicemail is working again.

Table 76 lists the effects of restoring optional components.

Table 76 Effects of a restore operation on the system

Component	**Effect**
Core Telephony	System interruption.
IP Telephony	System interruption.
Keycodes	Reboots the BCM50.
Network	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 <archiversystemlog>.

For information about BCM50 logs, see "Managing BCM50 Logs," on page 315.

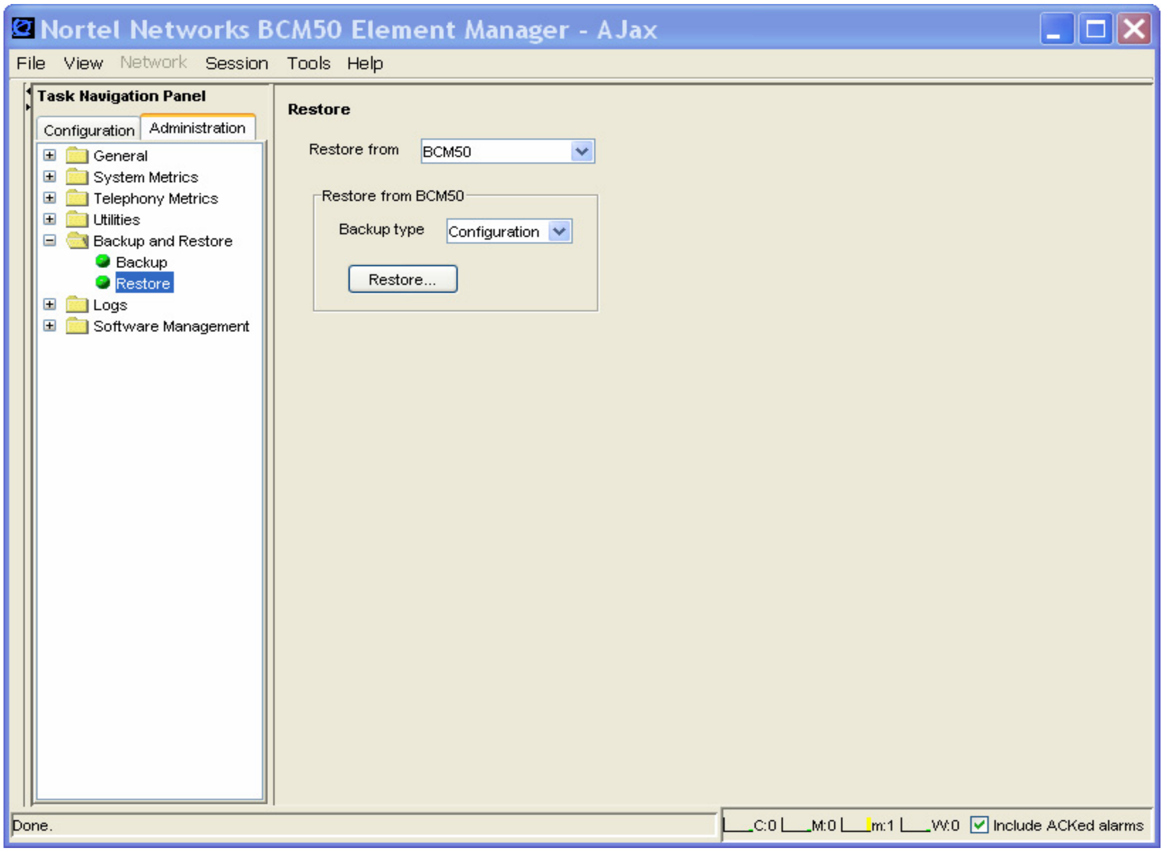
Restoring data from the BCM50

Caution: A restore operation is a service-affecting operation. A number of services running on the BCM50 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 the BCM50

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 **BCM50** as a default value.



Restore from: BCM50

Backup type: Configuration

Done.

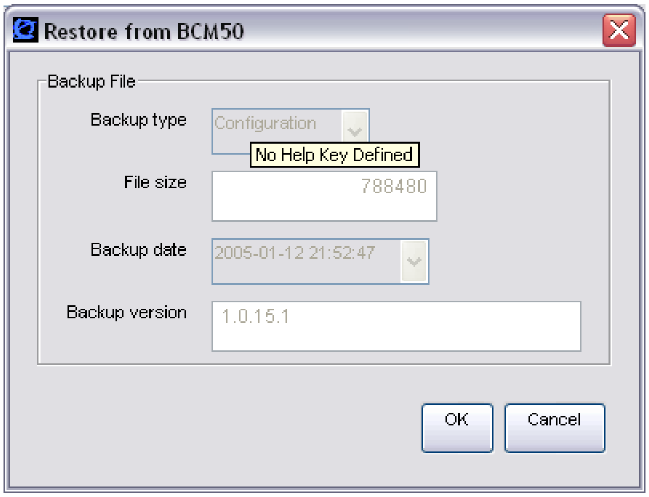
C:0 M:0 m:1 W:0 ☑ Include ACKed alarms

3 In the **Backup Type** selection field, select one of the following:

a **Configuration**

b **Application**

4 Click the **Restore** button.
The **Restore From BCM50** window opens.



Restore from BCM50

Backup File

Backup type: Configuration

No Help Key Defined

File size: 788480

Backup date: 2005-01-12 21:52:47

Backup version: 1.0.15.1

5 Click the **OK** 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 your personal computer

Caution: A restore operation is a service-affecting operation. A number of services running on the BCM50 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 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 In the **Backup Type** selection field, select one of the following:

- **Configuration**
- **Application**

5. Click the **Restore** button.
   The **Open** window opens.
6. Select the backup file, and then 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 restore operation is a service-affecting operation. All services running on the BCM50 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 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 77 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.

5 Click the **Restore** 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

Yoour BCM50 supports the ability to recover using the USB device. The backup must have been created on the USB device while directly attached to a BCM50. A backup file placed on a USB device by any other means can only be used by attaching the device to your computer and selecting Restore From: My Computer.

Caution: A restore operation is a service-affecting operation. A number of services running on the BCM50 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 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 In the **Backup Type** selection field, select one of the following:

   a **Configuration**

   b **Application**

5 Click the **Restore** 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 restore operation is a service-affecting operation. A number of services running on the BCM50 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 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 78 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.

5. Click the **Restore** 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 BCM50 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 79 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.

5. Click the **Restore** 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 BCM50 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 BCM50 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 BCM50 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 BCM50 Logs

This chapter contains information about viewing and managing log files generated by the BCM50.

Overview of BCM50 logs

A log file is a collection of individual log events generated by the BCM50. An administrator can use log files to monitor and analyze system behavior, user sessions, and events.

You manage log files by transferring selected BCM50 log files from the BCM50 to a specified location, such as your personal computer. You can then view individual log files using the BCM50 Element Manager Log Browser or your usual text editor. On BCM50 models with an integrated router, you can also retrieve router logs using the router WebGUI.

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 BCM50, the Element Manager itself generates a log file. This log is found under the Help selection of the BCM50 Element Manager toolbar. This log contains diagnostic information.

The BCM50 manages log files and archives 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 BCM50 is rebooted or when the log file reaches the 1 MB limit.

Log types

The BCM50 logs are grouped in four categories:

- Operational logs
- Diagnostic logs
- Third Party 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 files, a set of additional 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 BCM50 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 80 lists the logs that belong to the Operational logs category.

Table 80 Operational logs

Log type	BCM50 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 BCM50 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 BCM50 software components, except third party components or logs that contain sensitive information. These log files are required only if additional system information is required by Nortel Technical Support to help diagnose a BCM50 issue. Only an administrator can access Diagnostic logs.

Third-party logs

Third-party logs are diagnostic logs of third party software components. These log files are required only if additional system information is required to help diagnose a BCM50 issue. Only an administrator can access Third Party logs.

Sensitive logs

Sensitive logs are diagnostic logs that 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.

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.

Sensitive logs are usually required for support purposes only. Only authorized administrators can access these 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 the BCM50 system at the time of the log file transfer. These files 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 BCM50 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 BCM50 Element Manager to transfer log files from the BCM50 to an external location. You must transfer the log files to an external device before you can view them. If you are using the BCM50 Element Manager Log Browser to view the logs, you will also have to extract the log files from the log file “archive” that is transferred from the BCM50. The log archive contains a collection of log files.

When you transfer the log files 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 log files you want to transfer, such as Third Party logs or Sensitive Information logs
- a schedule for a log file transfer

You can also transfer log files using the BCM50 Web page if you cannot access the BCM50 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 BCM50 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 BCM50 Element Manager Log Browser, you can use an application such as WordPad to view the log files.

Using the BCM50 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 BCM50 Element Manager

Using the BCM50 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 BCM50 and the date/time are appended to the prefix. An example filename is Log_acme20050304063336.tar.

When you transfer log files to the computer on which your Element Manager is installed, the default location for the Logs folder is \BCM50ElementManager\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 BCM50 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 apply an update 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 BCM50

- the size of the log file is not greater than the capacity of the storage device

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.

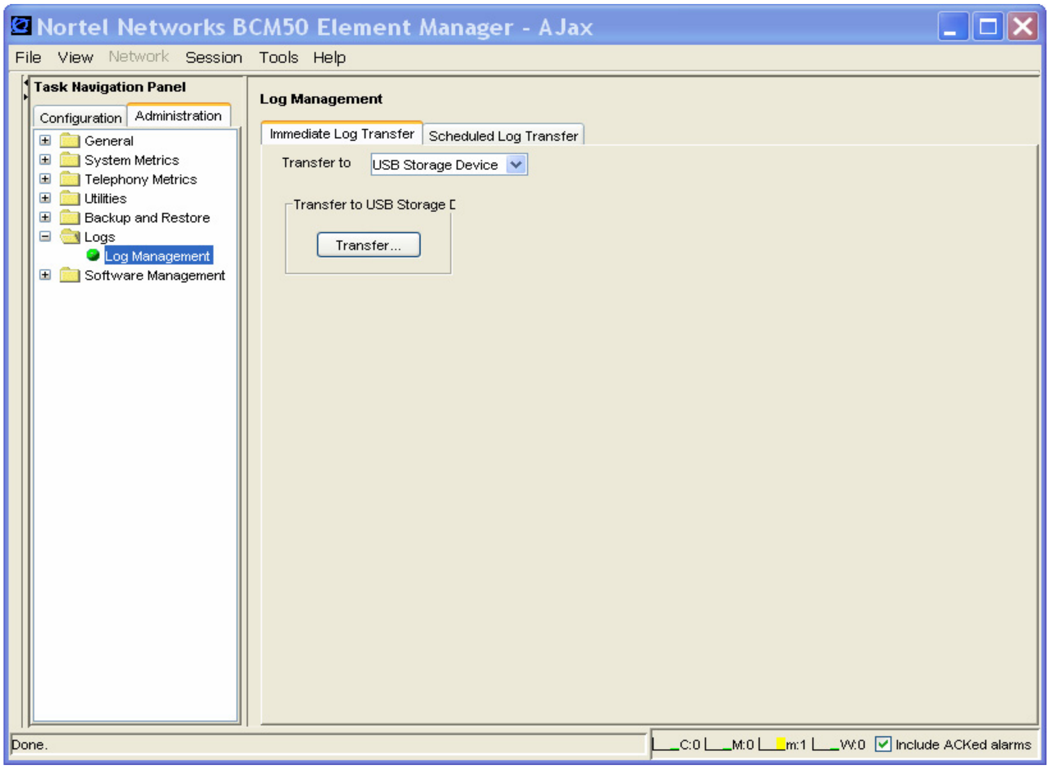
To perform an immediate log transfer to a USB storage device

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.**



Nortel Networks BCM50 Element Manager - AJax

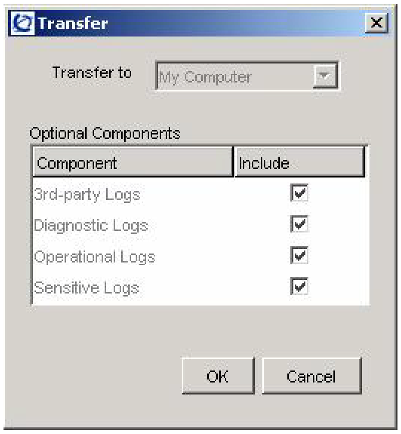
Log Management

Transfer to: USB Storage Device

Done.

