Part No. P0609330 3.0
October 29, 2004

Business Communications Manager

Management Guide

NORTEL NETWORKS

Copyright © 2004 Nortel Networks

Trademarks

Software licensing

The Apache Group

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
4. “This product includes software developed by the Apache Group for use in the Apache HTTP server project (*http://www.apache.org/*).”
5. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.
6. For written permission, please contact *apache@apache.org.*
7. Products derived from this software may not be called “Apache” nor may “Apache” appear in their names without prior written permission of the Apache Group.
8. Redistributions of any form whatsoever must retain the following acknowledgment:
9. “This product includes software developed by the Apache Group for use in the Apache HTTP server project (*http://www.apache.org/*).”

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see *http://www.apache.org/*.

Contents

Figures

Tables

Preface

The *Business Communications Manager Management Guide* describes how to manage, maintain and sustain Business Communications Manager 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 Business Communications Manager (BCM) and BCM network. This guide provides task-based information on how to detect and correct faults through the interfaces and reporting system.

Use the Nortel Networks Unified Manager (UM) 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 *Business Communications Manager Management Guide* is directed to network administrators responsible for maintaining BCM networks. This guide is also useful for network operations center (NOC) personnel supporting a Business Communications Manager managed services solution. To use this guide, you must:

- be an authorized Business Communications Manager administrator within your organization
- know basic Nortel Networks Business Communications Manager 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 Business Communications Manager network management applications.

Business Communications Manager Management User Guide organization provides a summary description of the contents of this document.

Table 1 Business Communications Manager Management User Guide organization

Chapter	Contents
1. Preface	An overview of the network management model, applications, tools, maintenance and monitoring objectives.
2. Fault Management System	Information on how to set-up and maintain a fault detection and maintenance program using the Unified Manager and SNMP toolsets.
3. Service Management System	Service manager capabilities available in the Unified Manager interface. This chapter also describes the properties of the services in the service manager and associated log and alarm notifications
4. Log Management	Explanation of the MSC (core telephony) log system. This chapter also describes how to access, display and erase logs and archlogs.
5. BCM Monitor	Instructions how to install, access and use the BCM Monitor application to analyze BCM system status and performance statistics.
6. Performance Management	Information on metrics gathering tools and applications to monitor the network traffic. The tools help you ascertain the performance and health of the network elements and telephony services.
7. Performance Management Using NetIQ	Information on the third-party NetIQ performance management solution for BCM.
8. Security Management	Information about how you can set up and maintain the access security to your system by users and client applications.
9. System Backup and Restore (BRU)	Information and procedures on how to execute a system Backup and Restore using the BRU.
10. Testing, Troubleshooting, and Diagnostics	Information about diagnosing module line performance issues and device line issues. The chapter also provides instructions on how to perform a system startup, set identification parameters and maintain telephony resources.
11. Management Information Base (MIB) System	BCM management information bases (MIB).

Symbols used in this guide

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

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 work improperly or to fail.

Note: Alerts you to important information.

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

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

Warning: Alerts you to remove the Business Communications Manager and Business Communications Manager expansion unit power cords from the AC outlet before performing any maintenance procedure.

Display Tips

You can best use and read this publication from your computer monitor. Use your computer to identify and access the numerous links throughout. Alternatively, you can print a hard copy. For best on-screen display results, use Adobe Acrobat Reader* version 4.0 or 5.0.

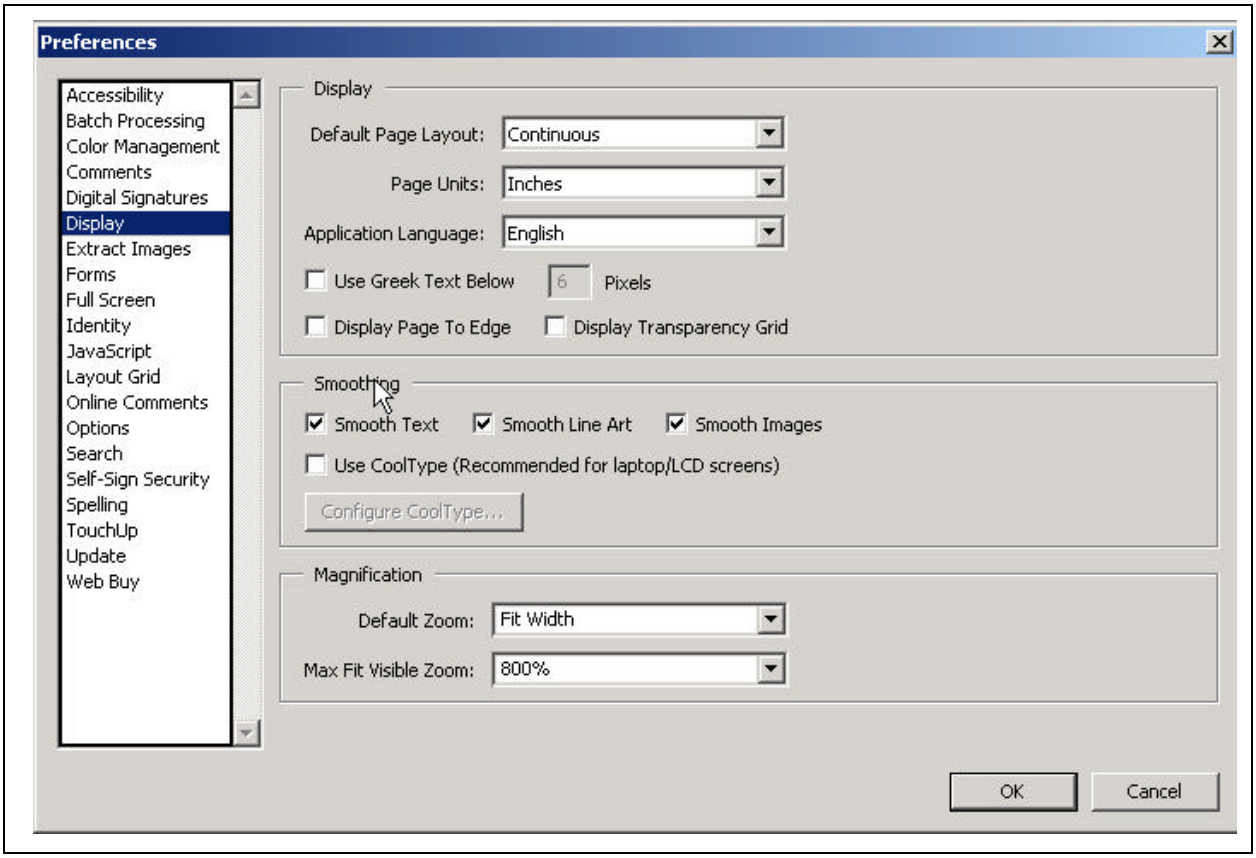
If you use Adobe Acrobat Reader, version 4.0, to optimize the illustrations:

- Increase display magnification
- Print the document

For Adobe Acrobat Reader, version 5.0, to optimize the graphical display:

1. Start the Adobe Acrobat Reader, version 5.0 application.
2. On the **Edit** menu click **Preferences** and then click **General**.
3. On the Preferences menu click **Display**.
   The Display setup page appears.
4. Select these smoothing options:
   - Smooth Text
   - Smooth Line Art
   - Smooth Images

Figure 1 Acrobat Reader display setup selections



Text conventions

This guide uses these text conventions:

`bold Courier text`	Indicates command names and options and text that you need to enter in a command-line interface. Example: Use the **`dinfo`** command. Example: Enter **`show ip {alerts|routes}`**.
italic text	Indicates file and directory names, new terms, book titles, Web addresses, and variables in command syntax descriptions.
bold text	Indicates command names, screen titles, options and text for a graphical user interface (GUI).
angle brackets (< >)	Indicates a keyboard key press or simultaneous key presses, i.e. <ENTER> or <CTRL j>

Acronyms used in this guide

This guide uses these acronyms:

API	Application Program Interface
ASM	Analog station module
ATA (or ATA2)	Analog Terminal Adapter
AWG	American Wire Gauge
BIOS	Basic Input Output System
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
CAP	Central Answering Position
COPS	Common Open Policy Service
CSU	Channel Service Unit
DASS2	Digital Access Signaling System Number 2
DECT	Digital enhanced cordless telecommunications or Digital European cordless telephone
DHCP	Dynamic Host Configuration Protocol.
DN	Directory Number
DNS	Domain Name Service (DNS)
DPNSS	Digital Private Network Signalling System
DTMF	Dual Tone Multifrequency.
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force.
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IVR	Interactive Voice Response
LAN	Local Area Network
MAC	Media Access Control
MCDN	Meridian Client Defined Network (PRI SL-1)
MIB	Management Information Base
NAT	Network Address Translation
NIC	Network Interface Card
NOC	Network Operations Center
OIT	Optivity Integration Toolkit

OSPF	Open Shortest Path First
PBX	Private Branch Exchange.
PCI	Peripheral Component Interconnect Slot
PDD	Partial Double Density
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Remote access service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
TAPI	Telephony Application Program Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
UDP	User Datagram Protocol
	Universal Dialing Plan
VoIP	Voice over IP
VPN	Virtual Private Networks
WAN	Wide Area Network

How to get help

Your local distributor provides technical support for your Business Communications Manager system or has access to that information through a Technical Service Center (TSC).

USA and Canada

Authorized Distributors - Technical Support

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

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

Presales Support (CSAN)

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

EMEA (Europe, Middle East, Africa)

Technical Support

Telephone:
00800 800 89009 or 33 4 9296 1341

Fax:
33 49296 1598

email:
emeahelp@nortelnetworks.com

CALA (Caribbean & Latin America)

Technical Support

Telephone:
1-954-858-7777

email:
csrmgmt@nortelnetworks.com

APAC (Asia Pacific)

Technical Support

Telephone:
+61 388664627

Fax:
+61 388664644

email:
asia_support@nortelnetworks.com

Related publications

These documents provide further information about the Business Communications Manager, related media bay modules, extension equipment, and system applications and software:

Business Communications Manager Programming Operations Guide

All optional Business Communications Manager applications have installation and user guides specific to that application. Refer to the *Programming Operations Guide* and *Telephone Features Programming Guide.* These guides describe core system operational configuration and how to program the Business Communications Manager equipment.

These guides provide programming for core telephony features and user features, such as:

- Voice telephony configuration for digital, IP, ISDN and radio-based telephones and equipment over analog, digital, ISDN, and voice over IP (VoIP) trunks.
- How to use and program user telephony features at the telephone
- Companion Application Server software that controls the interface between the Business Communications Manager system and the Companion wireless system (available for selected regions)
- Networking DPNSS (upgrade) (requires keycode) provides private voice networking for the UK Market.
- With Networking MCDN and ETSI Q.SIG Voice Networking (requires keycode) you can network your Business Communications Manager system, or a number of Business Communications Manager systems to a Meridian system. This lets the network use a common numbering plan, as well as common voice messaging and auto attendant systems connected to the Meridian.
- Data setup applications and protocols to configure the Business Communications Manager system to be part of a LAN or WAN network. See the next section for specifics.

Call Detail Recording System Administration Guide

Call Detail Recording (no keycode required) records and reports call activity from the Business Communications Manager. You can create reports from this information to help you manage system usage effectively.

IP Telephony Configuration Guide

- i2001, i2002, and i2004 IP telephones and the NetVision and NetVision Data telephones require a combination of data and telephony settings to work with the Business Communications Manager. These telephones can make or receive calls through either VoIP or PBX lines.
- Nortel Networks i2050 Software Phone turns your PC into a telephone interface which provides standard telephony operating features such as Voice Mail, Caller ID, and multiple telephone lines or line appearances. This application requires Windows 2000, a full duplex sound card, and a computer-telephony headset. This document describes what settings are required to use this application with the Business Communications Manager. The *i2050 Software Phone Installation Guide* provides specific installation information.
- VoIP Gateway (requires keycode) converts the voice in a call into a packet format and sends the call using an intranet trunk. With Business Communications Manager VoIP Gateway, you can make calls over any intranet connected to the Business Communications Manager system.

Chapter 1
Management Overview

This section is an introduction to the Business Communications Manager network-level management concepts and techniques.

The management overview is divided into three categories.

Management oncepts and models

Unified Manager

Management Guide overview

Network Administration Objectives

Network operations center (NOC) responsibilities encompass the operation of the entire network domain. Network administration is a complex task that requires intimate knowledge of the construction and workings of the network environment.

NOC activities

- Monitoring routers, switches, hubs, and auxiliary backup systems (power supply, data) equipment that comprise the enterprise data network.
- Monitoring network traffic trends and resolve network bottleneck problems.

- Managing and allocating IP addresses and domain names, recording and providing remote connectivity to the enterprise computing systems.

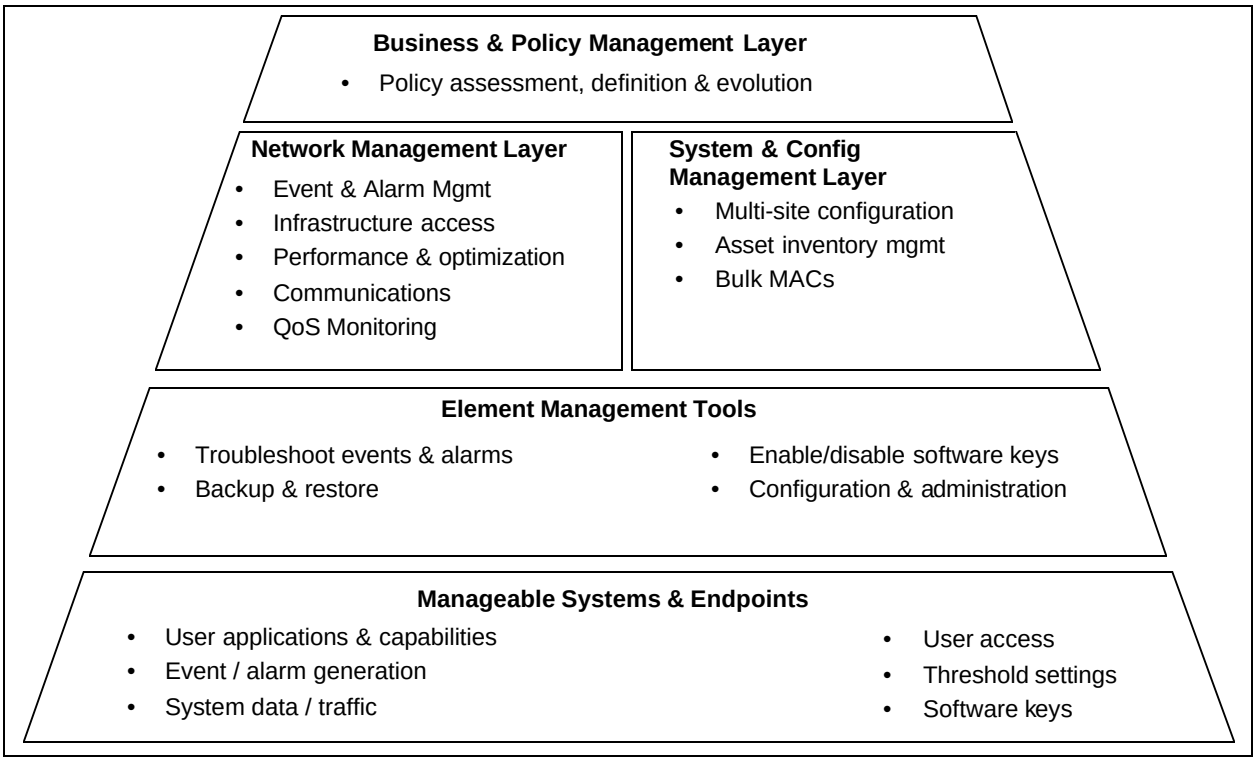
The descriptions and procedures in this guide that assist with service assurance:

- Monitoring the network for alarms and performance threshold
- Ensuring service network integrity
- Isolating, diagnosing and reparing faults
- Managing performance. NOC takes first call from the alarms and performs initial troubleshooting of the problem. Monitor link status and view, provision, edit and audit connections. Log into network elements. Monitor inventory. Monitor network performance (performance threshold provisioning).

Network management model

The Business Communications Manager network management model defines the management functions into layers that show the flow of management information between communicating entities. The Business Communications Manager network mode figure illustrates the management layers.

Figure 2 Business Communications Manager network model



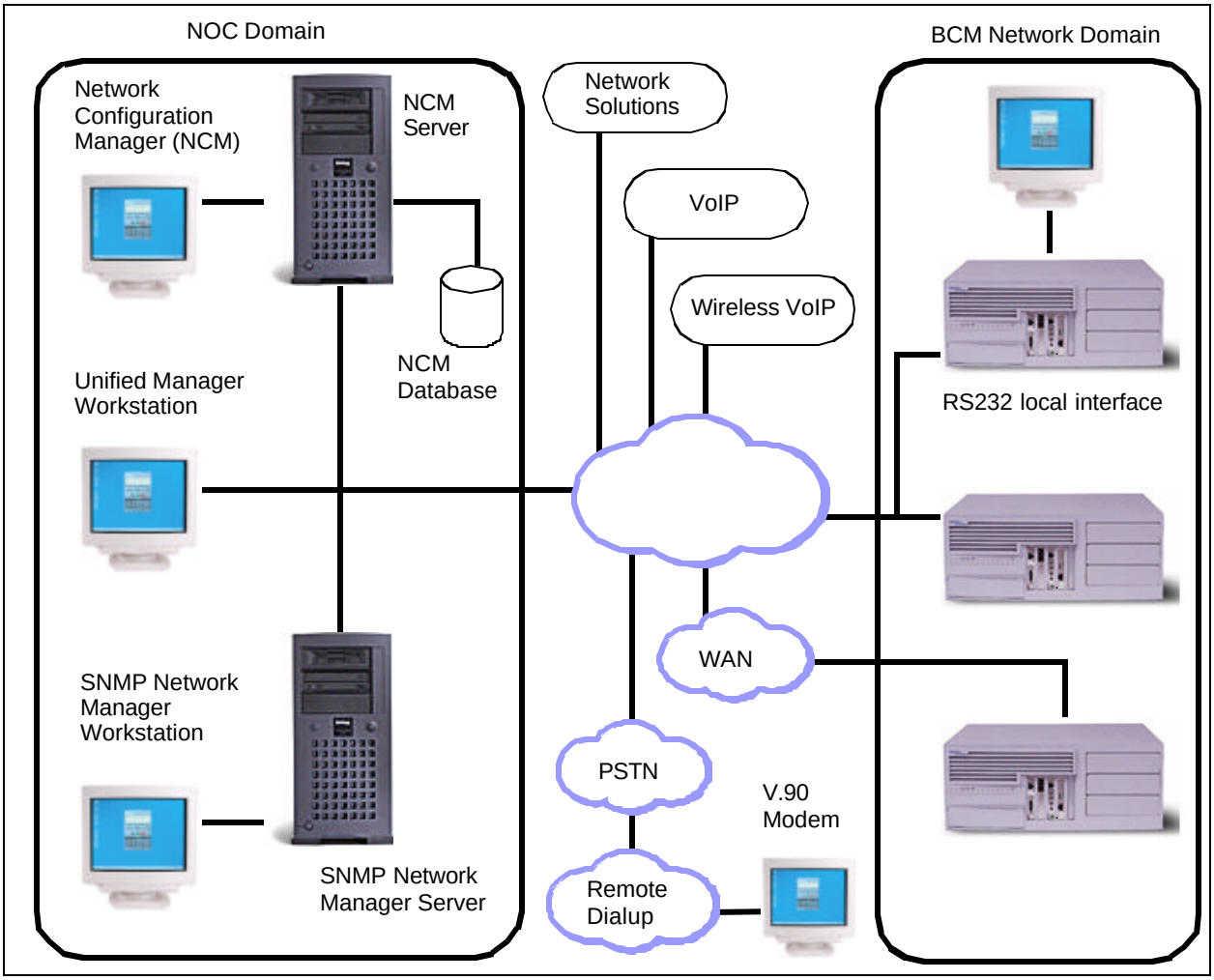
Network Topology and Management Interfaces

Business Communications Manager Unified Manager, Network Configuration Manager and SNMP Network manager support the objectives and knowledge requirements of NOC network administrators. These applications detect, observe and report on the state of the network elements and the overall health of the network.

"Business Communications Manager enterprise network model" on page 30 shows a sample Business Communications Manager enterprise network that illustrates the various communications links to end devices and control consoles. 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 the Business Communications Manager network. Unified Manager and Network Configuration Manager provide the software interface to perform network control and maintenance functions. The controller workstations can be located across different enterprise sites.
- The BCM network domain represents one or more Business Communications Managers networked through an enterprise LAN to one or more controller workstation. The Business Communications Managers need not be co-located at the same site. The WAN represents an adjacent network, external to the LAN.
- The VoIP and Wireless VoIP domains represent terminating IP devices.

Figure 3 Business Communications Manager enterprise network model



Network management physical interfaces

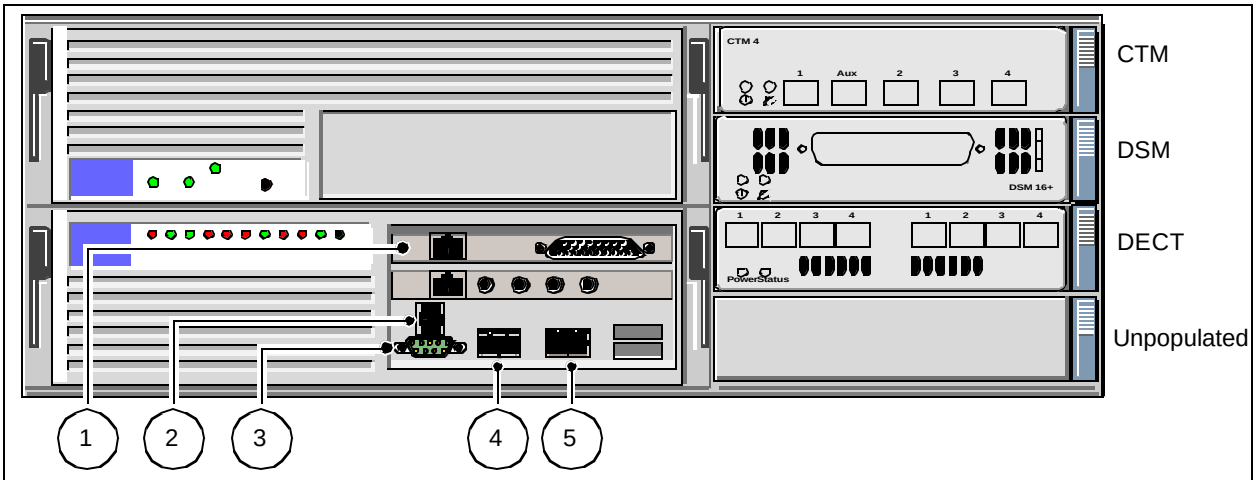
Business Communications Manager offers alternatives on how to connect to, and access, the Business Communications Manager unit and devices in the network (see "Business Communications Manager physical interfaces" on page 31). Connectivity to the network and Business Communications Manager depends on the network configuration and telephony resources built in the system.

Physically, the Business Communications Manager network can be distributed geographically across different sites. The network administrator must be able to access each BCM in the network.

Network administration personnel have the ability to configure, observe and control the operation and performance of the Business Communications Manager through one of the available access portals. These interfaces provide management access to the Business Communications Manager (see Figure 4):

- **WAN IP interface**: WAN internet access (IP access through the Unified Manager interface) The WAN interfaces use T1 (with CSU), V.35, X.21, PRI/BRI MBMs Dial on demand. Establish a connectivity path provided from the corporate LAN network to the end-user's WAN network or ISP over another WAN device (e.g. router elsewhere on the enterprise premises).
- **V.90 Dial-up modem interface**: (North America option only) The dial-up connection interface is available for occasional use. Due to modest dialup speeds, and potentially large file sizes, dial-up has limited use. For regular backup/restore and configuration tasks, use a higher bandwidth connection for management access to the Business Communications Manager.
- **Local RS232 serial interface (COM port)**: Local terminal emulation interface. The Business Communications Manager platform base chassis has a serial RS232 port. The RS232 port provides local terminal emulation connectivity to the BCM. This method is normally used upon initial install. Use local connectivity to set the system's IP address and other basic system and networking parameters to enable the BCM for remote access. Alternatively, the RS232 port is used to establish a local connection to perform local maintenance activities in the event of an IP network communications failure.
- **LAN IP interface**: local LAN port (IP access through the Unified Manager interface). The LAN Ethernet interface transmits at 10/100 Mbps. Use IP over a LAN Ethernet interface.

Figure 4 Business Communications Manager physical interfaces



1. WAN card (field upgrade) connects the Business Communications Manager system to the wide area network.
2. V.90 Modem port (available in North America only) provides PSTN dial-up access to the BCM.
3. Local RS232 COM port provides a serial connection to a laptop for maintenance purposes. Also supports a DB9 serial connection to a UPS for power monitoring (see *UPS Installation and Configuration Guide*).
4. Ethernet port connector #2 provides access to internal local area network
5. Ethernet port connector #1 provides access to external local area network

SNMP Network Management Concepts

Your Business Communications Manager network uses several hardware devices and various software applications. Network management software provides the ability to exercise control over the network devices.

Refer to these descriptions:

- "Network management communication protocols" on page 32
- "SNMP network structure" on page 32

Network management communication protocols

The SNMP, HTTP, Telnet, and FTP protocols are fundamental to management of a network of Business Communications Managers.

- **SNMP** (simple network management protocol): SNMP is application-layer software you use to communicate with and control devices in your network.
- **HTTP** (hypertext transport protocol): HTTP is a communications protocol that lets users establish a connection with a Web server and transmit HTML pages to a client browser. BCM is a web-server. HTTP also allows transmission of other files required by an HTTP application.
- **Telnet**: Telnet is a terminal emulation communications protocol used on the Internet and TCP/IP-based networks. Telnet allows a network administrator or user to use a local workstation to log onto a remote computer and run a program. Telnet is part of the TCP/IP protocol.
- **FTP** (file transfer protocol): FTP is a protocol used to transfer files over a TCP/IP network (Internet, Unix). With FTP you can log onto the network, list directories, and copy files from other workstations/servers. FTP operations are performed by typing commands at a command prompt or through an FTP utility running under a graphical user interface (GUI).

SNMP network structure

Network management objectives for the Business Communications Manager are based upon the FCAPS network management model (fault, configuration, administration, performance, security). To accomplish these objectives, the Business Communications Manager must have the ability to provide appropriate feedback to the network administrator.

Network administrators use SNMP data do manage network performance, find and solve network problems and plan for network expansion (see "Network Administration Objectives" on page 27.)

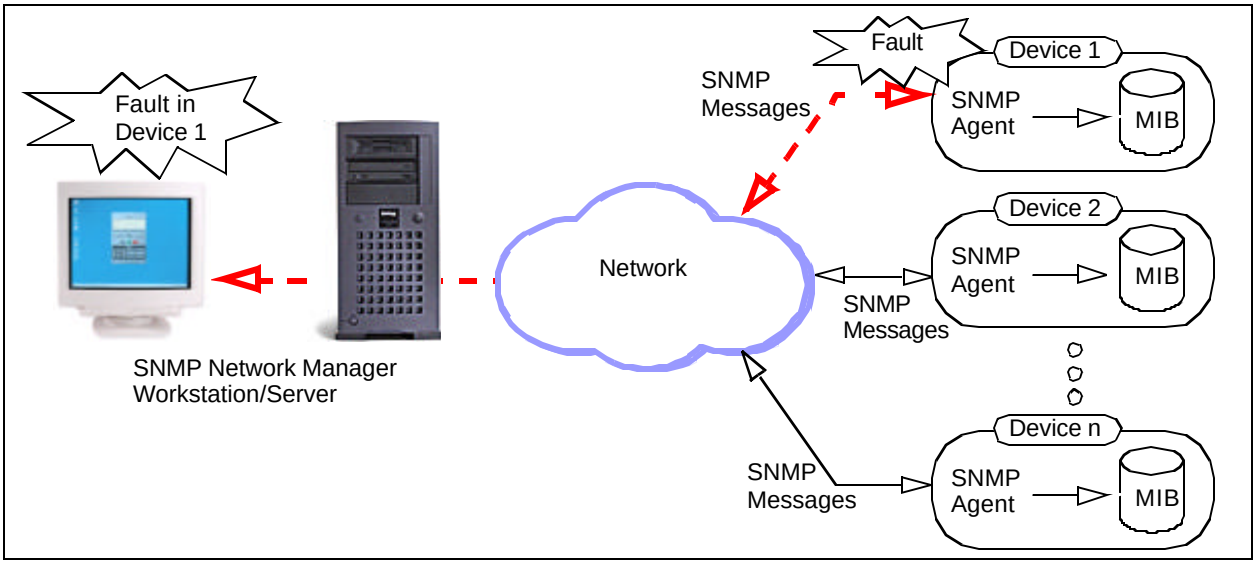
The Business Communications Manager network management system is composed of:

- **SNMP network management stations** (*NMS*): A console (server/workstation) through which the network administrator performs network management activities upon managed objects. The SNMP network manager server (workstation) is a physical control device equipped with network management software that interfaces with the Business Communications Manager(s) in your network.

- **SNMP agents**: SNMP agent software interfaces and handles interaction between the device and the SNMP network manager workstation. SNMP agents are software modules resident in network elements, in this case the BCM. The SNMP agent collects, stores and retrieves MIB (management information base) data and forwards the information to the SNMP network manager server.
- **Network elements** (*managed devices*)*:* Hardware components such as computers, routers, and terminal servers that are connected to networks.
- **Managed objects**: Hardware, configuration parameters or performance statistics that directly relate to the operation of a device. Bridges, hubs, routers, or network servers are examples of managed devices that contain managed objects.
- **Management information base** (*MIB*): The MIB is the software that defines the data reported by the device and the extent of control. A virtual information store that contains a collection of managed objects.
- **Management protocol (SNMP)**: Used to transport management information between the agents and console. Simple network management protocol (SNMP) is the standard management protocol. An SNMP trap is a message format used by the SNMP agent to inform the NMS of a system event.

Managed objects and agents illustrates the agent and object relationship in a network and how the system provides event notification to the SNMP network manager workstation. Data passes from SNMP agents (hardware/software processes that report activity in all network devices) to the SNMP Network Manager server.

Figure 5 Managed objects and agents



Network Management and Maintenance Applications

The tools and applications bundled with the BCM provide statistics and notifications of system status and operation. There are three categories of network management applications that are available and compatible for operation with the BCM or network elements:

- BCM-specific tools and applications
- optional tools and applications
- third-party tools and applications

BCM-specific tools and applications

- **Unified Manager** (see also "Unified Manager" on page 34) is web-based configuration and maintenance application bundled with the Business Communications Manager software. Unified Manager is the single point of access for managing all programming for individual BCM systems. Access to the Unified Manager is password protected, and is secure for both enterprise customers and small to medium sized businesses. Administrators use Unified Manager to quickly set up BCM telephony and data functions, as well as users, mailboxes, and directory numbers.
- **Network Configuration Manager (NCM)** 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.
- **BCM Monitor**: Use this standalone diagnostic application 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. You can also use BCM Monitor to save and process data at a later time to generate system utilization and traffic reports.

Optional tools and applications

- **Optivity Network Management System (ONMS)**: Use Optivity NMS to manage Nortel data devices such as Baystack switches, BPS2000, Passport LAN switches, BayRS, and Alteon. Integrate Unified Manager into the Optivity Network Management System (NMS) via the Optivity Integration Toolkit (OIT). Enable BCM discovery, launch, and alarm integration into Optivity NMS. Business Communications Manager appears as an element in an ONMS network discovery diagram. BCM SNMP traps are displayed by ONMS, and Unified Manager is launched from within Optivity.

Note: If you require an integrated Unified Manager/ONMS configuration, contact Nortel Networks to confirm the correct interoperation of the current releases BCM and ONMS.

Unified Manager

Unified Manager, a web-based navigation tool, provides access to all operations and maintenance programming functions on the Business Communications Manager system. Unified Manager allows authorized administration personnel to monitor and control BCM functions from a single site.

Unified Manager is the single point for managing all programming for individual BCM systems. You can access Unified Manager locally via the LAN or WAN. Remote access is available via a V.90 modem dialup. You can also access Unified Manager through a browser from across a WAN or Internet connection.

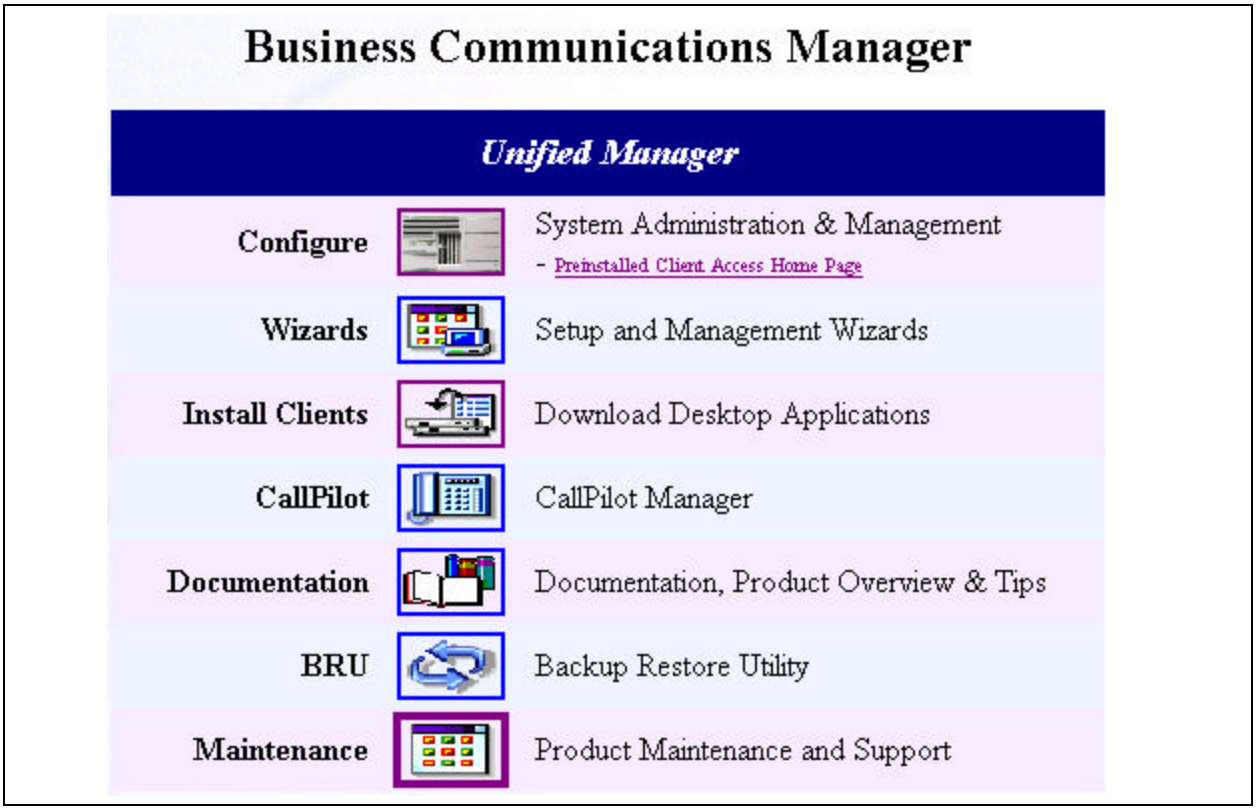
Use Unified Manager to configure data and voice services on Business Communications Manager. Unified Manager gives you data entry and performance tracking charts and tables for network monitoring, access to alarm and event notifications and diagnostic information.

This section includes information about:

Using the Unified Manager main page buttons

When you access the Unified Manager main page (see "Unified Manager main page" on page 36), several selections provide access to operations grouped under these functional categories:

Figure 6 Unified Manager main page



Configure

Access the Unified Manager programming interface for all services except those controlled by the CallPilot and IVR services.

Wizards

When you install your system, you run the Quick Start Wizard to set up your system parameters. This wizard is described in the Wizard help, that can be accessed after you from the Wizards page of the Unified Manager.

Use the Wizards to perform Quick Start, Add Users, Edit DN Record Template, DN Renumber, Network Update. See the *Programming Operations Guide* for more information.

The Wizards are self-contained task applications that you can use to speed up some configuration tasks. You access the Wizards from the Wizards button on the first page of the Unified Manager. See the *Programming Operations Guide* for more information.

Figure 7 Programming Wizards

Wizard	Action
Quick Start	Initializes the system and sets up your basic system information. This wizard is only run once, when your system is first set up.
Add Users	Changes the telephony settings for a set of DNs or for a single DN. You can define the settings in this Wizard, or you can use a pre-defined template, from a local site or from a remote site, created with the Edit DN Record Template wizard.
Edit DN Record Template	Selects Telephony User Templates and change and define the user settings for telephones. The Telephony Template is stored in a file for use with the Add Users Wizard.
DN Renumber	Renumbers a range of DNs.
Network Update	Updates your system data network settings any time after the Quick Start Wizard, which does the initial network setup.

Wizard	Action
Quick Start	Initializes the system and sets up your basic system information. This wizard is only run once, when your system is first set up.
DECT Mobile Recording	Enables and disables mobile recording for one of the base station ports.
DECT Configuration	Configures a DECT module. It also turns on one of the base station ports to allow mobile recording (handset registration). The DECT Wizards appear on the Wizards page only if there is a DECT module installed and identified to the system. These wizards are discussed in the *DECT Installation and Maintenance Guide*.

Navigating the wizards

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

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

Installing clients

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

You access optional applications through the **Install Clients** button. Many applications require a keycode. For information about how to set up these optional features, see the documentation for each application.

With the install clients utility you can select and download multimedia and telecommunications clients. Applications can require other components or software keys to be installed. Each application page identifies if anything else is required.

Clients you can download

Applications

- Call Center and Multimedia Call Center

- CallPilot
- Interactive Voice Response (IVR)
- Desktop assistant, i2050 software phone, Personal Call Manager, NetVision Symbol phone administrator

Toolkits

- CDR Client wrapper
- LAN CTE client
- TAPI 2.1 installation
- Unified Manager Java class library

Developer information

- Program description
- Developer categories
- Developer partners

Administrative tools

- Desktop assistant Pro E
- BCM Monitor
- SSH client

CallPilot

Click the CallPilot button to access CallPilot Manager, the CallPilot management application. CallPilot Manager is a web-based application that you use to administer:

- Voicemail
- Call answering
- Auto Attendant
- Custom Call Routing
- Fax answering
- Call Center
- Message Networking

Note: Basic CallPilot functions are standard on the Business Communications Manager and you define your region and basic settings when you run the Quick Start Wizard. See the *Programming Operations Guide* for more information.