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.



Transfer to: My Computer

Optional Components

Component	Include
3rd-party Logs	☑
Diagnostic Logs	☑
Operational Logs	☑
Sensitive Logs	☑

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.

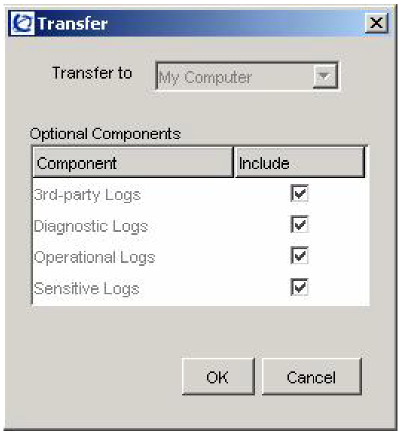
2 Click the **Log Management** task.
The **Log Management** panel opens.

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.



Transfer to: My Computer

Optional Components

Component	Include
3rd-party Logs	☑
Diagnostic Logs	☑
Operational Logs	☑
Sensitive Logs	☑

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 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 81 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.

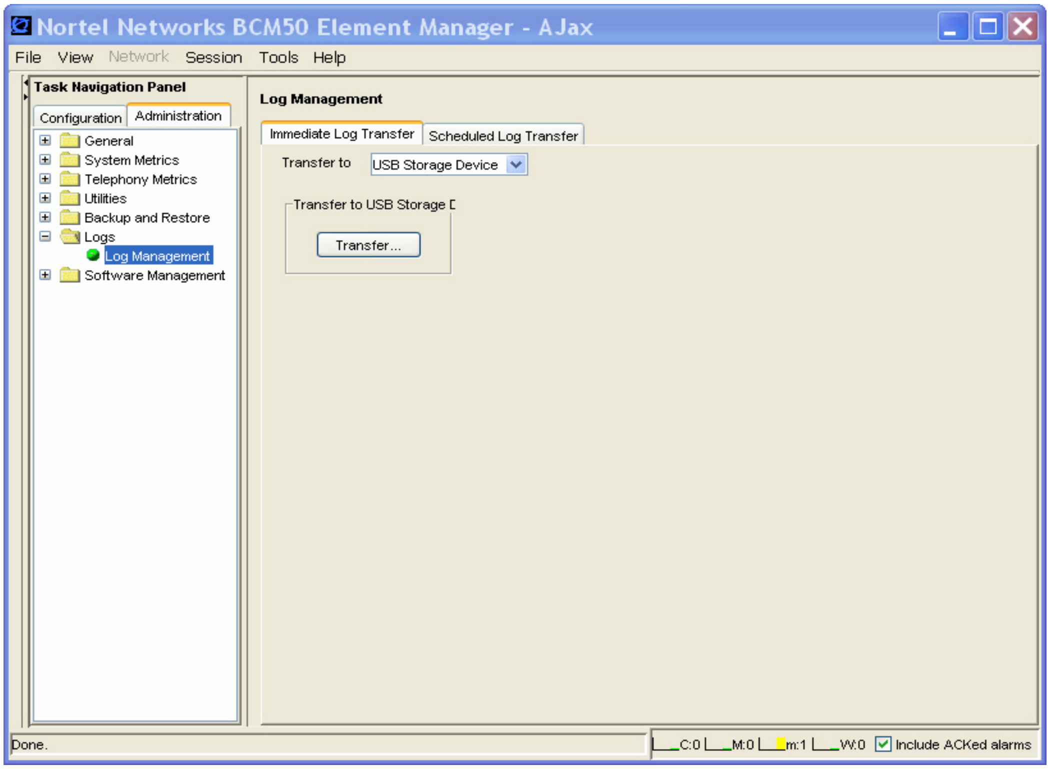
To perform an immediate log transfer to an FTP server

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.**


Nortel Networks BCM50 Element Manager - AJax
File View Network Session Tools Help
Task Navigation Panel
Configuration Administration
General
System Metrics
Telephony Metrics
Utilities
Backup and Restore
Logs
Log Management
Software Management
Log Management
Immediate Log Transfer Scheduled Log Transfer
Transfer to USB Storage Device
Transfer to USB Storage D
Transfer...
Done.
C:0 M:0 m:1 W:0 Include ACKed alarms

5 Configure the Transfer to FTP Server attributes.

Table 82 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 BCM50 to communicate with the SFTP server. For information about how to set up an SFTP server and about SSH keys, see “,” on page 81.

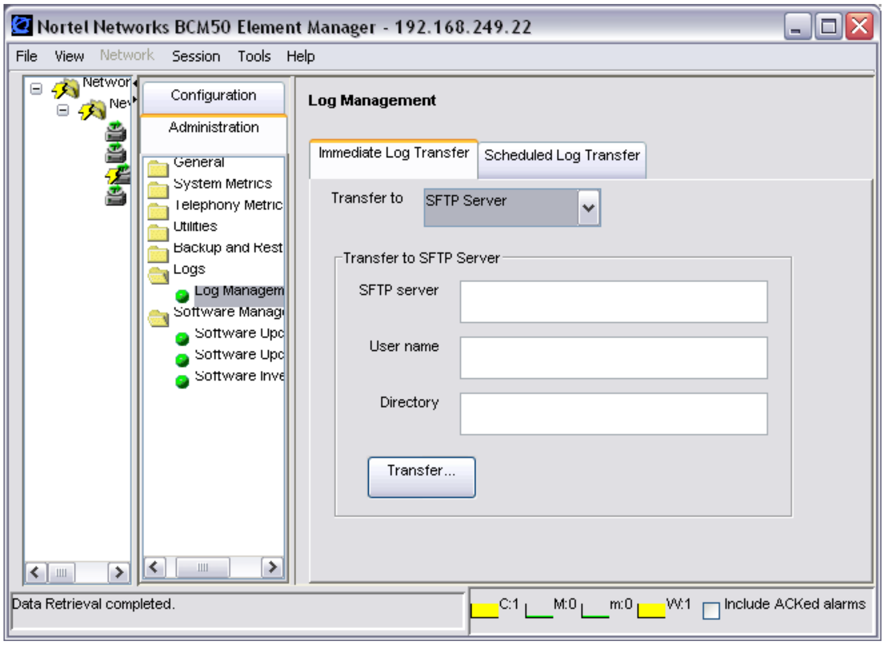
To perform an immediate log transfer to an SFTP server

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**.



Transfer to: SFTP Server

Data Retrieval completed.

5 Configure the Transfer to SFTP Server attributes.

Table 83 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 84 lists the information that is displayed in the Scheduled Log Transfer table.

Table 84 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 318.

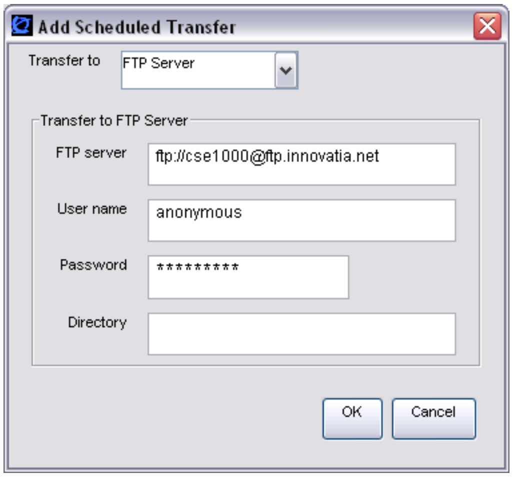
➡ **Note:** You cannot schedule a log transfer to your personal computer. Use a network folder, a USB storage device, an FTP server, or an SFTP server instead.

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


Add Scheduled Transfer

Transfer to: FTP Server

Transfer to FTP Server

FTP server: ftp://cse1000@ftp.innovatia.net

User name: anonymous

Password: *********

Directory:

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 318.

7 Click the **OK** button.
The **Add Scheduled Transfer** window opens.

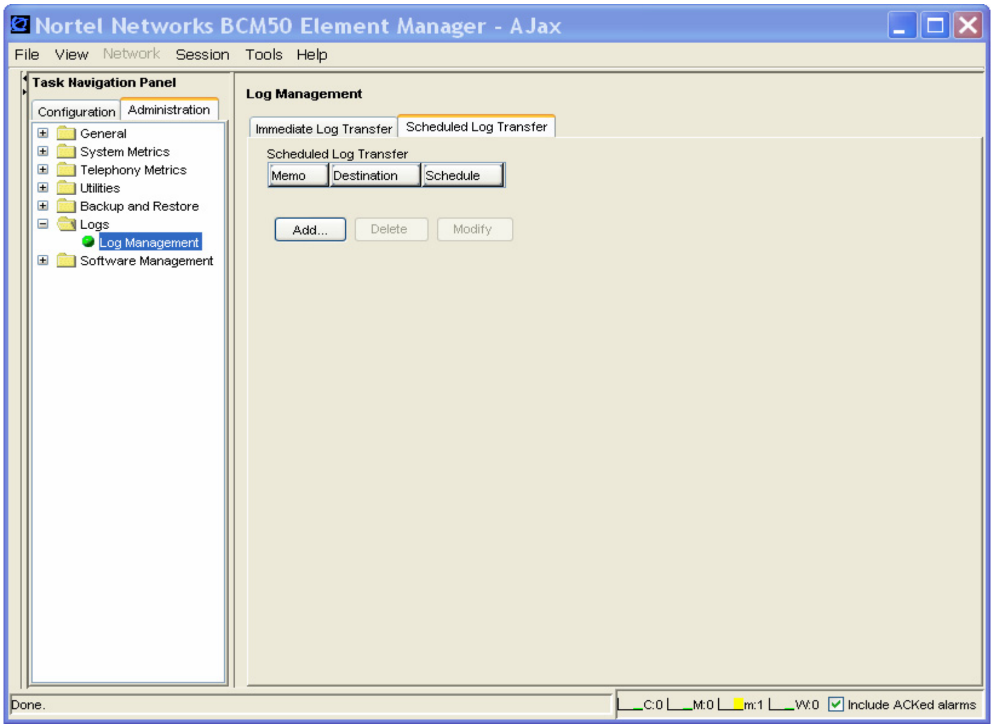
8 Select the log file categories that you want to include in the log file transfer.

9 Configure the schedule attributes.

Table 85 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 specify 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

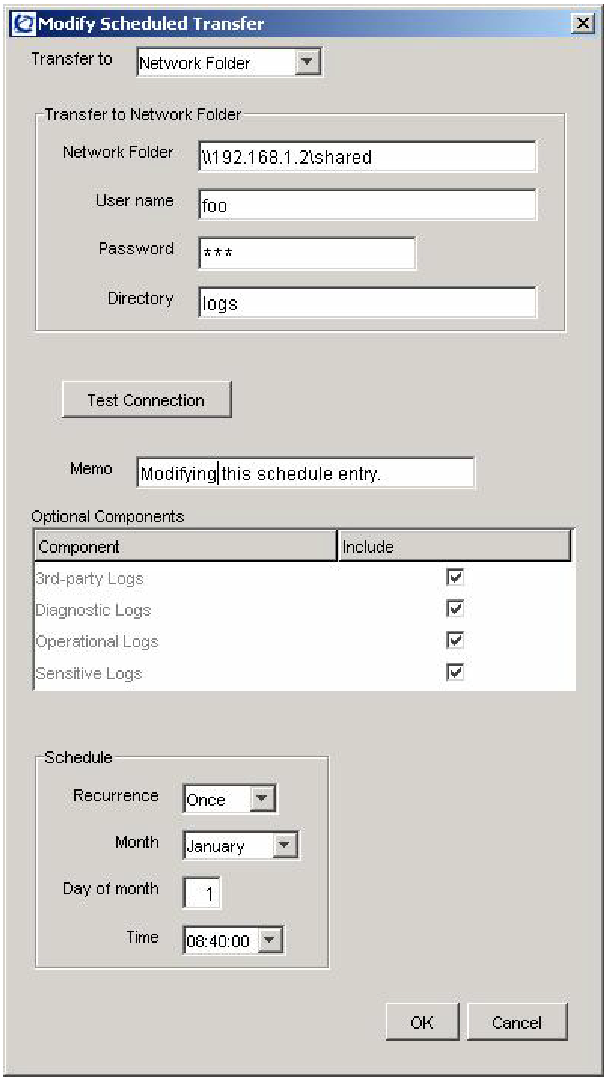
1 Click the **Administration** tab, and then open the **Logs** folder.

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.



Transfer to: Network Folder

Transfer to Network Folder

Network Folder: \\192.168.1.2\shared

User name: foo

Password: ***

Directory: logs

Memo: Modifying this schedule entry.

Optional Components

Component	Include
3rd-party Logs	☑
Diagnostic Logs	☑
Operational Logs	☑
Sensitive Logs	☑

Schedule

Recurrence: Once

Month: January

Day of month: 1

Time: 08:40:00

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 BCM50 Web page

You can transfer log files using the BCM50 Web page if you cannot access the BCM50 Element Manager.

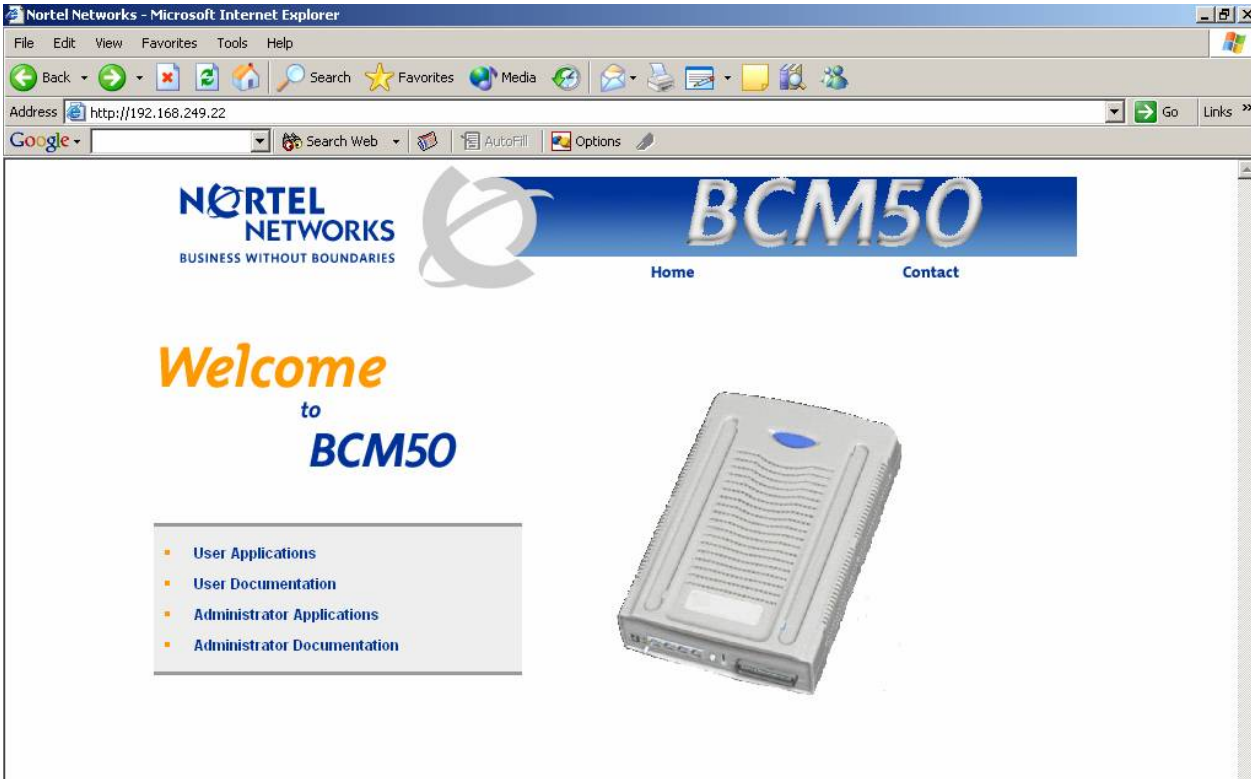
When you use the BCM50 Web page to transfer log files, you cannot choose the log file categories that you will transfer; all the log files in all the categories will be transferred.

Using the BCM50 Web Page to transfer log files to your personal computer

1 In your web browser, type the IP address of the BCM50 and click the **Go** button.
The login panel opens.

2 Log in to the BCM50 using the same username and password that you use to log into a BCM50 using the BCM50 Element Manager.
The BCM50 Web page opens.

3 Click the **Administrators Applications** link.


Nortel Networks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.249.22
Go Links
Google Search Web AutoFill Options
NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES
BCM50
Home
Contact
Welcome to BCM50
User Applications
User Documentation
Administrator Applications
Administrator Documentation

4 Click **Retrieve Logs**.

5 In the **Get Logs** area, click the **Download From Here** radio button.

6 Click the **Submit** button.
A **Working** panel opens. When the log retrieval is complete, the panel displays “Done.”

7 Click the **Click Here to Download Logs** link.
The **File Download** panel opens.

8 Click the **Save** button.
The **Save As** panel 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.

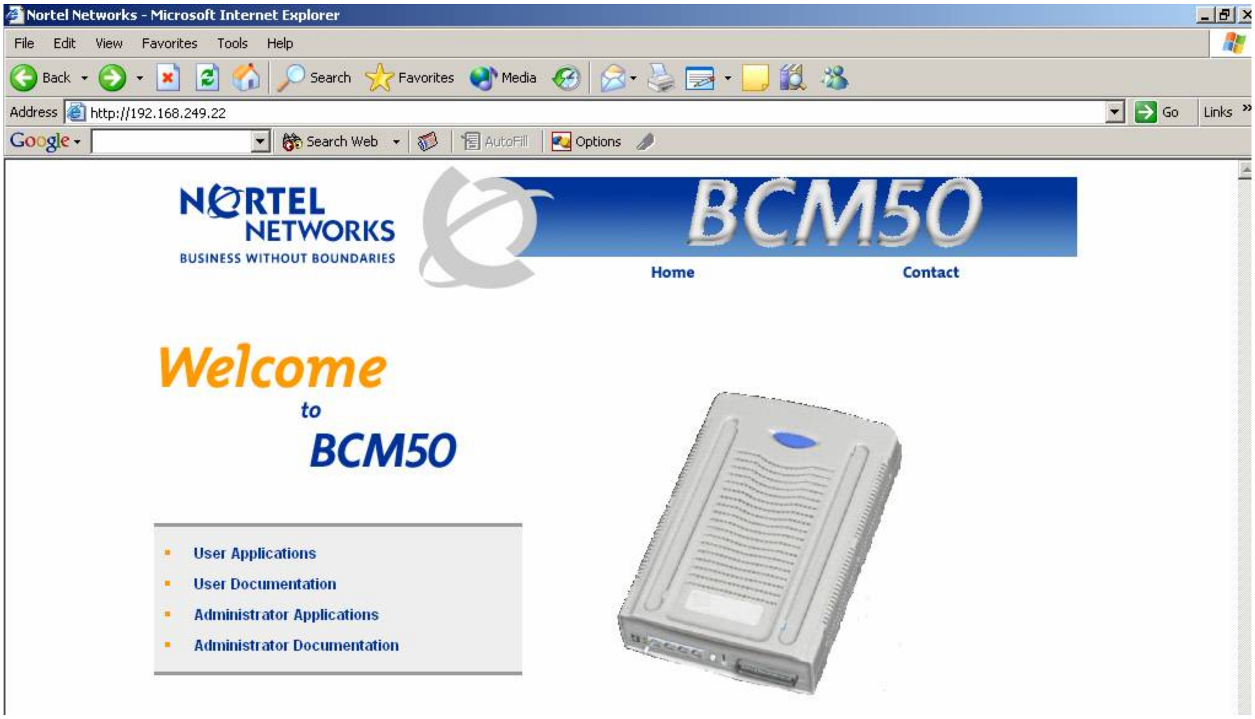
10 Click the **Save** button.
The file is saved.

To use the BCM50 Web Page to transfer log files to other destinations

1 In your web browser, type the IP address of the BCM50 and click the **Go** button.
The login panel opens.

2 Log in to the BCM50 using the same user name and password that you use to log into a BCM50 using the BCM50 Element Manager.
The BCM50 Web page opens.

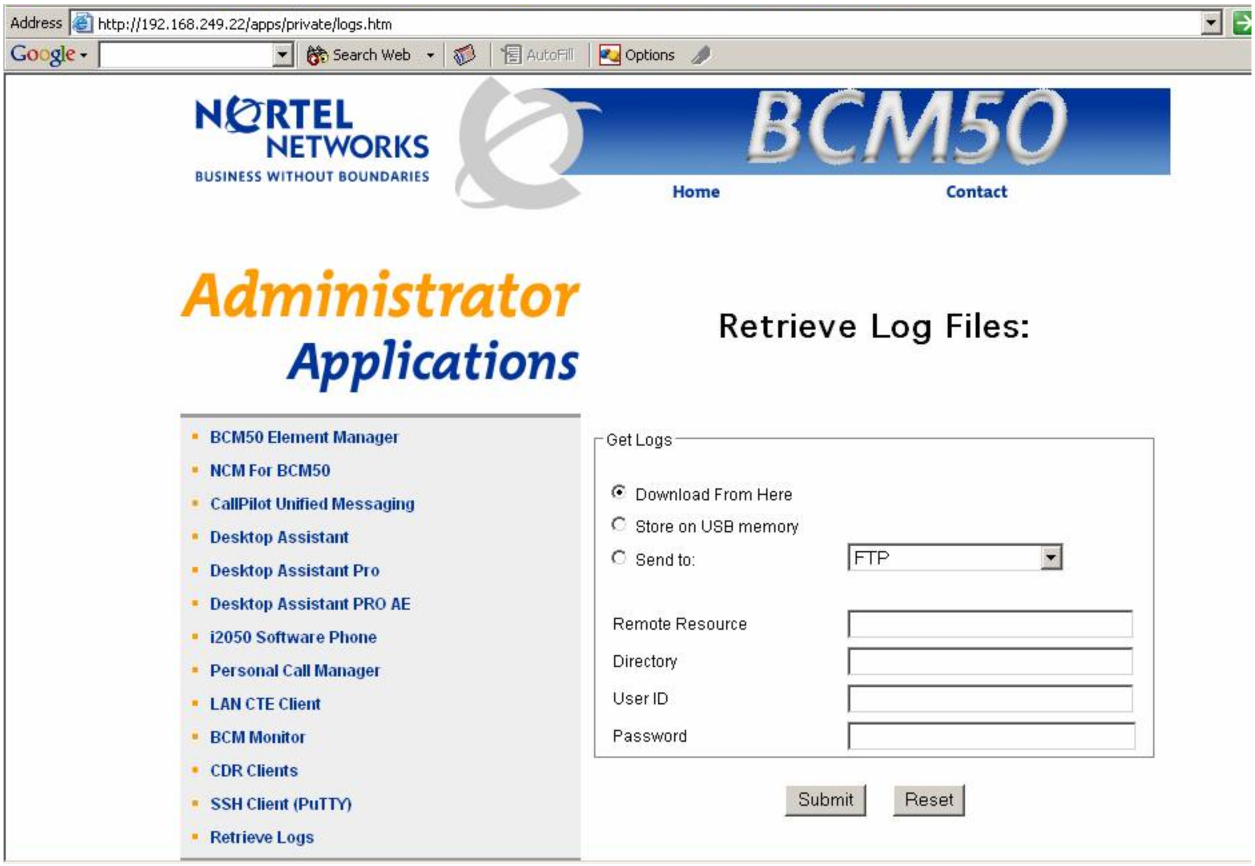
3 Click the **Administrators Applications** link.