Documentation

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

- Provides access to:
  - — Documentation on how to install hardware, configure and operate various BCM-specific applications.
  - — Product overview
  - — Download Adobe Acrobat Reader

BRU

Click the BRU (Backup and Restore Utility) button to access BRU functionality. BRU provides a way to back up your system data and configurations in the way that is most useful for your purposes. Backed up data can be restored to the BCM if a system failure occurs, such as a prolonged power outage. See System Backup and Restore (BRU) on page 381 for more information.

Maintenance

The Maintenance button accesses a number of maintenance tools that let you determine the current status of the various aspects of your Business Communications Manager system. For more information see the description “Unified Manager Maintenance Page Overview” on page 43.

Using Unified Manager

Unified Manager is a web-based navigation tool you use to view and change configurations for the Business Communications Manager system.

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

For more information on how to use the Unified Manager interface, see the *Programming Operations Guide.*

Understanding the navigation tree headings

The Unified Manager navigation tree contains five main headings that you use to access specific areas of the Business Communications Manager system. These headings are:

Table 2 Navigation tree menu functions

Heading	Programming
System	Provides access to Licensing, Identification and Security subheadings. This includes a form to enter keycodes, and a list of current supported services. From the Security heading you can determine the level of security within and entering the system. See Chapter 9, "Security Management". When you select the System heading, you can view system information such as your system name and a description about which resources and services are available. Selecting the System heading also enables Configuration, Performance, Fault, Logoff, View, and Help. With these commands you can: • enable/disable services • access CPU and memory status • access to the alarm banner, which displays totals of alarms • access or refresh a system inventory list • reboot the system or shut down operations
Resources	Provides access for configuring data and telephony resources for Business Communications Manager hardware setup. See the *Programming Operations Guide* as well as in the *DECT Installation and Maintenance Guide*.
Services	Provides access for configuring telephony and data networking services and various other related services. Telephony information is discussed in the *IP Telephony Configuration Guide*. System data configuration is discussed in the *Programming Operations Guide*. This section also supports the information found in the CallPilot documentation, and the documents for CDR Recording, LAN CTE, IVR, Doorphone, Network administration, *UPS Installation and Maintenance Guide*, and *DECT Installation and Configuration Guide*. To manually enable or disable the Telnet service, See "Manually activating Telnet" on page 431.
Management	Provides access to the User Manager, which you use to manage the users who have access to the Unified Manager (Chapter 9, "Security Management"), and to the Alarm Manager, which is used to define why types of alarms get reported by the system. For more information on alarms and SNMP traps, see Chapter 2, "Fault Management System".
Diagnostics	Provides access to items you can use to generate and access statistics on different system components. Business Communications Manager provides statistics, metrics and event logs on resources and services to help you carry out system maintenance activities. System metrics information is contained in the programming section to which they apply. See the *Programming Operations Guide* and the *IP Telephony Guide*. Split DS30 configuration and double density configuration are located under the Configuration menu of the MSC heading. These system features are discussed in the *Programming Operations Guide*.

Logging off Unified Manager

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

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

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

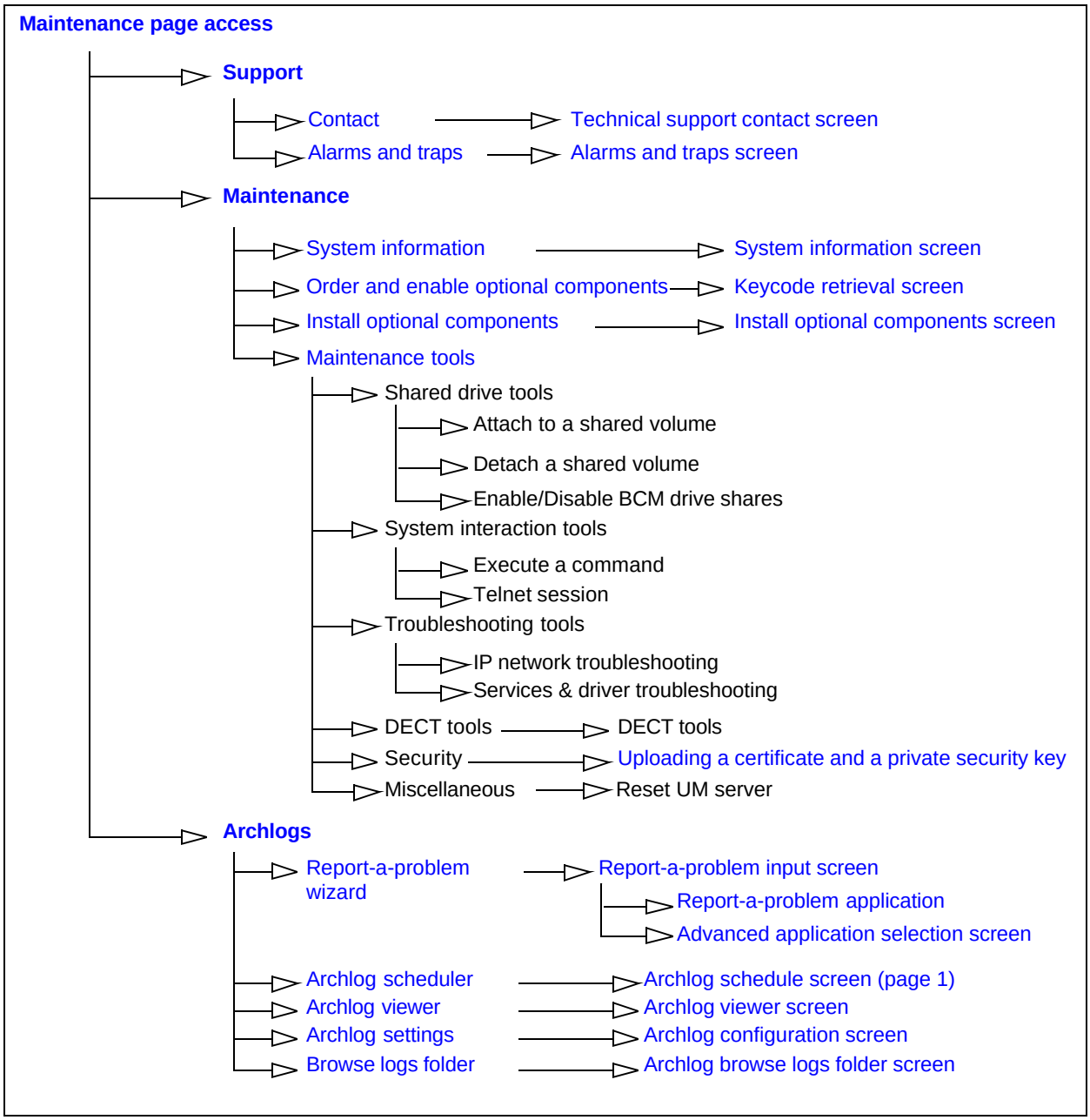
Note: Exit both Unified Manager browser windows, even if you want to re-log on to the Configuration area. After you exit both windows, you can reestablish a connection with the Business Communications Manager and log on as usual.
Failure to log out of both browser windows can result in a failed attempt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

Unified Manager Maintenance Page Overview

The maintenance page is a dedicated maintenance area that provides access to several maintenance tools and capabilities. Gathering these tools into one location provides the network administrator with a single source for maintenance information, helping to reduce errors and contribute to gaining overall serviceability efficiency.

Figure 8 summarizes the links through the maintenance page. Select any of the links in Figure 8 to display a description of the maintenance function.

Figure 8 Unified Manager maintenance page paths



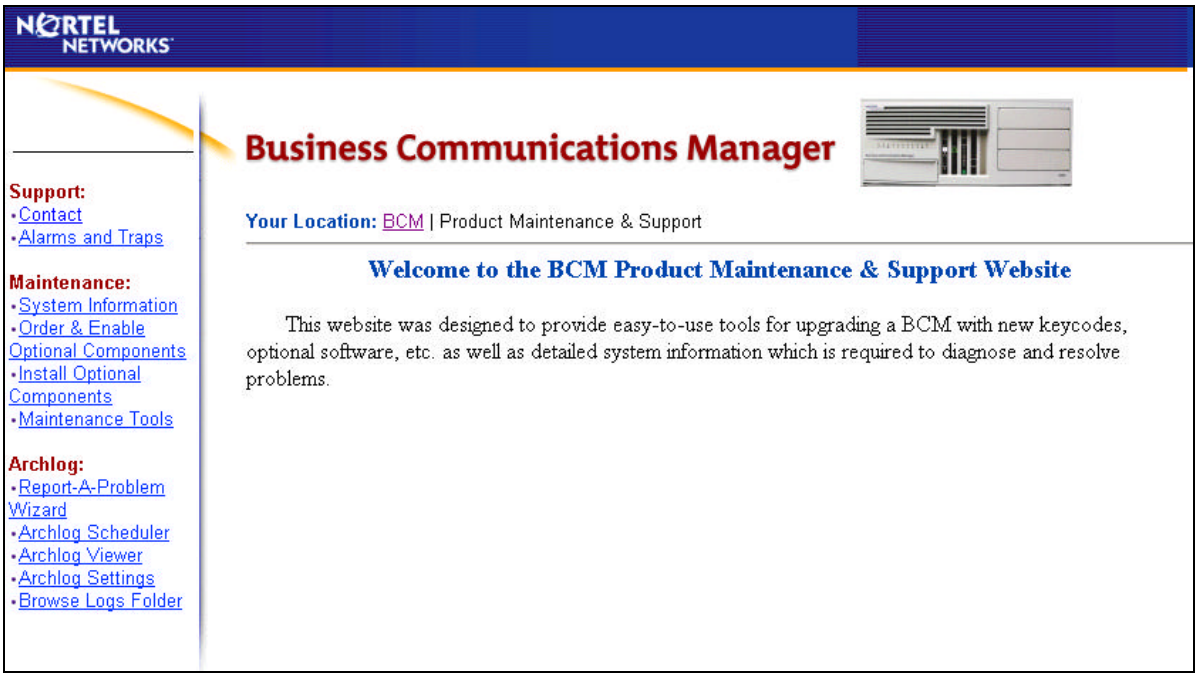
Maintenance page access

Access the Maintenance page by clicking the Maintenance button on the Unified Manager main page (see Figure6 on page36).

Tools and applications on the Unified Manager maintenance page

Support	Maintenance	Archlog
Contacts	System information	Report a problem wizard
Alarms and traps	Order & enable optional components	Archlog scheduler
	Install optional components	Archlog viewer
	Maintenance tools	Archlog settings
		Browse logs folder

Figure 9 Unified Manager Maintenance page selections



Support

Maintenance page support selections are:

- Contact
- Alarms and Traps

Contact

The contact screen displays the ITAS contact telephone numbers and contact instructions for all regions.

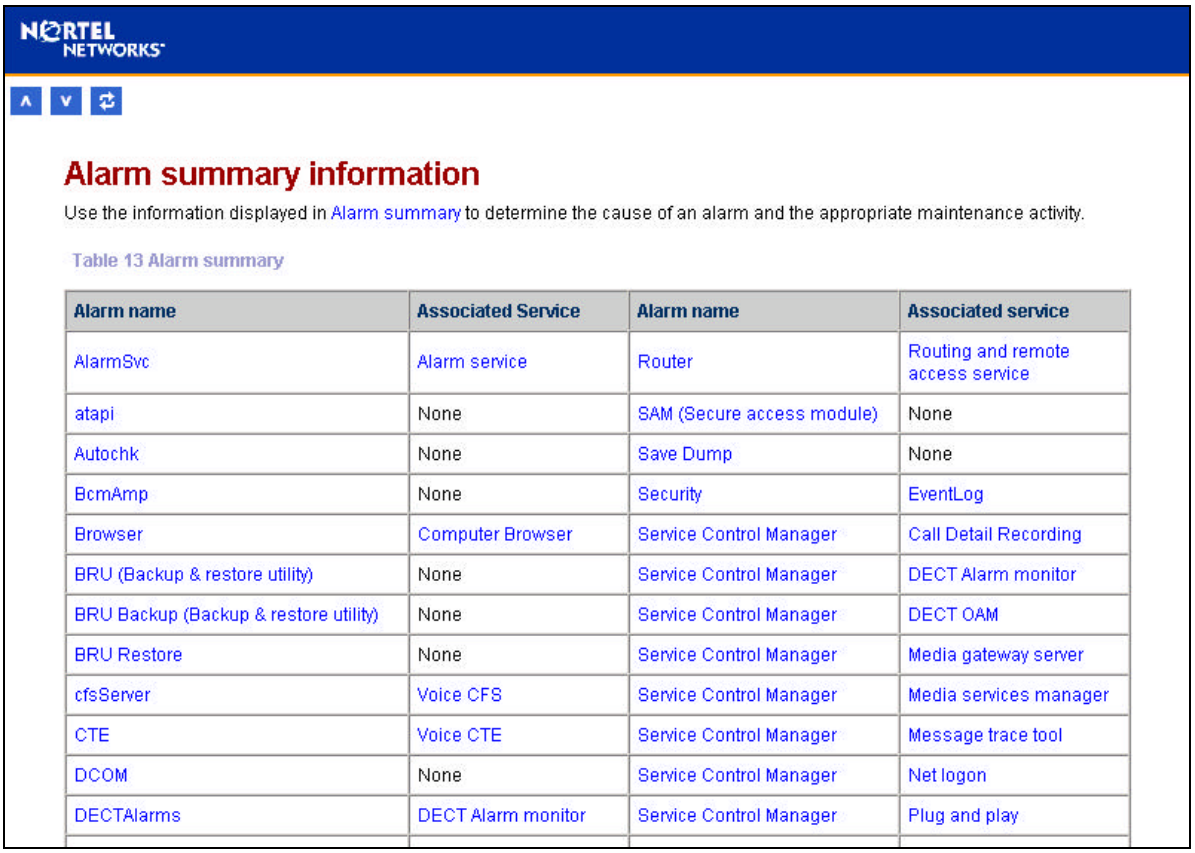
Figure 10 Technical support contact screen

Alarms and traps

The alarms and traps screen provides a summary list of BCM component ID alarms.

Select one of the component ID alarm links to navigate to a full description of the alarm and associated service (if any). For more information on alarms and traps, see Chapter2, “Fault Management System.

Figure 11 Alarms and traps screen



NORTEL NETWORKS

Alarm summary information

Use the information displayed in Alarm summary to determine the cause of an alarm and the appropriate maintenance activity.

Table 13 Alarm summary

Alarm name	Associated Service	Alarm name	Associated service
AlarmSvc	Alarm service	Router	Routing and remote access service
atapi	None	SAM (Secure access module)	None
Autochk	None	Save Dump	None
BcmAmp	None	Security	EventLog
Browser	Computer Browser	Service Control Manager	Call Detail Recording
BRU (Backup & restore utility)	None	Service Control Manager	DECT Alarm monitor
BRU Backup (Backup & restore utility)	None	Service Control Manager	DECT OAM
BRU Restore	None	Service Control Manager	Media gateway server
cfsServer	Voice CFS	Service Control Manager	Media services manager
CTE	Voice CTE	Service Control Manager	Message trace tool
DCOM	None	Service Control Manager	Net logon
DECTAlarms	DECT Alarm monitor	Service Control Manager	Plug and play

Maintenance

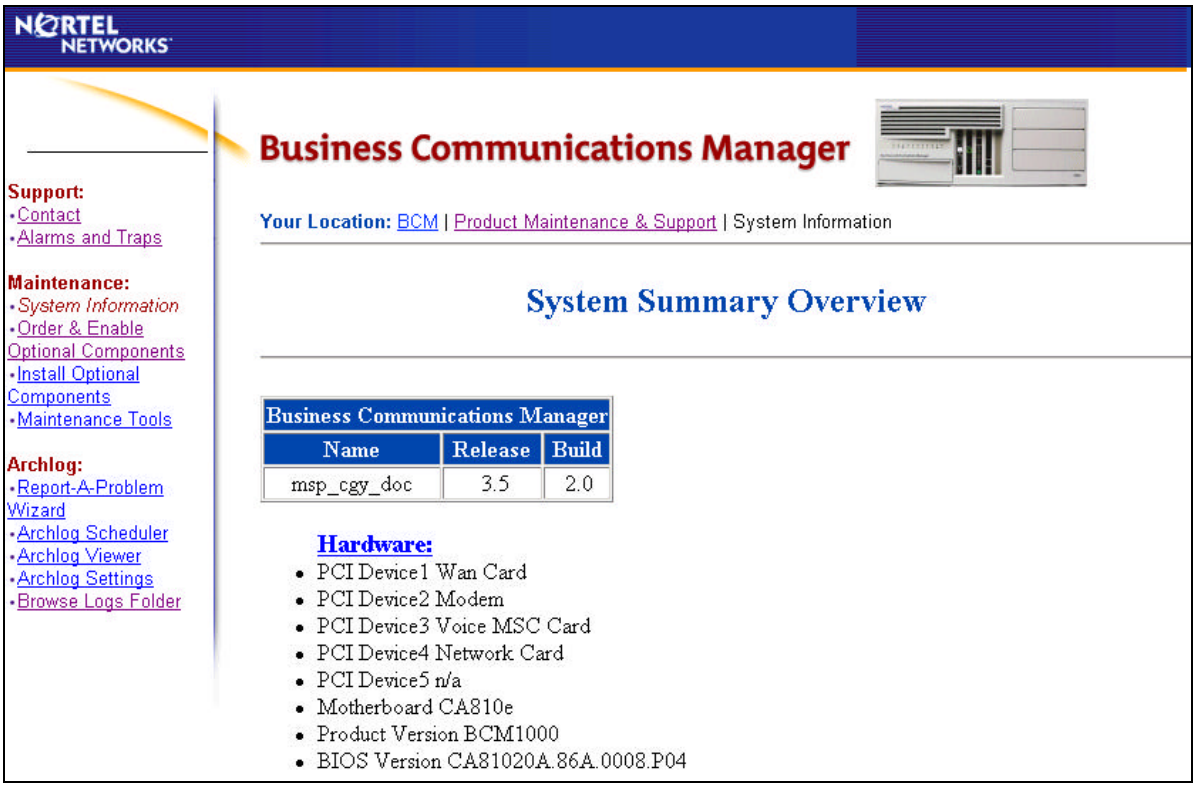
Maintenance selections are:

- System information
- Order & enable optional components
- Install optional components
- Maintenance tools

System information

The system information screen displays a summary of the software release and hardware inventory currently installed on your BCM system.

Figure 12 System information screen

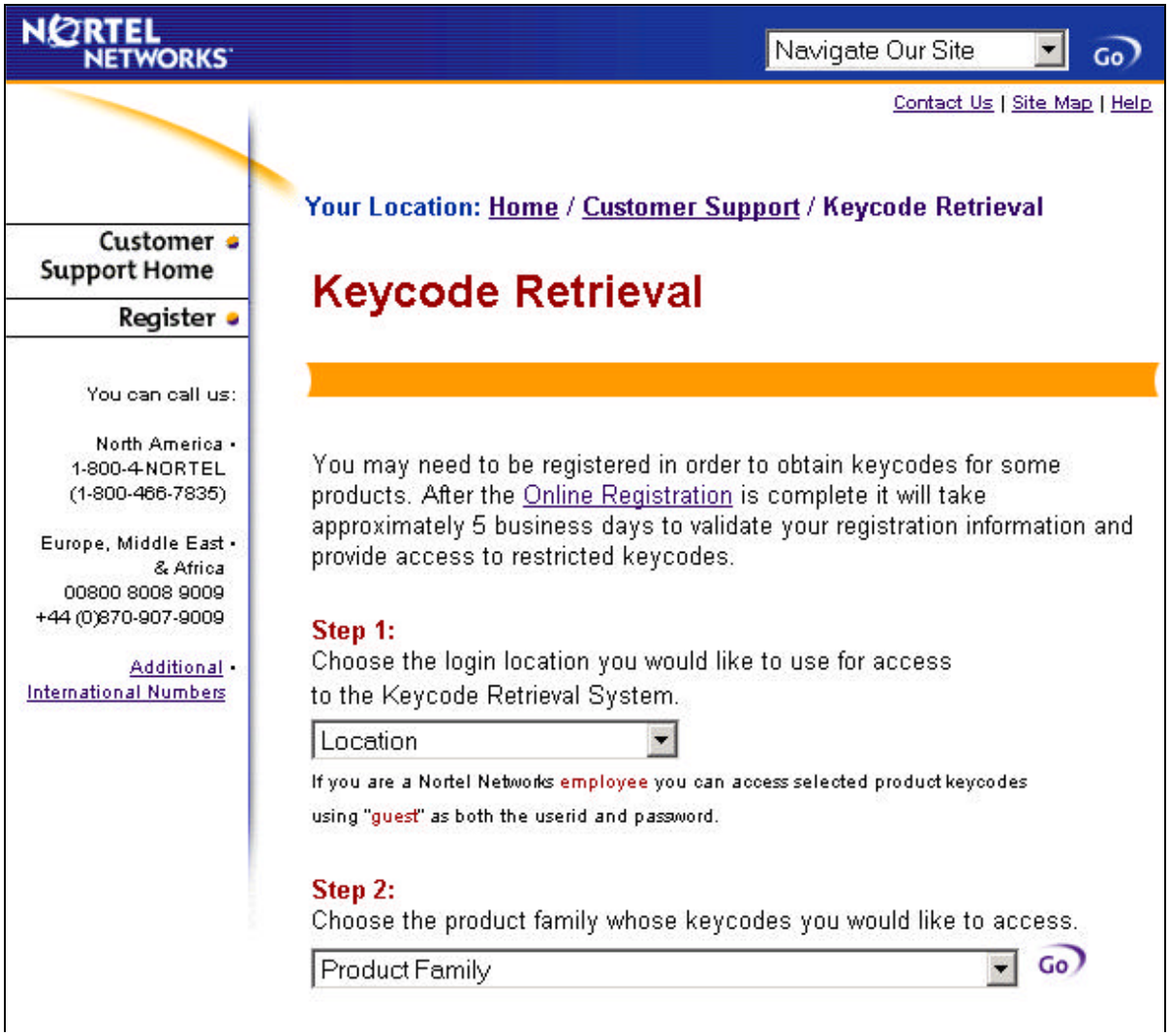


Order and enable optional components

The keycode retrieval search screen displays a search form you can use to:

- select the log on location to access the keycode retrieval system from
- select the product family for the keycodes you need to access
- search for keywords

Figure 13 Keycode retrieval screen



Install optional components

On the install optional components screen you can:

- install the IPX routing protocol and services on the BCM
- install PPPoE to enable Point-to-Point over Ethernet capability on the BCM (requires a keycode for installation). The PPPoE product is only available for BCMs that contain 2 LAN adapters

When you select either of the above options, the system displays an installation wizard to guide you through the installation process.

To display the install optional components screen, select Install optional components under the maintenance category. The install optional components screen appears.

Figure 14 Install optional components screen

Maintenance tools

Use the maintenance tools screen to select the tools necessary for these application categories:

Application	Tools
Shared drive	• Attach to a shared volume • Detach a shared volume • Enable/Disable BCM Drive Shares
System interaction	• Execute a command • Schedule a command to execute • Schedule a restart • Telnet session
Troubleshooting	• IP network troubleshooting • Services and driver troubleshooting
DECT (for more information see the *DECT Installation and Maintenance Guide*)	• Time synchronization • Backup firmware • Restore firmware • Firmware upload • Restore default configuration • A-law/Mu-law companding scheme
Security	Upload certificate and private key
Miscellaneous	Reset Unified Manager server

When you select a tool for any of the above applications, the system displays an installation wizard to guide you through the installation.

To display the maintenance tools screen, select Maintenance tools under the maintenance category. The maintenance tools screen appears.

Figure 15 Maintenance page maintenance tools screen

Management Guide Overview

This section summarizes the content of the Management Guide:

Fault management overview

This section describes the alarm management system, system events and SNMP traps. Administrators access alarms and perform fault analysis through the Unified Manager interface. Use Unified Manager to configure the fault system.

For more information on how to manage system faults, see Chapter 2, "Fault Management System," on page 59.

This section also provides a correlation between the event source (SNMP traps), components, logs and services. For more information see:

- "Component ID (alarm) summary information" on page 92
- "Component ID/SNMP Trap Error interpretation" on page 100

Service management overview

This section describes service manager capabilities in Unified Manager. This section also describes the properties of the services in the Service Manager and associated alarm notifications.

To more information about services see Chapter 3, "Service Management System," on page 251.

Use the Service Manager to access, assess or modify tervices running on Business Communications Managers in your network. Services control the functionality of Business Communications Manager. A service is a software process that controls interaction with Business Communications Manager hardware devices, computing environment, telephony or your browser interface.

Modification of any service has far-reaching effects on communications or event reporting capability. Nortel Networks strongly recommends you consult with your support group before you use the Service Manager.

There are two categories of services:

- **System level services**: software processes that are critical to essential operating system-level features (see "System-level service definitions" on page 258)
- **Nortel Networks configurable services**: software processes that are critical to the operation of Business Communications Manager software (see "Nortel Networks Configurable Services" on page 285)

Log management overview

This section describes the Media Service Card (core telephony) logs. Because every components of Business Communications Manager is logged, the system generates a large number of logs for a variety of purposes. In the case of faults, consult the logs to help you to diagnose and correct the problem.

Some logs run continuously and collect information to help you troubleshoot in the event of system problems. You can disable some logs because the information collected may not be of immediate or critical interest to maintain the system.

The system generates these MSC logs:

- **MSC System Test Log**: contains diagnostic test results, telephony events and alarms, audits. It has a maximum size of 20 items, after which events are aged out to make room for new events.
- **MSC System Administration Log**: contains log on, and log off information. Has a maximum of 10 entries. The 11th entry overwrites the 1st entry regardless of severity level.
- **MSC Network Event log**: contains T1 / PRI network interface events and alarms. This log has a maximum of 10 events.

For more information on Business Communications Manager logs, see Chapter 4, "Log Management," on page 315.

BCM Monitor overview

Business Communications Manager diagnostics involve both monitoring system status and assessing performance.

For how to download and use the BCM Monitor, see Chapter 5, "BCM Monitor," on page 335.

BCM Monitor is an optional, standalone application you can use to view system and IP telephony information for each Business Communications Manager. Open several instances of the application on a single PC to monitor the corresponding Business Communications Manager systems.

BCM Monitor supports real time troubleshooting and report generation. System administrators and support personnel obtain key, real-time information to perform troubleshooting if necessary. The system administrator accesses and saves information to generate system utilization and traffic reports.

Using BCM Monitor to monitor your system status

With BCM Monitor you can see the current status of various parts of your system services.

Use BCM Monitor during troubleshooting to confirm current configurations, including CallPilot applications and IP trunk information. You can find BCM Monitor under the **Install Clients** button on the first page of the Unified Manager. The BCM Monitor section describes:

- “Starting BCM Monitor” on page 336
- “Using BCM Monitor to analyze your system status” on page 337
- “BCM Monitor statistical values (minimum and maximums)” on page 346
- “BCM Monitor information capture” on page 347

Performance management overview

The Unified Manager System P erformance monitor provides detailed performance information for the system and the system resources. The statistics are shown in charts or table format. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

BCM performance and usage information can be queried by SNMP.

For more details on performance management, see Chapter 6, “Performance Management,” on page 351.

Use these tools and procedures to monitor the Business Communications Manager system performance:

- “System Performance tools and services” on page 351
- “Service Manager” on page 251
- “Base function tray system status display LEDs” on page 466
- “Using the Initialization menu to monitor system hardware” on page 470
- “Disk mirroring function” on page 471
- “Module Diagnostics” on page 433

If you determine through the use of the diagnostic tools, that a hardware problem exists, see the *Installation and Maintenance Guide* for information on component replacement.

Security management overview

Web access to Business Communications Manager now uses SSL encryption for system security. This includes the appearance of a security alert when you initiate a connection to the Unified Manager using SSL, which indicates site validation of the default certificate.

For more information on how to define security parameters for the system and for users, see Chapter 9, “Security Management,” on page 407.

Security management topics

Backup and restore overview

Use the Backup and Restore Utility (BRU) to preserve the integrity of your Business Communications Manager operating system software and configuration data. With BRU you can perform a backup, restore or upgrade through a web connection. BRU is a single-user application.

Before you perform any substantial maintenance on the Business Communications Manager, save your data to a safe storage module location elsewhere in the network. After hardware maintenance is complete, restore the data to your Business Communications Manager.

For more information on how to operate the Backup and Restore utility, see Chapter 8, “System Backup and Restore (BRU),” on page 381.

Backup and restore procedures

Troubleshooting and diagnostics activities overview

This section has information about diagnosing module line performance and device line issues. This section also tells you how to perform a system startup, set identification parameters and maintain telephony resources.

For more information on diagnostics activities, see Chapter 10, “Testing, Troubleshooting, and Diagnostics,” on page 433.

Troubleshooting and diagnostic activities topics

Chapter 2
Fault Management System

Business Communications Manager fault management topics

BCM Fault Management Tools

Fault management activities range from system setup, monitoring and reporting to fault identification, diagnosis and correction. The tools available to the BCM network administrator to access alarms and perform fault analysis are:

- Alarm management using the Unified Manager Interface
- SNMP traps for remote fault management

You access alarms and perform fault analysis through Unified Manager.

Alarm Management System

Business Communications Manager tracks and generates approximately 700 different alarms. Alarms can provide notification that a network interface is not behaving as expected, or that certain anomalies in system operation have been detected, for example.

When the Alarm Management system is enabled, all BCM alarms are recorded in the NT Event Log. Use the Unified Manager Alarm Banner to view alarms for each Business Communications Manager. A subset of the alarm information pertaining to BCM core telephony can also appear at the Alarm telephone, and in the MSC logs. Managing alarms within Unified Manager is described in “Alarm Analysis and Clearing Procedures” on page 89.

Note: Assign the Alarm telephone in Feature settings under System programming. Alarms have a higher severity than events. Attend to alarm codes before event messages Alarm code information that is specific to Companion components is included in the Windows NT Event Log.

Any information sent to the Windows NT event log can generate an SNMP trap.

All BCM alarms can also be sent to a remote management system through an SNMP trap. For how to perform remote fault management of BCM SNMP traps, see Configuring an SNMP Community on page 77.

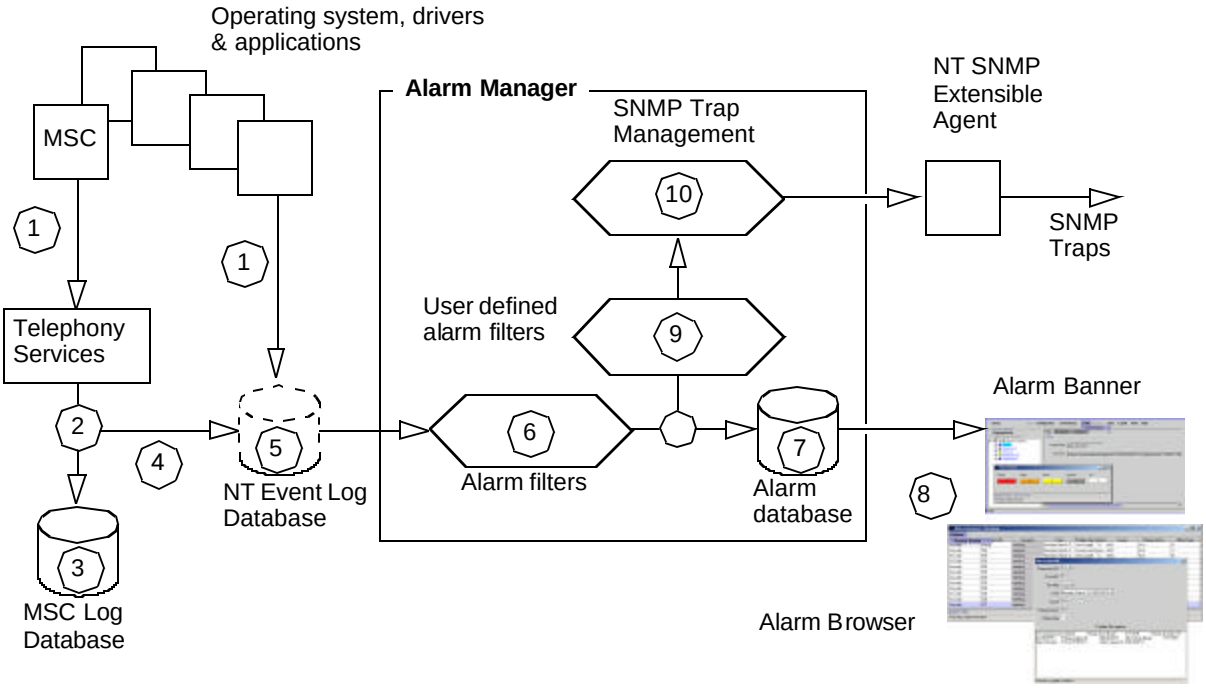
An alarm may not appear until two minutes after it is triggered. If the system is powered off when the alarm is triggered, the alarm does not appear until two minutes after the system is powered on.

For more information about	see
BCM alarms	“Alarm Analysis and Clearing Procedures” on page 89
BCM SNMP traps	“SNMP Traps” on page 75
MSC logs	“Media service card (core telephony) logs” on page 315

Alarm Reporting System

This figure illustrates how Business Communications Manager manages system events.

Figure 16 Business Communications Manager events and alarms



1. Core telephony services running on the Media Services Card (MSC), generate event outputs (see "Event sources" on page 62).
2. The system forwards BCM core telephony (MSC) events, including alarms, to the MSC telephony event logs.
3. BCM telephony (MSC) event logs include the MSC System Test Log, MSC System Admin Log, and MSC Network Event log. These logs capture all of the MSC (core telephony) system events (including MSC alarms).
4. BCM core telephony (MSC) alarms are written into the NT Event log database. A subset of the core telephony (MSC) events are also written into the NT Event log database.
5. The NT Event Log database captures events from all BCM components, including MSC alarm and some MSC event information.
6. The Alarm Manager applies system filters based on configuration inputs.
7. The Alarm database captures all NT event information after system filtering is applied.
8. Alarm Banner / Alarm Browser provides real-time display of alarms in Unified Manager.
9. The Alarm Manager SNMP subsystem applies filters to the BCM alarms based on user inputs about severity levels and event sources.
10. BCM alarms meeting the SNMP trap criteria are forwarded to the SNMP trap reporting interface according to the trap community list.

Event sources

All BCM components can be a source of BCM event information. An event is defined as a notification of an error or anomaly in operation, or a condition that can lead to an error or anomaly. The terms “event” and “alarm” are used interchangeably in the BCM environment.

Refer to “Business Communications Manager events and alarms” on page 61 when reviewing the description.

- BCM events derived from the operating system, drivers, services and applications, are captured in the NT Event Log (item 5).
- The BCM events are recorded in the BCM Alarm database (item 7) and displayed as alarms in the Alarm Banner (item 8). See also “Alarm banner and alarm browser” on page 64.
- The BCM events, or alarms, can also be made available to remote fault management systems as SNMP traps (item 10).

MSC events

Core telephony services, which run on the Media Services Card (MSC) (item 1 of “Business Communications Manager events and alarms” on page 61), represent one of the major BCM components that act as a source of events. Referred to as MSC events or core telephony events, these events are assigned an MSC event id and an event priority from P1 to P9, where P9 is the most severe. If an MSC event is serious enough to be considered an alarm, the system also assigns the MSC event an MSC alarm ID.

Refer to “Business Communications Manager events and alarms” on page 61 when reviewing the description.

- All core telephony (MSC) events, including telephony alarms, are recorded in a set of core system telephony logs (items 2 & 3).
- All core telephony (MSC) events designated as alarms are also written into the NT Event log (item 4). In most cases, the MSC alarm ID, assigned by the core telephony (MSC) service, is reused as the NT Event ID.
- Some of the core telephony (MSC) events, which are not alarms, are also written into the NT Event log, primarily MSC events of priority P5 and higher (item 4). MSC events of priority P4 and lower can be seen only in the MSC logs - see “MSC (core telephony) logs” on page 63). MSC events that are visible to the alarm service can also generate SNMP traps.

Due to the interaction between the MSC system and the BCM alarm system, an event in the NT event database that originates from the core telephony services (MSC) will have an NT event ID. An event will also have an associated core telephony (MSC) services event ID, and possibly also an MSC alarm ID.

MSC event and alarm conditions

- Software errors that do not affect system operation
- Software errors that affect system operation: feature failure dropped calls, or system resets.

- Events caused by hardware-related problems, but are not of sufficient severity as to be an alarm condition. Installers, however, may need to know of these events as they can indicate a hardware problem (for example, bad messages received on a signalling channel) or a PSTN- or private network-related problem (for example, no battery feed, no dial tone, invalid disconnect sequence).
- Events that are not of sufficient severity to be an alarm condition, but where the problem is related to system limits affected by system usage patterns, administration, or lack of resource. Examples are running out of autodialler/speed dialer bins, LHD nodes, DTMF/dial tone receivers. These events may not be apparent to users, but a degraded level of service will likely result.
- Information events, concerning a user action, typically in **ADMIN or **CONFIG. (for example, admin log cleared, user attempted to enter **ADMIN with wrong password).
- Permanent, service affecting events that an installer can fix. Typically these are also alarms, but that is not a prerequisite. An example of the latter is the defaulting of a portion of administration, without a cold start (installer action: readminister the data).

MSC (core telephony) logs

Refer to "Business Communications Manager events and alarms" on page 61 when reviewing the descriptions.

- MSC logs (item 3) are maintained on the Media Services card, MSC, which is the telephony side of the Business Communications Manager system.
- The MSC logs are a set of three logs: the MSC System Test, MSC System Administration, and MSC Network Event log. These logs capture all core telephony (MSC) system events, including alarms. For more information, see "Media service card (core telephony) logs" on page 315.
- Note that core telephony (MSC) events, designated as MSC alarms, are sent to the NT Event Log in addition to being recorded in the MSC (core telephony) logs (item 4). MSC events of priority 5 (P5) and higher are sent to the NT Event log (item 4). MSC events are shown in the BCM alarms under the Voice Software component ID.

NT Event log database

When the alarm service is enabled, all BCM alarms are recorded into the NT Event Log (item 5 of “Business Communications Manager events and alarms” on page 61).

For more information about how to view NT Event Logs, see “Obtaining NT Event Logs from Archlog” on page 332.

Alarm manager

See “Business Communications Manager events and alarms” on page 61 when reviewing the descriptions.

- The system forwards events from the NT Event log to the Alarm Manager.
- The Alarm Manager applies system filters based on configuration inputs.
- The events are recorded in the Business Communications Manager alarm database.

Alarm database

See “Business Communications Manager events and alarms” on page 61 when reviewing the descriptions.

- The alarm database (item 7) holds a maximum of 5000 alarm records. The network administrator configures the record capacity of the alarm database to a smaller size if required.
- Use the Alarm Manager batch archive function to archive the information in the alarm database. Set the batch job parameters (day of the week and time) and file destination. For how to configure and use the alarm manager, see Configuring Alarm Manager settings on page 70.

Alarm banner and alarm browser

The Alarm Banner and the Alarm Browser (item 8, “Business Communications Manager events and alarms” on page 61) provide real-time information about events occurring in the Business Communications Manager system.