Nortel Networks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.249.22
Go Links
Google Search Web AutoFill Options
NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES
BCM50
Home
Contact
Welcome to BCM50
User Applications
User Documentation
Administrator Applications
Administrator Documentation

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



http://192.168.249.22/apps/private/logs.htm

Retrieve Log Files:

Get Logs

● Download From Here
○ Store on USB memory
○ Send to: FTP

Remote Resource	
Directory	
User ID	
Password	

6 If you selected a Send To option, configure the destination attributes.

Table 86 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** panel opens. When the log retrieval is complete, the panel displays “Done.”

8 Click the **Click Here to Download Logs** link.
The **File Download** panel opens.

9 Click the **Save** button to save the backup.tar file.
The **Save As** panel 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 BCM50 Element Manager or the BCM50 Web page, you can extract the log files using the BCM50 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 BCM50 Element Manager

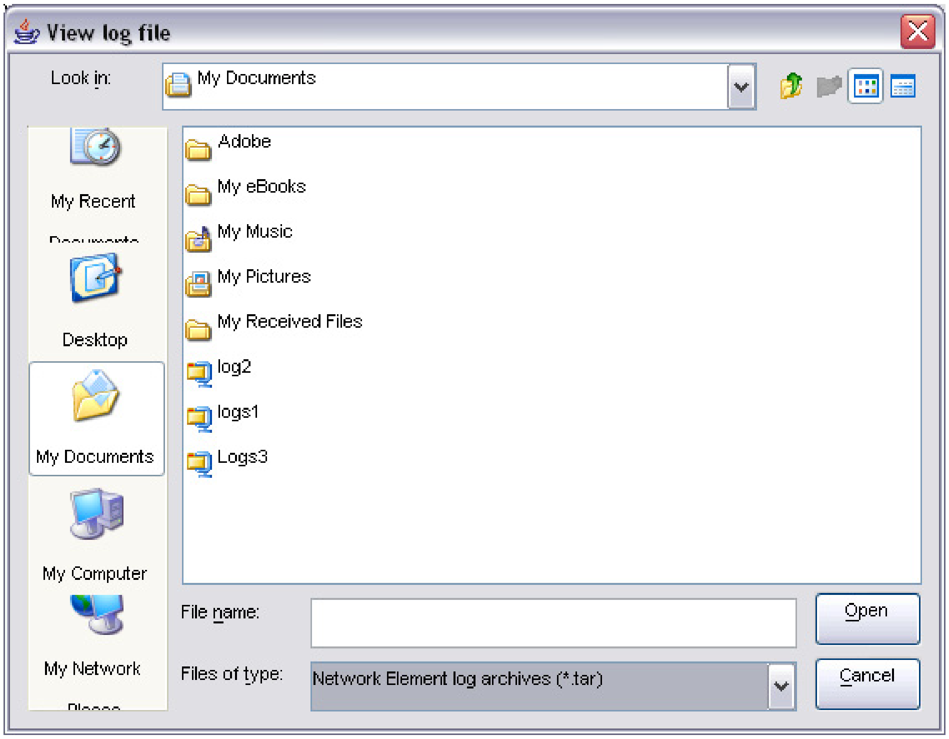
1 In the navigation pane, right-click a network element. The network element may be connected or disconnected.

2 Select **View Logs**.
The **View Log File** window opens.

3 Select the directory or location that contains the transferred BCM50 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.

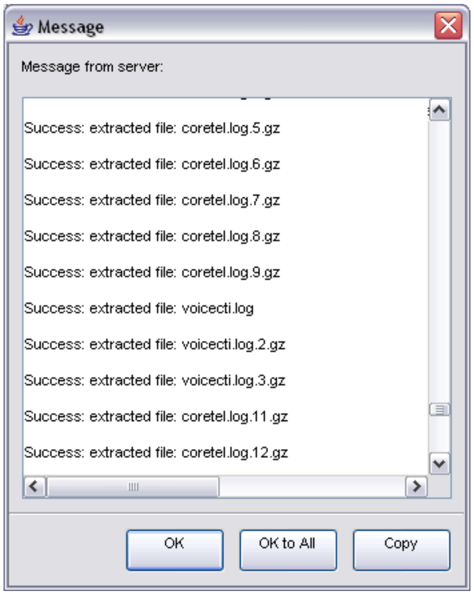


Look in: My Documents

Files of type: Network Element log archives (*.tar)

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.



Message from server:

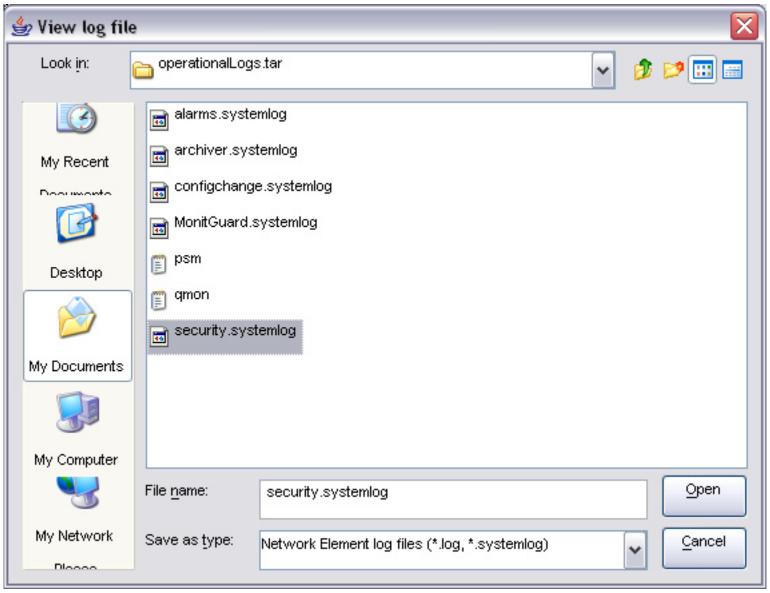
```
Success: extracted file: coretel.log.5.gz
Success: extracted file: coretel.log.6.gz
Success: extracted file: coretel.log.7.gz
Success: extracted file: coretel.log.8.gz
Success: extracted file: coretel.log.9.gz
Success: extracted file: voicecti.log
Success: extracted file: voicecti.log.2.gz
Success: extracted file: voicecti.log.3.gz
Success: extracted file: coretel.log.11.gz
Success: extracted file: coretel.log.12.gz
```

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.



Look in: operationalLogs.tar

File name: security.systemlog

Save as type: Network Element log files (*.log, *.systemlog)

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 BCM50 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 87 lists the log files that you can view using the Log Browser.

Table 87 Log files and the Log Browser

Log File	Can be viewed in the Log Browser?
Operational logs (.systemlog)	Yes
Diagnostic logs	Some can
Third Party logs	No
System Information	No
Sensitive Information	Yes

The Log Browser contains the following areas:

- Retrieval Criteria area
- Retrieval Results list
- Log Details area

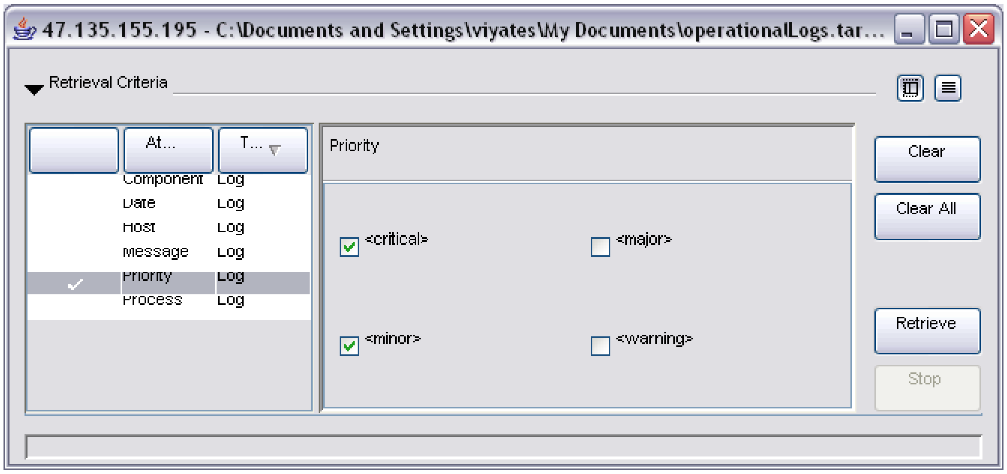
Retrieval Criteria area

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.



47.135.155.195 - C:\Documents and Settings\viyates\My Documents\operationalLogs.tar...

Retrieval Criteria

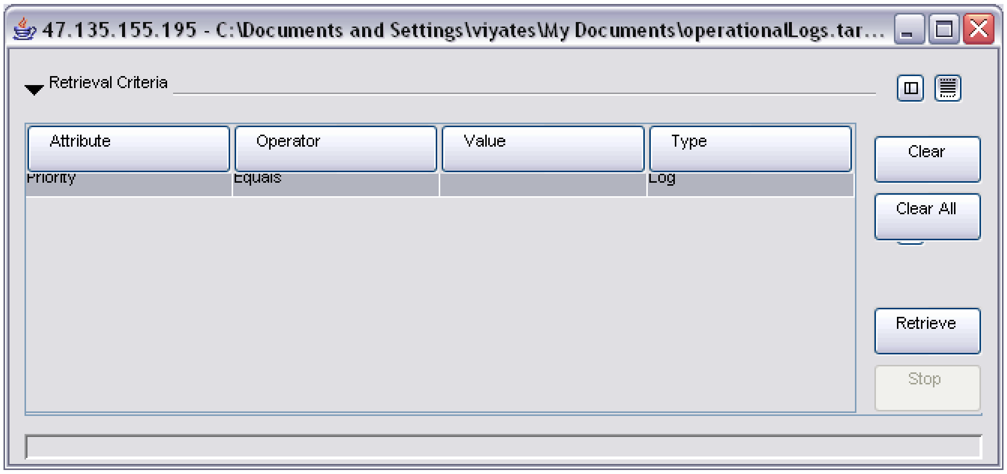
	At...	T...
	Component	Log
	Date	Log
	Host	Log
	Message	Log
✓	Priority	Log
	Process	Log

Priority

☑ <critical> ☐ <major>

☑ <minor> ☐ <warning>

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.


47.135.155.195 - C:\Documents and Settings\viyates\My Documents\operationalLogs.tar...
Retrieval Criteria
Clear
Clear All
Retrieve
Stop

Attribute	Operator	Value	Type
Priority	Equals		Log

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 337.

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

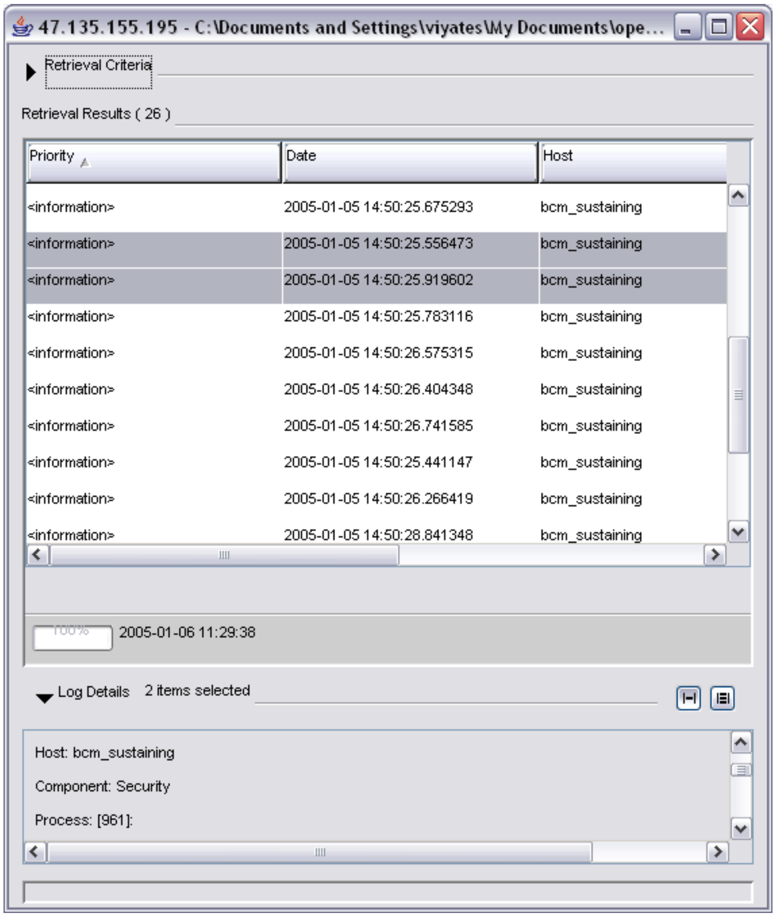
In the **Retrieval Results** list table, select a log record.
Log details for the selected log record are displayed in the **Log Details** area.

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.


47.135.155.195 - C:\Documents and Settings\viyates\My Documents\ope...
Retrieval Criteria
Retrieval Results (26)

Priority	Date	Host
<information>	2005-01-05 14:50:25.675293	bcm_sustaining
<information>	2005-01-05 14:50:25.556473	bcm_sustaining
<information>	2005-01-05 14:50:25.919602	bcm_sustaining
<information>	2005-01-05 14:50:25.783116	bcm_sustaining
<information>	2005-01-05 14:50:26.575315	bcm_sustaining
<information>	2005-01-05 14:50:26.404348	bcm_sustaining
<information>	2005-01-05 14:50:26.741585	bcm_sustaining
<information>	2005-01-05 14:50:25.441147	bcm_sustaining
<information>	2005-01-05 14:50:26.266419	bcm_sustaining
<information>	2005-01-05 14:50:28.841348	bcm_sustaining

2005-01-06 11:29:38

Host: bcm_sustaining

Component: Security

Process: [961]:

Viewing log files using other applications

Using the BCM50 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 BCM50 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 BCM50 Software Updates

This chapter contains information about managing BCM50 software updates.

During the lifecycle of the BCM50, you can apply software updates to the BCM50 unit to introduce new functionality. Between software upgrades, you may find it necessary to apply software updates to resolve field issues.

Using the BCM50 Element Manager, 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 BCM50
- apply and, in some cases, remove software updates
- view the software inventory of the BCM50
- apply software updates at a scheduled time

For information about managing software updates on the router, see the *BCM50a Integrated Router Configuration Guide* or the *BCM50e Integrated Router Configuration Guide*.

Overview of BCM50 software updates

Using the Software Management task, an administrator can view and manage software updates and upgrades to the BCM50.

The Software Management interface consists of three panels:

- Software Updates — used to manage the application of software updates to the BCM50
- Software Update History — used to view the history of updates that have been applied to the BCM50, 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 BCM50, you must obtain the software update. Authorized Nortel partners can download BCM50 software updates from the Nortel Technical Support web page.

To obtain updates from the Nortel Technical Support Web page

In your web browser, enter <address> and then click the **Go** button.
The Nortel Technical Support Web page opens. Download the required updates.

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. As soon as a software update is applied, the BCM50 Element Manager is disconnected and users cannot log in until the system has completed applying the software update.

Table 88 lists the information that is available on the Updates in Progress table.

Table 88 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 BCM50 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 89 for information.

Table 89 lists the statuses of software updates.

Table 89 Software update statuses

Status	Description
Available	The software update is available to be applied to the BCM50. Only an Available software update can be applied to the BCM50.
Invalid	A newer version of software has been applied to the BCM50 and has rendered this software update invalid.
Installed	The software update has been applied to the BCM50.
In Progress	The software update is in the process of being applied to the BCM50. An update may be In Progress for up to 15 minutes, depending on the size of the update file.

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 BCM50.

Applying a software update is a two-part process:

1. You transfer a software update to the BCM50, which validates the integrity of the software update and ensures that the BCM50 meets prerequisites for applying the software update.
2. You apply the software update to the BCM50, which then brings the update into service.

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager disconnects from the BCM50 and cannot log into the BCM50 until the software update has been completed. Nortel recommends that you schedule updates for low-traffic hours.

Caution: In the case of some software updates, the BCM50 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 BCM50 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 BCM50 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

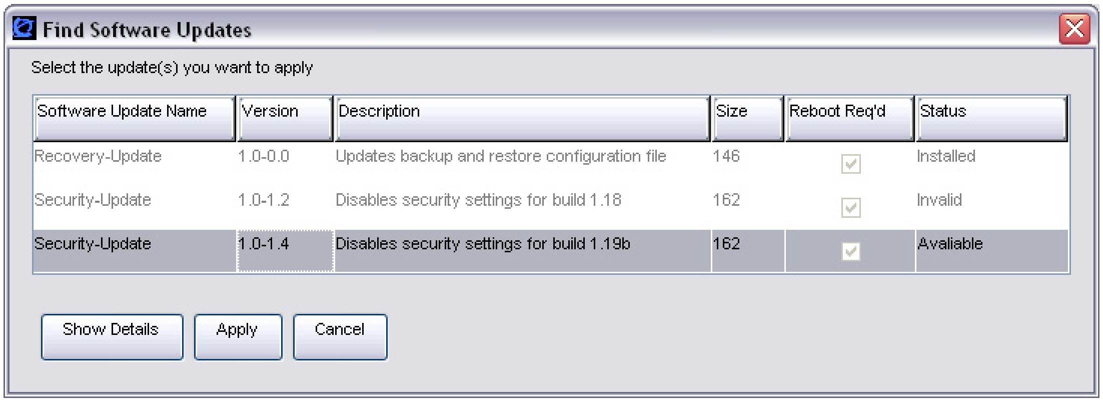
Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system are stopped. Users of the BCM50 Element Manager are disconnected from the BCM50 and cannot log into the BCM50 until the software update has been completed. Consequently, Nortel recommends 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 BCM50 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 **Open** window opens.

8 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.



Find Software Updates

Select the update(s) you want to apply

Software Update Name	Version	Description	Size	Reboot Req'd	Status
Recovery-Update	1.0-0.0	Updates backup and restore configuration file	146	☑	Installed
Security-Update	1.0-1.2	Disables security settings for build 1.18	162	☑	Invalid
Security-Update	1.0-1.4	Disables security settings for build 1.19b	162	☑	Avaliable

9 Select an update. The update must have a status of “Available.”

10 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.

11 Click the **Apply** button to apply the update.
A warning dialog box opens.

12 Click the **OK** button.
The **Software Update Complete** confirmation window opens.

13 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.

14 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 BCM50 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 BCM50

- the size of the software update is not greater than the capacity of the storage device

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update completes. Consequently, 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 BCM50 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 BCM50 once the update has been applied.

Applying an update from a shared folder

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update has been completed. Consequently, it is advisable 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 BCM50 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 90 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 BCM50 once the update has been applied.

Applying an update from an FTP server

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update has been completed. Consequently, it is advisable that you schedule updates for low-traffic hours.

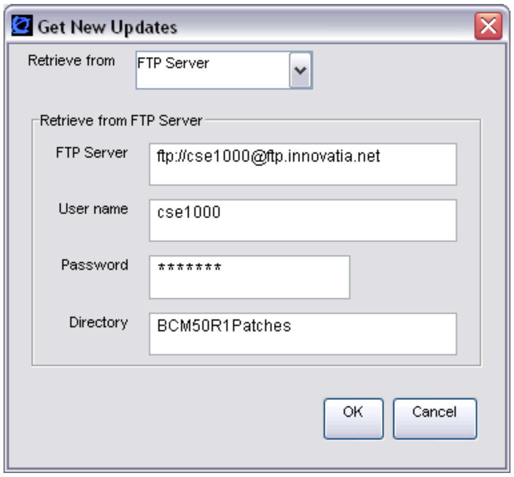
Caution: If a software update has a checkmark applied against it in the Reboot Req’d column of the Find Software Updates window, the BCM50 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

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 91 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.
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.



Retrieve from: FTP Server

Retrieve from FTP Server

FTP Server: ftp://cse1000@ftp.innovatia.net

User name: cse1000

Password: *******

Directory: BCM50R1Patches

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 BCM50 once the update has been applied.

Applying an update from an HTTP server

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update has been completed. Consequently, it is advisable 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 BCM50 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 92 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 BCM50 once the update has been applied.

Creating and modifying scheduled software updates

You can apply a software update to the BCM50 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 BCM50 when you create the schedule.

Table 93 lists the information that is displayed about scheduled software updates in the Scheduled Software Updates table.

Table 93 Information about scheduled software updates

Columns	Description
Name	The name of the update.
Version	The version of the update.
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 BCM50 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 94 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 94 lists the statuses of scheduled software updates.

Table 94 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 BCM50.

Creating a scheduled software update

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update has been completed. Consequently, it is advisable that you schedule updates for low-traffic hours.

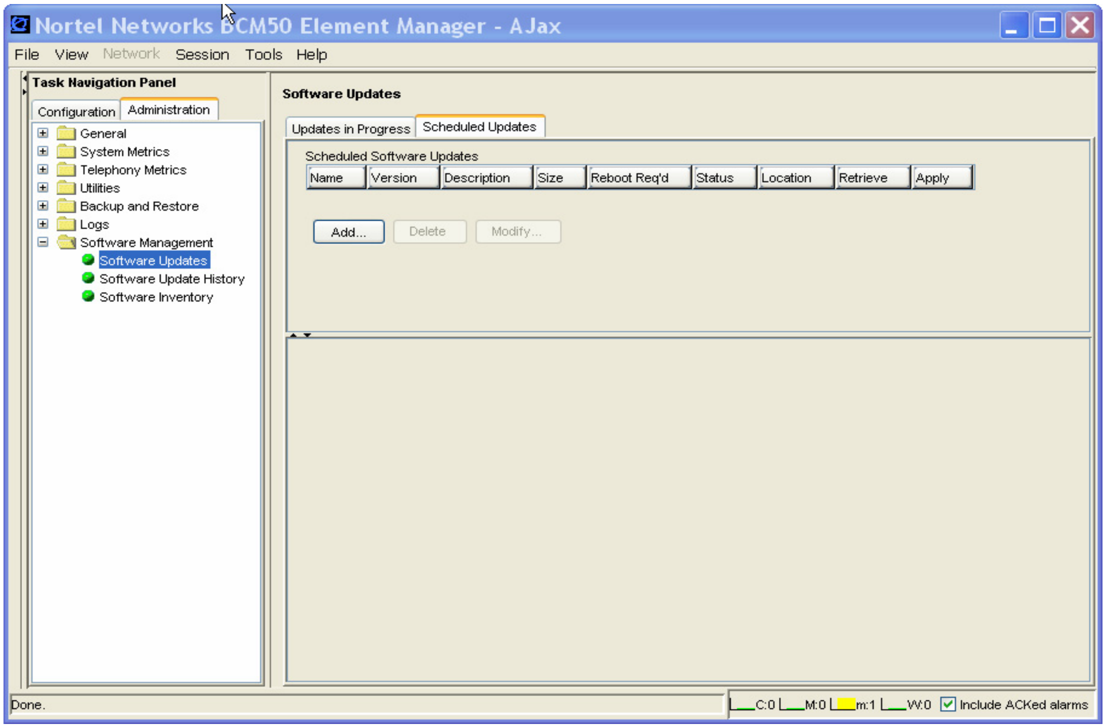
Caution: If a software update has a checkmark applied against it in the Reboot Req'd column of the New Updates Found window, the system will automatically reboot as soon as the patch has been applied. You will not receive a reboot confirmation before the reboot occurs.

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.