Alarm system interfaces

- With the Alarm Banner window you can continually monitor the Business Communications Manager system for alarms. For more information, see “Accessing the Alarm Banner to monitor alarm notification” on page 68.
- With the Alarm Browser window you can browse through a list of alarms and see detailed information for each one. For more information, see “Accessing the Alarm Browser to analyze alarm detail” on page 69.

- With Alarm Manager you can manage the collection and storage of alarm information. Use the Alarm Manager to enable or disable sending of all or some types of SNMP traps. The Alarm Backup Batch Job backs up old alarm records to an archive folder at scheduled time intervals. For more information on how to use the Backup Batch Job, see "Configuring Alarm Manager settings" on page 70.

BCM alarm severity

Alarm severity refers to a scale in which an alarm notification is categorized. The alarm severity prescribes the degree of appropriate user intervention.

There are four alarm severity levels:

- **Critical** alarms indicate system problems that require immediate corrective action.
- **Major** alarms indicate system problems that require corrective action.
- **Minor** alarms indicate system problems that do not affect system performance and may or may not require action.
- **Warning** alarms indicate system status changes that normally do no need any corrective action.

Accessing and configuring the Alarm System

The Alarm Service works to generate SNMP trap event notifications. You must also enable and configure SNMP traps.

Functions the Alarm Service performs

- monitoring Windows NT event logs for incoming events
- synchronizing Windows NT logs with Business Communications Manager alarm database
- receiving events (alarms) from other Business Communications Manager applications through its API and logs the events in the Business Communications Manager database
- archiving alarm history based on the criteria defined in Alarm Manager
- monitoring the alarm configuration changes and updates SNMP trap agent and Alarm Service

Note: When the Alarm Service is enabled, Business Communications Manager automatically archives the BCM Event logs. See “Enabling the alarm service” on page 67.

Note: The Alarm Service is disabled by default. You must enable the Alarm Service to view alarms on the Alarm Banner. See “Enabling the alarm service” on page 67.

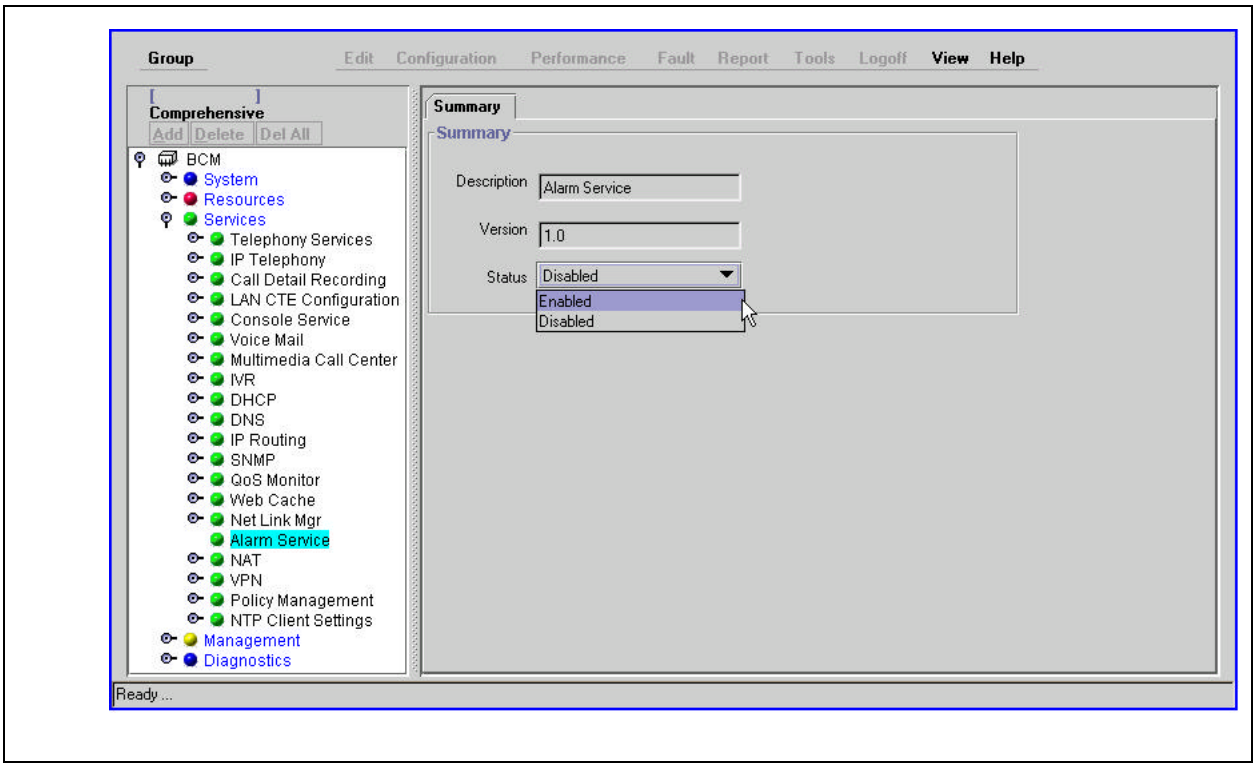
Note: You must configure how the system handles SNMP trap notifications. Events that arrive in the alarm database trigger an SNMP trap message to be generated. If you do not configure SNMP traps, you will not obtain optimum alarm reporting capability.

Enabling the alarm service

Use this procedure to enable the Alarm Service and view alarms on the Alarm Banner.

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On th e Unified Manager navigation tree, click the **Services** key and select the **Alarm Service** heading.
   The Alarm Service Summary screen appears.
3. From the **Status** list box, change the status of the alarm service to **Enabled**.

Figure 17 Alarm service selection screen



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

Accessing the Alarm Banner to monitor alarm notification

Use the Alarm Banner to continually monitor the Business Communications Manager system for faults or alarm conditions. The Alarm Banner stays active on your desktop for quick access. The banner displays color codes to represent the alarm severity and the number of alarms for each severity level. The Alarm Banner displays alarms in real time.

Note: You must enable alarm service before the Alarm Banner will function.To enable the alarm server, see "Enabling the alarm service" on page 67.

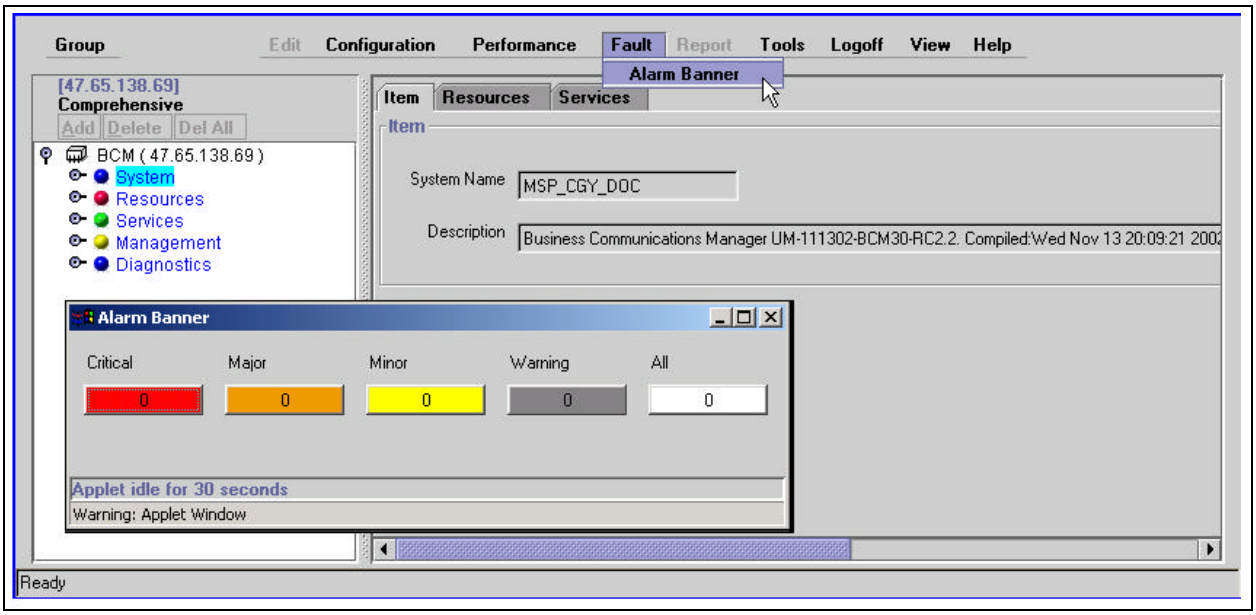
To access the Alarm Banner

1 Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.

2 On the Unified Manager navigation tree select the **System** heading.

3 From the **Fault** menu select **Alarm Banner**.
The Alarm Banner appears.

Figure 18 Alarm banner



4 Select any color-coded alarm button to view a report of active alarms.
The Alarm Browser appears. See "Accessing the Alarm Browser to analyze alarm detail" on page 69 for more information.

Accessing the Alarm Browser to analyze alarm detail

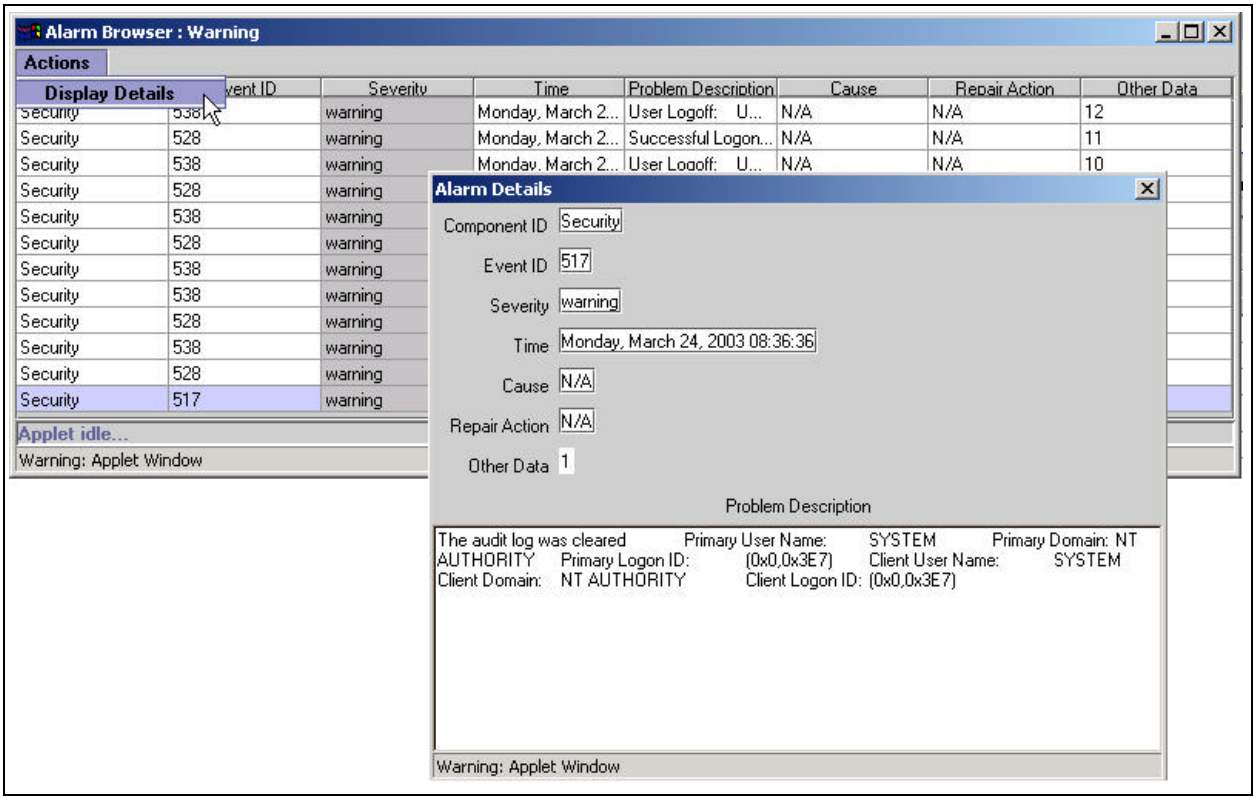
With the Alarm Browser you can access and detect an alarm occurring on the system, and display detailed information on each alarm to assist you to perform corrective action, if needed.

See the section "Alarm Analysis and Clearing Procedures" on page 89 for a detailed explanation of how to navigate through the alarm clearing process and the descriptions in this guide.

To access the alarm browser and alarm detail screen

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the navigation tree click the **System** heading.
3. On the **Fault** menu click **Alarm Banner**.
   The Alarm Banner appears.
4. Select any color-coded alarm buttonto display a report of active alarms. Select **ALL** (white button) to browse through the complete list of system alarms, regardless of the severity level.
   The alarm browser screen appears.
5. Select the row corresponding to the alarm for which you want detailed information.
6. On the Alarm Browser, click the **Actions** menu and select **Display Details**.
   The Alarm Details screen appears. The Alarm Details screen is a read-only display.

Figure 19 Alarm browser and detail screen



7 Close the Alarms Details screen and the Alarm Browser when you are finished viewing the alarms for this severity.

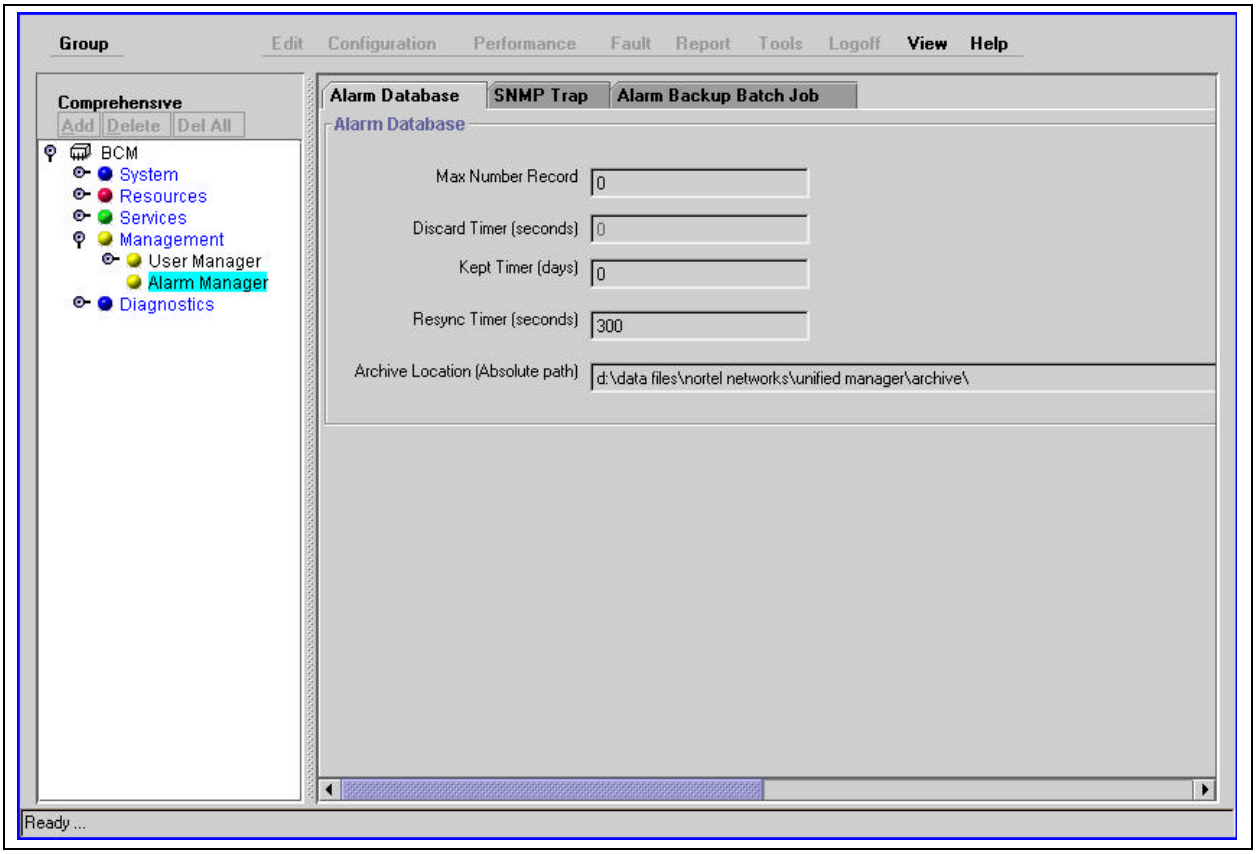
Configuring Alarm Manager settings

With Alarm Manager you can manage how you collect and store alarm information. With the Alarm Manager you can set different collection parameters for the Alarm Database. You can use the Alarm Manager to enable or disable the sending of all or some types of SNMP traps. The Alarm Manager provides the Alarm Backup Batch Job, which backs up old alarm records to an archive folder at a scheduled time.

To configure Alarm Manager settings

1 On the navigation tree, click the **Management** key and click the **Alarm Manager** heading.

Figure 20 Alarm database screen



2 Use the information in this table to configure the Alarm Database.

Table 3 Alarm Database settings

Attribute	Action
Maximum Number Record	Set the maximum number of records that the alarm database stores. The default is 0 (no limit). The range is from 0 to 5000 records. If you enter 0, there is no limit to the number of records. When the number of records reaches the maximum, the earliest record is removed to make room for the new alarm record.
Kept Timer (days)	Set the number of days that the records remain in the database before the records are archived.
Resync Timer (seconds)	Set, in seconds, the interval at which the alarm service initiates a synchronization operation with the Business Communications Manager's internal event logs. This synchronization is in addition to the normal synchronization operations triggered by the arrivals of new events.

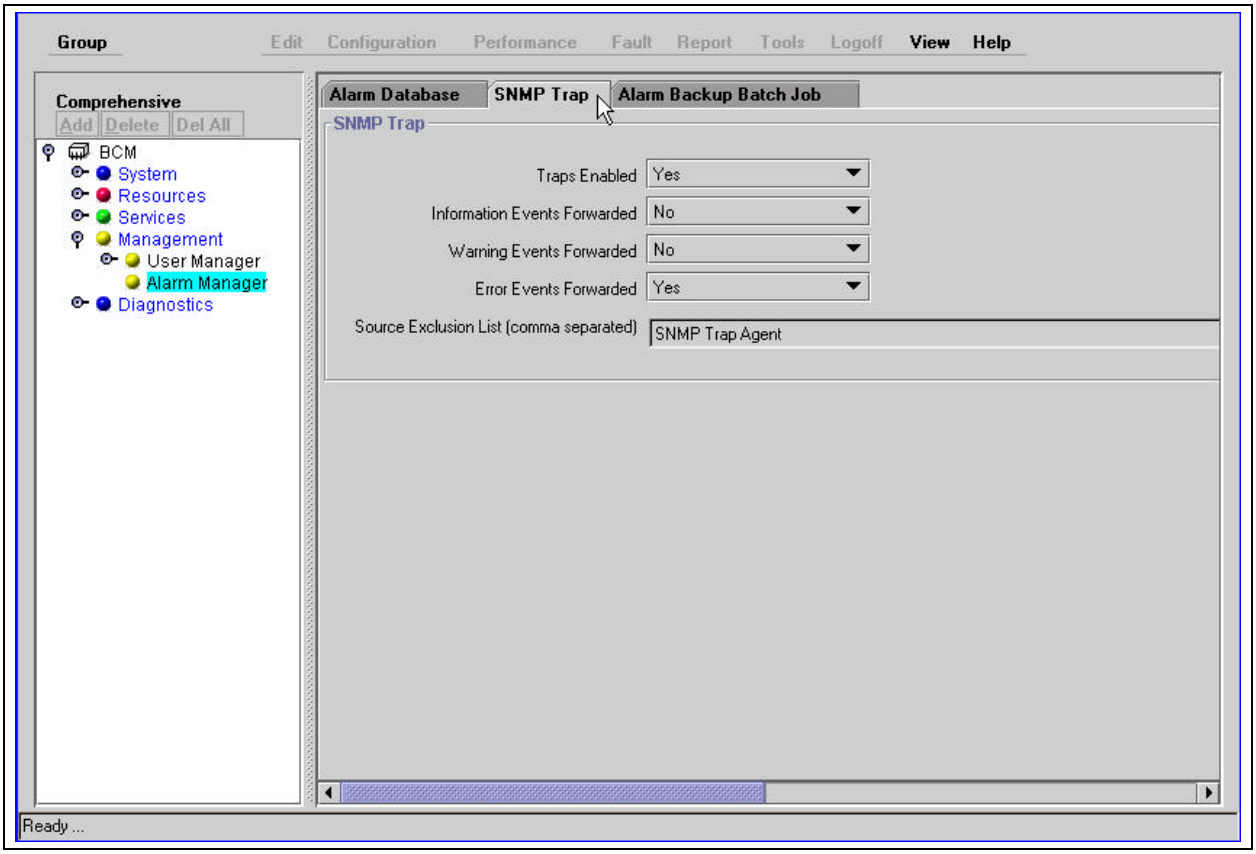
Table 3 Alarm Database settings (Continued)

Attribute	Action
Archive Location	Enter the path to the directory where the archives of alarm information are kept. The default path is: d:datafiles\nortel networks\unified manager\archive\. Nortel Networks highly recommends that you do not change this path from it default value. An archive of the alarm information is made when an Alarm Backup Batch Job is run or when the Alarm Service is started. During an archive operation, the alarm database is copied to the archive location and the alarm database is then emptied. During an archive operation, the Business Communications Manager's internal event logs are also copied to the archive location and the event logs are then emptied. The file names of these internal event log archives are: System Event Log SystemLogYYMMDDHHMM.evs Application Event LogApplicationLogYYMMDDHHMM.evs Security Event LogSecurityLogYYMMDDHHMM.evs Where: YY is the year the archive was created MM is the month the archive was created DD is the day the archive was created HH is hour the archive was created MM is the minute the archive was created

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

4 Click the **SNMP Trap** tab.

Figure 21 SNMP Trap screen



5 Use the information in this table to configure the SNMP Trap.

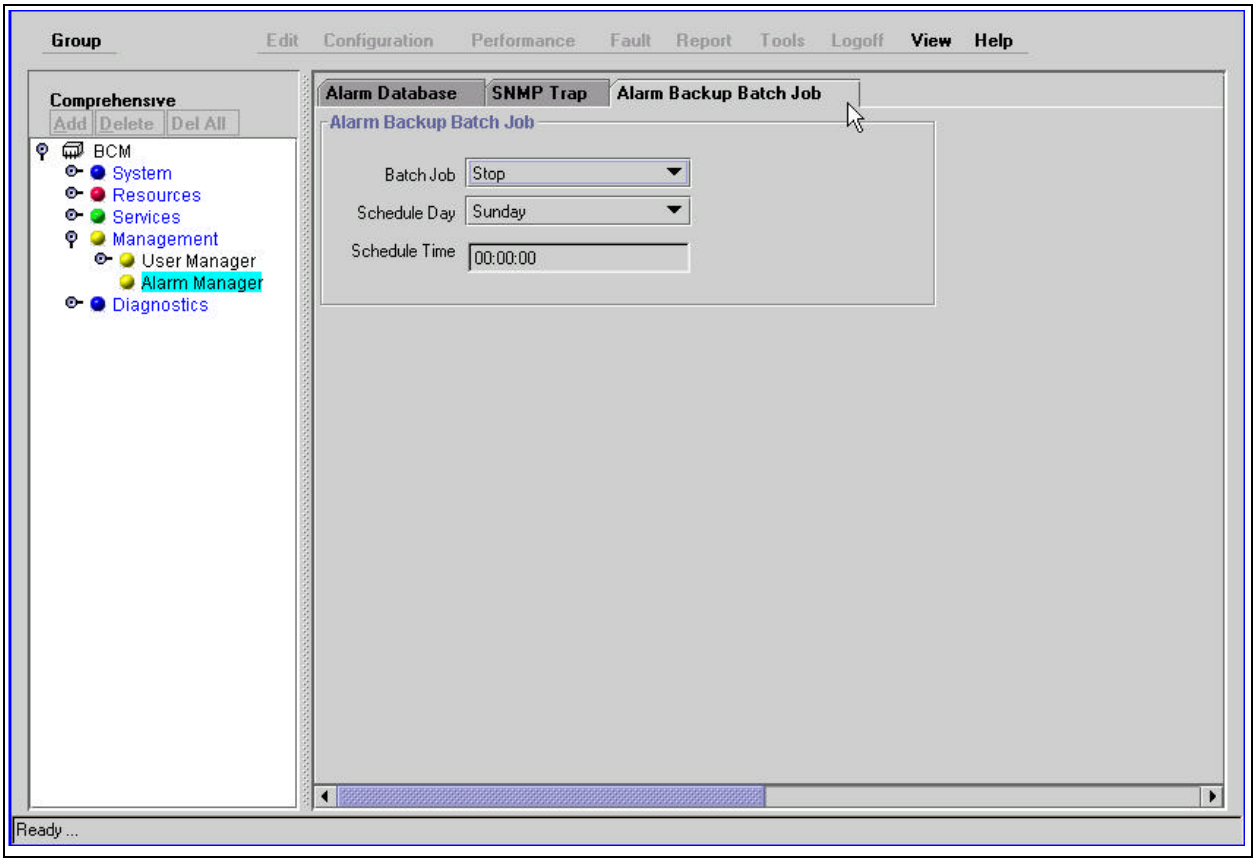
Table 4 SNMP Trap settings

Attribute	Action
Traps Enabled	Enable or disable the sending of SNMP traps when a new event arrives in the alarm database.
Information Events Forwarded	Enable or disable sending SNMP traps when an “Information” event arrives in the alarm database. If you have auto SNMP trap dial out set up, and the value for 'Traps Enabled' is 'Yes', setting "Information Events Forwarded" to "Yes" causes the BCM to repeatedly redial the trap client. Always set "Information Events Forwarded" to "No" when SNMP trap dial out is set up. If the name of a demand dial interface is selected as 'Interface' (when you add/modify a trap community entry) and the 'Traps Enabled' field value is 'Yes', Nortel Networks recommends you specify the value of the 'Information Events Forwarded' field as 'No'. If you specify a value of “Yes”, the BCM will constantly redial to the trap client. **Note**: Windows 95/98 is not supported on a receiving system for the 'SNMP trap dialout' feature.
Warning Events Forwarded	Enable or disable sending SNMP traps when a “Warning” event arrives in the alarm database.
Error Events Forwarded	Enable or disable sending SNMP traps when an “Error” event arrives in the alarm database.
Source Exclusion List	Add, in a comma-separated format, a list of event sources from which SNMP traps must not be generated. The source exclusion list prevents you from receiving SNMP traps which have no meaning to you.

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

7 Click the **Alarm Backup Batch Job** tab.

Figure 22 Alarm Backup Batch Job screen



8 Use the information in this table to configure the Alarm Backup Batch Job.

Table 5 Alarm Backup Batch Job settings

Attribute	Action
Batch Job	Start or stop a scheduled batch backup to an archive folder. The Alarm Backup Batch Job uses the Kept Timer value from the Alarm Database screen to determine when to archive an alarm record.
Schedule Day	Set the day for the backup.
Schedule Time	Set the time for the backup.

Tips

Before you change the day or time, or both, you must first stop the batch job, make your changes, and then start the batch job again.

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

SNMP Traps

A trap is a signal that tells a program that an event occurred in the system. When a program receives a signal, a specific set of activities take place.

The SNMP system enables SNMPv1 traps to be generated based on all or a subset of NT Events generated on the Business Communications Manager. Any information sent to the BCM Windows NT event log and shown in the Alarm Banner and Alarm Browser can generate an SNMP trap.

SNMP traps received from Business Communications Manager contain descriptions of the alarms that occur in the system. Additionally, SNMP generic traps such as coldStart, linkDown, linkup, authenticationFailure, are also generated from the Business Communications Manager, depending on the user's configuration.

For the BCM to generate SNMP traps, you must configure how the system handles SNMP trap notifications. When SNMP is enabled, events arriving in the alarm database trigger an SNMP trap message to be generated. Use the alarm manager to enable or disable sending of all or some types of SNMP traps.

The trap format is specified in the BCM "Small Site Event MIBs" on page 488 and is captured and viewed through any standard SNMP fault monitoring framework or trap watcher (see "Management Information Base (MIB) System).

BCM alarm and SNMP trap list

The complete set of BCM Alarms and SNMP traps is provided (see "Component ID (alarm) summary information" on page 92).

To view the BCM Alarms list

1. Access the Unified Manager Maintenance page.
2. Click the Alarms and Traps link.
   The Alarms and Traps screen displays a list of the events (see "Component ID (alarm)/ eventSource (trap) summary" on page 92).The events are organized by event source.
3. Contact your Business Communications Manager Nortel Networks Systems Engineer, Services organization, or PLM and request a list in Excel spreadsheet format.

Alarm banner, NT event database, and SNMP trap correlation

Although the same events (alarms) that are reported in the Alarm System are ade available remotely via SNMP traps and recorded in the NT Event logs, the terminology used for severity levels is not the same.

Refer to the table Alarm banner, NT Event and SNMP Trap Severities or Types to interpret the severity for each type of notification The terminology for severity levels between the NT Event log and in the Alarm Banner is not identical.

Table 6 Alarm banner, NT Event and SNMP trap severities or types

Alarm priority	Alarm Banner	NT Event	SNMP Trap Type
High	critical	Error	Error
Medium	major or minor	Warning	Warning
Low	warning	Information	Information

Refer to the table SNMP Trap Types to interpret the severity for each type of notification. The mapping between alarm severity levels and SNMP trap types (or 'specific-trap' code) is summarized in the table.

Table 7 SNMP trap types

Alarm Severity	SNMP Trap Type (specific-trap code)
critical	eventError (3)
major	eventWarning (2)
minor	eventWarning (2)
warning	eventInfo (1)

The BCM Alarm system denotes the source of a BCM alarm as “Component ID”, whereas the SNMP system denotes the source of the same information as a trap of source “eventSource”. The terminology used in this document of Component ID (alarm)/ eventSource (trap) is intended to show that these two systems call the same information by a different name.

SNMP trap filtering

Trap filtering is done on Business Communications Manager using a source exclusion list and severity levels of Error, Warning and Info. In this way, traps of type “error” (or severity level critical) are forwarded according to the trap community list. The trap filters limit the volume and type of SNMP information, and let you control essential information transferred on the network.

To set the filters

1 On the Unified Manager navigation tree, click the **Management** key and the **Alarm Manager**

heading.

2 Click the **SNMP** trap tab.

3 Use the list boxes on the SNMP Trap screen to set the filters for SNMP traps.

SNMP guidelines

The SNMP service in Business Communications Manager responds to requests from management stations, generates SNMP traps corresponding to events and reports to trap subscriber stations.

Use these SNMP guidelines

- Set read-only and read-write community names.
- Set a list of permitted managers. When set, the agent responds to SNMP managers requests from those IP hosts only.
- An empty list of permitted managers implies that the agent responds to requests from anyone.
- Set trap communities. Each trap entry identifies the community name that must be used and the manager addresses.
- Enable or disable sending authentication traps.
- Enable or disable the SNMP agent.

About defining SNMP trap destinations

SNMP trap destinations can be:

- a community list specifying community name and access privileges
- a manager list specifying SNMP manager IP addresses, that is, SNMP managers allowed to make SNMP queries to the Business Communications Manager
- a trap community list that specifies destinations to which SNMP traps should be sent if SNMP traps are enabled

Although no specific limit is set for the number of trap communities, Nortel Networks recommends that you limit the number of trap communities to a maximum of 5. Limiting the number of trap communities ensures that system performance does not degrade.

Configuring an SNMP Community

Use the procedures in this section to configure the Business Communications Manager to send SNMP messages to an SNMP workstation.

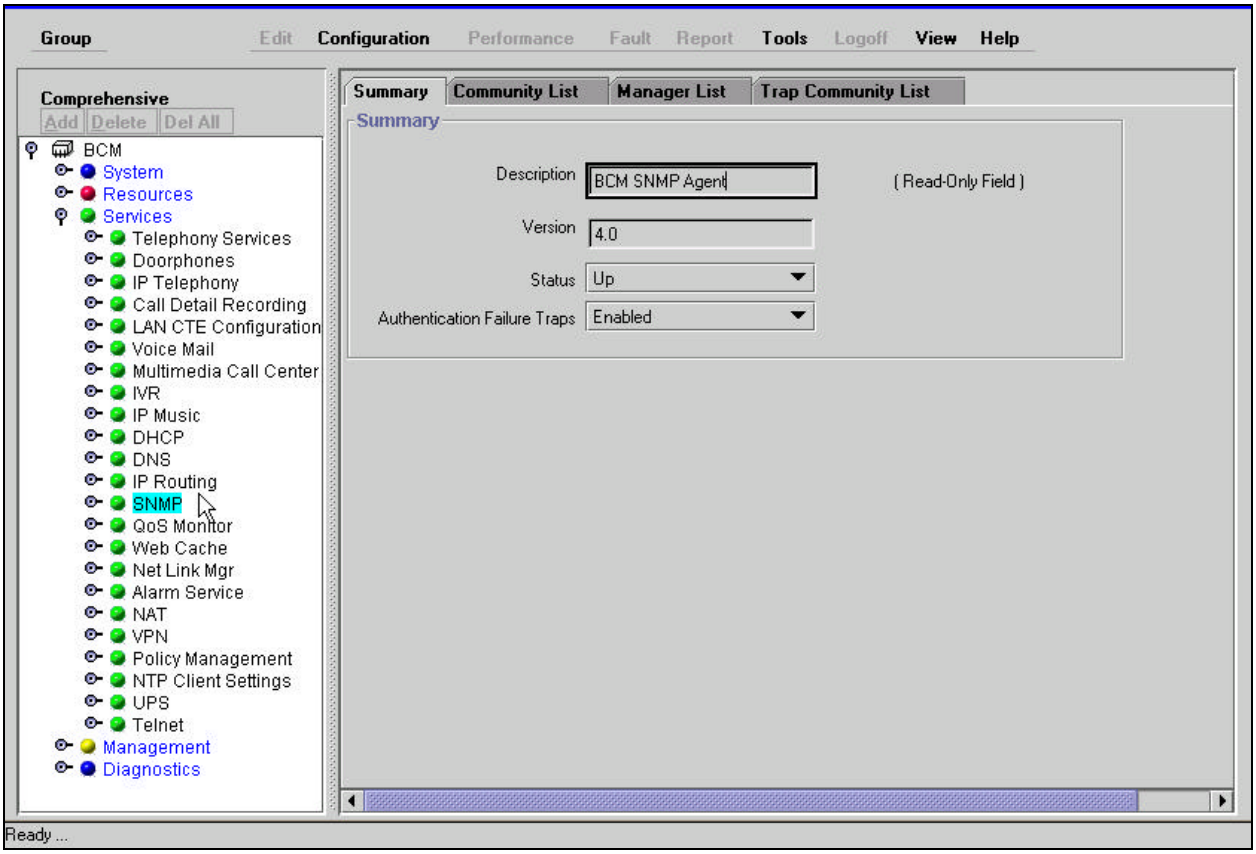
- "Configuring SNMP summary attributes" on page 78
- "Adding a community to an SNMP community list" on page 79
- "Modifying an SNMP community list" on page 81

- “Deleting an SNMP community” on page 81

Configuring SNMP summary attributes

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and the **SNMP** heading. The SNMP Summary screen appears.

Figure 23 SNMP summary screen



3. Configure the SNMP summary attributes.

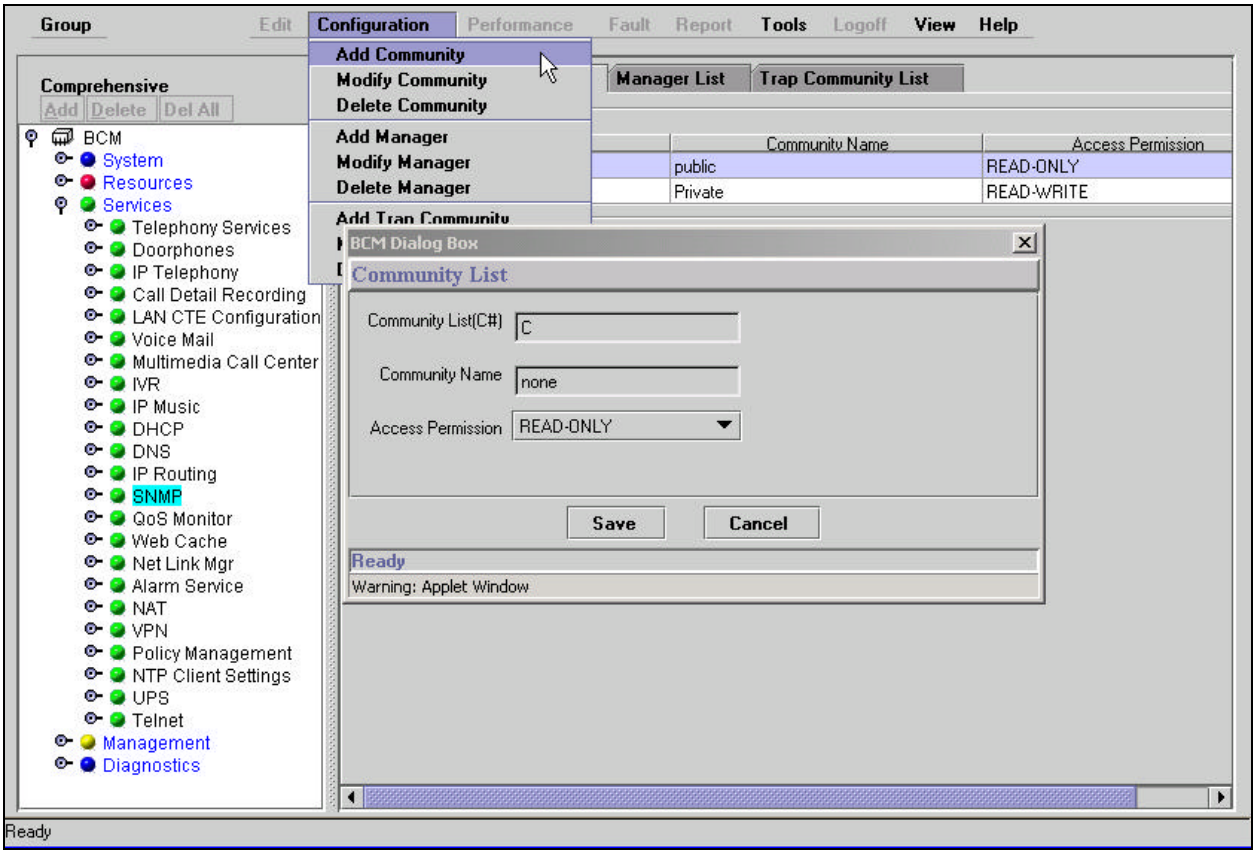
Table 8 SNMP Summary attributes

Attribute	Action
Description	View the description of the SNMP agent.
Version	View the version of the SNMP agent.
Status	Enable or disable the SNMP agent.
Authentication Failure Traps	Disable authentication failure traps. When enabled, the SNMP agent sends authentication failure traps if there is an authentication failure. Authentication failures happens if an SNMP manager application provides an incorrect community string or performs an operation that is not permitted for a community.

Adding a community to an SNMP community list

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and the **SNMP** heading. The SNMP Summary screen appears.
3. Click the **Community List** tab.
   The Community List screen appears.
4. From the **Configuration** menu click **Add Community**.
   The Community List dialog box appears.

Figure 24 Community list screen



5 Configure the Community List attributes.

Table 9 SNMP Community List attributes

Attribute	Action
Community List (C#)	Specify the entry name used as a key to uniquely identify an individual community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix C followed by a unique number that identifies the community name entry on the agent. For example, C2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing community entry name, it modifies the existing community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a community entry, you can't change the name. The community entry name does not have any significance other than to identify an entry.
Community Name	Specify the name of the community that the individual managers use to interact with this agent. The name is case sensitive. The default community names are **public** and **Private**. If there are no community names listed, then all community names are accepted. All the community names are global to the agent. In other words, you cannot associate a specific community name with a single management station.
Access Permission	Specify the read and write access for this community. Available options are: **READ-ONLY** and **READ-WRITE** The default value is **READ-ONLY**.

6 Click the **Save** button.

Modifying an SNMP community list

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading. The SNMP Summary screen appears.
3. Select the **Community List** tab.
   The Community List screen appears.
4. Select the community you want to modify.
5. On the **Configuration** menu click Modify Community.The Community List dialog box appears.
6. Modify the Community attributes as required.
7. Click the **Save** button.

Deleting an SNMP community

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading. The SNMP Summary screen appears.
3. Select the **Community List** tab.
   The Community List screen appears.
4. Select the community you want to delete.
5. On the **Configuration** menu select **Delete Community**.
   A message appears that asks you to confirm the deletion.
6. Click the **Yes** button.
   The community is deleted from the list.

Configuring an SNMP Manager List

Use the procedures in this section to add, modify or delete SNMP manager information in the Manager List.

- "Adding a manager to the SNMP manager list" on page 81
- "Modifying an SNMP manager" on page 84
- "Deleting an SNMP manager" on page 84

Adding a manager to the SNMP manager list

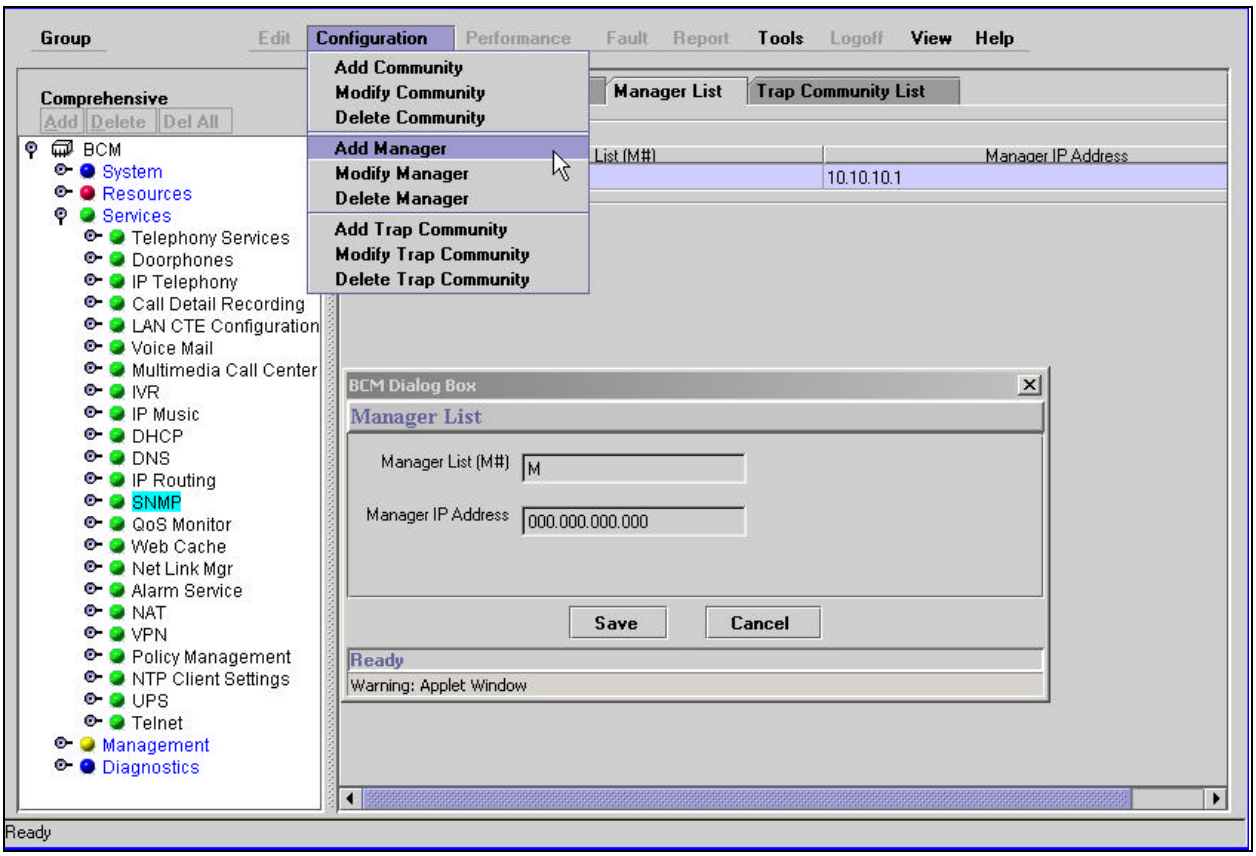
1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.

2 On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading.
The SNMP Summary screen appears.

3 Click the **Manager List** tab.
The Manager List screen appears.

4 On the **Configuration** menu click **Add Manager**.
The Manager List dialog box appears.

Figure 25 Manager list screen



5 Configure the Manager List attributes.

Table 10 SNMP Manager List attributes

Attribute	Action
Manager List (M#)	Specify the entry name used to identify an individual manager entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix M followed by a unique number that identifies the manager entry on the agent. For example, M2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing manager entry name, it modifies the existing manager entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a manager entry, you cannot change the name. The manager entry name uniquely identifies an entry.

Table 10 SNMP Manager List attributes (Continued)

Attribute	Action
Manager IP Address	Specify the IP Address of the SNMP Manager station corresponding to this entry. If no manager entries are created, the Business Communications Manager device accepts SNMP requests from all stations. If there is a list of manager entries, Business Communications Manager base unit accepts SNMP requests from the IP Addresses specified in the list.

6 Click the **Save** button.

Modifying an SNMP manager

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading.
   The SNMP Summary screen appears.
3. Click the **Manager List** tab.
   The Manager List screen appears.
4. Highlight the manager you want to modify.
5. On the **Configuration** menu select **Modify Manager**.
   The Manager List screen appears.
6. Modify the manager attributes.
7. Click the **Save** button.

Deleting an SNMP manager

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading.
   The SNMP Summary screen appears.
3. Click the Manager List tab.
   The Manager List screen appears.
4. Highlight the manager you want to delete.
5. On the **Configuration** menu select **Delete Manager**.
   A message appears to confirm the deletion.
6. Click the **Yes** button.

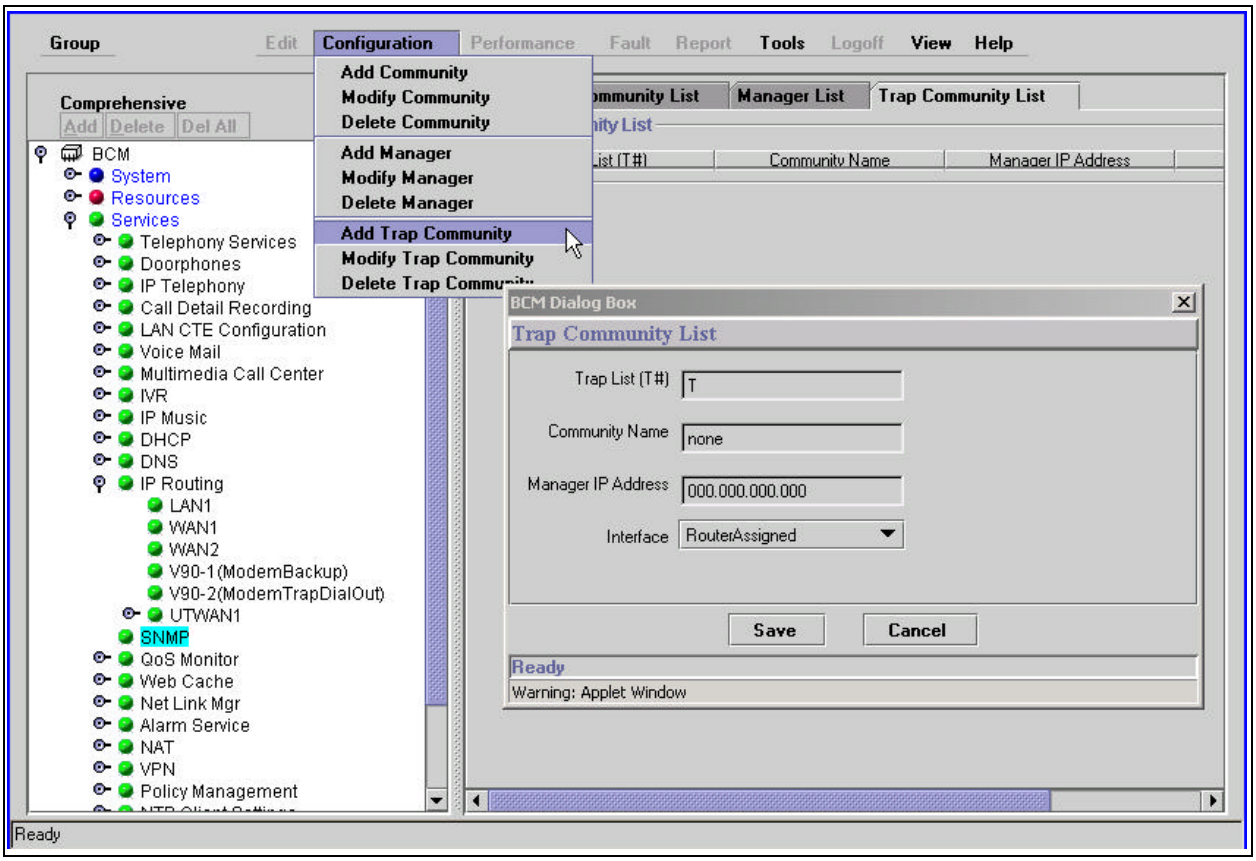
Configuring an SNMP Trap Community List

Use the procedures in this section to add, modify or delete information within the SNMP trap community list.

Adding a trap community to the SNMP community list

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading. The SNMP Summary screen appears.
3. Select the **Community List** tab.
   The Community List screen appears.
4. On the **Configuration** menu select **Add Trap Community**.
   The Trap Community List dialog box appears.

Figure 26 Trap Community list screen



5 Configure the Trap List attributes.

Table 11 SNMP Trap List attributes

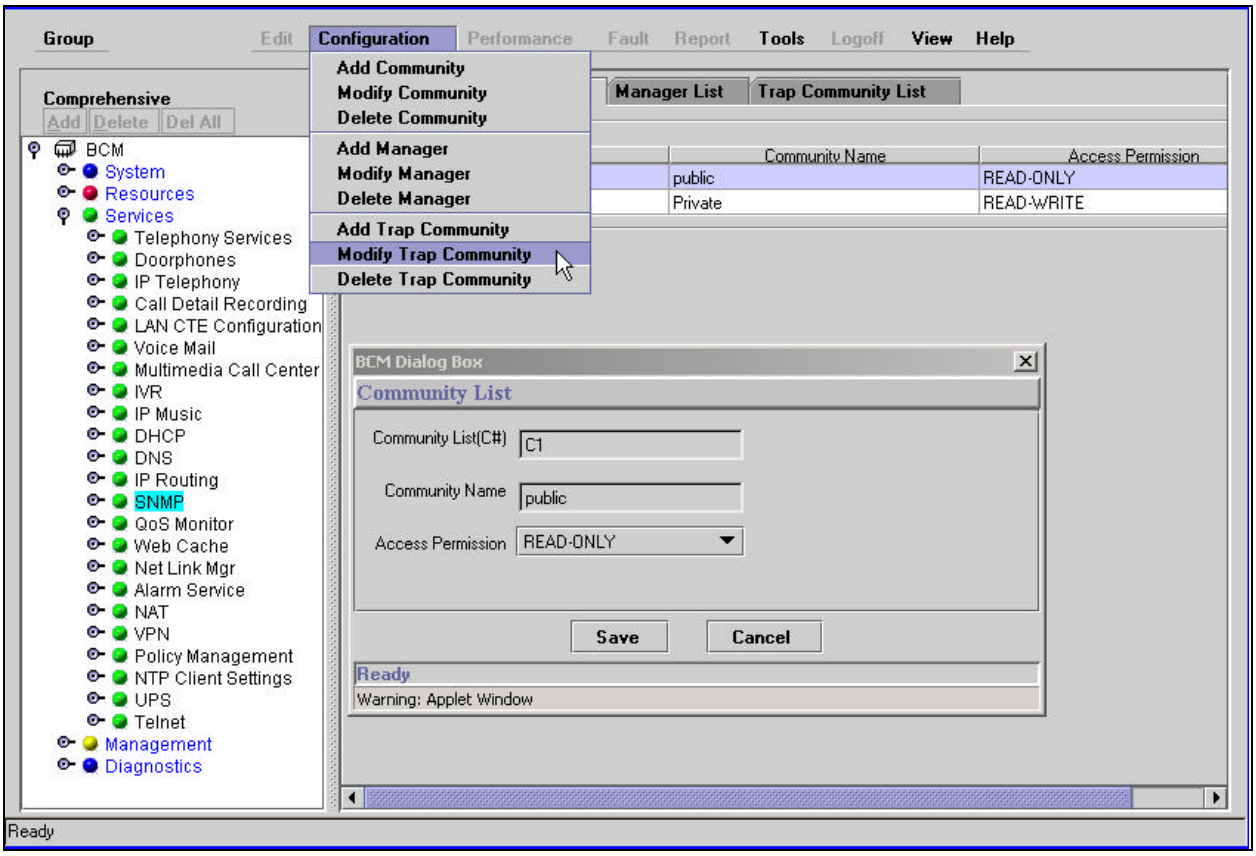
Attribute	Action
Trap List (T#)	Specify the entry name used to identify an individual trap community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix T followed by a unique number that identifies the trap community entry on the agent. For example, T2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing trap community entry name, it modifies the existing trap community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a trap community entry, you can't change the name. The trap community entry name does not have any significance, other than to uniquely identify an entry.
Community Name	View the community name. The community name is case sensitive and encoded in each trap message. This name cannot be in the Community List.
Manager IP Address	Specify the IP addresses of the SNMP trap subscriber stations. If you have too many IP addresses in the trap community list, the SNMP service may degrade system performance. 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 (as the BCM initiates dialing). Using the dynamic IP address causes the removal of the required static route.
Interface	Specify the method to route SNMP traps to the SNMP trap collector. If the trap collector is on the same subnet as one of the BCM LAN or WAN interfaces, select 'RouterAssigned' as the Interface value. The RRAS decides how to route the packet to the trap collector according to its current routing table. If you want to let the BCM send trap packets to the trap collector via the dialup interface, select a demand dial interface as 'Interface'. The BCM automatically adds (under IP routing) a static route for the trap collector that points to the dial-out V.90 modem or ISDN interface. Configure a trap community entry with the trap collector IP address as the trap destination. Select 'RouterAssigned' or one of the dial-out interfaces listed in the drop-down list. Types of communication links are: • Select **RouterAssigned**: The route for the trap destination is automatically determined and handled by the RRAS. Enter the IP address of the trap collector in the Manager IP Address field. • **V.90 Dial-out**: The interface is specified through Resources/dialup/V.90/Modemtrapdialout. The BCM will automatically dial-out to the SNMP trap collector telephone number. Specify the dial-out information under the **V.90 Link Parameters tab**. The Modembackup is not used for the auto SNMP trap dial-out feature. • **ISDN BRI (Europe/North America)** : The interface is specified through Resources/dialup/ISDN. The BCM will automatically dial-out to the SNMP trap collector phone number. • **ISDN PRI (Europe)**: The interface is specified through Resources/dialup/ISDN. The BCM will automatically dial-out to the SNMP trap collector phone number.

6 Click the **Save** button.

Modifying an SNMP trap community

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading. The SNMP Summary screen appears.
3. Click the **Trap Community List** tab.
   The Community List screen appears.
4. Highlight the list you want to modify.
5. On the **Configuration** menu select **Modify Trap**.
   The Trap Community List screen appears.

Figure 27 Modify trap community dialog box



6. Modify the trap community attributes.
7. Click the **Save** button.

Deleting an SNMP trap community

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.

2. On the Unified Manager navigation tree click the **Services** key and click the **SNMP** heading.
   The SNMP Summary screen appears.
3. Click the **Trap Community List** tab.
   The Community List screen appears.
4. Highlight the list you want to delete.
5. On the **Configuration** menu select **Delete Community**.
   A message appears that asks you to confirm or cancel the deletion.
6. Click the **Yes** button.
   The SNMP trap community list is deleted from the database.

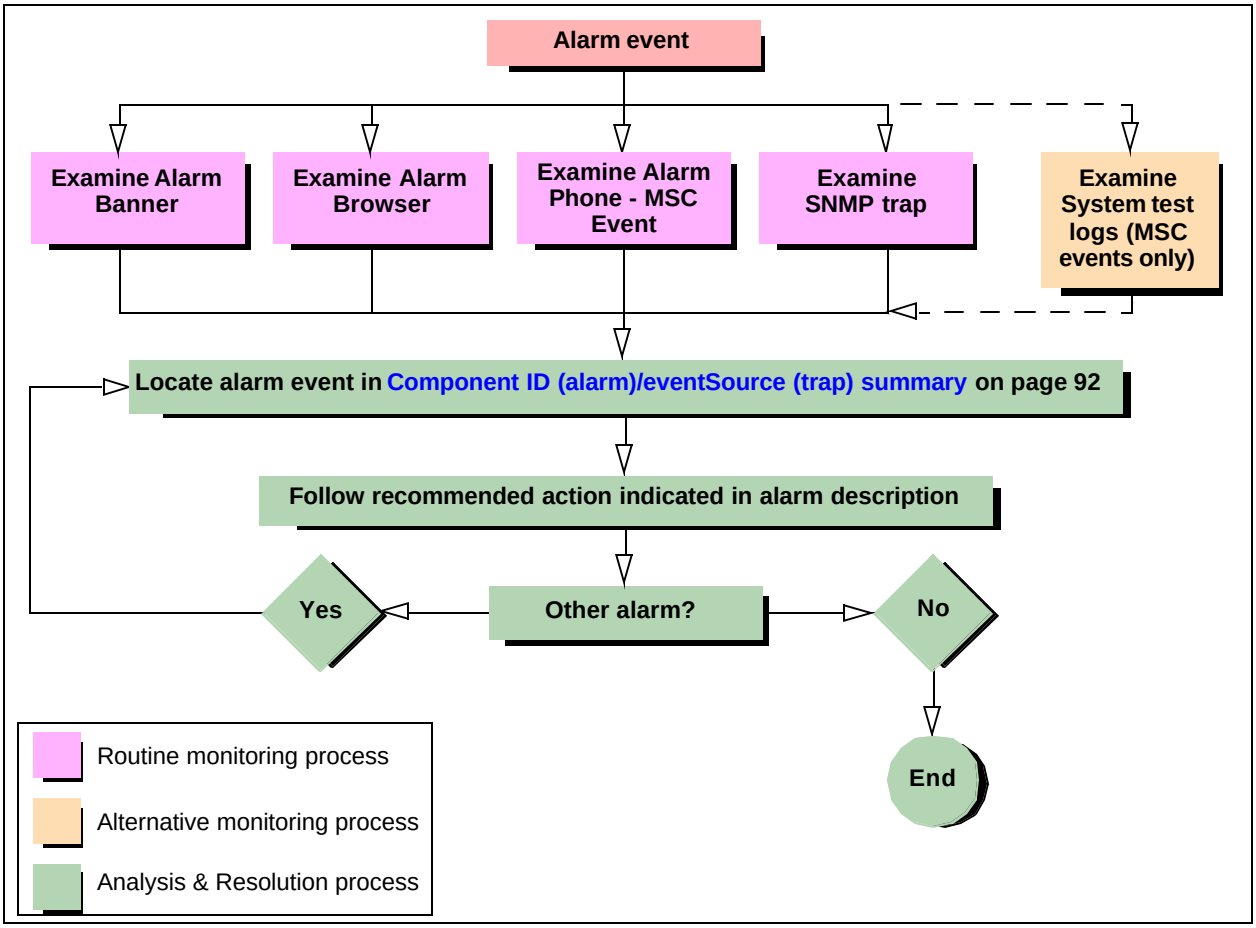
Alarm Analysis and Clearing Procedures

Use the information in this section to identify, analyze and clear alarm events. This section describes alarm messages and appropriate, associated maintenance activities (see the Alarm clearing flow chart below.). Use the information in this section as a reference to interpret and act upon event notifications from your alarm interface.

Unified Manager tools for detecting events that affect system performance or function

- The Alarm Banner and Alarm Browser. These are the primary Unified Manager alarm detectiontools.
- The phone alarm (if configured) provides both a visual and audible indication of an MSC alarm event.
- The event logs displayed through the SNMP trap watcher provide supporting information or as an alternative event reporting tool.
- The system test log provides supporting alarm information (for MSC events only).

Figure 28 Alarm clearing flow chart



SNMP Event Messages

SNMP Trap notifications (messages) are displayed in your SNMP trap watcher.

SNMP event messages are generated when

- a system level service is activated or stopped
- a Nortel Networks configurable service is activated or stopped

SNMP events severity levels

- Error
- Warning
- Information

Using the component ID and event ID summary tables

The Alarm System shows the source of a BCM alarm as “Component ID”, whereas the SNMP system shows the source of the same information as a trap of source “eventSource”. The terminology used in this document of Component ID (alarm) / eventSource (trap) is intended to show that these two systems call the same information by different names.

Use the table “Component ID (alarm)/eventSource (trap) summary” on page 92 to navigate to the SNMP event displayed in your SNMP trap watcher.

Alternatively, use “Component ID alarms/eventSource (Trap) by event ID” on page 95 to identify SNMP event ID and display the associated SNMP trap message and appropriate maintenance activity.

Alarm description information

- associated service name
- event ID number
- alarm interpretation and corrective actions
- associated logs

To use the alarm summary table

1. Examine the alarm name shown in the Alarm Browser.
2. Select the corresponding link shown in “Component ID (alarm)/eventSource (trap) summary” on page 92 under Alarm name.
   The alarm description is displayed.
   “Component ID (alarm)/eventSource (trap) summary” on page 92 also displays the service associated with the alarm.

3 Select the associated service name link to display the service description (see “Service Definitions” on page 257).

4 Select the **Return to table** link to display the alarm summary table to select another alarm or service description.

Component ID (alarm) summary information

Use the information displayed in this table to search for an alarm by the Component ID. Use the table to display the Component ID alarm description and to determine the cause of an alarm/trap and the appropriate maintenance activity.

Use the table to go to the descriptions you require:

- Click a link in the Component ID link (alarm)/eventSource (trap) column to review the alarm/trap description.
- Click a link in the Associated Service column to review the service associated with the Component ID (alarm). For example, discontinuation of a service or dependant service can trigger an event notification or SNMP Trap for a specific Component. For detailed descriptions of services see Chapter 3, “Service Management System.
- Use Component ID alarms/eventSource (Trap) by event ID to search for a Component ID (alarm) by the associated Event ID.

Table 12 Component ID (alarm)/eventSource (trap) summary

Component ID (alarm) / eventSource (trap)	Associated Service	Component ID (alarm) / eventSource (trap)	Associated Service
Atapi	None	SAM	None
Autochk	None	Save Dump	None
BCMAmp	None	Security	EventLog
Browser	Computer Browser	Serial	None
BRU	None	Service Control Manager	Call Detail Recording
CDRTransfer	None	Service Control Manager	DECT Alarm monitor
cfsServr	Voice CFS	Service Control Manager	DECT OAM
cfsServr	Voice Licensing services	Service Control Manager	Media gateway server
CTE	Voice CTE	Service Control Manager	Media services manager
DCOM	None	Service Control Manager	Message trace tool
DECTAlarms	DECT Alarm monitor	Service Control Manager	Net logon
DECTMtce	DECT Maintenance console	Service Control Manager	Plug and play
DhcpServer	Microsoft DHCP server	Service Control Manager	Remote access connection manager
disk	None	Service Control Manager	Task scheduler
DNS	Microsoft DNS server	Service Control Manager	UNISTIM Terminal proxy server
DrWatson	None	Service Control Manager	Voice CFS
emsManager	Media services manager	Service Control Manager	Voice CTE
eventLog	EventLog	Service Control Manager	VoiceCTI
FTMSS	None	Service Control Manager	Voice mail

Table 12 Component ID (alarm)/eventSource (trap) summary

Component ID (alarm) / eventSource (trap)	Associated Service	Component ID (alarm) / eventSource (trap)	Associated Service
HotDesking	HotDesking	Service Control Manager	Voice management subsystem
Inventory Service	Inventory service	Service Control Manager	Voice software alarm monitor
IPRIP2	None	Service Control Manager	VoIP Gateway
IPSecIKE	IPSecIKE service	Service Control Manager	Voice MSC service
IPXRouterManager	Routing and remote access service	Service Control Manager	Voice WAN
IVR	Nortel Networks IVR	SNMP	SNMP
JET	None	SNMP Trap Agent	SNMP Trap service
kbdclass	None	Srv	None
MGS	Media gateway server	SSH Secure Shell Server	None
Modem	None	Survivable Remote Gateway	None
MPS	None	System Status Monitor	System status monitor
MSPAlarmService	None	Tcpip	None
mspQoS	None	TlntSvr	Tlntsvr
mspQoSMP	None	ToneSrvr	None
NCM	None	UPS	UPS - APC Powerchute plus
NetBT	None	UTPS	UNISTIM Terminal proxy server
NetIQccm	NetIQ AppManager client communication manager	VBMain	VBMain
NetIQmc	NetIQ AppManager client communication manager	VNC Service	VNC server
NetIQObjMgr	NetIQ AppManager client communication manager	VNetManager	None
NetLinkManager	Net link manager	VoIPSipGateway	VoIP SIP Gateway
NetLogon	Net logon	VNetQosMonitor	Voice Net QoS monitor
NGRPCI	None	VNetVoIPGtwy	VoIP Gateway
Nnu	Voice NNU diagnostics	Voice CTE	Voice CTE
NSACD	NSACD	Voice software	Voice software alarm monitor
NwRdr	None	VoiceCTI	VoiceCTI
OSPFMib	None	VoiceManagementSubsystem	Voice management subsystem
Perfctrs	None	VoiceMSCService	Voice MSC service
Perflib	None	VoiceRecord	Call Detail Recording

Table 12 Component ID (alarm)/eventSource (trap) summary

Component ID (alarm) / eventSource (trap)	Associated Service	Component ID (alarm) / eventSource (trap)	Associated Service
Policy Services	Policy service	VoiceTimeSynch	Voice time synch
qos_flt_init	Qos_flt_init	VoiceWatchdog	Voice watchdog
Rdr	None	Wins	Windows internet name service
Router	Routing and remote access service	WINSCTRS	None
		Workstation	Workstation

Component event ID

Use the information in the table Component ID alarms/eventSource (Trap) by event ID to search for a Component ID (alarm)/eventSource (trap) by Event ID. The Event ID noted in the table is a short-form to indicate an Event ID (Alarm) / eventId (Trap). The Event ID applies to the Component ID (alarm) / eventSource (trap).

Use the Component ID alarm description to determine the cause of an alarm and the appropriate maintenance activity.

Use the links shown in the Component ID (Alarm) / eventSource (Trap) column to navigate.

- Click a Component ID name associated with the Event ID to display the Component ID alarm description.
- Use the table Component ID (alarm)/eventSource (trap) summary to search for the Component ID alarm description by the Component ID.

Table 13 Component ID alarms/eventSource (Trap) by event ID

Event ID (Alarm) / eventID (Trap)	Component ID (Alarm) / eventSource (Trap)
0	NetIQccm, NetIQmc, NetLinkManager, NSACD, qos_flt_init, SSH Secure Shell Server, VBMain
1	DNS, FTMSS, IVR, VNC Service, VoiceManagementSubsystem
2	DNS, FTMSS, IPSecIKE, OSPFMib, VoiceManagementSubsystem
3	DNS, FTMSS, IPSecIKE
4	FTMSS, IPSecIKE, NGRPCI
5	FTMSS, IPSecIKE, NGRPCI, Policy Services
6	FTMSS, IPSecIKE, Policy Services
7	FTMSS, IPSecIKE, kbdclass
8	FTMSS, JET, Serial
9	Atapi, IPSecIKE, JET
10 - 11	IPSecIKE
12 - 15	IPSecIKE
16	IPSecIKE, JET
17	IPSecIKE
18	Voice software
19	IPSecIKE
20	Voice software
21 - 24	IPSecIKE, Voice software
25 - 30	IPSecIKE
31 - 37	IPSecIKE, Voice software
39 - 40	Voice software

Table 13 Component ID alarms/eventSource (Trap) by event ID

Event ID (Alarm) / eventID (Trap)	Component ID (Alarm) / eventSource (Trap)
41 - 47	disk, Voice software
50 - 51	Voice software
52 - 55	Modem
59, 61 - 63, 67 - 68	Voice software
69	JET
71 - 72, 75, 77, 79 - 99	Voice software
100	cfsServr, FTMSS, VoiceManagementSubsystem , VoiceRecord
101	cfsServr, SNMP Trap Agent, VoiceRecord
102	SNMP Trap Agent, VNetVoIPGtwy, Voice software, VoiceRecord, VoIPSipGateway
103	Voice software, VoiceRecord
104	VoiceRecord
105	cfsServr, VNetVoIPGtwy, VoiceRecord, VoIPSipGateway
106	VoiceRecord
108	cfsServr, VoiceRecord,
109 - 111	cfsServr
113	cfsServr, VNetVoIPGtwy
114 - 119, 122 - 123, 125 - 126	cfsServr, VoIPSipGateway , VNetVoIPGtwy
130	VoIPSipGateway, VNetVoIPGtwy
131	VNetVoIPGtwy, VoIPSipGateway
194	Voice software
200 - 201	VNetVoIPGtwy, Voice software, VoIPSipGateway
202	Voice software
203 - 206	VNetQosMonitor, Voice software
207 - 209, 224, 226, 229, 247	Voice software
256	DECTAlarms, DECTMtce,
257	BCMAmp, CTE, NetIQccm, ToneSrvr, Voice CTE, VoiceCTI, VoiceMSCService
258	BCMAmp, CTE, ToneSrvr, VoiceCTI
259	VoiceCTI
260	Voice software
261	NetIQccm
262, 263	Voice software
264	NetIQccm
265, 270 - 271	Voice software
300	BRU
301	BRU, NCM, VNetManager

Table 13 Component ID alarms/eventSource (Trap) by event ID

Event ID (Alarm) / eventID (Trap)	Component ID (Alarm) / eventSource (Trap)
302	BRU, FTMSS, NCM
303	BRU, FTMSS
304	BRU, FTMSS, VNetManager
305	BRU, FTMSS
306	BRU, VNetManager
307 - 310	BRU
311 - 312	BRU, NCM
313 - 315	BRU
320 - 322	FTMSS
323	FTMSS, Voice software
324	FTMSS, Voice software
325 - 335, 367, 400 - 401	Voice software
512, 514 - 515, 528 - 529, 538, 577	Security
608, 617	Voice software
624, 626 - 628, 630, 632 - 633, 636 - 637	Security
639	Voice software
642, 644	Security
708	DNS
771 - 772	BCMAmp, ToneSrvr
773 - 775	BCMAmp
799, 894, 901, 949, 997 - 999	Voice software
1000	emsManager, Nnu, System Status Monitor, TlntSvr, UPS, VoiceWatchdog
1001	Autochk, emsManager, MGS, MPS, Save Dump, SNMP, System Status Monitor, UPS, VoiceTimeSynch, VoiceWatchdog
1002	MGS, MPS, System Status Monitor, UPS, VoiceTimeSynch
1003	MGS, System Status Monitor, VoiceWatchdog
1004 - 1005	MGS, System Status Monitor, UPS, VoiceWatchdog
1006	System Status Monitor, UPS, VoiceWatchdog
1007	System Status Monitor, VoiceWatchdog
1008	Perflib, System Status Monitor
1009 - 1010	System Status Monitor
1011	DhcpServer, System Status Monitor
1012 - 1015	System Status Monitor
1016	System Status Monitor, UPS
1018, 1030, 1033 - 1034, 1040, 1102, 1150, 1162, 1165	UPS

Table 13 Component ID alarms/eventSource (Trap) by event ID

Event ID (Alarm) / eventID (Trap)	Component ID (Alarm) / eventSource (Trap)
1200, 1204 - 1209	Survivable Remote Gateway
1253	UPS
2000	mspQoS, Srv, System Status Monitor, UTPS, VoiceWatchdog
2001	MGS, MPS, System Status Monitor , UPS
2002	MGS, MPS, Perflib, System Status Monitor
2003 - 2004	MGS, MPS, System Status Monitor
2005	MPS, System Status Monitor
2006 - 2008	System Status Monitor
2019, 2021	Srv
2030, 2036 - 2037	UPS
2088	CDRTransfer
2090	MGS
2200 - 2208	Survivable Remote Gateway
3000	emsManager , HotDesking, System Status Monitor, UTPS, VoiceWatchdog
3001 - 3002	emsManager , MGS, MPS, System Status Monitor, VoiceWatchdog
3003 - 3005	MGS, MPS, System Status Monitor , VoiceWatchdog
3006 - 3008	MGS, MPS, System Status Monitor
3009 - 3012	System Status Monitor
3013	Rdr, System Status Monitor
3014 - 3017	System Status Monitor
3087 - 3088	CDRTransfer, Workstation
3090	CDRTransfer, MGS
3091 - 3092	MGS
3095	NetLogon
3101	Perfctrs
3201 - 3203	Survivable Remote Gateway
3300 - 3302	Inventory Service
4003, 4014, 4019 - 4024, 4026, 4028, 4030 - 4032, 4034 - 4041, 4043 - 4055	mspQoSMP
4097	DrWatson, Wins
4098	Wins
4198 - 4199	Tcpip
4314	WINSCTRS
4319	NetBT
5000	NGRPCI
5001	mspQoSMP, NGRPCI

Table 13 Component ID alarms/eventSource (Trap) by event ID

Event ID (Alarm) / eventID (Trap)	Component ID (Alarm) / eventSource (Trap)
5003	NGRPCI
5005	mspQoSMP
5009	NGRPCI
5011	mspQoSMP
6005 - 6006, 6009	eventLog
7000 - 7001, 7009, 7023 - 7024, 7026	Service Control Manager
8007	NwRdr
8021, 8033	Browser
9001, 9004	mspQoSMP
10001	DCOM
10002, 10004 - 10005, 10010	DCOM
12288	SAM
15000, 15001, 15002	NetIQObjMgr
20013, 20015, 20031, 20048 - 20049, 20064, 20089, 20101, 20103, 20105, 20111	Router
20133	IPXRouterManager
20139	Router
30052	IPRIP2
100300, 100401 - 100403, 100500 - 100503, 100601, 100700, 100900, 101300, 101400, 101500, 101601, 101700, 103100, 103200, 103500, 103600, 103700, 103800, 110000, 110100, 200000 - 200008, 200200, 200301, 200400 - 200403, 200700, 201301 - 201302, 203100, 203200, 203300, 203400, 203500, 203600, 203800, 203900, 300000, 300100, 300200 - 300202, 300204 - 300206, 300300, 300400, 301000, 301301, 301302, 301303, 301304, 301400, 301500, 301600, 310001 - 310002, 310101 - 310102, 310700	UPS

Component ID/SNMP Trap Error interpretation

Use the information in this section to interpret the message displayed in the message field for all the Component ID / SNMP Traps.

Some error strings are specific to certain Component IDs, so the descriptions are more specific. Other descriptions are generic and the description can be applied to all instances regardless of the Component ID/ SNMP Trap error.

SNMP traps received from Business Communications Manager contain descriptions of the alarms that occurred in the system. These SNMP traps consist of the following Business Communications Manager-specific parameters in addition to the generic parameters. Refer to the IETF RFCs on SNMP traps for descriptions of these generic parameters. Additionally, SNMP generic traps such as coldStart, linkDown, linkUp, authenticationFailure, are also generated from Business Communications Manager according to the user's configuration. For details of these SNMP generic traps, see the relevant IETF RFCs.

Message (error string)	Description
<error string provided by CFS>	All those errors match internal CFS errors. If they occur, there is something wrong internally (i.e. no memory to allocate buffers, etc.). When those occur, that means there is usually something else wrong with the system. Contact your support organization for help.
%1, %2, etc.	Placeholders for values passed to the event message. This is the syntax used by the Event Log APIs in order to pass values into the string. If they appear without the correct text, then there is something wrong with how that value is passed.
Established IPsec SAs on <local IP Addr> with <remote IP Addr>: AH outbound SPI <Hex Number>, AH inbound SPI <Hex Number>.	The Inbound and Outbound SPI (Security Policy Index) is a unique number that is assigned to each IPSec QuickMode connection.
BCM has no IP Address on the IPSec Client private network: IP Address: %1 IP Mask: %2.	IP Addresses and masks in hexadecimal format. The example is the IP Address and subnet mask of the IP Address that will be given to the VPN client when they connect
Error notification (%d) received on <local IP Addr> from <remote IP Addr	These are the error notification messages as specified in the IPSec RFC 2401 - 2412.
Established IPsec SAs on <local IP Addr> with <remote IP Addr>: AH outbound SPI <Hex Number>, AH inbound SPI <Hex Number>.	The Inbound and Outbound SPI (Security Policy Index) is a unique number that is assigned to each IPSec QuickMode connection.
Oakley %d Mode proposal accepted on <local IP Addr> from <remote IP Addr>.	The %d should either display the text "Main" or "Aggressive" Main is for Branch Office connections and Aggressive is for VPN client connections. If it doesn't display one of these then it's an error.