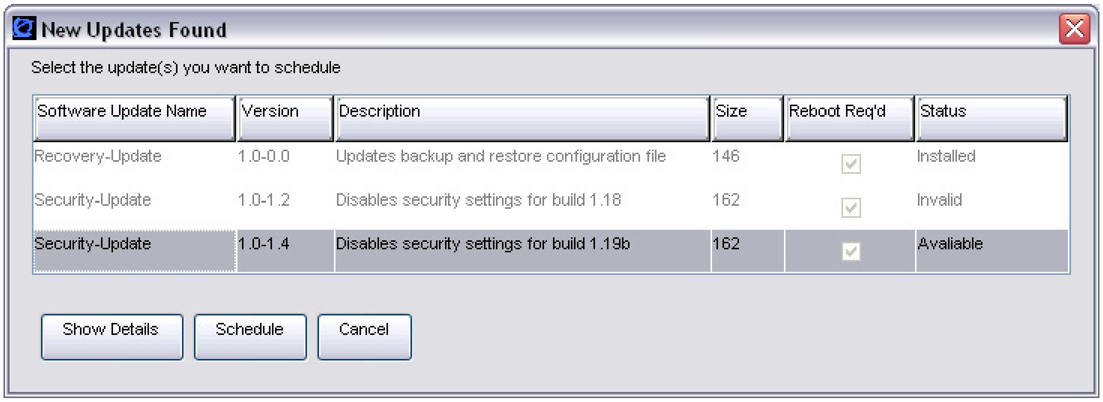
4 Click the **Add** button. The **Get New Updates** window opens.

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.



Select the update(s) you want to schedule

Software Update Name	Version	Description	Size	Reboot Req'd	Status
Recovery-Update	1.0-0.0	Updates backup and restore configuration file	146	☑	Installed
Security-Update	1.0-1.2	Disables security settings for build 1.18	162	☑	Invalid
Security-Update	1.0-1.4	Disables security settings for build 1.19b	162	☑	Avaliable

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.

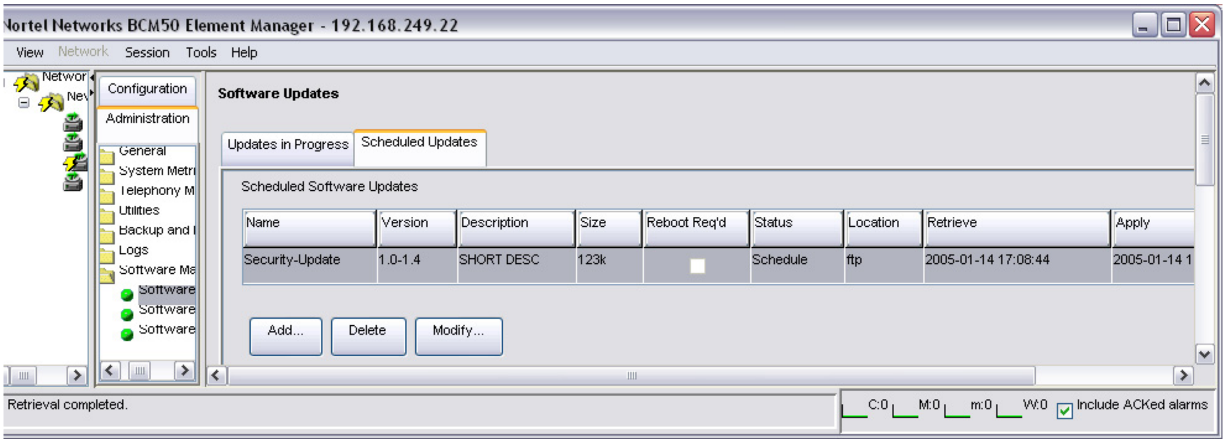
11 Click the **Retrieve** field to select a date and time at which to retrieve the update. A calendar window opens.

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”.



Nortel Networks BCM50 Element Manager - 192.168.249.22

Software Updates

Scheduled Software Updates

Name	Version	Description	Size	Reboot Req'd	Status	Location	Retrieve	Apply
Security-Update	1.0-1.4	SHORT DESC	123k	□	Schedule	ftp	2005-01-14 17:08:44	2005-01-14 1

Retrieval completed.

Modifying a scheduled software update

Caution: Applying a software update to the BCM50 is a service-affecting operation. All services running on the system will be stopped. Users of the BCM50 Element Manager will be disconnected from the BCM50 and will not be able to log into the BCM50 until the software update has been completed. Consequently, it is advisable 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 BCM50 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

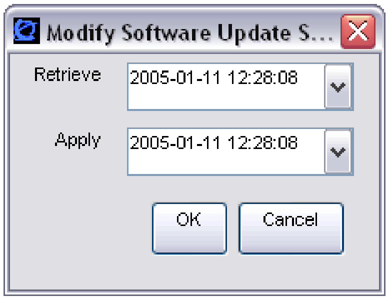
1 In the task panel, click the **Administration** tab.

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.



Retrieve: 2005-01-11 12:28:08

Apply: 2005-01-11 12:28:08

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 BCM50 since the BCM50 was shipped.

You can:

- view the current software release level of the BCM50
- view a history of all software updates (including upgrades) applied to the BCM50
- view release notes that apply to a particular software update

- remove certain software updates from the BCM50

Table 95 lists the information displayed in the Software Update History table.

Table 95 Information displayed in the Software Update History table

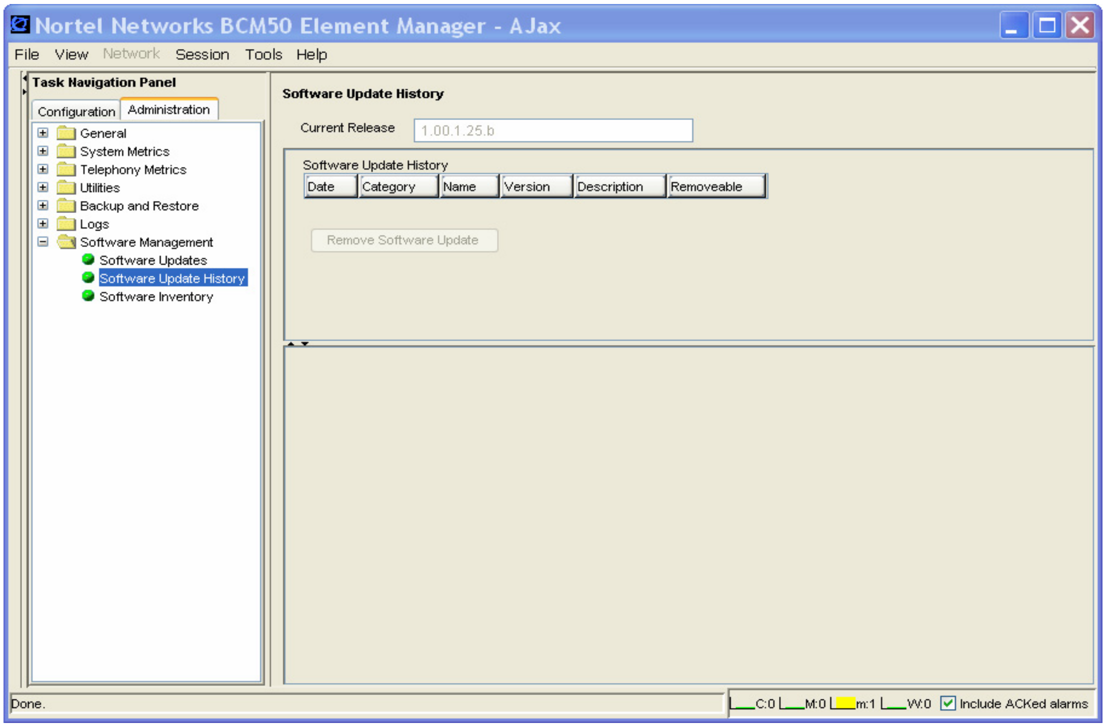
Columns	Description
Date	The date and time that the software update was applied.
Category	The software update category (Scheduled, Removed, Modified, Applied).
Name	The name of the software update.
Version	The version of the software update.
Description	A brief description of the software update.
Removeable	Indicates whether the software update can be removed from the BCM50. 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.

3 View the updates in the **Software Update History** table. If software updates have not been applied to your BCM50, the table is empty.



Current Release 1.00.1.25.b

4 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 BCM50. Not all software updates can be removed; whether a software update can be removed depends on the the particular software update.

Removing a software update does not remove the software itself from the BCM50; 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 BCM50.

Removing a software patch or upgrade from the BCM50 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 BCM50 and then removed, this information is displayed in the Software Update History table. A removal operation is logged by the BCM50, 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 BCM50 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 BCM50 software

BCM50 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 BCM50 to the component level.

You can view the complete inventory of software installed on the BCM50. The Software Inventory table displays all the software components installed on the system, the functional group and the software version of each component.

Table 96 lists the information displayed in the Software Component Version Information table.

Table 96 Information displayed in the Software Component Version Information table

Column	**Description**
Component	The name of the software component installed on the BCM50. For example, backup-recovery.
Group	The functional group to which the software component belongs. For example, Operating System. Are there other groups?
Version	The version of the software component.

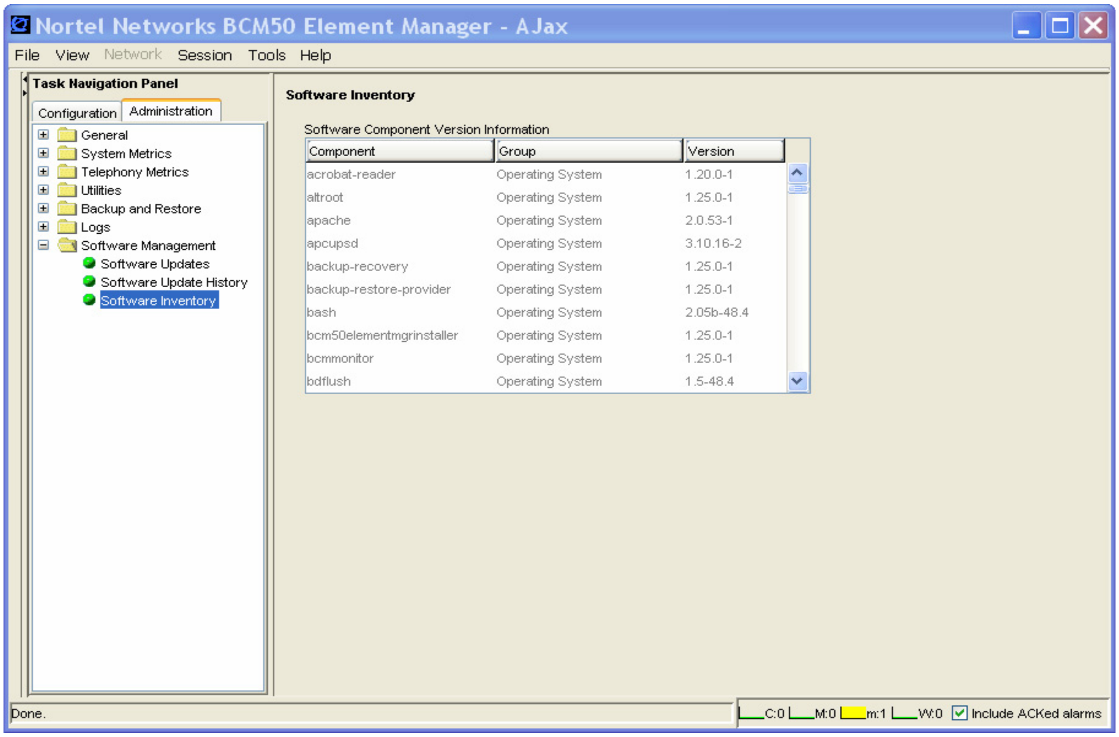
You can change the order of the information displayed in the table by clicking a column heading and dragging it to a new place in the table. You can also sort the information in a column by descending or ascending order, by clicking the column heading.

To view the BCM50 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.



Software Inventory

Software Component Version Information

Component	Group	Version
acrobat-reader	Operating System	1.20.0-1
altroot	Operating System	1.25.0-1
apache	Operating System	2.0.53-1
apcupsd	Operating System	3.10.16-2
backup-recovery	Operating System	1.25.0-1
backup-restore-provider	Operating System	1.25.0-1
bash	Operating System	2.05b-48.4
bcm50elementmgrinstaller	Operating System	1.25.0-1
bcmmonitor	Operating System	1.25.0-1
bdflush	Operating System	1.5-48.4

Chapter 14
Accounting Management

This chapter describes how to manage accounts in a BCM50 system.