Message (error string)	Description
NSACD service there is an Event ID: 0 Message: ITGNS error: < >, Exit code: < >.	These events may occur when the services are booting up and attempting to register and run as an NT service. The error code is an integer returned by the Win32 GetLastError function, and can be mapped back to a specific Windows error using the System Error Codes table. The exit code may be one of {-1, -2, -3}, depending on how far service initialization processed before it failed. 1 = Invalid payload type, 2 = Domain of Interpretation not supported, 3 = Situation not supported
VBMAin service Event ID: 0 VBMain error: %d, Exit code: %d	These events may occur when the services are booting up and attempting to register and run as an NT service. The error code is an integer returned by the Win32 GetLastError function, and can be mapped back to a specific Windows error using the System Error Codes table. The exit code may be one of {-1, -2, -3}, depending on how far service initialization processed before it failed. 1 = Invalid payload type, 2 = Domain of Interpretation not supported, 3 = Situation not supported

Component ID alarm descriptions

Use the descriptions in this section to obtain more information on Component ID alarms and the appropriate maintenance activities.

Note: If you need more information about the Component ID differences between Business Communications Manager software loads, contact Nortel Support.

Use the links in the Component ID alarm descriptions to navigate

- Click a Component ID (alarm)/eventSource (trap) summary link to select an alarm by the Component ID (alarm)/eventSource (trap).
- Click a Component ID alarms/eventSource (Trap) by event ID link to select a Component ID (alarm) by the Event ID. The Event ID noted in the descriptions is a short-form to indicate an Event ID (Alarm)/eventId (Trap). The Event ID applies to the Component ID (alarm)/ eventSource (trap).
- Click the Service link to review the service description associated with the Component ID (alarm.)/eventSource (trap).
- Click the Logs link to review the log description associated with the Component ID (alarm.)/ eventSource (trap).

Atapi

Atapi provides the disk controller IDE (standard) driver for hard drives installed in the BCM.

atapi	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 9	Message:	The device, \Device\ScsiPort0, did not respond within the timeout period.
	User action:	For the drives in question, these timeout message are not serious if they occur at system boot. However, if several of these messages appear in the system log during normal system operation, contact Nortel Networks support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	

Autochk

Autochk provides the file system check function for hard drives.

Autochk	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 1001	Message:	Checking file system on <drive>: The type of the file system is …
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

BCMAmp

BCMAmp provides the music on hold player on the BCM.

BcmAmp	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	IpMusic (BcmAmp)
Event ID: 257	Message:	BcmAmp version %s has started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

BcmAmp	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 258	Message:	Shutdown complete.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 771	Message:	IP Music Error: Integrated MOH player - malformated songs .cfg file. Unable to proceed, ervice shutting down.
	User action:	Disable the BcmAmp player by configuring your IP Music source as either: Audio Jack or Network Audio. Contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 772	Message:	IP Music Error: Integrated MOH player - unable to initialize network connection. Service shutting down.
	User action:	Disable the BcmAmp player by configuring your IP Music source as either: Audio Jack or Network Audio. Contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 773	Message:	IP Music Error: Integrated MOH player - initialization error. Unable to proceed. Service shutting down.
	User action:	If stopping and starting the IP Music service via the Unified Manager fails to rectify the problem, disable the IP Music service and contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 774	Message:	IP Music Error: Integrated MOH player - initialization failure. Service shutting down.
	User action:	If stopping and starting the IP Music service via the Unified Manager fails to rectify the problem, please disable the IP Music service and contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 775	Message:	IP Music Error: Integrated MOH player - unable to allocate resources. Service shutting down.
	User action:	If stopping and starting the IP Music service via the Unified Manager fails to rectify the problem, please disable the IP Music service and contact Customer Support for more assistance.
	Alarm severity:	Critical

BcmAmp	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None

Browser

Browser	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Computer Browser
Event ID: 8021	Message:	The browser was unable to retrieve a list of servers from the browser master <PDC> on the network \device\<protocol_netcard>. The data is the error code.
	User action:	Check the network setup.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 8033	Message:	The browser has forced an election on network \device\<protocol_netcard> because a master browser was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

BRU

BRU provides the backup and restore utility function on the BCM (see Chapter8, “System Backup and Restore (BRU)”).

BRU (Backup & restore utility)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 300	Message:	BRU Backup Starting.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 301	Message:	Backup finished successfully
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 302	Message:	Backup finished with warnings. Warnings were logged in %DESTINATION_NAME%.rep on the destination.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning

BRU (Backup & restore utility)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 303	Message:	Backup finished with errors. Errors were logged in %DESTINATION_NAME%.rep on the destination.
	User action:	Review log files to determine FAILED component. Take corrective action if necessary and retry backup.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 304	Message:	BRU Restore Starting
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 305	Message:	Restore finished successfully.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 306	Message:	Restore finished with warnings. Warnings were logged in BRURest.log and %~n0.rep.txt on the source.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 307	Message:	Restore finished with errors. Errors were logged in BRURest.log and %~n0.rep.txt on the source.
	User action:	Review log files to determine FAILED component. Take corrective action if necessary and retry restore.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 308	Message:	An error has occurred when trying to access the UTPS pipe.
	User action:	During BRU activity, IP sets may reset. No action necessary.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 309	Message:	BRU has increased set watchdog from 30 sec. to 15 minutes.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information

BRU (Backup & restore utility)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 310	Message:	BRU has decreased set watchdog from 15 minutes to 30 sec.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 311	Message:	An error %RetV% has occurred when trying to start the voice services.
	User action:	Review voice services and restart if necessary through Unified Manager. See service specific logs for cause of failure.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 312	Message:	All voice mail services have been started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 313	Message:	All voice mail services have been stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 314	Message:	Error: %DriveType% drive not connected.
	User action:	Ensure destination drive is visible on the network and that correct permissions are set.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 315	Message:	Error: %DriveType% drive not connected. %MapPath% not found.
	User action:	Ensure destination drive is visible on the network and that correct permissions are set.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

CDRTransfer

CDRTransfer provides the call detail recording transfer function on the BCM.

CDRTransfer)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 2088	Message:	Not Push
	User action:	Check if there are actual CDR data files under the CDR data file directory.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2088	Message:	No more CDR data files!!!
	User action:	Check if there are actual CDR data files under the CDR data file directory.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 3087	Message:	ZpInit() error!!!
	User action:	Check if Zip32.dll is installed properly under the CDRTransfer directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3087	Message:	ZpSetOpt() error!!!
	User action:	Check if Zip32.dll is installed properly under the CDRTransfer directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Can't open reg key err = %1
	User action:	Check if CDRTransfer registry entries are damaged
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Can't get current dir err = %1
	User action:	Check if you have permission to get current directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

CDRTransfer)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 3088	Message:	Can't change to working dir err = %1
	User action:	Check if you have permission to go to CDRTransfer working directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Clip CDR data file error err = %1
	User action:	Check if CDRClip.exe is installed properly under the CDR directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Find CDR data file error err = %1
	User action:	Check if there are CDR data files under CDR data file directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Can't get FTP connection err = %1
	User action:	Check if FTP configuration or network goes wrong.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	Can't go to remote dir on FTP server err = %1
	User action:	Check if permission of des tination directory on the client PC is granted to CDRTransfer.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3088	Message:	ZpArchive() err = %1
	User action:	Check if Zip32.dll is installed properly under the CDRTransfer directory.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3090	Message:	Multiple instances are running, exit!
	User action:	Means multiple CDRTransfer instances are running simultaneously, but only one survives. No action is required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3090	Message:	Can't Get the value of %1 err= %2
	User action:	Check if CDRTransfer registry entries are damaged.

CDRTransfer)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3090	Message:	Can't transfer file %1 err= %2
	User action:	Check if FTP configration or network goes wrong.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3090	Message:	Can't delete CDR data file transferred %1 err= %2
	User action:	Check if you have permission to delete this file.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3090	Message:	Can't -A CDR data file transferred %1 err= %2
	User action:	Check if you have permission to change the attribute of this file.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

cfsServr

cfsServer (Component feature service)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice CFS, Voice Licensing services
Event ID: 105	Message:	The service was installed.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 108	Message:	The service was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 109	Message:	<error string provided by CFS>.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 110	Message:	Duplicate keycode has been entered - this keycode has been previously entered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 111	Message:	Keycode <24 digit number - keycode value> is invalid.
	User action:	Confirm that the keycode was entered correctly and that the applicable functionality is available on the BCM.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 113	Message:	Verification of System Licensing in progress.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

cfsServer (Component feature service)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 114	Message:	Verification of System Licensing completed.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 115	Message:	Verification of system licensing failed due to error: <error Information>.
	User action:	Specific to error Information.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 116	Message:	Keycode <keycode value> applied. <name of functionality enabled by keycode - Component-defined string> activated.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 117	Message:	Unable to apply keycode: <keycode value>.
	User action:	The service associated with the keycode is not running properly. If it is stopped, then start it. If it is running, then stop it and restart it.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 118	Message:	Processing of keycode input file in progress.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 119	Message:	Processing of keycode input file completed.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 122	Message:	Trial has expired.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 123	Message:	Error applying keycode: <keycode value> <out of range or unsupported keycode value Information from component>.

cfsServer (Component feature service)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Specific to Information from component.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 125	Message:	Error applying keycode: <keycode value>.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 126	Message:	<Keycode functionality Trial functionality> expired.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

CTE

CTE	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice CTE
Event ID: 257	Message:	Changes have been detected in the KSU configuration.
	User action:	Restart all TAPI applications to use with the new configuration.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 258	Message:	A CTE application attempted to register with CTE before the Voice CTE service had fully initialized (error <error code>). If the application is not behaving correctly restart it after the Voice CTE service has started. <RTR001>
	User action:	If the application is not behaving correctly restart it after the Voice CTE service has started.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 258	Message:	KSU connection is down all devices are disabled.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

DCOM

Distributed Components (Microsoft API) provides the components needed for Unified manager.

DCOM	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 10001	Message:	Unable to start a DCOM Server: %3 as %4%5.\r\n The error: %n"%%%2"%nHappened while starting this command:%n%1\r\n
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

DCOM	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 10002	Message:	Access denied attempting to launch a DCOM Server. The server is: {CF6B5196-5214-11D3-8A85-000000000000} The user is %2%3, SID=%4.
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 10004	Message:	DCOM got error "Logon failure: unknown user name or bad password " and was unable to logon <computer name>\ee_admin in order to run the server: {1338C614-888C-11D2-8F01-0080C79B65A2}
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	There is a possibility that user can change password for ee_admin either from VNC or UM. So to figure out what user did, we can get the recording logs from BCM.
Event ID: 10005	Message:	DCOM got error "The specified service is disabled and cannot be started. " attempting to start the service <Service Name> with arguments "-Service" in order to run the server:.
	User action:	Verify if the service <Service Name> is disabled, and enable the service <Service Name> if needed.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 10010	Message:	The server {1338C620-888C-11D2-8F01-0080C79B65A2} did not register with DCOM within the required timeout.
	User action:	Only Nortel Networks' personnel should do these actions: (1) reboot, (2) if problem persists, through VNC run miserver shutdown, and mspTrace -mutils -d0xffffffff, (3) try again, collect the trace files in …\Unified Manager\log, and forward them to developers.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

DECTAlarms

DECTAlarms	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	DECT Alarm monitor
Event ID: 256	Message:	01:10:03.694 [DECT Alarm Monitor:4.]DECT Alarm Manager Started
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

DECTMtce

DECTMtce	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	DECT Maintenance console
Event ID: 256	Message:	The description for Event ID (256) in Source (DECTMtce) could not be found. It contains the insertion string(s): 01:10:03.895 [DECT MaintenanceConsole:4.]MCServer Started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

DhcpServer

DhcpServer	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Microsoft DHCP server
Event ID: 1101	Message:	The DHCP server issued a NACK to the client (MAC Address of the Requesting Client) for the address (Requested IP Address) request.
	User action:	Please make sure that the address pool for dial in user is outside or is excluded from the DHCP server scopes.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

disk

Disk provides the hard disk drivers on the BCM.

disk	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 41	Message:	The file system structure on the disk is corrupted and unusable. Please run chkdsk utility on the device \Device\Harddisk0\Partition3 with label "".
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

DNS

DNS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Microsoft DNS server
Event ID: 1	Message:	Starting Microsoft DNS Server (Windows NT 4.0 Service Pack 5).
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2	Message:	The DNS Server has started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 3	Message:	The DNS Server has shutdown.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 708	Message:	The DNS Server has no 'primary' or 'secondary' zones. The DNS Server will run as a caching-only server
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 708	Message:	The DNS Server has no 'primary' or 'secondary' zones. The DNS Server will run as a caching-only server, but will not be authoritative for any zones
	User action:	No action required.

DNS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

DrWatson

DrWatson provides a debug utility which saves error files.

DrWatson (Application Dump Events)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4097	Message:	The application, <application name>, generated an application error The error occurred on <data>@<time> The exception generated was <exception code> at address <address> (symbol)
	User action:	Contact your Nortel Networks support team.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

emsManager

emsManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Media services manager
Event ID: 1000	Message:	Service started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1001	Message:	Service terminated.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 3000	Message:	MSC Driver is in the core upload mode - aborting.
	User action:	If this happens due to an interrupted upload of the core image, the user must upload the core. Once the upload procedure completes successfully, the error will go away. If this happens during a core upload, no action is required (it should not happen, because during the core upload, there is no reason to start the MSM).
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3001	Message:	Registry contains an invalid published IP address.

emsManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	This happens only if the IP address of a NIC, that is currently selected in the Published IP Address field of the UM, has been changed and due to some kind of an error the registry was not properly updated. Use the Unified Manager to select the Published IP Address again. Recommended method is to change it to another NIC and then back to the desired NIC.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3002	Message:	BCM switch reset - disconnecting all applications
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

eventLog

eventLog	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	EventLog
Event ID: 6005	Message:	The Event log service was started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 6006	Message:	The Event log service was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 6009	Message:	Microsoft (R) Windows NT (R) 4.0 1381 Service Pack 5 Uniprocessor Free.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

FTMSS

FTMSS provides the core telephony services under the Unified Manager (telephony navigation tree) component.

FTMSS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 1	Message:	Service started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2	Message:	Service stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

FTMSS	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 3	Message:	The Service control request handler could not be registered.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 4	Message:	Received a bad service request.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 5	Message:	Couldn't open the Service Control Manager.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 6	Message:	Couldn't open the %1 service.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 100	Message:	(dynamic)
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 304	Message:	(dynamic)
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 305	Message:	(dynamic)
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 320	Message:	Map file: '%s' is required, but could not be found.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error

FTMSS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 321	Message:	Could not open map file: '%s'. No file handles.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 322	Message:	Map file: '%s' is corrupted and must be re-installed.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 323	Message:	Map file: '%s' is not compatible with this version of '%s'.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 324	Message:	Could not open map file: '%s'.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

HotDesking

HotDesking	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	HotDesking
Event ID: 3000	Message:	HotDesking: Unable to create registry entry
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	HotDesking: Unable to open registry data
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	** UTPS Services table is full.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	** Hot desking being terminated by UTPS.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	Hot Desking server is unable to connect to the UTPS.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	*** Unable to get a timer from the OS.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.
Event ID: 3000	Message:	Hot Desking is unable to initiate the registry.

HotDesking	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service will shut down and be re-started by the watchdog.

Inventory Service

Inventory Service	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Inventory service
Event ID: 3300	Message:	Inventory Service may have generated an incomplete or incorrect report. Exception caught while loading DLLs: missing %s.dll
	User action:	Contact customer support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3301	Message:	Inventory Service may have generated an incomplete or incorrect report. %s GetInventoryDocument() returned error.
	User action:	Contact customer support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3302	Message:	Inventory Service may have generated an incomplete or incorrect report. Failed to open Software resource: %s
	User action:	Contact customer support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

IPRIP2

IPRIP2 provides the routing information protocol (RIP) v2 component for BCM router. RIP is a simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

IPRIP2	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 30052	Message:	IPRIPv2 could not join the multicast group 224.0.0.9 on the local interface with IP address x.x.x.x. The data is the error code.
	User action:	Make sure that IP RIP v2 is properly configured on the local interface from which the event is received. If the problem persists, even after configuring the interface to RIP v2, please contact tech support.
	Alarm severity:	Critical

IPRIP2	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None

IPSecIKE

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	IPSecIKE service
Event ID: 2	Message:	ISAKMP SA established on <local IP Addr> with <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 3	Message:	Could not initiate ISAKMP SA <local IP Addr> to <remote IP Addr>
	User action:	Check settings and Connection
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 4	Message:	Deleting ISAKMP SA from <local IPAddr> to <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 5	Message:	No response on <local IP Addr> from <remote IP Addr> - logging out.
	User action:	Check settings and Connection.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 6	Message:	<local IP Addr> Local interface down - logging out of <remote IP Addr>.
	User action:	Check local interface setup.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 7	Message:	Could not initiate Quick Mode from <local IP Addr> to <remote IP Addr>.
	User action:	Check settings and Connection.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 9	Message:	PFS required on <local IP Addr> but not provided by <remote IP Addr>.
	User action:	Check PFS setting on remote side.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 10	Message:	No local interface for <local IP Addr>.
	User action:	Check local interface setup.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 11	Message:	Unauthenticated Informational message received on <local IP Addr> from <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 12	Message:	Informational message received on <local IP Addr> from <remote IP Addr> not authentic.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 13	Message:	Unprotected Notify message on <local IP Addr> from <remote IP Addr> being dropped.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 14	Message:	Bad length on Notify message received on <local IP Addr> from <remote IP Addr> - dropping it.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 15	Message:	No SPI on Notify message received on <local IP Addr> from <remote IP Addr> after Phase 1 - dropping it.
	User action:	No action required.

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 16	Message:	Unprotected Delete message on <local IP Addr> from <remote IP Addr> being dropped.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 17	Message:	Bad length on Delete message on <local IP Addr> from <remote IP Addr> - dropping it.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 18	Message:	Bad length on Delete message on <local IP Addr> from <remote IP Addr> - dropping it.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 19	Message:	Could not find SPI for message received on <local IP Addr> from <remote IP Addr> - message dropped.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 20	Message:	Error notification (%d) received on <local IP Addr> from <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 21	Message:	Delete message (for protocol %1) received on <local IP Addr> from <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 22	Message:	Established IPsec SAs on <local IP Addr> with <remote IP Addr>: AH outbound SPI <Hex Number>, AH inbound SPI <Hex Number>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 23	Message:	Established IPsec SAs on <local IP Addr> with <remote IP Addr>: ESP outbound SPI <Hex Number>, ESP inbound SPI <Hex Number>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 24	Message:	Deleting IPsec SAs on <local IP Addr> with <remote IP Addr>: AH outbound SPI <Hex Number>, AH inbound SPI <Hex Number>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 25	Message:	Deleting IPsec SAs on <local IP Addr> with <remote IP Addr>: ESP outbound SPI <Hex Number>, ESP inbound SPI <Hex Number>.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 26	Message:	Failed to Establish IPsec SAs on <local IP Addr> with <remote IP Addr>.
	User action:	Check settings and Connection.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 27	Message:	Oakley %d Mode proposal accepted on <local IP Addr> from <remote IP Addr>.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 28	Message:	Unknown Notify message (%d) received on <local IP Addr> from <remote IP Addr>.

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 29	Message:	Remote system <remote IP Addr> not responding! Deleting SA on interface: <local IP addr>
	User action:	Check settings and Connection.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 30	Message:	Idle timeout condition on IPSec SA between Local: <local IP addr>, Remote: <remote IP addr>. Delete SA.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 31	Message:	IPSec Client connection request on %1 from %2 Rejected. No Default Route Set on BCM. IPSec Client Termination is not supported.
	User action:	Use Net Link Manager to set a Default Route.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 32	Message:	ISAKMP Socket Open Failed on interface %1. Trying to re-init Socket Interfaces.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Warning
	Logs:	None
Event ID: 33	Message:	ISAKMP Socket Open Failed on interface %1.
	User action:	Stop and Re-start IPSecIKE service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 34	Message:	BCM has no IP Address on the IPSec Client private network: IP Address: %1 IP Mask: %2.
	User action:	Set an interface to have a valid IP Address on the same network as assigned IP Address for IPSec client.
	Alarm severity:	Critical
	Trap-type:	Error

IPSecIKE (Internet protocol security - Internet key exchange)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 35	Message:	BCM interface that IPSec client is trying to connect to (%1) is on the private network (%2).
	User action:	PC IPSec Client should connect to a different interface on the BCM.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 36	Message:	The IP Address of the PC running the IPSec client (%1) is on the private network (%2).
	User action:	PC IPSec Client is not on the correct network.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 37	Message:	IPSec Client connection request on %1 from %2 Rejected. BCM only supports IPSec Client connection requests from PCs on a different subnet that come in over the Interface connected to the Next Hop Router.
	User action:	If there is a router between the PC running IPSec client and the interface you are trying to connect to on the BCM, then the NetLinkManager needs to be defined to use this interface in order to support IPSec Client.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

IPXRouterManager

IPXRoutManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Routing and remote access service
Event ID: 20133	Message:	IPX Routing failed to start because IPX forwarder driver could not be loaded.
	User action:	See Microsoft article Q180602. If the solutions provided in the article do not work, please re-install IPX. Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

IVR

IVR	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Nortel Networks IVR
Event ID: 1	Message:	Severity:<severity> Component:<comp> Message:<message>
IVR process-name	User action:	See the IVR Alarm List for actions for these generic IVR alarms.
	Alarm severity:	warning/critical/warning
	Trap-type:	Information/Error/Warning
	Logs:	None
	Comments:	These are general IVR events; they are not BCM specific.
Event ID: 1	Message:	Severity: 7 Component: #vps.<IVR#>/<BCM-name> Message: Failed to read xref file %s::%s.
IVR(bim)	User action:	Verify that the mmfxref.dat file exists in the specified location and if not restore it. Otherwise delete and redo MMF to VFS conversions.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The first %s is the path and the second %s is the reason for failure.
Event ID: 1	Message:	Severity: 7 Component: #vps.<IVR#>/<BCM-name> Message: Play Failure. Unable to add vocab item '%s' to play list:%s.
IVR(bim)	User action:	Modify PeriProducer application to decrease the number of items in the play request.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 1	Message:	Severity: 7 Component: #vps.<IVR#>/<BCM-name> Message: Play Failure. Unable to add vocab item '%s' to play list:%s

IVR	Return to table:	Component ID (alarm)/eventSource (trap) summary
IVR(bim)	User action:	Inspect reason for failure and take appropriate action. If the reason is ME_PLAY_LIST_FULL then modify PeriProducer application to decrease the number of items in the play request.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The first %s is the path and the second %s is the reason for failure.
Event ID: 1	Message:	Severity: 7 Component: #vps.<IVR#>/<BCM-name> Message: Play Failure. Unknown vocabulary item '%s'.
IVR(bim)	User action:	Verify it is a recorded element in the MMF and the MMF has been converted to VFS. If not record element and perform conversion.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	First %s is the vocab item.
Event ID: 1	Message:	Severity: 7 Component: #vps.<IVR#>/<BCM-name> Message: Can't set port capabilities to %s:%s.
IVR(bim)	User action:	Reconfigure the number of media gateways.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	First %s is the port caps and second%s is reason for failure.
Event ID: 1	Message:	Severity: 1 Component: #vps.<IVR#>/<BCM-name> Message: Call presented and no ports available to receive the call.
IVR(bim)	User action:	Configure more IVR ports.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1	Message:	Severity: 1 Component: #vps.<IVR#>/<BCM-name> Message: Class=<Subsystem[MX]> mx_AnswerCall: Invalid Handle (2)
IVR(bim)	User action:	Terminate application from all administrative lines.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

JET

Joint Engine Technology (JET) provides the JET database driver for BCM. The database engine used in Microsoft Access that accompanies Visual Basic and C++. Jet is typically used for storing data in the client machine.

JET	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 8	Message:	((215)) The database engine 04.909.0000 started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 9	Message:	The database engine stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 16	Message:	((xxx)) The database is running recovery steps.
	User action:	No action required. See Microsoft Article Q165915.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 69	Message:	Redoing log file.\wins\j50.log.
	User action:	No action required. See Microsoft Article Q165915.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

kbdclass

Kbdclass provides the keyboard driver.

Kbdclass	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None

Kbdclass	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 7	Message:	Could not locate the device object for one or more keyboard port devices.
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	BCM FP1 Upgrades will fail to install, no longersupported, replace BCM hard drive.

LLNail

Kbdclass	Return to table:	
	Service:	None
Event ID: 8001	Message:	UTWAN: 2% channel(s) configured
	User action:	No action required.
	Alarm severity:	warning
	Trap-type:	information
	Logs:	None
Event ID: 8002	Message:	UTWAN: KSU ready
	User action:	No action required.
	Alarm severity:	warning
	Trap-type:	information
	Logs:	None
Event ID: 8003	Message:	UTWAN: Issued a command to create WAN task.
	User action:	No action required.
	Alarm severity:	warning
	Trap-type:	information
	Logs:	None
Event ID: 8004	Message:	UTWAN: Successfully created a WAN task.
	User action:	No action required.
	Alarm severity:	warning
	Trap-type:	information
	Logs:	None
Event ID: 8005	Message:	UTWAN: Failed to create a WAN task.
	User action:	No action required.
	Alarm severity:	minor
	Trap-type:	warning
	Logs:	None

MGS

MGS (Media gateway server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Media gateway server
Event ID: 1001	Message:	***** MGS <version> started on <date> *****
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

MGS (Media gateway server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1002	Message:	Mgs: Initialization complete (max=<x>, min=<n>)
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1003	Message:	Mgs: Shutting down on request from the SCM
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1004	Message:	MediaTransport:(OID=<oid>) Received valid ports
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	The problem reported in an earlier event 2001 has now returned to normal.
Event ID: 1005	Message:	MsmProxy: <interface> succeeded
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	The problem reported in an earlier event 2004 has now returned to normal.
Event ID: 2001	Message:	MediaTransport:(OID=<oid>) Received bad ports: <port1> <port2>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Resource Manager allocated invalid RTP ports. This is not an MGS issue
Event ID: 2002	Message:	MediaTransport:(OID=<oid>) Codec and/or frames per packet mismatch <details>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	There was a problem establishing a call.
Event ID: 2003	Message:	MediaTransport:(OID=<oid>) Transport mismatch <details>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).

MGS (Media gateway server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	There was a problem establishing a call.
Event ID: 2004	Message:	MsmProxy: <interface> returned error <error>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	There was a problem establishing a call.
Event ID: 2090	Message:	<entity>: <interface> returned error <error>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	There was a problem establishing a call.
Event ID: 3001	Message:	<entity>: Caught <exception>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Software bug.
Event ID: 3002	Message:	Mgs: Shutting down due to gateway creation failure
	User action:	Look to previous log entries for error details.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	A Gateway could not be created.
Event ID: 3003	Message:	Mgs: Shutting down due to gateway initialization failure
	User action:	Look to previous log entries for error details.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	A request to the Media Path Server (MPS) or Media Services Manager (MSM) failed. This is not an MGS issue.
Event ID: 3004	Message:	Mgs: Shutting down due to fatal error
	User action:	Look to previous log entries for error details.
	Alarm severity:	Critical
	Trap-type:	Error

MGS (Media gateway server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	A fatal error was reported by an MGS component.
Event ID: 3005	Message:	Mgs: Shutting down due to MSM communication failure
	User action:	Investigate and correct the cause, and restart the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The Media Services Manager (MSM) has shut down unexpectedly. This is not an MGS issue.
Event ID: 3006	Message:	Mgs: Shutting down due to MPS communication failure
	User action:	Investigate and correct the cause, and restart the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The Media Path Server (MPS) has shut down unexpectedly. This is not an MGS issue.
Event ID: 3007	Message:	Mgs: Shutting down due to resource limits query failure
	User action:	Look to previous log entries for error details.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	A request to the Media Services Manager (MSM) failed. This is not an MGS issue.
Event ID: 3008	Message:	Mgs: Shutting down due to configuration query failure
	User action:	Look to previous log entries for error details.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	A request to the Media Services Manager (MSM) failed. This is not an MGS issue.
Event ID: 3090	Message:	<entity>: Caught <exception>
	User action:	Submit a CR and attach ZIP'ed log files (archlog).
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Software bug.
Event ID: 3091	Message:	ScmProxy: NnuServiceStartService returned error <error>
	User action:	Investigate and correct the cause, and restart the system.
	Alarm severity:	Critical
	Trap-type:	Error

MGS (Media gateway server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	NNU failed to start the MGS as a service. This is not an MGS issue.
Event ID: 3092	Message:	ScmProxy: NnuCallback returned error <error>
	User action:	Investigate and correct the cause, and restart the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	NNU failed to start the MGS as a service.This is not an MGS issue.

Modem

Modem provides the modem driver resource.

Modem	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 52	Message:	The specified resource type can not be found in the image file.
	User action:	Contact customer support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	This item only shows up as an alarm.

MPS

MPS is the media path server which controls media between IP sets/trunks.

MPS (Media path server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 1001	Message:	MPS service started
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	MPS service is successfully started.
Event ID: 1002	Message:	MPS service stopped
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	MPS service is stopped.
Event ID: 2001	Message:	**WARNING** Unable to register as a Service
	User action:	Restart system; contact customer support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	NNU could not start MPS as a service; this is not an MPS issue.

MPS (Media path server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 2002	Message:	*WARNING** Unable to stop service
	User action:	Contact customer support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	NNU could not stop MPS as a service; this is not an MPS issue.
Event ID: 2003	Message:	**WARNING** FUMP message could not be sent
	User action:	Contact customer support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Could not send fump message through EMS FUMP channel; this is not an MPS issue.
Event ID: 2004	Message:	**WARNING** Codec incompatible; call dropped
	User action:	Change or make available the correct Codec to match the Codec supported by the software at the far end of the call.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Call dropped due to incompatible codecs; this is not an MPS issue.
Event ID: 2005	Message:	**WARNING** Endpoint%d:%d registration failed
	User action:	Contact customer support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Failed to register an endpoint due to unknown endpoint type or duplication; this may not be an MPS issue.
Event ID: 3001	Message:	**ERROR** Unable to allocate memory; MPS service aborted
	User action:	May need to reboot the system
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	System is low on memory and cannot allocate resources in the driver; this is not an MPS issue.
Event ID: 3002	Message:	**ERROR** Unable to initialize MPSMI;MPS service aborted
	User action:	Restart system; contact customer support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Cannot initialize MPSMI; this is not an MPS issue.
Event ID: 3003	Message:	**ERROR** Unable to connect to MSM, rc=%d;MPS service aborted

MPS (Media path server)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Restart system; contact customer support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Cannot connect to Media Service Manager; this is not an MPS issue.
Event ID: 3004	Message:	**ERROR** Unable to open FUMP channel; MPS service aborted
	User action:	Restart system; contact customer support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Media service manager could not open a FUMP channel for MPS; this is not an MPS issue.
Event ID: 3005	Message:	**ERROR** FUMP channel not ready; MPS service aborted
	User action:	Restart system; contact customer support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Fump channel is not ready; this is not an MPS issue.
Event ID: 3006	Message:	**ERROR** Reset by Network Manager
	User action:	Submit a CR and attach archlogs
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Network manager thinks MPS is dead.
Event ID: 3007	Message:	**ERROR** Received EMS_EVENT_CONNECTION_LOST from MSM;MPS service aborted
	User action:	Restart system; contact customer support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Lost connection to Media Service Manager; this is not an MPS issue.
Event ID: 3008	Message:	**ERROR** Unable to create event; MPS service failed to start
	User action:	May need to reboot the system
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	System is low on resources and cannot allocate event handle in the driver; this is not an MPS issue.

MSPAlarmService

MSPAlarmService translates events into SNMP traps.

MSPAlarmService	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: N/A	Message:	Failed to open client end of SNMP Trap Agent mailslot using CreateFile. Win32 GetLast Error() value = %value%.
	User action:	Contact customer support.
	Alarm severity:	Major
	Trap-type:	N/A
	Logs:	None
	Comments:	This item only shows up as an alarm.

mspQoS

MspQoS provides the Quality of Service driver which controls NAT/QoS/IPSec/Firewall.

mspQoS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 2000	Message:	The description for Event ID (2000) in Source (mspQoS) could not be found. It contains the insertion string(s):
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comment:	This item will only show up in DEBUG builds of mspqos. Perfmon has opened the mspqos performance collector, mspperf.dll.

mspQoSMP

MspQoSMP Quality of Service driver which controls NAT/QoS/IPSec/Firewall.

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4003	Message:	Memory allocation failed on%2.
	User action:	May need to reboot system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Comments:	System is low on memory and cannot allocated resources in the driver.
Event ID: 4014	Message:	%2: Maximum filter limit has been reached.
	User action:	Need to remove other QoS filters.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The maximum number of QoS filters has been reached.
Event ID: 4019	Message:	Too many ports specified for %2 - Max: 256.
	User action:	Reduce the number of QoS Ports specified.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 4022	Message:	Could not read port values for %2.
	User action:	Fix Port Range entries. They are invalid.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Entries in Port Range field are invalid.
Event ID: 4023	Message:	Could not create symbolic link %3 of %2.
	User action:	QoS driver has failed to load. Reboot system. If this error persists, contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Catastrophic driver failure.
Event ID: 4024	Message:	Could not create %2.
	User action:	QoS driver has failed to load. Reboot system. If this error persists, contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Catastrophic driver failure.
Event ID: 4026	Message:	%2 failed to register as an Intermediate Miniport.
	User action:	QoS driver has failed to load. Reboot system. If this error persists, contact Customer Support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Catastrophic driver failure.

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 4028	Message:	Unable to read "PortTable" registry entry for device %2. The default port range of 28000 - 28511 will be used.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Registry value has not been initialized. The default range will be used. Unless other ports are chosen, this message will continue to appear. This will not cause problems.
Event ID: 4030	Message:	Zero bandwidth, disabling QoS! Check the WAN drivers.
	User action:	Possibly caused by the WAN driver. Contact Customer Support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	The values used to calculate the Bandwidth resulted in a zero value.
Event ID: 4031	Message:	Error in reading IP addresses, disabling QoS! Check that the LAN and WAN are properly installed.
	User action:	Check that all LAN and WAN interfaces are valid. Contact Customer Support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 4032	Message:	Error in Wan Premium Percentage. Value must be between 0 and 100. Use default value for now. Reset the WAN Premium Percentage in OAM.
	User action:	Enter a valid Premium Percent value. Must be between 0 and 100.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 4034	Message:	NAT %3 values are invalid.
	User action:	Fix Port Range entries. They are invalid.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The Inside or Outside port values are invalid.
Event ID: 4035	Message:	Could not read registry value "%3". %2.
	User action:	Possible registry corruption. Check to see if \Machine\ System\ Current ControlSet\ mspQoSMP\ Parameters\ FWFilters\ Status is set to either Disabled or Enabled.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Could not set the Firewall status. Setting status to Disabled

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 4039	Message:	Terminating logging thread. Logging will not be enabled on any interface.
	User action:	Problem with Firewall Filters logging function. Contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Catastrophic failure of Firewall Filters logging.
Event ID: 4040	Message:	Can't read an NDIS OID value.
	User action:	Possible network interface card failure.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Cannot read the MAC address from one of the network interfaces.
Event ID: 4041	Message:	Can’t start logging for device mspQoSMP%d.
	User action:	System may be low on resources. Try rebooting the system to see if problem goes away. If not, contact Customer Support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Driver could not start the worker thread that logs packets.
Event ID: 4043	Message:	Possible infinite loop. %2.
	User action:	Possible link list corruption in driver. Reboot system and contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Detected possible linked list corruption. Attempts to repair list.
Event ID: 4044	Message:	Linked List has unexpected number of entries. %2.
	User action:	Reboot system.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Count of entries in linked list is out of sync with the actual number.
Event ID: 4045	Message:	%2: H225 setup message exceeds message fragment buffer. %3
	User action:	Need to reduce the number of codec choices. This will reduce the size of the setup message.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	H.225 setup message is larger than internal storage buffer. Call may not go through properly. i.e. one-way speech

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 4046	Message:	%2: Processing more than one fragmented H.225 setup message.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Informational
	Logs:	None
	Comments:	Detects when two setup messages are being processed at the exact same time.
Event ID: 4047	Message:	SIP parser error: %2
	User action:	Send NT event log and stlog to development / ITAS. Check if there are any non-SIP packets going through the BCM via the port 5060.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	This can happen when there is a SIP parser error or when a non-SIP packet passes the driver via the default 5060 SIP port.
Event ID: 4048	Message:	SIP Init Failure. %2: %3. Please check that mspqos.sys is properly loaded.
	User action:	If SIP is to be used as the VOIP protocol, reboot system to make sure mspqos.sys is loaded properly and that there are no memory allocation issues.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	SIP structures used in driver are not properly initialized.
Event ID: 4049	Message:	OSIP Failure. %2: %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Error in decoding or encoding SIP packet using the OSIP parser.
Event ID: 4050	Message:	SIP Call State Machine Failure. %2: %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Unexpected state machine transition for SIP processing.
Event ID: 4051	Message:	SIP Proxy Failure. %2: %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Unexpected SIP data structure manipulations.

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 4052	Message:	SIP Firewall Failure. %2: %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Firewall functionalities failed for SIP call.
Event ID: 4053	Message:	SIP Nat Failure. %2: %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Nat functionalities failed for SIP call.
Event ID: 4054	Message:	Non-SIP Packet through SIP default port 5060
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Send logs to support team. Check if there are any non-SIP packets going through the BCM via the port 5060.
Event ID: 4055	Message:	%2 link is %3.
	User action:	Send NT event log and stlog to development / ITAS.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	If WAN link is down, check the cable and make sure the configuration on both ends matches.
Event ID: 5001	Message:	%2 : Could not allocate the resources necessary for operation.
	User action:	System is low on memory. Reboot system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 5005	Message:	%2 : Has encountered an internal error and has failed.
	User action:	QoS driver has failed to load. Reboot system. If this error persists, contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Catastrophic driver failure.
Event ID: 5011	Message:	%2: A required parameter is missing from the Registry.
	User action:	Possible problem with LAN or WAN drivers.
	Alarm severity:	Critical
	Trap-type:	Error

mspQoSMP	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	Could not get Information from one of the network interface drivers.
Event ID: 9001	Message:	%2 could not allocate a resource of type %3 due to system resource problems.
	User action:	System is low on memory. Reboot system.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 9004	Message:	%2 failed to register itself with the NDIS wrapper.
	User action:	QoS driver has failed to load. Reboot system. If this error persists, contact Customer Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Catastrophic driver failure.

NCM

NCM provides the Network Configuration Manager component.

NCM (Network Configuration Manager)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 301	Message:	The description for Event ID (311) in Source (NCM) could not be found. It contains the insertion string(s): NCM config import started. Command option - /k.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 302	Message:	The description for Event ID (311) in Source (NCM) could not be found. It contains the insertion string(s): NCM config command completed.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 311	Message:	The description for Event ID (311) in Source (NCM) could not be found. It contains the insertion string(s): NCM file import started. Command option - /l.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 312	Message:	The description for Event ID (311) in Source (NCM) could not be found. It contains the insertion string(s): NCM file command completed.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

NetBT

NetBT provides NetBios over TCP. NetBIOS is the native networking protocol in Windows-based

networks.

NetBT	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4319	Message:	A duplicate name has been detected on the TCP network. The IP address of the machine that sent the message is in the data. Use nbtstat -n in a command window to see which name is in the Conflict state.
	User action:	The most likely reason for this is that a duplicate name has been detected on the network. Use the NBTSTAT -N command to see the name of the computer in the conflict state. The IP address of the node that sent the message is in the data returned by this command, offset by 28 bytes.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

NetIQccm

NetIQccm provides the NetIQ connection manager.

NetIQccm	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	NetIQ AppManager client communication manager
Event ID: 0	Message:	From NetIQ AppManager: SERVICE_STOPPED.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 257	Message:	From NetIQmc: [764] NetIQmc warm started.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 261	Message:	From NetIQmc: [187] NetIQccm warm started.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 264	Message:	NetIQ ADMIN message: [195] Ping MS <XYZ.XYZ.XYZ.XYZ> fail with error 1.
	User action:	No action required
	Alarm severity:	Warning

NetIQccm	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Information
	Logs:	None
Event ID: 264	Message:	NetIQ ADMIN message: [195] ccm is having intermittent communication/map file full failures while communicating with MS <XYZ.XYZ.XYZ.XYZ>. 1 of XYZ attempts failed withing the last XYZ minutes. Last attempt succeeded.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

NetIQmc

NetIQmc provides the NetIQ connection manager.

NetIQmc	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	NetIQ AppManager client communication manager
Event ID: 0	Message:	From NetIQ AppManager: SERVICE_STOPPED.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

NetIQObjMgr

NetIQObjMgr provides the NetIQ object Manager.

NetIQObjMgr	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	NetIQ AppManager client communication manager
Event ID: 15000	Message:	The value for Authorized Management Server(s) was changed to XYZ.
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 15001	Message:	The Bind Management Server Port was changed to XYZ.
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 15002	Message:	The NetIQ Agent Listing Port number was changed to XYZ.
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

NetLinkManager

NetLinkManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Net link manager
Event ID: 0	Message:	The description for Event ID (0) in Source (NetLinkManager) could not be found. It contains the insertion string(s): Service started.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 0	Message:	The description for Event ID (0) in Source (NetLinkManager) could not be found. It contains the insertion string(s): Service stopped.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

NetLogon

NetLogon	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Net logon
Event ID: 3095	Message:	This Windows NT computer is configured as a member of a workgroup, not as a member of a domain. The Netlogon service does not need to run in this configuration.
	User action:	The Netlogon service should not be configured to start automatically on a server that is not a domain member. Configure the Netlogon service so that its startup type is set to "Manual."
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

NGRPCI

NGRPCI provides the network card (PCI) driver.

NGRPCI (Netgear PCI driver)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4	Message:	Adapter NGRPCi#: Adapter Link Down.

NGRPCI (Netgear PCI driver)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Please make sure the LAN cards inside BCM is connected properly.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	This is not valid before BCM 3.0 release.
Event ID: 5	Message:	Adapter NGRPCi#: Adapter Link Up.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	This is not valid before BCM 3.0 release.
Event ID: 5000	Message:	NGRPCI Adapter instance NGRPCI# Cable Connected Successfully.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	This event is only valid before BCM 3.0 release.
Event ID: 5001	Message:	NGRPCI Adapter instance NGRPCI# LAN Cable Disconnected
	User action:	Please make sure the LAN cards inside BCM is connected properly.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	This event is only valid before BCM 3.0 release.
Event ID: 5003	Message:	Could not find an adapter
	User action:	Please check the profiles first. If the BCM has only one LAN adapter installed, ignore this message. Otherwise, change the LAN adapter.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 5009	Message:	Does not support the configuration supplied.
	User action:	Please check the PCI Slot and make sure that the Netgear FA310 10/100 Fast Ethernet adapter is plugged into the slot properly. Otherwise swap the Ethernet Adapter.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Nnu

NNU (Nortel Networks Utilities)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice NNU diagnostics
Event ID: 1000	Message:	An NNU Logging application has registered and will process logging messages.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

NSACD

NSACD (Norstar Automated Call Distribution)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	NSACD
Event ID: 0	Message:	ITGNS error: %d, Exit code: %d
	User action:	Send NT event log and stlog to development / ITAS. Manually restart service or reboot BCM
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Logged if service failed to start.

NwRdr

NwRdr	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 8007	Message:	The Microsoft Client Service for NetWare redirector has timed out one or more requests to <Server name>.
	User action:	Contact Support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

OSPFMib

OSPFMib provides the (open shortest path OSPF MIB) component. OSPF is a routing protocol that determines the best path for routing IP traffic over a TCP/IP network. The route is based on distance between nodes and several quality parameters.

OSPFMib	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 2	Message:	Service initializing.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

Perfctrs

Perfctrs provides the performance counters component on the BCM.

Perfctrs	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 3101	Message:	Unable to read IO control information from NBT device.
	User action:	In most cases, no action is required. However, please check if the network connections of the BCM are working.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	See Microsoft Article Q275586. NBT=NetBIOS over TCP/IP. THis can happen when trying to monitor statistics from and inactive network adapter. It can generally be ignored.

Perflib

Perflib provides a performance counters library on the BCM.

Perflib	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None

Perflib	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1008	Message:	The Open Procedure for service "RasRad" in DLL "rasrad.dll" failed. Performance data for this service will not be available. Status code returned is DWORD 0.
	User action:	This event should not be seen in BCM 3.0. In case of its occurrence in a BCM 3.0 machine, please contact Nortel Networks support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 2002	Message:	The open procedure for service (service name) in DLL (DLL name) has taken longer than the established wait time to complete. The wait time in milliseconds is shown in the date.
	User action:	No action required. However, please report the message indicating the service name and the DLL name to support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

Policy Services

Policy Services	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Policy service
Event ID: 5	Message:	Policy Service started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 6	Message:	Policy Service stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

qos_flt_init

qos_flt_init (Quality of Service driver initialization)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Qos_flt_init
Event ID: 0	Message:	The description for Event ID (0) in Source (qos_flt_init) could not be found. It contains the insertion string(s): Service started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 0	Message:	The description for Event ID (0) in Source (qos_flt_init) could not be found. It contains the insertion string(s): Service stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

Rdr

Rdr (Redirector) provides the Microsoft API component on the BCM.

Rdr	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 3013	Message:	The redirector has timed out a request to <Server Name or IP>.
	User action:	Check the server and the connection to the server.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 8003	Message:	The master browser has received a server announcement from the computer <computer name> that believes that it is the master browser for the domain on transport <transport name>. The master browser is stopping or an election is being forced.
	User action:	To stop the 8003 error messages, make sure the routers on the network are not forwarding UDP broadcasts, keeping browser elections on NetBT local to each subnet and enable WINS or lmhosts on the network for netbios name resolution.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Router

Router	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Routing and remote access service
Event ID: 20013	Message:	The communication device attached to port COM2 is not functioning.
	User action:	Contact Nortel Network's support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 20015	Message:	The authentication is successful.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 20031	Message:	Remote Access Connection Manager failed to start because it could not locate port information from media DLLs. Restart the computer, if the problem persists.
	User action:	Contact Nortel Network's support team.
	Alarm severity:	Critical
	Trap-type:	Error

Router	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	Backup configuration data using BRU, re-ghost the hard disk with the image of the same release, and then restore the backup data.
Event ID: 20048	Message:	A successful dialin session is ending.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 20049	Message:	A user with invalid username/password combination or a user without dialin permission tries to dial in to the system.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 20064	Message:	The authentication for a dial-in user is successful and the BCM dials back to the user on a specific number.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 20089	Message:	The remote client is busy or the callback number is wrong when a user with callback enabled tries to dial in to the system.
	User action:	Check whether the callback number is right.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 20101	Message:	Using the default value for Registry parameter Enabled because the value given is not in the legal range for the parameter.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 20103	Message:	Unable to load C:\winnt\system32\ipxrtmgr.dll.
	User action:	Contact support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 20105	Message:	Unable to load the interface ModemBackup from the registry. The following error occurred: There are no routing enabled ports available for use by this demand dial interface

Router	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Contact Nortel Network's support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Backup configuration data using BRU, re-ghost the hard disk with the image of the same release, and then restore the backup data.
Event ID: 20105	Message:	Unable to load the interface TivDialup from the registry. The following error occurred: There are no routing enabled ports available for use by this demand dial interface.
	User action:	Contact Nortel Network's support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Backup configuration data using BRU, re-ghost the hard disk with the image of the same release, and then restore the backup data.
Event ID: 20111	Message:	The demand dial connection fails to complete because of no answer, or invalid user, or busy line.
	User action:	N/A
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 20139	Message:	The port COM2 has been disconnected due to inactivity
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 20139	Message:	The dial-up link drops.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

SAM

SAM (secure access module) provides managed user/file security.

SAM (Secure access module)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 12288	Message:	SAM failed to write changes to the database. This is most likely due to a memory or disk-space shortage. The SAM database will be restored to an earlier state. Recent changes will be lost. Check the disk-space available and maximum pagefile size setting.
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Save Dump

Save dump is a debug utility that saves memory dump files on the BCM.

Save Dump	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 1001	Message:	The computer has rebooted from a bugcheck. The bugcheck was: 0x0000000a (0x000002d8, 0x00000002, 0x00000001, 0xf3e9f7c1). Microsoft Windows NT [v15.1381]. A dump was saved in: E:MEMORY.DMP.
	User action:	Contact Nortel Network's support team. Please forward the message for to the support team. Please do not remove the dump file.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

Security

Security	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	EventLog
Event ID: 512	Message:	Windows NT is starting up.
	User action:	No action required.

Security	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 515	Message:	A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests. Logon Process Name: \inetinfo.exe
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 528	Message:	Successful Logon: User Name: <user name> Domain: <domain> Logon ID: <id> Logon Type: <type> Logon Process: User32 Authentication Package: <package version> Workstation Name: <name>
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 529	Message:	Logon Failure: Reason: Unknown user name or bad password User Name: <user name> Domain: <domain> Logon Type: <type> Logon Process: User32 Authentication Package: <package version> Workstation Name: <name>
	User action:	No action required. However, this event may indicate an un-authorized access attempt.
	Alarm severity:	Major
	Trap-type:	Failure / Audit
	Logs:	None
Event ID: 538	Message:	User Logoff: User Name: <name> Domain: <domain> Logon ID: <id> Logon Type: 3
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 577	Message:	Privileged Service Called: Server: NT Local Security Authority / Authentication Service Service: LsaRegisterLogonProcess() Primary User Name: SYSTEM Primary Domain: NT AUTHORITY Primary Logon ID: (0x0,0x3E7) Client User Name: <User> Client Domain: <Domain> Client Logon ID: (0x0,0x1234) Privileges: SeTcbPrivilege
	User action:	No action required. This event does not indicate a security breach; you can safely ignore it.
	Alarm severity:	Major
	Trap-type:	Failure / Audit
	Logs:	None

Security	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 577	Message:	Privileged Service Called: Server: NT Local Security Authority / Authentication Service Service: LsaRegisterLogonProcess() Primary User Name: SYSTEM Primary Domain: NT AUTHORITY Primary Logon ID: <id> Client User Name: ee_admin Client Domain: <domain> Client Logon ID: <id> Privileges: SeTcbPrivilege
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 624	Message:	User Account Created: Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. Note that a user account is created.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 626	Message:	User Account Enabled: Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id>
	User action:	No action required. Note that a user account is enabled.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 628	Message:	User Account password set: Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id>
	User action:	No action required. (a password set)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 630	Message:	User Account Deleted: Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. (a user account is deleted.)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 632	Message:	Global Group Member Added: Member: <member id> Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. (a global group member added.).
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None

Security	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 633	Message:	Global Group Member Removed: Member: <member id> Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. (a global group member removed.)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 636	Message:	Local Group Member Added: Member: <member id> Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -.
	User action:	No action required. (a local group member added.)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 637	Message:	Local Group Member Removed: Member: <member id> Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. (a local group member removed.)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 642	Message:	User Account Changed: Target Account Name: <name> Target Domain: <domain> Target Account ID: <id> Caller User Name: <name> Caller Domain: <domain> Caller Logon ID: <id> Privileges: -
	User action:	No action required. (a user account is changed.)
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None
Event ID: 644	Message:	User Account Locked Out: Target Account Name: <account name> Target Account ID: <SID number> Caller Machine Name: localhost/ 127.0.0.1 (Jintegra) Caller User Name: SYSTEM Caller Domain: NT AUTHORITY Caller Logon ID: (xxxxxxx)
	User action:	The user account will automatically be unlocked after 30 minutes (default settings). The administrator can unlock the account through the User Manager interface in Unified Manager. If this activity persists, this may be an indication that someone is attempting an unauthorized access to the BCM. The organization's security prime should be notified.
	Alarm severity:	Warning
	Trap-type:	Success / Audit
	Logs:	None

Serial

Serial provides the serial port driver on the BCM.

Serial	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 8	Message:	Not enough resources were available for the driver.
	User action:	This is not a problem. This message can be ignored.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

Service Control Manager

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	See event descriptions
Event ID: 7000	Message:	The Voice MSC Service service failed to start.
	User action:	If voice services (i.e. voice mail, IP calls etc.) are available then there is no action required. Otherwise a restart of the BCM is required. This is not only for BCM 3.0.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice MSC service
	Comments:	The service did not respond to the start or control request in a timely fashion.
Event ID: 7000	Message:	The WANic 500 Driver service failed to start
	User action:	Contact your technical support representative.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice WAN
	Comments:	A device attached to the system is not functioning.
Event ID: 7000	Message:	The Isecdrv service failed to start
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	None
	Comments:	BCM FP1 Upgrades will fail to install, no longersupported, replace BCM hard drive.

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 7000	Message:	The Voice Net QoS Monitor service failed to start due to the following error: %%1053
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice Net QoS monitor
	Comments:	BCM FP1 Upgrades will fail to install, no longersupported, replace BCM hard drive.
Event ID: 7001	Message:	The Call Detail Recording service depends on the Media Services Manager service which failed to start
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Call Detail Recording, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The DECT Alarm Monitor service depends on the DECT OAM service which failed to start
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	DECT Alarm monitor, DECT OAM, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The DECT OAM service depends on the Media Services Manager service which failed to start
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	DECT OAM, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Media Services Manager service depends on the Voice MSC Service service which failed to start.
	User action:	Start Voice MSC Service. If the problems persist, contact your technical support representative.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice MSC service, Media services manager
	Comments:	The service did not respond to the start or control request in a timely fashion.

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 7001	Message:	The Message Trace Tool service depends on the Media Services Manager service which failed to start.
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Message trace tool, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Task Scheduler service depends on the Net Logon service which failed to start.
	User action:	Start Net Logon service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Net logon, Task scheduler
	Comments:	The service has returned a service-specific error code.
Event ID: 7001	Message:	The UNISTIM Terminal Proxy Server service depends on the Media Gateway Server service which failed to start.
	User action:	Start the Media Gateway Server.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	UNISTIM Terminal proxy server, Media gateway server
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Voice CFS service depends on the Media Services Manager service which failed to start.
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice CFS, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Voice CTE service depends on the Media Services Manager service which failed to start.
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice CTE, Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Voice Mail service depends on the VoiceCTI service which failed to start.
	User action:	Start VoiceCTI service.

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	VoiceCTI, Voice mail
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Voice Software Alarm Monitor service depends on the Media Services Manager service.
	User action:	Start the Media Services Manager service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice software alarm monitor , Media services manager
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The VoIP Gateway service depends on the Media Path Server service which failed to start.
	User action:	Start the Media Path Server service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	VoIP Gateway, Media path server
	Comments:	The dependency service or group failed to start.
Event ID: 7001	Message:	The Remote Access Connection manager service depends on the workstation service which failed to start because of the following error: A duplicate name exists on the network.
	User action:	The BCM name should be unique in the network.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Remote access connection manager
	Comments:	The dependency service or group failed to start.
Event ID: 7009	Message:	Timeout (120000 milliseconds) waiting for service to connect.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	See event descriptions
Event ID: 7022	Message:	The Voice MSC Service service hung on starting
	User action:	Contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice MSC service

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 7023	Message:	The Call Detail Recording service terminated.
	User action:	Contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Call Detail Recording
Event ID: 7023	Message:	The Voice Management Subsystem service terminated.
	User action:	Supply archlog and report to support team.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice management subsystem
	Comments:	Incorrect function.
Event ID: 7023	Message:	The workstation service terminated with the following error: A duplicate name exists on the network.
	User action:	THe BCM should be unique in the network.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Workstation
Event ID: 7024	Message:	The Net Logon service terminated with service-specific error 3095.
	User action:	The Netlogon service should not be configured to start automatically on BCM that is not a domain member. Configure the Netlogon service so that its startup type is set to "Manual."
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Net logon
Event ID: 7024	Message:	The VoiceCTI service terminated with service-specific error 204.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	VoiceCTI
Event ID: 7024	Message:	The Remote Access Connection Manager service terminated with service-specific error 620.
	User action:	Please contact support. (Note for support: Start the Plug and Play service, and change the Startup mode from Manual or Disabled to Enabled.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Service Control Manager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Service:	Plug and play, Remote access connection manager
	Comments:	See Microsoft Article Q170029.)
Event ID: 7024	Message:	The Voice MSC Service service terminated with service-specific error 85.
	User action:	If voice services (i.e. voice mail, IP calls etc.) are available then there is no action required. Otherwise a restart of the BCM is required. This is not only for BCM 3.0.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	Voice MSC service
Event ID: 7026	Message:	The following boot-start or system-start driver(s) failed to load: intlfxsr kbdclass mouclass nullinp nullvga
	User action:	Contact Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Service:	None
	Comments:	BCM FP1 Upgrades will fail to install, no longersupported, replace BCM hard drive.

SNMP

SNMP (Simple network messaging protocol)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	SNMP
Event ID: 1001	Message:	The SNMP Service has started successfully.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

SNMP Trap Agent

SNMP Trap agent	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	SNMP Trap service
Event ID: 101	Message:	The Small Site Trap Agent DLL has been loaded.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 102	Message:	The Small Site Trap Agent DLL has been unloaded.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

Srv

Relates to the server service on BCM. The Server service acts as the key to all server-side NetBIOS applications and provides support for print, file, and named pipe sharing through the SMB services. The service is a subsystem for NT sharing (directories and printers).

Srv	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None

Srv	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 2000	Message:	The server's call to a system service failed unexpectedly.
	User action:	Contact support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 2019	Message:	The server was unable to allocate from the system nonpaged pool because the pool was empty.
	User action:	Contact support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 2021	Message:	The server was unable to allocate a work item 2 times in the last 60 seconds.
	User action:	Contact support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

SSH Secure Shell Server

SSH Secure shell server	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 0	Message:	Warning: DNS lookup failed for "xxx.xxx.xxx.xxx".
	User action:	No action required. DNS lookup is not required in order to log in through SSH.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

Survivable Remote Gateway

Survivable remote gateway	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 1200	Message:	SRG Starting
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1204	Message:	DN:XXXX, Test Local Mode
	User action:	Test feature
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1205	Message:	DN:XXXX, Firmware is Out of Sync with the Main Office Call Server
	User action:	Indicates that IP set FW on main office has been upgraded and the required FW version is available on the SRG
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1206	Message:	DN:XXXX, Local Mode - Firmware Upgrade in Progress
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

Survivable remote gateway	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1207	Message:	DN:XXXX, Normal Mode – Redirected to Main Office
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1208	Message:	DN:XXXX, Local Mode - Redirection Pending (Set on call)
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1209	Message:	DN:XXXX, Local Mode - Firmware Upgrade Pending (Set on call)
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2200	Message:	DN:XXXX, Invalid ID (1) – ID has no endpoint in Gatekeeper database
	User action:	Indicates configuration problem
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2201	Message:	DN:XXXX, Invalid ID (2) – ID unknown within the Call Server
	User action:	Indicates configuration problem
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2202	Message:	DN:XXXX, Invalid ID (3) - Endpoint in Gatekeeper database is Originating Call Server
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2203	Message:	Permission Denied (1) – No configured Installer Password
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2204	Message:	Permission Denied (2) - Branch User already registered with the TN associated with the UserID

Survivable remote gateway	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2205	Message:	Permission Denied (4) – i2002 set used to register with i2004 or i2050 TN
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2206	Message:	Permission Denied (6) – Retry Allowed
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2207	Message:	Locked from Login (1) – Password failed 3 times
	User action:	Indicates configuration problem.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2208	Message:	DN:XXXX, Local Mode - Main Office Parameters not Provisioned
	User action:	Indicates configuration problem.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 3201	Message:	DN:XXXX, Local Mode - Net Connect Server Unreachable
	User action:	Indicates connectivity problem.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3202	Message:	DN:XXXX, Local Mode - Main Office TPS Unreachable
	User action:	Indicates connectivity problem.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3303	Message:	DN:XXXX, Local Mode - Firmware isnot available on the SRG
	User action:	Indicates that IP set FW on main office has been upgraded and the required FW version is not available on SRG.
	Alarm severity:	Critical

Survivable remote gateway	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None

System Status Monitor

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	System status monitor
Event ID: 1000	Message:	%1 reports activity.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	A process has reported to the SSM that either it, or its monitored services are indicating activity.
Event ID: 1001	Message:	%1 reports all of its services are functioning correctly.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	A process has reported to the System Status Monitor that either it, or its monitored services are functioning properly.
Event ID: 1002	Message:	The System Service Monitor has been stopped
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	A process has reported to the System Status Monitor that either it, or its monitored services are stopped normally.
Event ID: 1003	Message:	The System Status Monitor has been started
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	A process has reported to the System Status Monitor that either it, or its monitored services are started normally.
Event ID: 1004	Message:	1. %PCI Device Driver% Driver Recovered. 2. %Device Name% Device Recovered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	PCI Devices and Drivers Information

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1005	Message:	1. %Power Value% Power Recovered. 2. Power Supply Fan1 Recovered. 3. Power Supply Fan2 Recovered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Power Supply Information.
Event ID: 1006	Message:	1. CPU Fan Recovered. 2. Fan1 Recovered in Tolerance %#%. 3. Fan2 Recovered in Tolerance %#%.
	User action:	No Action Required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	CPU Fan, Fan1 and Fan2 Recovery Information
Event ID: 1007	Message:	CPU Temperature Recovered.
	User action:	No Action Required. CPU Temperature recovered to less than 100 degrees °C.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	CPU Temperature Recovery Information
Event ID: 1008	Message:	HDD %#% Recovered.
	User action:	No Action Required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Hard Drives Capacity Information
Event ID: 1009	Message:	1. Physical Memory Recovered. 2. Virtual Memory Recovered.
	User action:	No Action Required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Physical and Logical Memories Recovery Information
Event ID: 1010	Message:	%1, Physical RAM Recovered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Physical RAM size Recovery Information
Event ID: 1011	Message:	CPU load Recovered.

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	CPU Load Recovery Information
Event ID: 1012	Message:	1. RAID HW Found. 2. RAID HW Recovered. 3. Primary Single HDD Mode. 4. Mirrored Single HDD Mode. 5.Mirror Drives Mode. 6.Rebuilding Mirror Master HDD. 7. Rebuilding Primary Master HDD. 8. Mirror Master HDD Rebuild Complete. 9. Primary Master Rebuild Complete. 10. Replace Mirror Master HDD. 11. Replace Primary Master HDD. 12. Replace Parimay & Mirror Master HDDs.
	User action:	For 1 to 9, No Action Required. For 10, 11 and 12 replace HDD in next maintenance window.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	RAID Hardware Recovery Information
Event ID: 1013	Message:	1. Bytes Total/sec Recovered. 2. getting Network Information Recovered. 3. Bytes Sent/sec Recovered. 4. Bytes Received/sec Recovered. 5. Packets Received Error/sec Recovered. 6. Packets Received Discarded/sec Recovered. 7. Packets Outbound_Error/sec Recovered. 8. Packets found Discarded/sec Recovered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	LAN1, LAN2 and WAN Information.
Event ID: 1014	Message:	Non-PAged Memory Recovered.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Non-Page Memory Recovery Information
Event ID: 1015	Message:	Telephony Services %1
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Telephony Services Status Information. When this indicate “Up” Unified Manager can be accessed.
Event ID: 1016	Message:	Temperature Recovered.
	User action:	No Action Required. Temperature recovered to less than 40 degrees °C.
	Alarm severity:	Warning

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Information
	Logs:	None
	Comments:	Temperature Recovery Information
Event ID: 2000	Message:	1. %CPUFan Value% Below normal Tolerance. 2. %Fan1 Value% failed in Tolerance %#%. 3. %Fan2 Value% failed in Tolerance %#%.
	User action:	1. Check CPU Fan 2. Check Fan 1 3. Check Fan 2
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	CPU FAN, FAN1 And FAN2 Warnings
Event ID: 2001	Message:	HDD %#% near or on its capacity.
	User action:	Check HDD %#% Capacity
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Hard Drives Capacity Warnings.
Event ID: 2002	Message:	Unable to get %#% Drive from system environment.
	User action:	No Action Required. SSM failed to retrieve the information of HDD %#% from system. This HDD drive will not be monitored by SSM.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	SSM failed to retrieve the information of HDD %#% from system. This HDD drive will not be monitored by SSM.
Event ID: 2003	Message:	1. Physical Memory near or on its capacity. 2. Virtual Memory near or on its capacity.
	User action:	No Action Required. Its recommended that an assessment be made of memory utilization of your BCM.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Physical and Logical Memories Warning
Event ID: 2004	Message:	%1, Physical RAM size less than expected.
	User action:	Increase Physical RAM size in next maintenance window to increase the BCM performance.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Increase Physical RAM size.

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 2005	Message:	1. %#% Bytes Total/sec greater than 25% of LAN/WAN %#% speed 2. Failed to get Network Information. 3. %#% Bytes Sent/sec greater than 50% of LAN/WAN %#% speed. 4. %#% Bytes Received/sec greater than 50% of LAN/WAN %# %speed. 5. Packets Received Error/sec of LAN/WAN%#%. 6. Packets Received Discarded/sec of LAN/WAN%#%. 7. Packets Outbound_Error/sec of LAN/WAN%#%. 8. Packets found Discarded/sec of LAN/WAN%#%.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	LAN1, LAN2 and WAN Warnings
Event ID: 2006	Message:	CPU load above 98%.
	User action:	Check System Services to identify which service are consuming the CPU cycles.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	CPU load above 98% for more than 2 minutes.
Event ID: 2007	Message:	Non-Paged Memory near or on its capacity.
	User action:	No Action Required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Non-Page Memory Warning
Event ID: 2008	Message:	CPU Temperature Above Tolerance 100 °C for more than one Minute
	User action:	SSM will shutdown the BCM if the CPU temperature doesn't recovered within two Minutes
	Alarm severity:	Critical
	Trap-type:	Warning
	Logs:	None
	Comments:	CPU Temperature above Tolerance 100 ° C for more than one Minute, SSM will shutdown the BCM if the CPU temperature doesn't recovered within two Minutes
Event ID: 3000	Message:	%1 reports some of its services are not functioning correctly
	User action:	Check the service that is reporting that some services are down.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	A process has reported to the SSM that either it, or its monitored services are not fully functional.
Event ID: 3001	Message:	%1 reports that all of its services are down
	User action:	Check the service that is reporting services are down.
	Alarm severity:	Critical

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None
	Comments:	A process has reported to the SSM that either it, or its monitored services are all not functioning.
Event ID: 3002	Message:	The time interval could not be set on the L.E.D.'S. Board
	User action:	No immediate Action Required but If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Upon SSM initialization the time could not be set on the L.E.D.'S. board. A default value will be used.
Event ID: 3003	Message:	The number of time-outs could not be set on the L.E.D.'S. Board
	User action:	No immediate Action Required but If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Upon SSM initialization the time could not be set on the L.E.D.'S. board. A default value will be used.
Event ID: 3004	Message:	BCM Reset could not be set on the L.E.D.'S. Board
	User action:	No immediate Action Required but If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Upon SSM initialization the time could not be set on the L.E.D.'S. board. A default value will be used.
Event ID: 3005	Message:	The SSM thread that responds to sanity checks from the L.E.D.'S. board could not be created.
	User action:	No immediate Action Required but If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Windows was not able to create a thread required for the SSM to perform sanity checking while initializing the SSM. Sanity checking will be disabled.
Event ID: 3006	Message:	Sanity Information could not be retrieved from the registry. Using defaults
	User action:	There is a problem with the Windows registry. The SSM service should be re-started. If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	Upon SSM initialization the sanity Information could not be retrieved from the registry. Default values will be used.
Event ID: 3007	Message:	The SSM received a bad service request.
	User action:	The SSM service should be re-started. If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The SSM received a bad service request from Service Control Manager (SCM).
Event ID: 3008	Message:	The Service Request handler is not installed, the SSM will not be started
	User action:	The SSM service should be re-started. If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Upon SSM initialization the Service Request handler was not correctly loaded.
Event ID: 3009	Message:	A problem occurred initializing the SSM. Sanity checking is being turned off.
	User action:	The SSM service should be re-started. If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Windows was not able to create "Events" required to perform sanity checking. Sanity checking will be disabled, the board is being switched to quiet mode.
Event ID: 3010	Message:	Unable to access COM2. The SSM cannot be started
	User action:	End the process that is using COM2 and restart SSM Service. If the condition persists contact Nortel Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The SSM could not access COM2. The SSM will not be started.
Event ID: 3011	Message:	1. PCI Card Does not Exist. 2. %PCI Device Driver% Driver Failed. 3. %PCI Device Name% Device Failed.
	User action:	1. Check for existence of the PCI device or replace it. 2. Check for PCI device driver. 3. Check for existence of the PCI device, and make sure its installed properly.
	Alarm severity:	Critical
	Trap-type:	Error

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	1. SSM Failed to detect the device. 2. PCI Device Driver failed or not working properly. 3. The PCI Device failed while it's functioning
Event ID: 3012	Message:	1. %Power Value% Power Failed. 2. %Power Supply Fan1 Value% Failed. 3. %Power Supply Fan2 Value% Failed.
	User action:	1. Check the Power Supply (Module1, Module2 on redundant System) 2.Check Power Supply Fan1 3.Check Power Supply Fan2
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	1. SSM detects there is a failure in one of the power supply modules. 2. SSM detects there is a failure in power supply Fan1 3. SSM detects there is a failure in power supply Fan2
Event ID: 3013	Message:	1. CPU Fan Stopped. 2. %Fan1 Value% Below Tolerance %#% 3. %Fan2 Value% Below Tolerance %#%
	User action:	1. Check CPU Fan 2. Check Fan 1 3. Check Fan 2
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	1. CPU Fan stopped or failed. 2. Fan 1 speed below tolerance level %#% 3. Fan 2 speed below tolerance level %#%
Event ID: 3014	Message:	1. DupliDisk Mirroring Kit not found. 2. DupliDisk Mirroring failed. 3. Mirror Software shut down. 4. Mirror Master HDD failed reading/ Writing 5. Primary Master HDD Failed. Reading/Writing. 6. Replacement HDD Smaller than Active Drive. 7. Mirror HDD Smaller than Active Drive. 8. Check Mirror Master HDD. 9. Check Primary Master HDD.
	User action:	1. Check DupliDisk Mirroring KIT. 2. Check DupliDisk Mirroring KIT. 3. Check SSM status. 4. Check Mirror Master HDD power/Data cable. 5. Check Mirror Master HDD power/Data cable. 6, 7. Replacement HDD size should be equal or Larger that the Active HDD. 8. Check Mirror Master HDD. 9. Check Primary Master HDD.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	1. SSM failed to detect the RAID CARD (Disk Mirroring). 2. SSM detects there is a failure in Disk Mirroring HW or DLL. 3. SSM Detects the Mirror software shuts it self down. 4. SSM detects there is a failure in Primary Master HDD 5. SSM detects there is a failure in Mirror Master HDD. 6, 7. Replacement HDD size should be equal or Larger that the Active HDD. 8. Mirror Master HDD not working properly. 9. Primary Master HDD not working properly.
Event ID: 3015	Message:	CPU Temperature Above Tolerance 100 °C for more than two Minutes, SSM shutting down the power supply
	User action:	BCM 1000 will reboot automatically, BCM200/400 need restart.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

System Status Monitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Comments:	CPU Temperature Above Tolerance 100 °C for more than two Minutes, SSM shutting down the power supply
Event ID: 3016	Message:	Non-paged memory on its capacity, SSM rebooting the BCM
	User action:	BCM 1000 will reboot automatically, BCM200/400 need restart.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Non-paged memory on its capacity, SSM rebooting the BCM
Event ID: 3017	Message:	Temperature Above Tolerance 40 °C
	User action:	Check BCM's environment temperature
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	BCM's environment temperature is too high.

Tcpip

Tcpip	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4198	Message:	The system detected an address conflict for IP address <IP Address> with the system having network hardware address <Hardware Address>. Network operations on this system may be disrupted as a result.
	User action:	Disconnect the network connection for the interface with <IP Address>, resolve the address conflict, reconnect the network connection, and reboot the machine if needed.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 4199	Message:	The system detected an address conflict for IP address <IP Address> with the system having network hardware address <Hardware Address>. Network operations on this system may be disrupted as a result.
	User action:	Disconnect the network connection for the interface with <IP Address>, resolve the address conflict, reconnect the network connection, and reboot the machine if needed.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

TlntSvr

TlntSvr (Telnet service)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Tlntsvr
Event ID: 1000	Message:	The MS Telnet Service has started successfully.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

ToneSrvr

ToneSrvr provides the music on hold server application for BCM.

ToneSvr	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	IpMusic (Tone Server)
Event ID: 257	Message:	ToneSrvr Starting.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 258	Message:	ToneSrvr Terminated.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 771	Message:	IP Music - initialization failure. Service shutting down.
	User action:	Please disable the ToneSrvr by configuring your IP Music source as: Audio Jack. Contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 772	Message:	IP Music Error: IP Gateway - unable to open the FUMP channel. Service shutting down.
	User action:	Please disable the ToneSrvr by configuring your IP Music source as: Audio Jack. Contact Customer Support for more assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

UPS

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	UPS - APC Powerchute plus
Event ID: 1000	Message:	***PowerChute PLUS Version 5.2.1 stopped***
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1001	Message:	***PowerChute PLUS Version 5.2.1 started***
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 1002	Message:	Communication Established
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1004	Message:	UPS self-test passed
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1005	Message:	Administrative shutdown
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1006	Message:	Shutdown cancelled
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1016	Message:	System Shutdown started
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1018	Message:	Smart Cell signal restored
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1030	Message:	Minimum redundancy regained
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1033	Message:	Battery added

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1034	Message:	Battery removed
	User action:	None, if sufficient battery power still exists to support the load. If battery removal causes another event of higher severity, re-insert or replace the battery immediately.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1040	Message:	Bypass contactor OK
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1102	Message:	UPS internal temperature in bounds
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1150	Message:	Normal power restored: UPS on line
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1162	Message:	UPS on battery: Blackout
	User action:	Restore power to the UPS. If there is not a general power failure (that is, if only the UPS has lost input power), check building wiring and circuit breakers. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 1165	Message:	UPS on battery: Deep momentary sag
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1253	Message:	Self-test at UPS passed
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2001	Message:	System shutdown Complete
	User action:	For an administrative shutdown or a shutdown because of input power failure, wait for the UPS to reboot and to start the supported equipment. If you specified a shutdown without a reboot sequence, you must restart the UPS.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2030	Message:	Minimum redundancy lost
	User action:	The UPS has too great a load, or too few operational power modules to support the configured redundancy. Check that all modules are functioning properly and that the redundancy configuration is correct. If the condition persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 2036	Message:	System level fan failed
	User action:	Check the fan for obstructions. If you cannot resolve the problem immediately, contact APC Support for assistance.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 2037	Message:	Bypass contactor failed
	User action:	An internal hardware failure exists. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 100401	Message:	Scheduled UPS self-test passed
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100402	Message:	User-initiated UPS self-test passed
	User action:	No action required.