Overview of accounting management

BCM50 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 BCM50 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

BCM50 Call Detail Recording is covered in detail in the Call Detail Recording System Administration Guide. 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 BCM50 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 BCM50 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 BCM50 system. These are the Call Pilot Mailbox activity report and the All Mailbox Activity Report.

CDR Toolkit

A CDR Toolkit is provided with the BCM50 to enable third-party developers to retrieve BCM50 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 BCM50.

About SNMP MIBs

A MIB enables access to the managed objects of a system. A MIB is software that defines the data reported by a computing or network device and the extent of control over that device. MIBs are managed using a network management protocol, such as Simple Network Management Protocol (SNMP).

BCM50 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

MIB file descriptions

BCM50 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 97 lists the file names and file descriptions of each supported standard MIB.

Table 97 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 BCM50.
ENTITY-MIB	rfc2737.mib	This MIB defines physical and logical system components on the BCM and associations between these components.

Table 97 MIB file descriptions for standard MIBs

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.

Table 98 lists the file names and file descriptions of each supported Nortel MIB.

Table 98 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 BCM50, 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 BCM50 Web Page. You can also access BCM50 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 BCM50 Web Page

1. Go to the BCM50 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 **BCM50 MIB** link.
   The **Software Detail Information** page opens.
9. Right-click the **BCM50 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 BCM50 SNMP traps. For more information, see Table 101 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:** BCM50 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 BCM50 main unit, as well as the ADSL and Ethernet integrated routers. Table 99 summarizes the sysObjectID assignments.

Table 99 sysObjectID assignments

Model	Main Unit sysObjectID	Integrated Router sysObjectID
BCM50	1.3.6.1.4.1.562.37.1.4	—
BCM50a	1.3.6.1.4.1.562.37.1.4	1.3.6.1.4.1.562.37.1.5
BCM50e	1.3.6.1.4.1.562.37.1.4	1.3.6.1.562.37.1.6

Small Site Event MIB

The Small Site Events MIB defines events (SNMP traps) that can be used by any Small Site product or component. BCM50 traps can be captured and viewed using a standard SNMP fault monitoring framework or trap watcher.

SNMP traps are generated by the BCM50 if you have enabled SNMP for specific BCM50 alarms. You configure SNMP settings using the Alarm Settings task in the BCM50 Element Manager. For information about how to configure SNMP traps, see Chapter 6, “,” on page 137.

Table 100 lists the BCM50-specific SNMP trap fields for Small Site Event MIBs.

Table 100 BCM50-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 BCM50 interfaces
Generic trap type	6 for Enterprise-specific traps

Table 100 BCM50-specific SNMP trap fields for the Small Site Event MIB

Specific trap type	1 = eventInfo trap type 2 = eventWarning trap type 3 = eventError trap type
Time stamp	the system up time

Table 101 lists the BCM50-specific SNMP variable bindings.

Table 101 BCM50-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

Glossary

The following sections provide brief explanations of the terms used in this documentation.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

3

3DES

Triple (3) Data Encryption Standard is a type of DES encryption algorithm that encrypts data three times. Instead of one encryption key, there are three 64-bit keys used. This creates an overall key length of 192 bits. The first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key.

A

AES ch 5

Alarm Indication Signal (AIS)

The Alarm Indication Signal is a signal transmitted in place of the normal signal to maintain transmission continuity and indicate to the receiving terminal of a transmission fault located either at the transmitting terminal or between the two terminals.

ATA 2

A device that connects analog telecommunication devices, such as fax machines, answering machines, and single line telephones to the Business Communications Manager system through a Digital station module.

B

B-channel

This is an ISDN line bearer channel which is used for voice or data transmission.

Business Communication Manager (BCM)

The Business Communications Manager delivers small/medium-sized businesses and branch offices the only converged voice/data solution in the industry, providing a choice of IP-enabled or pure-IP strategy. The BCM uses existing Meridian, Norstar, and Succession 1000 equipment and software. BCM has telephony, unified messaging, multimedia call center, interactive voice response, IP routing and data services such as firewall and wireless.

BCM Monitor

The BCM Monitor is a standalone diagnostic application allows you to view system and IP telephony information on individual Business Communications Manager units. Open several instances of BCM Monitor to monitor several remote BCM systems on a single PC simultaneously. This tool supports real-time debugging. This tool also allows you to save and process data at a later time to generate system utilization and traffic reports.

Basic Rate Interface (BRI)

The Basic Rate Interface is an ISDN interface that uses two B channels and a D channel (2B+D). ETSI BRI is the European Telecommunications Standards Institute specification for BRI ISDN service

C

Call-by-Call services (CbC)

This is a PRI (North American) line feature that provides a system of remapping specific incoming lines for specific destinations. These services include INWATs (800), foreign exchange (FX), international 800, switched digital (SDS), and nine hundred (900). The type of service is based on the type of central office switch from which the line originates.

Call Detail Recording (CDR)

Call Detail Recording is an application that records and reports call activity. Each time a telephone call is made to or from your company, you can record the information about the call. When the call is completed, you can print information about the call in a report. Call Detail Recording also provides information on incoming calls as the events occur. This information appears in a Real Time Call record.

Carrier Failure Alarms (CFA)

Carrier Failure Alarms are BCM50 System alarms concerning loss of signal (LOS), out of frame (OOF), alarm indication signal (AIS), and remote alarm indication (RAI).

Custom Local Area Signaling Services (CLASS)

Custom Local Area Signaling Services is a collection of services from the local telephone company.

Calling Line Identification (CLID)

When available from the local telephone company, Calling Line Identification shows the calling number on the telephone display.

Call Management Services (CMS)

Call Management Services is a collection of services from the local telephone company. CMS is a part of CLASS.

CIM/XML

The CIM/XML language is a language for programming power system models.

Codec

Equipment or circuits that digitally code and decode voice signals. Software that provides compression/decompression algorithms for voice traffic over IP networks and VoIP trunks.

For IP telephones, the Business Communications Manager supports the G.711 CODEC, as well as the G.729 and G.723 CODECS.

The G.711 CODEC samples the voice stream at a rate of 64Kbps (Kilo bits per second), and is the CODEC to use for maximum voice quality.

The G.729 CODEC samples the voice stream at 8Kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.

The G.723 CODEC should be used only with third party devices that do not support G.729 or G.711.

Codecs with VAD (Voice Activity Detection) make VAD active on the system, which performs the same function as having silence suppression active.

The G.729A CODEC samples the voice stream at 8Kbps. It is the same as the G.729 with reduced complexity.

cron deamon

A UNIX operating system that initiates all timed events.

Customer Premise Equipment (CPE)

Customer Premise Equipment is all the telecommunications equipment located at a business or private house.

Control Slip (CS)

Control slip

Channel Service Unit (CSU)

A Channel Service Unit is a device on the Digital Trunk Interface that is the termination point of the T1 lines from the T1 service provider. The CSU collects statistics on the quality of the T1 signal. The CSU ensures network compliance with FCC rules and protects the network from harmful signals or voltages.

CTE ch 6

CTI ch 6 and 9

D

D-channel

A data channel transmission channel which is packet-switched is referred to as a D-channel. It is used for call setup, signaling and data transmission.

Digital Drop and Insert Mux (DDI Mux)

The Digital Drop and Insert Mux media bay module is a specialized two-level module allows you to choose which channels on a T1 line you want to dedicate to data transmissions and which channels you want to dedicate to telephony operations.

DECT OAM

The DECT administration, maintenance and operations (OAM) management interface service is used to enable the administration of the DECT media bay module from the Element Manager. If the management function from Element Manager (or the wizards) does not function correctly, verify the correct operational status of this service.

Data Encryption Standard (DES)

The Data Encryption Standard is a private encryption key with 72 quadrillion combinations. A 56-bit key is applied to each 64-bit block of data and recoded 16 times. Both the sender and receiver must have the key.

Diagnostic Log

Diagnostic Logs contain BCM50 logs generated by BCM50 software components but not third party components, or logs containing sensitive information. These logs are usually only needed in the event of a support situation.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol is a protocol that allows network administrators to centrally manage and automate the assignment of IP addresses in an network. When an organization sets up its computer users with a connection to the internet, internet protocols (TCP/IP) demands that an IP address must be assigned to each machine as well as to any device connected to the network.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP allows the network administrator to supervise and distribute IP addresses from a central point. It also automatically sends a new IP address when a computer is plugged into a different place in the network.

Directory Number (DN)

Directory Number is a unique number that the Business Communications Manager system assigns to every telephone or data terminal. You use the DN to identify a device for the Business Communications Manager configurations that require telephone-specific features. The system also assigns DNs to other applications such as Call Center and Hunt groups. Companion and ISDN and DECT equipment have separate sets of DNs that are exclusive that type of device.

Directory numbers are the digit string that the system uses to identify telephones and system devices and applications. The DN record provides access to configuring telephone functionality, including defining the features the user can access, the features the telephone supports, and the lines that can be used by the telephone to send and receive calls.

Dialed Number Identification Service (DNIS)

The Dialed Number Identification Service provides the number the caller dialed to reach the Business Communications Manager system.

Digital Trunk Module (DTM)

The digital trunk media bay module provides the connection between a standard digital PSTN T1 or PRI line and the Business Communications Manager system.

E

Element Manager (EM)

The BCM50 Element Manager is a web-based configuration and maintenance application bundled with the Business Communications Manager software. The BCM50 Element Manager is the single point of access for managing all programming for individual BCM systems. Access to the BCM50 Element Manager is password protected, and is secure for both enterprise customers and small to medium sized businesses. Administrators use the BCM50 Element Manager to quickly set up BCM telephony and data functions, as well as users, mailboxes, and directory numbers.

Error Seconds

Error Seconds These parameters are defined as per TIA-547A.

F

Fault-management, Configuration, Accounting, Performance, and Security (FCAPS)

FCAPS is a categorical model of the working objectives of network management. There are five levels: fault-management level (F), the configuration level (C), the accounting level (A), the performance level (P), and the security level (S).

FEPS ch 9

Frame Per Packet (FPP)

Frames per Packet is a measure of a quantity of data on a Ethernet network.

File Transfer Protocol (FTP)

The file transfer protocol allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.

Frame relay

A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.

G

G.711

The G.711 CODEC samples the voice stream at a rate of 64Kbps (Kilo bits per second), and is the CODEC to use for maximum voice quality.

Codecs with VAD (Voice Activity Detection) make VAD active on the system, which performs the same function as having silence suppression active.

G.723

A codec that provides the greatest compression, 5.3 kbit/s or 6.3 kbit/s. Normally used for multimedia applications such as H.323 video conferencing. Allows connectivity to Microsoft-based equipment.

The G.723 CODEC should be used only with third party devices that do not support G.729 or G.711.

Codecs with VAD (Voice Activity Detection) make VAD active on the system, which performs the same function as having silence suppression active.

G.729

A codec that provides near toll quality at a low delay. Uses compression to 8 kbit/s (8:1 compression rate).

The G.729 CODEC samples the voice stream at 8Kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.

Codecs with VAD (Voice Activity Detection) make VAD active on the system, which performs the same function as having silence suppression active.

G.729A

The G.729A CODEC samples the voice stream at 8Kbps. It is the same as the G.729 with reduced complexity.

GET ch 3

H

HP Open View

A widespread system management software developed by Hewlett Packard.

Hypertext Transfer Protocol (HTTP)

The set of rules used for exchanging text, graphic images, sound, video, and other multimedia files on the world wide web.

Hunt Group

Hunt groups are groups of telephones that have been configured to answer all calls to a Hunt DN. Call appearance on each telephone depends on programming. This feature allows you to direct specific lines to specific groups of people, such as a sales group, or technical group for a specific product.

I

ICMP

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, however, the messages are processed by the TCP/IP software and are not directly apparent to the application user.