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100500	Message:	Administrative shutdown started
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100501	Message:	Administrative shutdown: User initiated
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100502	Message:	Administrative shutdown: Weekly shutdown
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100503	Message:	Administrative shutdown: Daily shutdown
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100601	Message:	User-initiated shutdown cancelled
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100700	Message:	UPS returned from low battery condition
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100900	Message:	UPS batteries no longer need replacing
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 101300	Message:	UPS overload condition solved
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 101400	Message:	UPS runtime calibration initiated
	User action:	A runtime calibration deeply discharges UPS batteries. Avoid performing critical operations until battery recharges sufficiently to support the load in case a condition occurs that requires battery operation.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 101500	Message:	UPS runtime calibration completed
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 101601	Message:	User-initiated shutdown started
	User action:	Save files and shut down programs, or cancel the shutdown.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 101700	Message:	UPS returned from bypass
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 103100	Message:	UPS module added
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 103200	Message:	UPS module removed
	User action:	This is the first step in replacing a failed module. Continue with the replacement
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 103500	Message:	Main Intelligence module OK
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 103600	Message:	Main Intelligence module added
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 103700	Message:	Redundant intelligence module OK
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 103800	Message:	Redundant intelligence module added
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 110000	Message:	Ambient temperature back within thresholds
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 110100	Message:	Ambient humidity back within thresholds
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 200000	Message:	UPS on battery
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). (1) If input power is still present or becomes present again quickly, decrease the sensitivity of the UPS. (2) If the UPS has switched to battery operation because of complete loss of utility power, wait for power to be restored to the UPS. If the condition persists, contact an electrician to analyze your utility power. (3) If only the UPS has lost input power, check building wiring and circuit breakers.
	Alarm severity:	Warning

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Information
	Logs:	None
Event ID: 200001	Message:	UPS on battery: High input line voltage
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200002	Message:	UPS on battery: Brownout
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200004	Message:	UPS on battery: Small momentary sag
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200005	Message:	UPS on battery: Small momentary spike
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200007	Message:	UPS on battery: Large momentary spike
	User action:	This event can be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200008	Message:	UPS on battery: Simulated power failure
	User action:	Wait for this test to complete.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 200200	Message:	UPS enabling SmartBoost
	User action:	If this event occurs frequently, decrease the Low Transfer Voltage of your UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 200301	Message:	Low battery condition
	User action:	The UPS cannot continue to use its battery power to support its equipment load. The remaining runtime equals, or is less than, the runtime defined by its "Low Battery" setting. Consider upgrading to a UPS that provides more runtime. You can use the APC UPS Selector page to identify the UPS that best meets your system's requirements. http://www.apc.com/go/direct/index.cfm?tag=selectors
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200400	Message:	UPS runtime calibration cancelled
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 200401	Message:	UPS runtime calibration cancelled by user
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 200402	Message:	UPS runtime calibration aborted by power failure
	User action:	Retry the calibration when power is restored
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 200403	Message:	UPS unable to perform runtime calibration: Capacity < 100%
	User action:	The UPS battery capacity is less than 100%, probably because of recent battery operation of the UPS. Wait for the batteries to recharge and then retry the runtime calibration.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200700	Message:	UPS enabling SmartTrim

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	If this event occurs frequently, increase the High Transfer Voltage of your UPS. If the condition persists, contact an electrician to analyze your utility power.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 201301	Message:	UPS on bypass: user set via software or panel
	User action:	The front panel or a software command was used to put the UPS into bypass mode, typically for maintenance. Since the UPS cannot support its load if a power failure occurs, return the UPS to online operation as soon as possible.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 201302	Message:	UPS system is in maintenance bypass set by switch
	User action:	The switch at the UPS was used to put the UPS into bypass mode, typically for maintenance. Since the UPS cannot support its load if a power failure occurs, return the UPS to on-line operation as soon as possible.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 203100	Message:	UPS module failed
	User action:	Replace the failed module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 203200	Message:	Main intelligence module removed
	User action:	This is the first step in replacing a failed module. Continue with the replacement
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 203300	Message:	Main intelligence module failed
	User action:	Replace the failed module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 203400	Message:	Redundant intelligence module removed
	User action:	This is the first step in replacing a failed module. Continue with the replacement
	Alarm severity:	Minor

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Warning
	Logs:	None
Event ID: 203500	Message:	Redundant intelligence module failed
	User action:	Replace the failed module.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 203600	Message:	System level fan OK
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 203800	Message:	Input circuit breaker tripped
	User action:	Reset the circuit breaker. If the problem persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 203900	Message:	Input circuit breaker reset
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 300000	Message:	Unable to communicate with UPS
	User action:	Check cable connections, make sure UPS is on, and check network status. If the condition persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300100	Message:	UPS output overload
	User action:	The UPS has sensed a load greater than 100 percent of its rated capacity. Remove some attached equipment from the UPS. If this condition happens occasionally and briefly, check for attached equipment that typically uses high power periodically (such as laser printers and photocopiers). If the condition persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 300200	Message:	UPS self-test failed
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300201	Message:	Scheduled UPS self-test failed
	User action:	Run an unscheduled self-test. If the UPS fails the second self-test contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300202	Message:	Scheduled UPS self-test failed: Invalid test
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300204	Message:	User-initiated self-test failed
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300205	Message:	Self-test at UPS failed
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300206	Message:	User-initiated self-test failed: Invalid test
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 300206	Message:	User-initiated self-test failed: Invalid test
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300206	Message:	Self-test at UPS failed: Invalid test
	User action:	Run another self-test. If the UPS fails the self-test again, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300300	Message:	UPS battery is discharged
	User action:	Wait for the UPS battery power to recharge.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 300400	Message:	Communication lost while on battery
	User action:	Prepare for possible abrupt shutdown with no warning. The UPS has switched to battery operation but communication with the UPS has been lost, making it impossible to determine how much runtime the UPS has available. Check network connections, and check input power source.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 301000	Message:	Check installation of Smart Cell signal cable
	User action:	Check cable connections to batteries.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 301300	Message:	UPS internal temperature over limit
	User action:	Make sure that there is adequate clearance around the UPS, and that the UPS ventilation ports are not blocked. Allowing the UPS to continue to operate in this condition can damage the UPS. If the condition persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 301301	Message:	UPS battery charger failure
	User action:	An internal hardware failure exists. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 301302	Message:	UPS on bypass: severe DC imbalance overload
	User action:	An internal hardware failure exists. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 301303	Message:	UPS on bypass: output voltage outside limits
	User action:	The UPS has switched automatically to bypass mode because its output voltage was too high. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 301304	Message:	UPS on bypass: top module fan needs repair
	User action:	A hardware failure has caused the UPS to switch to bypass operation. Since the UPS cannot support its load if a power failure occurs, correct the failure as soon as possible. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 301400	Message:	Base module fan needs repair
	User action:	An internal hardware failure exists. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 301500	Message:	Base module bypass power supply needs repair
	User action:	An internal hardware failure exists. Contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 301600	Message:	UPS battery needs replacing

UPS (Uninterruptible power supply)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Replace all faulty batteries. To order replacement batteries, see the following Web page. :http://www.apc.com/go/direct/index.cfm?tag=battery
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 310001	Message:	Below lower ambient temperature threshold
	User action:	Check heating and ventilation systems
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 310002	Message:	Exceeded upper ambient temperature threshold
	User action:	Check air conditioning systems and make sure equipment is adequately spaced for proper ventilation.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 310101	Message:	Below humidity threshold
	User action:	Check air conditioning and humidity-control systems.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 310102	Message:	Exceeded upper humidity threshold
	User action:	Check air conditioning and humidity-control systems.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 310700	Message:	Maximum internal UPS temperature exceeded
	User action:	Make sure that there is adequate clearance around the UPS and that the UPS ventilation ports are not blocked. Allowing the UPS to continue to operate in this condition can damage the UPS. If the condition persists, contact APC Support for assistance. http://www.apc.com/go/direct/index.cfm?tag=support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

UTPS

UTPS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	UNISTIM Terminal proxy server
Event ID: 2000	Message:	DN xyz is experiencing incoming voice packet loss while on a call. It is receiving fewer voice packets than it is expecting.
	User action:	If the message is persistent, the BCM is experiencing network routing difficulties. More quantitative information is available in the UTPS log.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	xyz is the IP set's DN
Event ID: 3000	Message:	<date><time> (UTPS:1.) *** MPSMI is OFF LINE.
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** RUDPInit initialization failure; error …
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** UTPS terminating due to problem with RUDP Rx socket; error …
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** Unable to connect to the Media Services Manager; error …

UTPS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** Unable to open a FUMP channel; error …
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** Unable to open RUDP socket; error …
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** Unable to get a timer from the OS
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	*** UTPS is being shut down.
	User action:	If the voice watchdog service is NOT running, you will need to restart the UTPS service.
	Alarm severity:	Critical
	Trap-type:	Error

UTPS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
	Comments:	All UTPS events written to the NT event log are fatal, and will cause the UTPS to shutdown. The reasons for these events are either a missing dependent component (MPS or MSM), or an OS related problem (Unable to initialize a timer, socket, signalling channel to the core).
Event ID: 3000	Message:	12:30:34.040 [UTPS:1.]***MSM has closed the pipe to the UTPS; shutting down.
	User action:	Restart the BCM.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

VBMain

VBMain (VoiceButton Multimedia call centre	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	VBMain
Event ID: 0	Message:	VBMain error: %d, Exit code: %d
	User action:	Send NT event log and stlog to development / ITAS. Manually restart service or reboot BCM. Logged if service failed to start.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Logged if service failed to start. Error number is that returned by GetLastError()

VNC Service

VNC Service (Virtual network computing)	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	VNC server
Event ID: 1	Message:	The VNC service was started from the Product Maintenance & Support website. Virtual network computing.
	User action:	Most likely, this BCM has been accessed through VNC. Other than this information, no action is required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

VNetManager

VNetManager provides the management interface for the VoIP gateway.

VNetManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 301	Message:	Voice Net Manager started.
	User action:	No action required.
	Alarm severity:	Warning

VNetManager	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Information
	Logs:	None
Event ID: 304	Message:	Voice Net Manager stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

VNetQosMonitor

VNetQosMonitor	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice Net QoS monitor
Event ID: 203	Message:	Voice Net QoS Monitor started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 204	Message:	Voice Net QoS Monitor stopped.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 205	Message:	Voice Net QoS Monitor flagged fallback.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Indication. VoIP gw has taken action.
Event ID: 206	Message:	Voice Net QoS Monitor exited fallback.
	User action:	No action required.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
	Comments:	Indication. VoIP gw has taken action.

VNetVoIPGtwy

VNetVoIPGtw	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	VoIP Gateway
Event ID: 102	Message:	Service VoIP Gateway started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 105	Message:	Service VoIP Gateway stopped.

VNetVoIPGtw	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 113	Message:	Syntax error in configuration file 'D:\Data Files\Nortel Networks\VoIP Gateway\localgateway.cfg'.
	User action:	Check "Local Gateway IP interface" for correct information.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 114	Message:	Invalid Configuration file parameter
	User action:	Check gateway type parameter in remotegateway.cfg table file.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 120	Message:	Cannot initialize H323 stack
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 122	Message:	Cannot read info from license server
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 123	Message:	Keycode applied for unknown feature
	User action:	Keycode applied for more recent feature than software knows of.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 124	Message:	Quality of Service monitor connection not established
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Minor
	Trap-type:	Error
	Logs:	None
Event ID: 130	Message:	Call setup rejected because of insufficient QoS bandwidth
	User action:	Confirm engineering traffic guidelines for network configuration.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

VNetVoIPGtw	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 131	Message:	Dropped connected call from DN X to DN Y. Incompatible codecs or insufficient media gateway resources
	User action:	Change or make available the correct Codec to match the Codec supported by the software at the far end of the call.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200	Message:	Generic system error
	User action:	A wide assortment of problems. See event text for details. Report error to Nortel Networks support.
	Alarm severity:	Major
	Trap-type:	Error
	Logs:	None
Event ID: 201	Message:	Generic system error
	User action:	A wide assortment of problems. See event text for details. Report error to Nortel Networks support.
	Alarm severity:	Major
	Trap-type:	Warning
	Logs:	None

Voice CTE

VoiceCTE	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice CTE
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x03nn.
	User action:	Error 0x03nn. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	All CTE device driver errors have the hex base 0x0300. Driver errors which do not have specific messages are reported as “Error 0x03nn”. This generic message is rare.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0301
	User action:	An invalid handle passed to the driver. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative. <UDR0015>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Internal unexpected error.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0302
	User action:	Device is not open. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative. <UDR0016>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Internal unexpected error.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0306
	User action:	Device is already open. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative. <UDR0017>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Internal unexpected error.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0307
	User action:	The requested CTI device cannot be used with this version of Windows. Please verify the installation of the Voice CTE service. <UDR0018>

VoiceCTE	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Most likely an installation problem.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0310
	User action:	The device driver for the requested CTI device is not installed. Install the device driver and restart your application. <UDR001>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Most likely an installation problem.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0311
	User action:	The device driver interface module for the CTI device is invalid. Please reinstall the device driver software. <UDR002>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Most likely an installation problem.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0x0315
	User action:	Unable to start a new device driver execution thread. Terminate some applications and restart your application. <UDR006>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Windows system resource problem during initialization.
Event ID: 257	Message:	CTE / MSC Driver Initialization Error. Exit Error is 0xFFnn
	User action:	Error 0xFFnn. Please ensure the Voice CTE service has restarted. If this fails to correct the problem then please collect the files CteDiag.log and CteDiag.bak, ensure the Voice MSC service has restarted and report this problem to your support representative.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Error from MSC driver initialization.
Event ID: 257	Message:	Other CTE Initialization Error. Exit Error is 0x0002
	User action:	“Error 0x0002. Please verify the installation of the Voice CTE service.”
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Generic unexpected error. This error is only reported as an event when it causes CTE initialization to fail. In this case it is most likely an installation problem.
Event ID: 257	Message:	Other CTE Initialization Error. Exit Error is 0x0003

VoiceCTE	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	“Error 0x003. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative."
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Generic internal unexpected error. This error is only reported as an event when it causes CTE initialization to fail.
Event ID: 257	Message:	Other CTE Initialization Error. Exit Error is 0x0009
	User action:	Cannot create a window. Terminate some applications and restart the Voice CTE service. <CTE006>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	CTE initialization failed due to Windows system problem.
Event ID: 257	Message:	Other CTE Initialization Error. Exit Error is 0x00nn
	User action:	CTE could not download FUMP Information about the telephony switch. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative. <CTE005>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	CTE initialization failed because it could not download KSU identification fump. Applications are sent a CTE event with the failed ME_xxx return code.
Event ID: 257	Message:	Other CTE Initialization Error. Exit Error is 0x0009 or 0c0055
	User action:	A CTE application attempted to register with CTE before the Voice CTE service had fully initialized (error%led). If the application is not behaving correctly, restart it after the Voice CTE service has started. <RTR001>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Missing service dependency or install problem: Either CTE service is not fully initialized and some application tried to register with CTE or CTE is not registered as a service and application registration failed to launch CTE.
Event ID: 257	Message:	CTE Runtime Error. Exit Error is 0x0000
	User action:	Your CTI device has been reset. All call processing has been disabled. Ensure the Voice MSC service has restarted. <CTE002>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

VoiceCTE	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Comments:	MSC communication error (reset). CTE responds by sending it's apps a shutdown event with the reason CTE_SHUTDOWN_DEVICE_RESET, and then shutting down with no error.
Event ID: 257	Message:	CTE Runtime Error. Exit Error is <No Error>
	User action:	The CTE atom table is corrupt or full. Please collect the files CteDiag.log and CteDiag.bak, ensure the Voice CTE service has restarted and report this problem to your support representative. <CTE003>
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	CTE has run out of memory or it's internal memory structure is corrupt. CTE continues to run. Applications receive the CTE response ME_NO_HEAP_MEMORY until some memory is freed or CTE is restarted.

Voice software

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice software alarm monitor
Event ID: 11	Message:	All lines were disconnected. Power down the system and check all line connections on the system.
	User action:	Power down the system and check all telephone connections on the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 254, Sev=P9, Cat=C
Event ID: 18	Message:	DSP message queue (messages to be sent to DSP firmware) is full. Message not sent may cause application to timeout waiting for resource. Users may experience call failures.
	User action:	Customer should report event to installer to get tracebacks.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 254, , Sev=P9, Cat=C
Event ID: 20	Message:	Wireless re-evaluation required. Initiate data re-evaluation.
	User action:	Re-Evaluation should be initiated by the system administrator.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 665, Sev=P8, Cat=F
Event ID: 21	Message:	Wireless re-evaluation in progress.
	User action:	No action required. This ALARM only alerts the system administrator/ installer that mobility data re-evaluation has started.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 878, Sev=?, Cat=E
Event ID: 22	Message:	Wireless re-evaluation completed.
	User action:	No action required. This aALARM only alerts the system administrator/ installer that mobility data re-evaluation has finished.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 879, Sev=?, Cat=E
Event ID: 23	Message:	Configured cell %1 (cell number) failed to come on-line.
	User action:	Determine which basestations belong to the failed cell. Replace the basestations and invoke a data re-evaluation, or warm start the system.
	Alarm severity:	Critical
	Trap-type:	Error

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	MSC event 881, Sev=?, Cat=F
Event ID: 24	Message:	Etiquette: There is insufficient data to capture an RSSI signature.
	User action:	Run a re-evaluation with a suitable configuration that will provide an adequate RSSI signature.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 664, Sev=P9, Cat=F
Event ID: 31	Message:	The download of firmware to DTCM %1 has failed.
	User action:	Check the logs for occurrences of Event 338. Record the message registered in the log and contact your local support group. Power down the system and check the DTCM hardware and the link to the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 339, Sev=P6, Cat=F
Event ID: 32	Message:	A BRI has been selected as the primary clock source rather than a DTCM.
	User action:	The slot containing the DTCM must be configured as the primary clock source.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 351, Sev=P6, Cat=F
Event ID: 34	Message:	Device firmware download started. This event may occur more than once per device type.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 355,Sev=P7,Cat=E)
Event ID: 35	Message:	Device firmware download failure. Reported by the data transfer server. Event parameters: %1. The device has not been brought on-line by the system.
	User action:	Check that the device is properly installed and reset the device. Try replacing device. If the problem persists, contact you local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 356, Sev=P6, Cat=F
Event ID: 36	Message:	Device firmware download failure. Reported by the data transfer slave. Event parameters: %1. The device has not been brought on-line by the system.
	User action:	Check that the device is properly installed and reset the device. If the problem persists, replace the device.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 358, Sev=P6, Cat=F

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 37	Message:	Protocol or country profile download failure. Event parameters: %1.
	User action:	Check that the device is properly installed and reset the device.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 361, Sev=P6, Cat=F
Event ID: 39	Message:	The Market Profile is invalid. The installer must select the appropriate profile.
	User action:	The installer must select the appropriate profile.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 350, Sev=P9, Cat=F
Event ID: 40	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the Unavailable Seconds Error. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 315, Sev=P8, Cat=F
Event ID: 41	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Loss of Signal. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 316, Sev=P8, Cat=F
Event ID: 42	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Loss of Signal. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 317, Sev=P8, Cat=F

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 43	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Alarm Indication Signal. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 318
Event ID: 44	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Remote Alarm Indication. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 319, Sev=P8, Cat=F
Event ID: 45	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Loss of Signal on time-slot 16. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 320, Sev=P8, Cat=F
Event ID: 46	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Alarm Indication Signal on time-slot 16. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 321, Sev=P8, Cat=F

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 47	Message:	The long term alarm threshold has been surpassed in DTCM %1 for the detection of Remote Alarm Indication on time-slot 16. The most likely cause is an irregularity with the PSTN connections. The cable connecting the DTCM to the network termination point or external CSU has been disconnected, or there is a problem with the signal from the network.
	User action:	Check the logs and look for Events ranging from 315-336. If this alarm occurs more than once over a two-week period, contact your local support group.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 322, Sev=P8, Cat=F
Event ID: 50	Message:	A Digital Station Computer Module on bus %1 has been disconnected or powered down.
	User action:	Power down the system and check all connections to the module. If the problem persists, replace the module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 250, Sev=P9, Cat=C
	Comments:	MSCid=250, Sev=P9, Cat=C. On system boot-up the BCM waits 3 minutes before reporting alarm 50/51 to give the modules time to boot up. On a running system the BCM requires a module to be lost for at least 2 minutes before reporting alarm 50/51.
Event ID: 51	Message:	A Digital Trunk Computer Module or Called ID Computer Module on bus %1 has been disconnected or powered down.
	User action:	Power down the system and check all connections to the module. If the problem persists, replace the module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 251, Sev=P9, Cat=C
	Comments:	MSCid=251, Sev=P9, Cat=C. On system boot-up the BCM waits 3 minutes before reporting alarm 50/51 to give the modules time to boot up. On a running system the BCM requires a module to be lost for at least 2 minutes before reporting alarm 50/51.
Event ID: 52	Message:	A Trunk Computer Module has been disconnected. Event parameters: %1 (Module - Card).
	User action:	Power down the system and check all connections to the module. Check that the module is properly seated. If the problem persists, replace the module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 252, Sev=P9, Cat=C
		This only applies to trunk MBMs that share a DS30 bus. So CTM and BRI MBMs can generate this. To reproduce this bring 2 CTMs or BRI MBMs on a single DS30 and disconnect 1 of the MBMs. ON a running system the BCM requires a module to be lost for at least 2 minutes before reporting alarm 50/51/52.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 53	Message:	Radio %1 has been removed from service due to an error. An accompanying Event message will indicate an explicit reason for the radio failure.
	User action:	Perform diagnostics on the basestation.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 300, Sev=P6, Cat=C
Event ID: 54	Message:	A software download to the basestations has started. No action required. During basestation download, system performance may be sluggish, and wireless functionality will not be complete.
	User action:	Wait for Event 55.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 55	Message:	All downloads are complete.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 59	Message:	No more credits available for portables or sets. More credits must be acquired before all the registered portables or installed sets can be activated. Parameters: %1 (0=Portable credit required, 1=Set credit required)
	User action:	Acquire more portable credits.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 275, Sev=P9, Cat=F
Event ID: 61	Message:	Incompatible Trunk Computer Module. A Trunk Computer Module cannot operate with the trunk Type assigned to it in Configuration. Event parameters: %1 (Module - Card). Check that the trunk Type programmed matches the module.
	User action:	Check that the trunk Type programmed matches the module.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 255, Sev=P9, Cat=F
Event ID: 62	Message:	Invalid Auto Answer Setting. What this means is that a line has been set to auto answer but the type of trunk is not suitable for auto answer. Event parameters: %1 (Module - Card). Change the trunk programming to manual answer.
	User action:	Change the trunk programming to manual answer.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 256, Sev=P9, Cat=F

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 63	Message:	There are no more DTMF receivers that can be allocated. DTMF receivers are busy, not working properly, or have not been installed. The line requesting a receiver is on port %1.
	User action:	If this alarm occurs frequently, add additional DTMF receivers to the system.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 267, Sev=P8, Cat=F
Event ID: 67	Message:	An invalid Trunk Computer Module has been connected to port %1.
	User action:	Power down the system. Disconnect the Trunk Computer Module from the indicated port and check module compatibility for the specific country. Replace the module with as required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 343, Sev=P8, Cat=f
Event ID: 68	Message:	A device has been connected to a port which is not available for the device Type. The affected port is %1.
	User action:	Power down the system and disconnect the device from the port identified. Reconnect it to a valid port.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 863, Sev=P4, Cat=F
Event ID: 71	Message:	A log Event has activated the emergency transfer relay.
	User action:	No action required. The alarm was generated by a power failure.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 72	Message:	TEI request error for ISDN emulator. Event parameters: %1.
	User action:	Withdraw the last request for a TEI.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 352, Sev=P1, Cat=D
Event ID: 75	Message:	Clock control is in free run. This could indicate a problem with the cable connection, or with the signal from the network.
	User action:	Check the cable connection or the signal from the network
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 447, Sev=P1, Cat=D
Event ID: 79	Message:	Analog Station Computer Module firmware download failure. Event parameters: %1. The ASCM will not be brought on-line by the system.
	User action:	Perform diagnostics on the ASCM.
	Alarm severity:	Critical
	Trap-type:	Error

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	MSC event 369, Sev=P6, Cat=F
Event ID: 80	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 81	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 82	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 83	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 84	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 85	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 86	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 87	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None
Event ID: 88	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 89	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 90	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 91	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 92	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 93	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 94	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 95	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 96	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 97	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 98	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 99	Message:	An alarm generated by a server application.
	User action:	See application documentation for appropriate action.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 102	Message:	Two modules have been configured to use the same DS30 but cannot co-exist at the configured offsets.
	User action:	Correct the DS30 assignments using the dip-switches on the modules.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 376, Sev=P7, Cat=F
Event ID: 103	Message:	The trial period for a feature has expired. Feature Parameter: %1 (00=Hunt Groups, 01=Hospitality Services, 02=DPNSS Networking, 03=MCDN Networking, 04=Q.Sig Networking). The permanent software key may be purchased to allow continued use of this feature.
	User action:	Purchase permanent licenses
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 465, Sev=P8, Cat=F
Event ID: 194	Message:	The Call Server Operating System software has returned an error code. A restart will occur. Record the traceback and event parameters and report the error.
	User action:	Record the traceback and event parameters and report the error.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 200	Message:	Etiquette: insufficient CFP credits.
	User action:	Purchase additional Portable licenses
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 665, Sev=P8, Cat=F
Event ID: 201	Message:	Etiquette: CFP credits decreased.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 666, Sev=P8, Cat=E
Event ID: 202	Message:	Etiquette: UTAM keys required.
	User action:	Purchase a UTAM key
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 667, Sev=P8, Cat=F
Event ID: 203	Message:	Etiquette: UTAM test failed.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 668, Sev=P8, Cat=F
Event ID: 207	Message:	Ettiquette: System startup. No action required.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 672, Sev=P1, Cat=E
Event ID: 208	Message:	Ettiquette: System online. No action required.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 673, Sev=P8, Cat=E
Event ID: 224	Message:	Could not re-enable all devices after a Call Server restore took place. Call Server will be restarted. Customer should report event to installer to get tracebacks.
	User action:	Customer should report event to installer to get tracebacks.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 224, Sev=P8, Cat=B

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 226	Message:	Call Server backup failed. Customer should contact installer to get the SP event tracabecks.
	User action:	Customer should contact installer to get the SP event tracabecks.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 226, Sev=P8, Cat=A
Event ID: 229	Message:	Call Server restore failed. Call Server will be restarted. Customer should contact installer to tracabecks.
	User action:	Customer should contact installer to tracabecks.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 229, Sev=P8, Cat=B
Event ID: 247	Message:	An invalid event was received on a TCM channel. Check that all devices on the system are supported and that the wiring to the devices is correct.
	User action:	Check that all devices on the system are suported and that the wiring to the devices is correct.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSCid event 247, Sev=P8, Cat=B
	Comments:	MSCid=247, Sev=P8, Cat=B
Event ID: 260	Message:	No battery feed. When the system is booted a check is made to determine if lines are physically attached to the line ports. This is done by performing a line presence test. If this test fails then it indicates that a line is not attached. Line taken out of service. If no line is attached to the port attach a line. Port = %1. If a line is attached then determine if the line is operational.
	User action:	If no line is attached to the port, attach a line. If a line is attached, then determine if the line is operational.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 260, Sev=P8, Cat=C
Event ID: 262	Message:	No dialtone. When a line is seized a test is made to determine if dial tone is present. If this test fails this event is raised. Port = %1. Check the physical trunk line to see if it operating correctly.
	User action:	Check the physical trunk line to see if it operating correctly.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 262, Sev=P7, Cat=C
Event ID: 263	Message:	Invalid disconnect sequence. The handshake which occurs between the analog trunk and the network when a line is released was not properly completed. The analog trunk is unusable until the disconnect completes. Port = %1. Check the trunk interface with the network to determine if it operating correctly.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Check the trunk interface with the network to determine if it operating correctly.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 263, Sev=P8, Cat=C
Event ID: 265	Message:	When seizing a trunk to make an outgoing call a handshake must occur between the Call Server trunk and the network before digits can be dialled. This event indicates that this handshake failed since the network did not acknowledge the Call Server request to seize the line. The trunk is unusable until the handshake is properly completed. Port = %1. Check the trunk interface with the network to determine if it operating correctly.
	User action:	Check the trunk interface with the network to determine if it operating correctly.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 265, Sev=P7, Cat=C
Event ID: 270	Message:	Invalid Message. The Call Server is dealing with a multi byte message that it does not understand while trying to initialize a set. TN = %1. If the event occurs many times, unplug the set, wait for 3 minutes, then replug the set. May be caused by a noisy line.
	User action:	If the event occurs many times, unplug the set, wait for 3 minutes, then replug the set.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 270, Sev=P8, Cat=A
Event ID: 271	Message:	A set has firmware that is incompatible with the current Call Server load. Customer should contact installer to change Call Server load or the set.
	User action:	Customer should contact installer to change Call Server load or the set.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 271, Sev=P8, Cat=A
Event ID: 323	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of a degraded minute. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 323, Sev=P5, Cat=C

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 324	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of a severely errored second. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 324, Sev=P5, Cat=C
Event ID: 325	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of an errored second. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 325, Sev=P5, Cat=C
Event ID: 326	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of controlled slip underflow. The module is in a no-new-calls state. DTCM = %1.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 326, Sev=P5, Cat=C
Event ID: 327	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of controlled slip overflow. The module is in a no-new-calls state. DTCM = %1.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 327, Sev=P5, Cat=C
Event ID: 328	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of controlled slip overflow. The module is in a no-new-calls state. DTCM = %1.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 328, Sev=P5, Cat=C

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 329	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of loss of signal. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 329, Sev=P5, Cat=C
Event ID: 330	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of loss of frame. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 330, Sev=P5, Cat=C
Event ID: 331	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of controlled slip overflow. The module is in a no-new-calls state. DTCM = %1.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 331, Sev=P5, Cat=C
Event ID: 332	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of remote alarm indication. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 332, Sev=P5, Cat=C
Event ID: 333	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of loss of frame in timeslot 16. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 333, Sev=P5, Cat=C

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 334	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of alarm indication signal in time slot 16. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 334, Sev=P5, Cat=C
Event ID: 335	Message:	This event is generated when the short-term alarm threshold has been surpassed in the Digital Trunk Interface module for the detection of remote alarm indication in time slot 16. The module is in a no-new-calls state. DTCM = %1. Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	User action:	Intervention is required to find out why the Digital Trunk Interface module is alarmed.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 335, Sev=P5, Cat=C
Event ID: 367	Message:	A reset has occurred in the Basic Rate Interface or Digital Trunk Interface module. This event should only occur when the system first boots.
	User action:	Obtain the traceback for the module that reset.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 367, Sev=P5, Cat=B
Event ID: 400	Message:	A warm start has been done. No action required.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 400, Sev=P9, Cat=E
Event ID: 401	Message:	A search of the terminal address table failed to find a TN that matched the TN of the device that is initializing and requesting its LAD. The device will fail to initialize. This is a software error that can occur on initialization of any TCM peripheral. Report the problem and the software version.
	User action:	Report the problem and the software version.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 401, Sev=P4, Cat=B
Event ID: 608	Message:	Attempt to attach a device type to a port that is not supported in the software. The device will not initialize nor be operational. Verify that all types of attached peripherals initialize and function. Remove any unsupported device types.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Verify that all types of attached peripherals initialize and function. Remove any unsupported device types.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 608, Sev=P6, Cat=F
Event ID: 617	Message:	Cannot acquire a session. This happens only on Companion devices. Contact the installer to get the traceback data.
	User action:	Contact the installer to get the traceback data.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 617, Sev=P4, Cat=A
Event ID: 639	Message:	A bad message has been received by a CAP while getting key information. Contact the installer to get the event traceback data.
	User action:	Contact the installer to get the event traceback data.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 639, Sev=P4, Cat=A
Event ID: 799	Message:	A call processing error has occurred on an ISDN line. No action required.
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 799, Sev=P7, Cat=B
Event ID: 894	Message:	An attempt was made to enqueue a message into the DASS2/DPNSS layer 3 flow control queue, but the queue was full. The message has been dropped, and will not be sent out to the network. This can arise if the link has gone down but the Digital Trunk Interface module has failed to report it. Port = %1. Customer should report the problem. Installer should verify that the link is operational and the module is still functioning.
	User action:	Customer should report the problem. Installer should verify that the link is operational and the module is still functioning.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 894, Sev=P4, Cat=C
Event ID: 901	Message:	Part or all of the telephony system memory has been corrupted. A coldstart of the telephony subsystem will occur. This problem should be reported. All telephony data will need to be reprogrammed.
	User action:	Report the problem. All telephony data will need to be reprogrammed.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 901, Sev=P8, Cat=F
Event ID: 949	Message:	A bad protocol call control has been received from the Basic Rate Interface module. Determine reason for event and resolve.

Voice software	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Determine reason for event and resolve.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	MSC event 949, Sev=P6, Cat=B
Event ID: 998	Message:	Telephony time has been synchronized with the System time.
	User action:	No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	MSC event 998, Sev=P4, Cat=B
Event ID: 999	Message:	Unknown alarm detected. Alarm code: %1.
	User action:	Contact your local support group.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	MSC event 999, Sev=P7, Cat=B

VoiceCTI

VoiceCTI	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	VoiceCTI
Event ID: 257	Message:	Less than 5% voice file space avail. To delete voice messages (especially check the General Delivery Mailbox).
	User action:	Disk full (data partition) condition.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 257	Message:	All CallPilot ports busy, change resource allocation.
	User action:	All voice ports in use. Enable additional ports to avoid this situation.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 258	Message:	Restart BCM, so that change in Call Center refresher channel will take effect.
	User action:	Restart VoiceMail to have the new Refresher Channel value in effect
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 258	Message:	SetPortCapability voice failed - no resource
	User action:	Voice ports need to be allocated for the media services card so that voice mail will function.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 259	Message:	A call to SetServiceStatus failed. If Voice Mail has started normally, then no action is required. However Voice Mail may not have started. You may have to restart the system If problem persists, contact your service representative. These are 259, even though they are errors.
	User action:	SetServiceStatus
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	This event Is NOT passed via the mbLogMessage API
Event ID: 259	Message:	Current number of mbxes is greater than keycoded limit.
	User action:	If the number of mailboxes initialized is greater than the number of mailboxes enabled by keycode when a user attempts to login via unified messaging or the telset this event will be generated. To resolve apply a mailbox expansion keycode to ensure the number of keycoded mailboxes is sufficient to enable all initialized mailboxes.

VoiceCTI	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	This typically occurs immediately after a restore to a new system where keycodes have not yet been applied.
Event ID: 259	Message:	AA/CCR calls cannot be parked since park prefix is set to None.
	User action:	To resolve please configure the park prefix from Unified Manager.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 259	Message:	Voice Mail is operational
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

VoiceManagementSubsystem

Voice Management Subsystem	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice management subsystem
Event ID: 1	Message:	Voice Management Subsystem Service started.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2	Message:	Voice Management Subsystem Service stopped.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 100	Message:	The 'Restore' of the 'System programming' option has FAILED (Reason: internal error.).
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 100	Message:	The 'Restore' of the 'System programming' option has FAILED (Reason: open session rejected - auto admin re-eval is occurring, wireless.)
	User action:	No action required
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None

VoiceMSCService

VoiceMSCService	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice MSC service
Event ID: 257	Message:	!* DN length change detected.
	User action:	This is an event which indicates an MSC reset due to an administered change to the internal dialling plan length (number of digits). There is no action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	shutting down...

VoiceMSCService	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 257	Message:	!* StartD1Channels: we were told to shutdown the KSU
	User action:	This no longer applies to BCM 3.0. Earlier it was a log indicating that the MSC was being put into upload mode. There is no action required.
	Alarm severity:	Error
	Trap-type:	Critical
	Logs:	None
	Comments:	shutting down...

VoIPSipGateway

VoiceRecord	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	VoIP SIP Gateway
Event ID: 102	Message:	The service was started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 105	Message:	The service was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 106	Message:	Unexpected services request generated internally or by WinNt Services. Execution continues. The service received an unsupported request.
	User action:	No action required.
	Alarm severity:	Error
	Trap-type:	Critical
	Logs:	None
Event ID: 108	Message:	The service was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 114	Message:	Invalid configuration file parameter.
	User action:	Check gateway type parameter in remotegateway.cfg table file.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 120	Message:	Cannot initialize H323 stack
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 122	Message:	Cannot read info from license server.
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Critical

VoiceRecord	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None
Event ID: 123	Message:	Keycode applied for unknown feature.
	User action:	Keycode applied for more recent feature than software knows of.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 124	Message:	Quality of Service monitor connection not established.
	User action:	Report error to Nortel Networks support.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 130	Message:	Call setup rejected because of insufficient QoS bandwidth.
	User action:	Confirm engineering traffic guidelines for network configuration.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 131	Message:	Dropped connected call from DN X to DN Y. Incompatible Codecs or insufficient media gateway resources.
	User action:	Change or make available the correct Codec to match the Codec supported by the software at the far end of the call.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 200	Message:	Generic system error.
	User action:	A wide assortment of problems. See event text for details Report error to Nortel Networks support.
	Alarm severity:	Major
	Trap-type:	Error
	Logs:	None
Event ID: 201	Message:	Generic system error.
	User action:	A wide assortment of problems. See event text for details Report error to Nortel Networks support.
	Alarm severity:	Major
	Trap-type:	Error
	Logs:	None

VoiceRecord

VoiceRecord	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Call Detail Recording
Event ID: 105	Message:	The service was started.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 106	Message:	Unexpected services request generated internally or by WinNt Services. Execution continues. The service received an unsupported request.
	User action:	No action required.
	Alarm severity:	Error
	Trap-type:	Critical
	Logs:	None
	Comments:	Can never occur on BCM during normal operation.
Event ID: 108	Message:	The service was stopped.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

VoiceTimeSynch

VoiceTimeSynch	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice time synch
Event ID: 1001	Message:	Starting up NTP service version 3.0, server
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1001	Message:	No Time Adjustment:"Seconds" seconds > max of "Seconds".
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

VoiceTimeSynch	Return to table:	Component ID (alarm)/eventSource (trap) summary
Event ID: 1001	Message:	No Time Adjustment: "Seconds" seconds > min of "Seconds".
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1001	Message:	time adjustment of "Seconds" seconds > max of "Seconds"
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1002	Message:	No response from NTP server, check IP number or network connection
	User action:	Check IP number or network connection.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

VoiceWatchdog

VoiceWatchdog	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Voice watchdog
Event ID: 1000	Message:	KSU Down.
	User action:	Telephony services will be stopped temporarily. The alarm KSU_UP will be received when the telephony services are being restarted.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Voice Watchdog received the KSU Down from the VoiceMSCService. All services depending on VoiceMSCService will stopped
Event ID: 1001	Message:	KSU Reset.
	User action:	Telephony services being restarted and will be up within 10~15 minutes.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Voice Watchdog received the KSU UP from the VoiceMSCService. VoiceMSCDriver and all its dependencies will be stopped/Restarted. Wait for 15 minutes to get telephone sets back.
Event ID: 1002	Message:	KSU UP.
	User action:	Telephony services being restarted and will be up within 10~15 minutes.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Voice Watchdog received the KSU UP from the VoiceMSCService, VoiceMSCDriver and all its dependencies will be Restarted. Wait for 15 minutes to get telephone sets back.
Event ID: 1003	Message:	%Date/Time% Received KSU DN Length change notice.
	User action:	No action required. Voice Watchdog received the KSU DN Length change from the VoiceMSCService, VoiceMSCDriver and all its dependencies will be stopped/Restart. Wait for 15 minutes to get telephone sets back.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1004	Message:	Restarting All Monitored Services.
	User action:	No action required. Voice Watchdog restarting the root service and all it's dependencies.
	Alarm severity:	Warning
	Trap-type:	Information

VoiceWatchdog	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Logs:	None
Event ID: 1005	Message:	%Service Name% was manually restarted and Watchdog is monitoring its tree again.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
	Comments:	Voice Watchdog started monitoring this service.
Event ID: 1006	Message:	Watchdog was started as a service
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 1007	Message:	%Service Name% started successfully.
	User action:	No action required.
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 2000	Message:	ATTENTION: Communication with LED panel has been lost. Status LED may not reflect true system status.
	User action:	Investigate the possible cause in the next maintenance window.
	Alarm severity:	Minor
	Trap-type:	Warning
	Logs:	None
Event ID: 3000	Message:	%Service Name% failed:%#% --> Format Message failed: Unknown error.
	User action:	Call for Support and advise of "unknown error" received
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Voice Watchdog received an unknown error number from the Service Control Manager while querying the Service Status.
Event ID: 3001	Message:	%Service Name% failed:%#% --> %Error Message%.
	User action:	Start this service manually. If unable to resolve the problem call for Support and advise of the error message.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	Voice Watchdog received error message from the Service Control Manager while querying the Service Status
Event ID: 3002	Message:	Service %Service Name% has reached the failure repeat limit and must be restarted manually

VoiceWatchdog	Return to table:	Component ID (alarm)/eventSource (trap) summary
	User action:	Start this service manually. If unable to resolve the problem call for Support. Voice Watchdog encountered the maximum limit of services restarting times and the service needs to be restarted manually.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3003	Message:	%Service Name% Start Service failed: The dependent service or group failed to start.
	User action:	Start the root service of failed service manually. If unable to resolve the problem call for Support
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
	Comments:	The service failed to start according to the failure in the root (parent) service. The root service needs to be started manually.
Event ID: 3004	Message:	%Service Name% Failed to start.
	User action:	Start this service manually. If unable to resolve the problem call for Support.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None
Event ID: 3005	Message:	Service %Service Name% stopped unexpectedly.
	User action:	Watchdog will restart this service, No action required.
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Wins

Wins	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Windows internet name service
Event ID: 4097	Message:	WINS has initialized properly and is now fully operational.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None
Event ID: 4098	Message:	WINS was terminated by the service controller. Wins will gracefully terminate.
	User action:	No action required
	Alarm severity:	Warning
	Trap-type:	Information
	Logs:	None

WINSCTRS

WINSCTRS provides WINS server statistics.