Internet Protocol (IP)

The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into units called packets. Each of these packets contains the Internet address of the sender and the receiver.

IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

Interactive Voice Response (IVR)

Interactive Voice Response is an automated telephony application that prompts callers with a combination of recorded menus and prompts, and real-time data from databases. Users enter digits from their touch tone key pad that directs the IVR application to access databases and play information back to the caller.

Integrated Switched Digital Network (ISDN)

A digital telephone service that allows for a combination voice and data connection over a single, high-speed connection. ISDN service can operate over the same copper twisted-pair telephone line as analog telephone service. The Business Communications Manager uses two versions of ISDN, BRI and PRI.

J

K

Kbyte

The abbreviation for kilobyte. A kilobyte is equal to 1024 bytes.

Keycode

This code is used to enable application options on the Business Communications Manager. These codes are entered by the installer or system administrator. Keycodes are a combination of access codes that are encrypted to open a single application on a specific Business Communications Manager. Refer to the Keycode Software Installation Guide for details.

L

Local Area Network (LAN)

A network of interconnected computers, such as the Business Communications Manager, sharing the resources of a single processor or server within a relatively small geographic area.

Line pool

A group of lines used for making external calls. Line pools provide an efficient way of giving a group of users access to a group external lines using one line button. This also provides cost saving because you can assign a greater number of telephones to fewer lines, depending on your system traffic rates. Assign a line to be part of a line pool under Trunk, Line data. (Services, Telephony Services, Lines, Physical lines or VoIP lines).

Note that PRI lines have a separate line pool collection (PRI A to PRI 0). PRI line pools cannot be directly accessed. They must be put configured into routes, which are then assigned a destination code.

Log Snapshot

A log file containing system information and settings at the moment this event occurs.

Loss of Signal (LOS)

The loss of signal is the detection of a loss of data or voice transmission on a line.

M

Media Bay Module (MBM)

A media bay module is a computer module which provides access to telecommunications trunks.

- The digital trunk media bay module (DTM) provides the connection between a standard digital PSTN T1 or PRI line and the Business Communications Manager system.
- The Caller ID trunk media bay module (CTM)/Global analog trunk module (GATM) provides the ability to access four (CTM/GATM4) or eight (CTM8/GATM8) analog Caller ID PSTN lines. The 4X16 module combines a CTM and a DSM to support four lines and 16 telephone connections on one module.

  The GATM, connects to the lines through an amphenol connector rather than an RJ connector like the CTM. The GATM also supports downloadable firmware (BCM 3.5 and newer software), depending on how the country DIP switches are set. Currently the GATM is only supported in North America, Australia, United Kingdom and Taiwan markets.
- The Basic Rate Interface media bay module (BRI) provides access to a maximum of eight BRI ISDN telephone lines, two per loop. Each loop on the BRI can be configured for either ISDN trunks or ISDN station devices.MCDN

  Although defined as a Meridian Customer-Defined Network, this network protocol provides Meridian system attendant features (break-in and camp-on) to Business Communications Manager systems that are network to the Meridian over PRI SL-1 lines, providing the MCDN keycode has been entered at the Business Communication Manager. There are setup requirements from both ends of this network link to properly enable the features. The MCDN protocol also provides network trunking features such as Trunk Anti-Tromboning (TAT) and Trunk Route Optimization (TRO). Business Communications Managers can also be networked without a Meridian system, but in this case, the Meridian attendant features are not supported. VoIP trunks can also provide MCDN networking features if the MCDN keycode is applied to the system.

Management Information Base (MIB)

The Management Information Base is a virtual information store that contains a collection of objects that are managed using Simple Network Management Protocol (SNMP). The MIB is the software that defines the data reported by a computing or network device and the extent of control over that device.

Media Gateway Server (MGS)

The Media gateway server (MGS) service provides a means to bridge calls between the IP and time division multiplexing (TDM) domains independently of the type of IP endpoint, whether UniStim or H.323 terminal, H.323 trunk, or Voice Mail.

Mean Opinion Score (MOS)

The mean opinion scores are a measure of the quality of the voice link, while using an IP trunk, for each codec type.

Media Path Server (MPS)

The Media path server is an NT service which manages the allocation of media paths over the IP network.

N

Network Address Translation (NAT)

The Network Address Translation feature is a network security feature. NAT translates the IP addresses used within your private network to different IP addresses known to Internet users outside your private network. NAT helps ensure network security because each outgoing or incoming request must go through a translation process that also provides the opportunity to qualify or authenticate the request or match it to a previous request. NAT also translates port numbers.

NAT is defined by creating a set of rules and then defining the order in which these rules are evaluated.

Network Configuration Manager (NCM)

The Network Configuration Manager provides centralized configuration and system management capabilities for a number of Business Communications Manager in a network. This centralized functionality is required to enable multi-site Business Communications Manager customers and channel partners to significantly reduce the cost of ownership of their systems.

Network Operations Center (NOC)

The Network Operations Center domain represents the tools, equipment and activities used to analyze and maintain the operation of the Business Communications Manager network. The BCM50 Element Manager and Network Configuration Manager applications provide the software interface to perform network control and maintenance functions. The controller workstations can be located across different enterprise sites.

Network Time Protocol (NTP)

Network Time Protocol (NTP) is an IP protocol that allows you to synchronize the time on your network devices. The NTP Client allows you to synchronize the time on your Business Communications Manager system with the NTP Server on your network. This ensures that your Business Communications Manager is using the same time as the other Business Communications Manager systems and servers on your network.

O

OAM

See DECT OAM

Out of Frame (OOF)

Out of Frame is an alarm signal that indicates that some or all frame bits have been lost.

Operational Log

Operational logs contain information about the system and its use. The information captured is of interest to administration and users and may require monitoring on a regular basis. Operational logs all follow the same format and all are viewable in the log browser tool. Operational logs are accessible by users and administrators.

P

PDR

Ping

This utility is used to echo messages to a host over an IP network. This allows you to find out if the other point is available. Ping also can include statistics about how long it took from end to end, which provides information about routing.

Point-to-Point Protocol (PPP)

Point-to-point protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected to a server by a telephone line. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

Point-to-Point over Ethernet (PPoE)

Point-to-Point over Ethernet is the protocol Business Communications Manager uses when connecting to a data network using a broadband modem. Digital Subscriber Line (DSL) modems and cable modems are examples of broadband modems.

When the Business Communications Manager uses a PPPoE connection, the Internet Service Provider (ISP) can control access, billing and other types of service on a per-user, rather than a per-site basis.

Primary Interface (PRI)

Primary Interface (PRI) ISDN lines use 23 B-channels (North America) and a D-channel (23B+D). E1 PRI provides 30 B-channels and a D-channel (30B+D).

Private Branch Exchange (PBX)

A PBX is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external telephone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company central office since the PBX is owned and operated by the enterprise rather than the telephone company.

Public Switched Network (PSTN)

The Public Switched Network (PSTN) provides central office lines that connect the system to the public network. Configure lines under Telephony Services, Lines.

Note: Private network lines are PSTN lines that have been designated by the central office as exclusive lines that directly connect two private telephony systems. In a private network, toll charges are not charged on a per-call basis, but are figured into the cost of the line services.PSTN Fallback

VoIP trunks can be configured to revert to land lines processed over the PSTN (public switched telephony network) if the IP network experiences quality issues. This process occurs during call setup. QoS must be active on the network to use this feature.

Public Key

A public key is known to the public and used by a transmitting person or device to encrypt data. A private key is then used to decrypt it.

PUT ch 3

PuTTY

A SSH client application used to provides an access interface that allows you to connect to the text interface used by the Business Communications Manager.

Q

Quality of Service (QoS)

On the Internet and in other networks, Quality of Service (QoS) refers to guaranteed throughput level. QoS allows a server to measure, improve and, to some level, guarantee the transmission rates, error rates, and other data transmission characteristics. QoS is critical for the continuous and real-time transmission of video and multimedia information which use high bandwidth.

R

Remote Alarm Indication (RAI)

A Remote Alarm Indication is an outgoing signal that a device sends when it has lost an incoming signal.

Real-Time Transport Protocol (RTP)

The Real-Time Transport Protocol is an Internet protocol that specifies a way for programs to manage the real-time transmission of data over network services. RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data because of various network characteristics.

S

SAMBA

SAMBA is the open source implementation of the SMB file sharing protocol that provides file and print services to SMB/CIFS clients. Samba allows non-Windows servers to communicate with the same networking protocol as Windows products.

SCP ch 3

Severely Error Seconds (SES)

Severely Error Seconds These parameters are defined as per TIA-547A.

Sensitive Logs

Sensitive logs are diagnostic logs which may contain sensitive customer information such as personal identification numbers.These logs are usually only needed in the event of a support situation.

Secure File Transfer Protocol (SFTP)

Secure File Transfer Protocol is a secure version of the File Transfer Protocol (FTP). It uses FTP commands to transfer files securely between accounts, whether the accounts are on the same device or on different devices if it is properly configured.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is the protocol governing network management and the monitoring of network devices and their functions. This protocol uses Management Information Bases to define what information is available from a device.

System Information Logs

System information log files are not strictly log files. Rather, the log file captures information about the system and its settings at the time of the log snapshot. This file is generated automatically so a user or administrator does not specifically have to request to save or transfer it.

SSH

SSH service software is a secure software application from SSH Communications Security used on the BCM System.

SSH Key-Pair

SSH key pairs consist of a public key and a private key. The private key contains data which only the device you are working on should have to decrypt incoming data. The public key will be uploaded to remote hosts when connecting.

Secure Socket Layer (SSL)

Secure Sockets Layer is a security protocol that the Business Communications Manager uses to provide secure access to the system, including the Element Manager. The access application recommended by Nortel is PuTTY SSH (by SSH inc.). This application replaces the Telnet access used on BCM 3.0 and previous versions of the Business Communications Manager.

T

T1

Digital carrier system or line that carries data at 1.544 Mb/s.

Tar File

A Unix-based file that does a similar compression function as Winzip. It is primarily used in the backup and logs feature of the BCM50 Element Manager.

TDM ch 9

Third Party Log

A log file of third party hardware or software in the BCM System.

Trace Route

Trace route is a utility that traces a packet from a device to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes.

Time-to-live (TTL)

Time-to-live is a field in the Internet Protocol header which indicates how many hops a packet should be allowed to make before being discarded or returned.

U

Unavailable Time Seconds (UAS)

Unavailable Time Seconds These parameters are defined as per TIA-547A.

UIP ch 9

Universal ISDN Protocol

Universal Power Supply (UPS)

The Universal Power Supply is a third-party piece of hardware that attaches through the Business Communications Manager serial port to provide power backup in case of a power failure.

Universal Serial Bus (USB)

Universal Serial Bus is a standard bus type for all kinds of devices, including mice, scanners, digital cameras, printers, and memory storage devices. The transfer rate is 12 Mbps. Devices can be connected and disconnected while the computer is on.

UTPS

This is a Nortel-designed protocol for IP telephony applications. The Nortel IP telephones, for instance, use this protocol to communicate with the Business Communications Manager.

V

V.90

A data transmission standard used by the modem installed in the Business Communications Manager base unit. This standard allows data to be transmitted to the modem at 56 kbit/s and transmitted from the modem at 33 kbit/s.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol is the capability to deliver voice using the Internet Protocol. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN).

Virtual Private Network (VPN)

The Business Communications Manager uses the Internet and tunneling protocols to create secure extranets. These secure extranets require a protocol for safe transport from the Business Communications Manager to another device through the Public Data Network (PDN). Business Communications Manager uses the PPTP and IPSec tunneling protocols. Both of these protocols have encryption, but IPSec has a slightly more secure hashing algorithm for negotiating keys.

When connecting two branch offices, the use of a VPN over the public data network is very efficient if the connection is required only intermittently or a dedicated point-to-point link is considered too expensive. Also, with the advent of business-to-business solutions, VPNs can be deployed to provide secure connections between corporations.

W

Wide Area Network (WAN)

A collection of computers or Business Communications Managers connected or networked to each other over long distances, normally using common carrier facilities.

X

Y

Z

Index