WINSCTRS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	None
Event ID: 4314	Message:	WINSCTRS could not get the WINS statistics.
	User action:	No action required
	Alarm severity:	Critical
	Trap-type:	Error
	Logs:	None

Workstation

WINSCTRS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Return to table:	Component ID alarms/eventSource (Trap) by event ID
	Service:	Workstation
Event ID: 3870	Message:	“System name” is not a valid computer name.
	User action:	The BCM name should be unique in the network.
	Alarm severity:	Critical

WINSCTRS	Return to table:	Component ID (alarm)/eventSource (trap) summary
	Trap-type:	Error
	Logs:	None

Events that cause a system restart

Some events cause an automatic system restart. If the system follows normal recovery routines an event message doesn't appear. This table lists all the events associated with system restarts.

Table 14 Events that cause a system restart

Log events that cause a restart	Log events that cause a restart
MSC event 101 (System test log)	MSC event 265 (System test log)
MSC event 102 (System test log)	MSC event 266 (System test log)
MSC event 103 (System test log)	MSC event 267 (System test log)
MSC event 104 (System test log)	MSC event 268 (System test log)
MSC event 105 (System test log)	MSC event 269 (System test log)
MSC event 106 (System test log)	MSC event 270 (System test log)
MSC event 108 (System test log)	MSC event 271 (System test log)
MSC event 109 (System test log)	MSC event 285 (System test log)
MSC event 110 (System test log)	MSC event 286 (System test log)
MSC event 111 (System test log)	MSC event 287 (System test log)
MSC event 112 (System test log)	MSC event 288 (System test log)
MSC event 114 (System test log)	MSC event 289 (System test log)
MSC event 115 (System test log)	MSC event 290 (System test log)
MSC event 116 (System test log)	MSC event 291 (System test log)
MSC event 118 (System test log)	MSC event 292 (System test log)
MSC event 119 (System test log)	MSC event 293 (System test log)
MSC event 120 (System test log)	MSC event 294 (System test log)
MSC event 124 (System test log)	MSC event 295 (System test log)
MSC event 125 (System test log)	MSC event 296 (System test log)
MSC event 130 (System test log)	MSC event 297 (System test log)
MSC event 133 (System test log)	MSC event 298 (System test log)
MSC event 134 (System test log)	MSC event 400 (System Admin log)
MSC event 137 (System test log)	MSC event 426 (System test log)
MSC event 151 (System test log)	MSC event 427 (System test log)
MSC event 224 (System test log)	MSC event 428 (System test log)
MSC event 245 (System test log)	MSC event 429 (System test log)
MSC event 246 (System test log)	MSC event 430 (System test log)
MSC event 247 (System test log)	MSC event 432 (System test log)
MSC event 248 (System test log)	MSC event 600 (System test log)
MSC event 260 (System test log)	MSC event 601 (System test log)
MSC event 261 (System test log)	MSC event 602 (System test log)
MSC event 262 (System test log)	MSC event 614 (System test log)
MSC event 263 (System test log)	MSC event 630 (System test log)
MSC event 264 (System test log)	803, 808, 810, 823

Chapter 3
Service Management System

This section describes service manager capabilities in Unified Manager and the properties of the services in the Service Manager and associated alarm notifications.

Service Management topics

Service Manager

Use the Service Manager to access, assess or modify the services running on Business Communications Managers in your network.

Use Unified Manager to configure services individually on each Business Communications Manager in your network. Services running on a single Business Communications Manager in a network are independent of other Business Communications Managers in the same network. Services do not interact between Business Communications Managers.

Services control the fundamental functionality of Business Communications Manager. A service is a software process that controls interaction with Business Communications Manager hardware devices, computing environment, telephony or your browser interface.

Modification of any service has far-reaching effects on communications or event reporting capability. Nortel Networks strongly recommends that you consult with your support group before you use the service manager interface.

There are two categories of services:

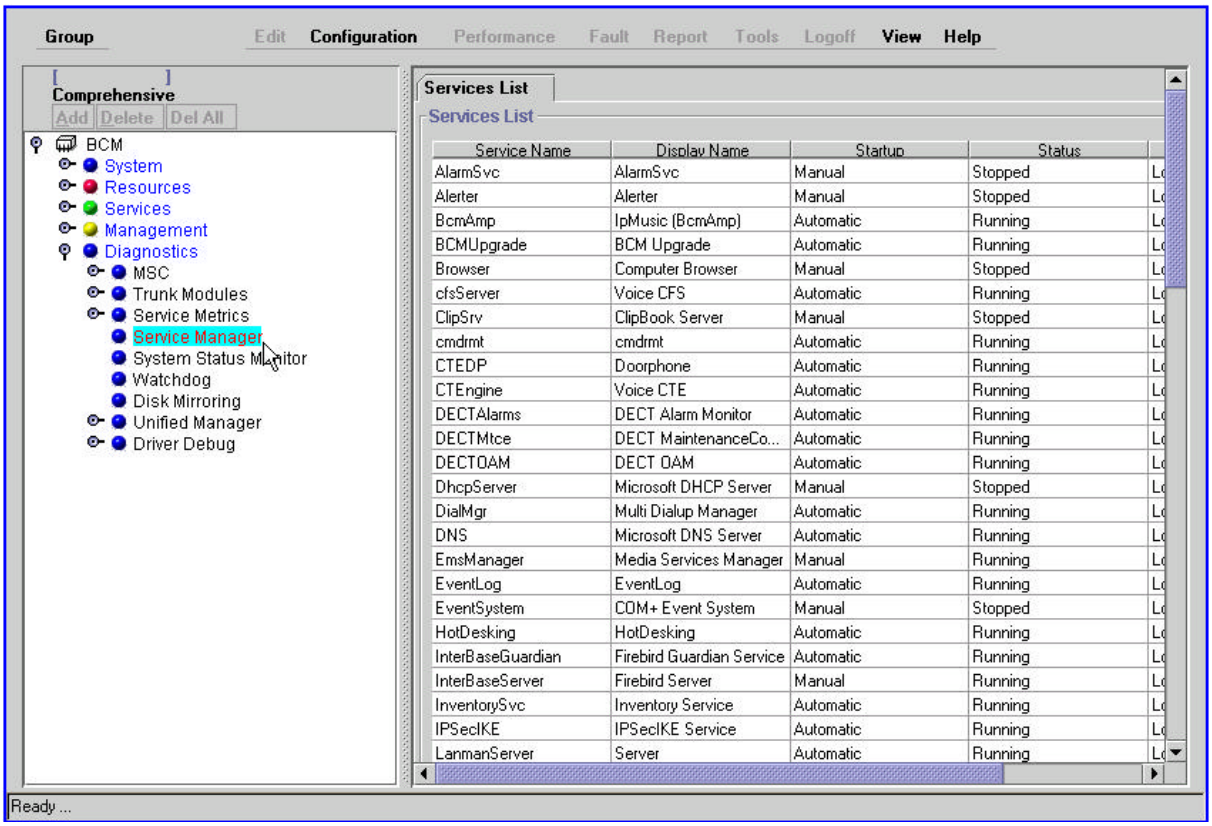
- ***System level services***: Software processes that are critical to essential system-level features. See "System-level service definitions" on page 258.
- ***Nortel Networks configurable services***: Software processes that are critical to Business Communications Manager software. See "Nortel Networks Configurable Services" on page 285.

Accessing Service Manager

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.

2 On the Unified Manager navigation tree click **Diagnostics** and click the **Service Manager** heading.
The Services List screen displays a list of services, and information about how the system is started, and the current status.

Figure 29 Services List



3 From the **Configuration** menu select **Modify Service**.
The Services List dialog box appears.

Figure 30 Modify services selection

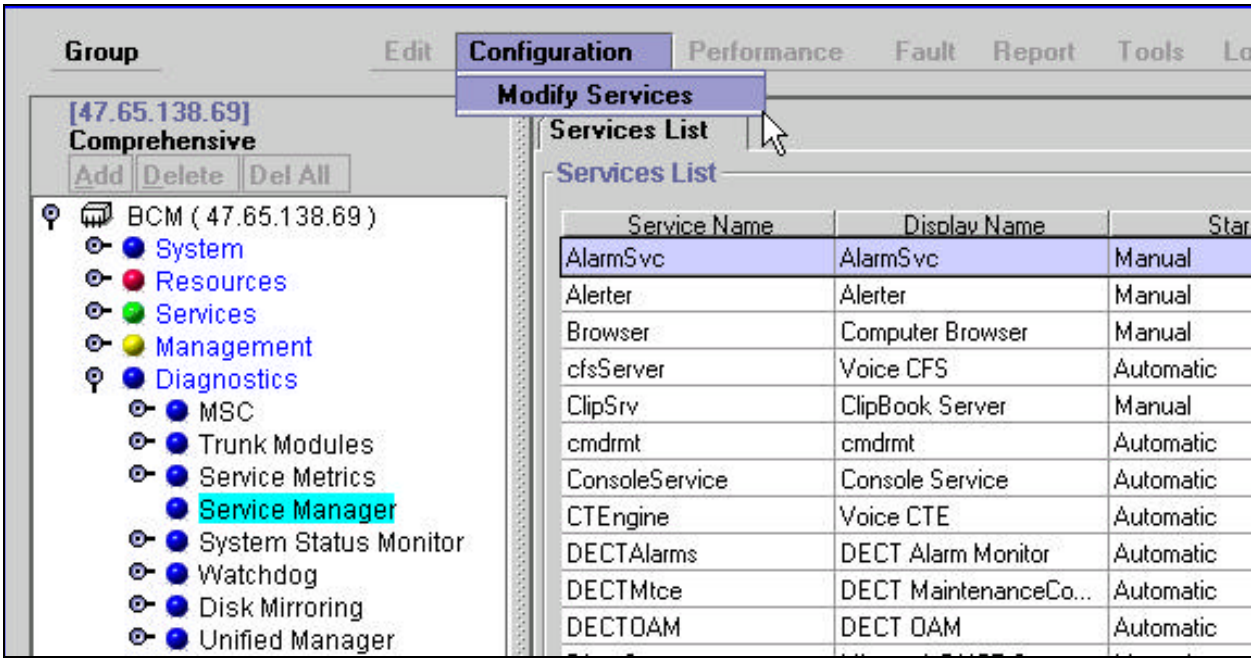
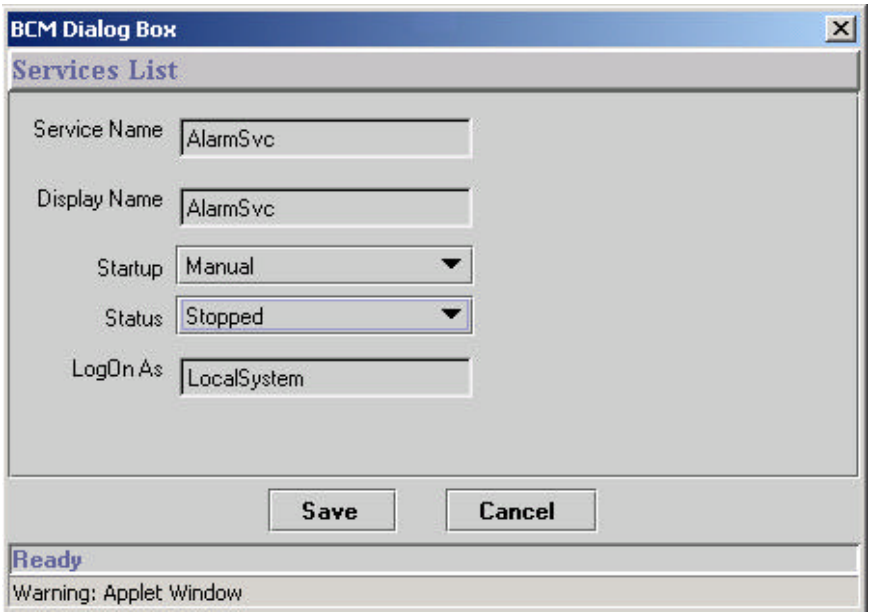


Figure 31 Services list dialog box



4 Modify the service **Startup** if required. Choose how you want the system software to activate the service. Startup attribute values are: Automatic, Manual or Disabled.

- Automatic service activation lets the system start the service during system boot up or restart and does not require user intervention. If a service fails due to a problem event, the system automatically attempts to restart the service. A child service (set to automatic) forces activation for any associated parent service (set to manual). A parent service (set to automatic) cannot force activation for any associated child service (set to manual).

- Manual service activation normally requires user intervention to start the service after system boot-up or restart. If the service experiences a failure due to a problem event, the system automatically attempts to restart the service. The service starts only in a time of need (if it's a dependency service, for example).
- Disabled service cannot be started, even by the system, without user intervention

Warning:
Ensure you understand the implications of any modifications before you change service settings on your system. Call Nortel Networks Support before you modify any service.

5 Modify the service **Status**, if required. Choose the current operational status of the service. Status attribute values are: Start, Stop or Stopped.

- Start service status activates the service immediately
- Stop service status discontinues the service immediately
- Stopped service status

6 Click the **Save** button to save your changes.

Accessing services and driver status reports

You generate reports of the system services status from the Unified Manager Maintenance page. The reports can be created for all services, or filtered by whether the service or driver is running or disabled.

Access the Maintenance page to obtain more information on the status of the services and drivers currently running on Business Communications Manager. Use the procedure in this section to access the Maintenance page and produce a report on the status of the services and drivers from Unified Manager.

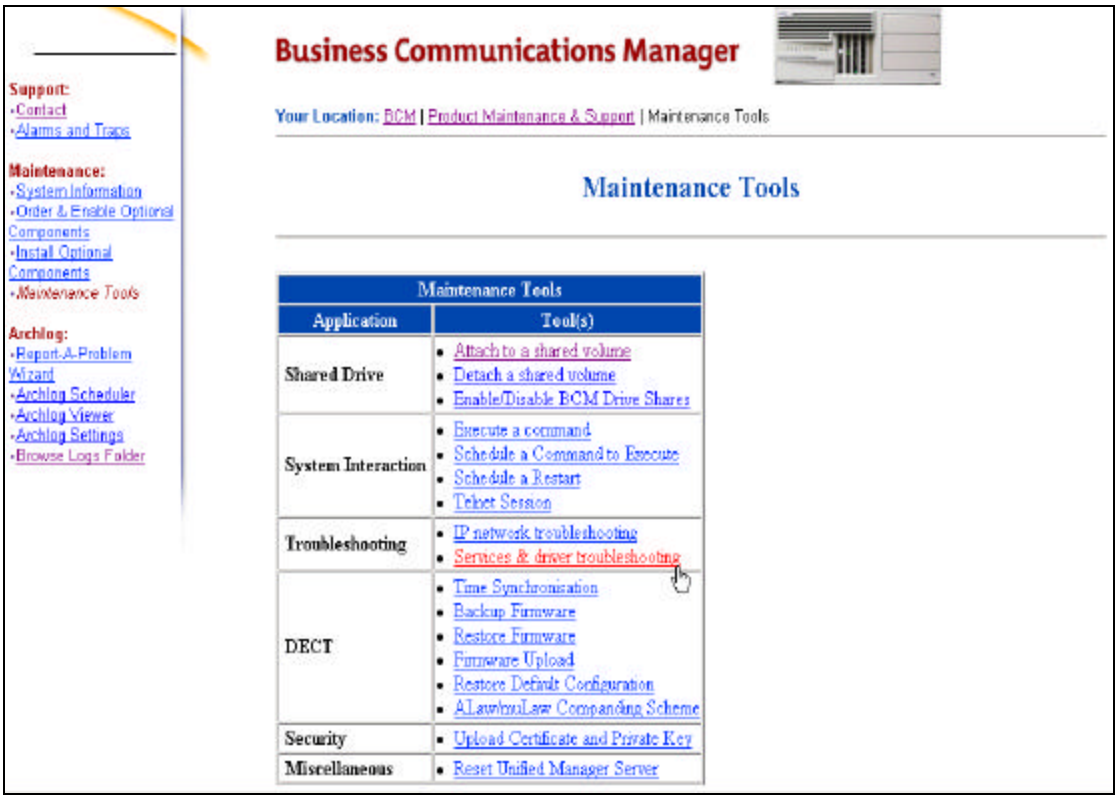
Report options

- All services status
- Automatic services status
- Non-started automatic services
- All running services
- All disabled services
- All drivers status
- Automatic drivers status
- Non-started automatic drivers
- All running drivers
- All disabled drivers
- All drivers and services status

To access the Unified Manager maintenance page

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager main page click the **Maintenance** icon.
3. In the Enter Network Password dialog box, type your network administrator user ID and password and click the **OK** button.
   The Product Maintenance and Support page appears.
4. Under the **Maintenance h**eading click the **Maintenance Tools** link.
   The Maintenance Tools page appears.

Figure 32 Product maintenance and support page - Maintenance tools



5 From the **Troubleshooting** row select **Services & driver troubleshooting**.
From the list box select from a list box the services and drivers you want a report on and click the **Execute** button.

Figure 33 Services and drivers list

Service Definitions

The descriptions and definitions in this section provide essential information for you to understand the purpose and system dependencies for each service. Each definition describes the service properties and corresponding event or alarm notifications. Use the definitions to analyze and diagnose system alarms or events and perform appropriate corrective actions.

The system definitions apply to both System -level services and the Nortel Networks Configurable services. See System-level services for a summary of the System-level services.
See Nortel Networks configurable services for a summary of the Nortel Networks configurable services.

Warning:
Make sure you understand the implications of modifications before you change service settings on your system. Call Nortel Networks Support before you modify any service.

Many services have a hierarchical structure and parent/child dependencies on each other. If a parent service stops, the associated child services are discontinued. If a child service stops or fails, the parent service continues without interruption. Some services have parallel relationships, such as a service component that branches to two or more different services. The system generates an alarm or event notification if a service is stopped through administrator action or through a fault. See “Alarm Analysis and Clearing Procedures” on page 89.

Service definition properties

Each service definition describes the properties and corresponding event, alarm and log notifications. Each definition has a display and service name.

The display name appears in the Unified Manager system manager interface and is shown as the title in the service descriptions. The service name is used at the code-level of the software. The display and service names also appear in the events and logs.

A hierarchy map, appearing below the service descriptions, displays all parent/child dependencies. The hierarchy map shows the service names. Each definition contains cross-references to other dependant services, events, logs and alarm information. Select a cross reference as required to view the descriptions. Use the service definitions to analyze, diagnose and correct (if necessary) the alarm, SNMP Trap and log notifications.

Service definitions contain

- summary
- service type (system-level or Nortel Networks configurable service)
- display and system code names
- default status setting
- default startup setting
- MSC or NT event cross reference
- log cross reference
- Alarm cross reference
- hierarchy map

System-level service definitions

System-level services are software processes that are critical to essential operating system level features. Do not modify the system level services unless explicitly instructed by Nortel Networks support groups. Use this section for information purposes only.

See System-level services for a summary of the system-level services.
See Nortel Networks configurable services for a summary of the Nortel Networks configurable services.

Warning:
Make sure you understand the implications of modifications before you change service settings on your system. Call Nortel Networks Support before you modify any service.

Select a display name from the table to display the full service description.

Table 15 System-level services

Display name (Service name)	Default status/ startup
Alerter (Alerter)	Stopped/Manual
ClipBook server (ClipSrv)	Stopped/Manual
COM + Event System (EventSystem)	Stopped/Manual
Computer Browser (Browser)	Stopped/Manual
EventLog (EventLog)	Running/Automatic
Firebird Guardian Service (InterBaseGuardian)	Running/Automatic
Firebird Server (InterBaseServer)	Running/Manual
License logging service (LicenseService)	Stopped/Manual
Messenger (Messenger)	Running/Automatic
MSDTC (MSDTC)	Stopped/Manual
MSSQLServer (MSSQLServer)	Stopped/Manual
MSSQLServerADHelper (MSSQLServerADHelper)	Stopped/Manual
Multi-dialup manager (DialMgr)	Running/Automatic
NetIQ AppManager client communication manager (NetIQccm)	Stopped/Disabled
NetIQ AppManager client resource manager (NetIQmc)	Stopped/Disabled
Network DDE (NetDDE)	Stopped/Manual
Network DDE DSDM (NetDDEdsdm)	Stopped/Manual
Net logon (Netlogon)	Stopped/Manual
Network monitor agent (nmagent)	Stopped/Manual
NSACD (NSACD)	Running/Automatic
NT LM Security support provider (NtLmSsp)	Running/Manual

Display name (Service name)	Default status/ startup
Remote access connection manager (RasMan)	Running/Manual
Remote access server (RemoteAccess)	Stopped/Manual
Remote procedure call locator (RPCLOCATOR)	Stopped/Manual
Remote procedure call service (RpcSs)	Running/Automatic
Routing and remote access service (Router)	Running/Automatic
Serial port manager (CMDRMT)	Running/Automatic
Server (LanmanServer)	Running/Automatic
Services Monitor (ServicesMon)	Running/Automatic
Spooler (Spooler)	Stopped/Manual
SQLServerAgent (SQLServerAgent)	Stopped/Manual
SSH Secure Shell 2 (SSHSecureShell2Server)	Running/Automatic
Survivable remote gateway (SRG)	Running/Automatic
System event notification (SENS)	Stopped/Manual
Task scheduler (Schedule)	Running/Automatic
TCP/IP NetBIOS helper (LmHosts)	Running/Automatic
Tomcat (Tomcat)	Running/Automatic
UPS - APC Powerchute plus (UPS)	Stopped/Manual
UPS Console Toggle (UPSConsoleToggle)	Stopped/Automatic
Voice Licensing services (LSManager)	Running/Automatic
VNC server (winvnc)	Running/Manual
Windows installer (MSIServer)	Stopped/Manual

Table 15 System-level services

Display name (Service name)	Default status/ startup	Display name (Service name)	Default status/ startup
Plug and play (PlugPlay)	Running/Automatic	Windows internet name service (Wins)	Stopped/Manual
Protected storage (ProtectedStorage)	Running/Automatic	Windows management (WinMgmt)	Running/Automatic
Qos_flt_init (Qos_flt_init)	Stopped/Automatic	Workstation (LanmanWorkstation)	Running/Automatic
RDS self-certifying (rdscert)	Stopped/Disabled	World wide web publishing service (W3SVC)	Stopped/Manual
Remote access autodial manager (RasAuto)	Stopped/Manual		

Alerter

Alerter	The Alerter service distributes administrative notices to users. Alerter messages initiated by the network administrator, are pop-up notifications or pre-determined network information. Use the Alert box under Server properties to enter alert text. Nortel Networks recommends that you disable the Alerter service on your Business Communications Manager due to its NetBIOS dependency and infrequent usage. The Alerter service requires the Messenger and Workstation services to be started and relies on NetBIOS over TCP/IP for network communication.
Type	System-level services
Service name:	Alerter
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Alerter - service structure:

Parent	Child
TDI ▲ └ – – Workstation ▲ └ – – **Alerter**	None

ClipBook server

ClipBook server	The ClipBook service provides support for the Clipbook Viewer. This server service allows sharing of the contents of the clipboard over a network. The service gives remote access to the source machine's clipboard from the target computer's Clipbook viewer. Nortel Networks recommends you disable this service due to the possibility of remote intrusion. The ClipBook server service relies on NetBIOS over TCP/IP for network communication.
Type	System-level services
Service name:	ClipSrv
Default status:	Stopped
Default startup:	Manual
Alarms:	None

ClipBook server - service structure:

Parent	Child
Network DDE DSDM Network DDE **ClipBook Server**	None

COM + Event System

COM + Event System	The Component Object Model (COM) + Event system service provides automatic distribution of event notification to subscribing (Component Object Model) COM components. The service extends the COM+ programming model to support late-bound events or method calls between the publisher or subscriber and the event system. Instead of repeatedly polling the server, the event system notifies interested parties as information becomes available. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	EventSystem
Default status:	Stopped
Default startup:	Manual
Alarms:	None

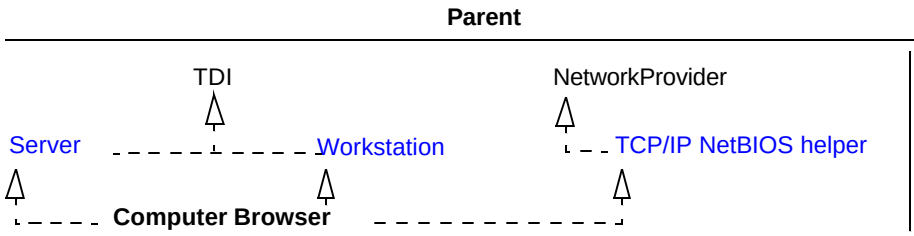
EventSystem - service structure

Parent	Child
Remote procedure call service **COM + Event system**	**COM + Event system** System event notification

Computer Browser

Computer Browser	The Computer Browser service collects the names of NetBIOS resources on the network. The service creates a list so the workstation can participate as a master browser or basic browser (one that takes part in browser elections). Any PC on the network can be the master browser. With the Computer Browser service you can view, through Network Neighborhood & Server Manager, the list of NetBIOS resources (computers). When active on a Business Communications Manager server, the server registers its system name through a NetBIOS broadcast or directly to a WINS server. Nortel Networks recommends that you disable this service.
Type	System-level services
Service name:	Browser
Default status:	Stopped
Default startup:	Manual
Alarms:	Browser

Computer Browser - service structure:



EventLog

EventLog	The EventLog service supports recording of three events categories: System, Security, and Application. The events recorded can be viewed under the system tool Event Viewer (eventvwr.exe). The service is responsible for logging activity on the server, including security activity. Errors, events, security, alarms are recorded using this service. Alarm, SNMPTrap service applications are affected if the service is down.
Type	System-level services
Service name:	EventLog
Default status:	Running
Default startup:	Automatic
Alarms:	• eventLog • Security

EventLog - service structure:

Parent	Child
None	**EventLog** SNMP Trap service SNMP

Firebird Guardian Service

Firebird Guardian Service	The Firebird Guardian service provides an on-board database engine.
Type	System-level services
Service name:	InterBaseGuardian
Default status:	Running
Default startup:	Automatic
Alarms:	None

Firebird guardian service - service structure:

Parent	Child
None	None

Firebird Server

Firebird Server	The Firebird Server service provides an on-board database engine.
Type	System-level services
Service name:	InterBaseServer
Default status:	Running
Default startup:	Manual
Alarms:	None

Firebird Server - service structure:

Parent	Child
None	None

License logging service

License logging service	The Licence Logging service tracks use of client access licenses by applications such as IIS, terminal services and file or print services. The licensed services typically reside on a server or domain controller. If disabled, user access is no longer tracked. Licensing for applications continues to work properly. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	LicenseService
Default status:	Stopped
Default startup:	Manual
Alarms:	None

LicenseService - service structure

Parent	Child
None	None

Messenger

Messenger	The Messenger service is similar to the Alerter service in design and function. The service processes the delivery of pop-up messages sent by the Alerter service or an administrator. Messages appear on the target machine. The user must select OK to accept the message. This service is also required to receive any messages sent by the Messenger service from another machine. Little or no effect on the system if the service is down. The Messenger service relies on NetBIOS over TCP/IP for network communication.
Type	System-level services
Service name:	Messenger
Default status:	Running
Default startup:	Automatic
Alarms:	None

Messenger - service structure

Parent	Child
TDI NetBios Workstation **Messenger**	None

MSDTC

MSDTC	The MSDTC service is a database used for Call Center components.
Type	System-level services
Service name:	MSDTC
Default status:	Stopped
Default startup:	Manual
Alarms:	None

MSDTC - service structure

Parent	Child
None	None

MSSQLServer

MSSQLServer	The MSSQLServer service is a database used for Call Center components.
Type	System-level services
Service name:	MSSQLServer
Default status:	Stopped
Default startup:	Manual
Alarms:	None

MSSQLServer - service structure

Parent	Child
None	None

MSSQLServerADHelper

MSSQLServerADHelper	The MSSQLServerADHelper service is a database used for Call Center components.
Type	System-level services
Service name:	MSSQLServerADHelper
Default status:	Stopped
Default startup:	Manual
Alarms:	None

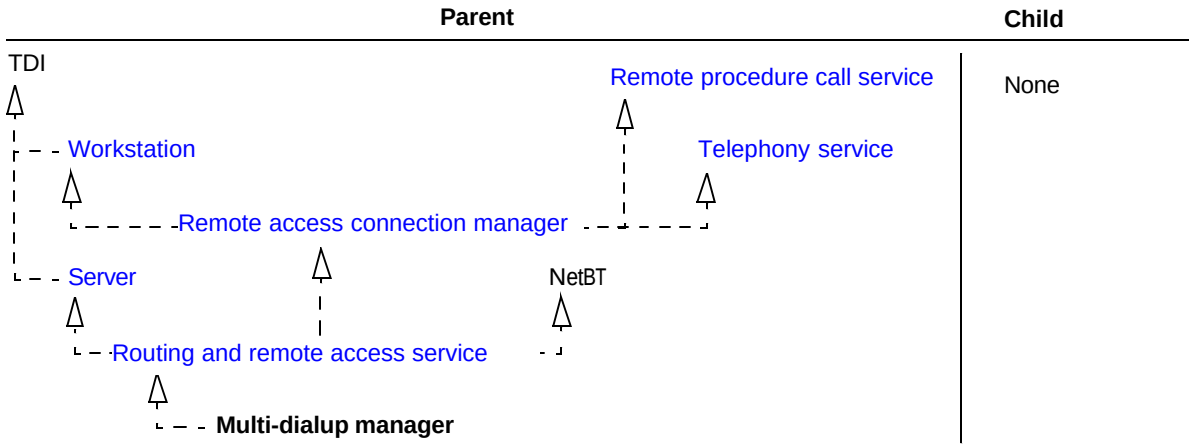
MSSQLServerADHelper - service structure

Parent	Child
None	None

Multi-dialup manager

Multi-dialup manager	The Multi-dialup manager service is used for dialup interfaces on Business Communications Manager's data side. V.90 and ISDN dialup interfaces rely on this service. If V.90 or ISDN dialup connections are not working this could be an issue. Typically this service is not configured.
Type	System-level services
Service name:	DialMgr
Default status:	Running
Default startup:	Automatic
Alarms:	None

Multi-dialup manager - service structure:



NetIQ AppManager client communication manager

NetIQ AppManager client communication manager	The NetIQ AppManager client communication manager service is an optionally enabled system monitoring component.
Type	System-level services
Service name:	NetIQccm
Default status:	Stopped
Default startup:	Disabled
Alarms:	• NetIQccm • NetIQmc • NetIQObjMgr

NetIQ AppManager client communication manager - service structure

Parent	Child
None	None

NetIQ AppManager client resource manager

NetIQ AppManager client resource manager	The NetIQ AppManager client resource manager service is an optionally enabled system monitoring component.
Type	System-level services
Service name:	NetIQmc
Default status:	Stopped
Default startup:	Disabled
Alarms:	None

NetIQ AppManager client resource manager - service structure

Parent	Child
None	None

Network DDE

Network DDE	The Network DDE (Dynamic Data Exchange) service supports network transport of DDE connections. The service provides network transport and security functionality for DDE by applications running on the same computer or on remote computers. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	NetDDE
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Network DDE - service structure

Parent	Child
Network DDE DSDM △ └ _ _ **Network DDE**	**Network DDE** △ └ _ _ ClipBook server

Network DDE DSDM

Network DDE DSDM	The Network DDE DSDM (Dynamic Data Exchange Share Database Manager) service provides dynamic data exchange. DDE is used for applications such as chat and is not essential for Business Communications Manager functionality. The Network DDE service requires this service to be started. Nortel Networks recommends that you do not disable this service.
Type	System-level services

Service name:	NetDDEdsdm
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Network DDE DSDM - service structure

Parent	Child
None	**Network DDE DSDM** Network DDE ClipBook server

Net logon

Net logon	The Net Logon service is responsible for network authentication and is used by Server and Workstation to provide for user authentication. Authentication processes include these sub-components: • maintaining a synchronized domain directory database between the PDC and BDC(s) • handling authentication of respective accounts on the domain controller • processing authentication of domain accounts on networked machines If the Net Logon service is down, you can't access the operating system.
Type	System-level services
Service name:	Netlogon
Default status:	Stopped
Default startup:	Manual
Alarms:	• NetLogon • Service Control Manager

Net logon - service structure

Parent	Child
TCP/IP NetBIOS helper Server **Net Logon**	None

Network monitor agent

Network monitor agent	The Network monitor agent service is a tool used by Nortel Networks support teams. It captures data packets for analysis purposes, and is not user accessible.
Type	System-level services
Service name:	nmagent
Default status:	Stopped

Default startup: Manual

Alarms: None

Network monitor agent - service structure

Parent	Child
BH △ **Network monitor agent**	None

NT LM Security support provider

NT LM Security support provider: The NT LM Security support provider service assists with backward compatibility and authentication with older DOS versions.

It extends NT security to Remote Procedure Call (RPC) programs using various transports other than named pipes.

The server experiences a loss in DNS cache if this service is down.

Type: System-level services

Service name: NtLmSsp

Default status: Running

Default startup: Manual

Alarms: None

NT LM Security support provider - service structure

Parent	Child
None	**NT LM security support provider** △ Windows internet name service World wide web publishing service FTP Publishing service Microsoft DNS server Microsoft DHCP server

NSACD

NSACD: The NSACD (Norstar Automated Call Distribution) service is used for Multimedia Call Center. If you have purchased Multimedia Call Center and it is not functioning, check to ensure this service is operational.

Type: System-level services

Service name: NSACD

Default status: Running

Default startup:	Automatic
Alarms:	NSACD

NSACD - service structure

Parent	Child
None	None

Plug and play

Plug and play	The Plug and play service is used to detect and configure plug & play (PnP) hardware devices (such as a video card).
Type	System-level services
Service name:	PlugPlay
Default status:	Running
Default startup:	Automatic
Alarms:	• NSACD • Service Control Manager

Plug and play - service structure

Parent	Child
None	None

Protected storage

Protected storage	The Protected storage service provides secure storage for sensitive data and prevents access by unauthorized services processes or users. Protected Storage is a set of software libraries that let applications fetch and retrieve security and other information from a personal storage location, while hiding the implementation and details of the storage itself. The Protected storage service encrypts and stores: • SSL certificates • application passwords (Outlook, Outlook Express) • information stored by Profile Assistant • information maintained by MS Wallet • digitally signed S/MIME keys This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	ProtectedStorage
Default status:	Running
Default startup:	Automatic
Alarms:	None

Protected storage - service structure

Parent	Child
Remote procedure call service ▲ └ – – **Protected storage**	**Protected storage** ▲ └ – – RDS self-certifying

Qos_flt_init

Qos_flt_init	The QoS_flt_init (Quality of service driver initialization) service initiates the QoS filters in Unified Manager. If your QoS filters aren't functioning correctly, check the status of this service.
Type	System-level services
Service name:	Qos_flt_init
Default status:	Stopped
Default startup:	Automatic
Alarms:	Qos_flt_init

Quality of service fault initialization - service structure

Parent	Child
Remote procedure call service ▲ └ – – **Qos_flt_init**	None

RDS self-certifying

RDS self-certifying	The Remote data service (RDS) self-certifying service relates to security functions in Internet applications and relies on protected storage. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	rdscert
Default status:	Stopped
Default startup:	Disabled
Alarms:	None

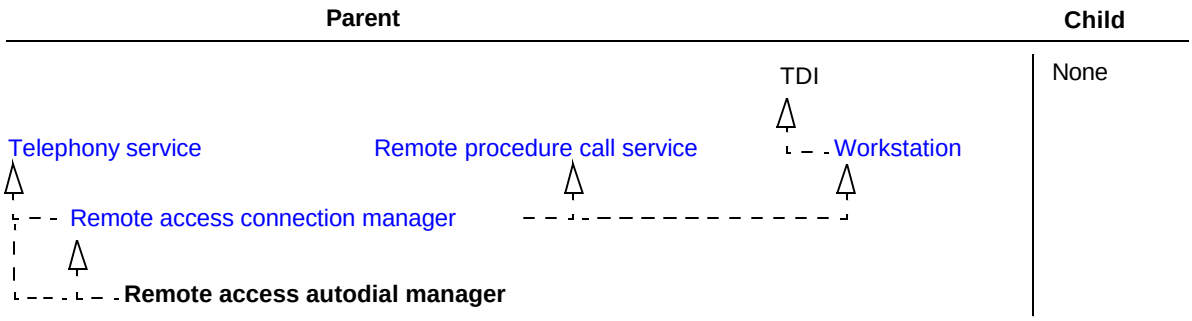
RDS self-certifying - service structure

Parent	Child
Remote procedure call service ▲ └ – – Protected storage ▲ └ – – RDS self-certifying	None

Remote access autodial manager

Remote access autodial manager	The Remote access autodial manager service manages dial-in and dial-out connections. The service initiates the dial-up, procures the resources and parameters, and completes the call.
Type	System-level services
Service name:	RasAuto
Default status:	Stopped
Default startup:	Manual
Alarms:	None

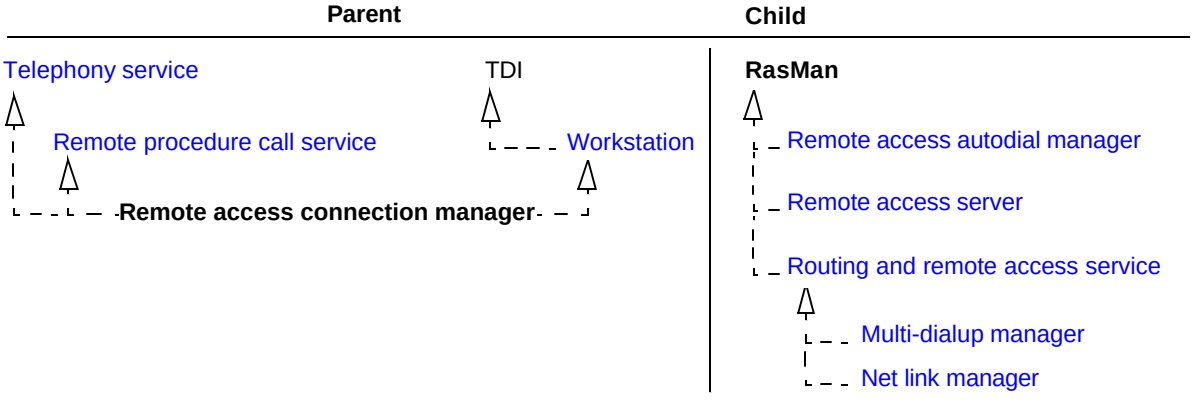
Remote access autodial manager - service structure



Remote access connection manager

Remote access connection manager	The Remote access connection manager service manages dial-in and dial out connections. The service initiates the dial-up, procures the resources and parameters, and performs the call.
Type	System-level services
Service name:	RasMan
Default status:	Running
Default startup:	Manual
Alarms:	Service Control Manager

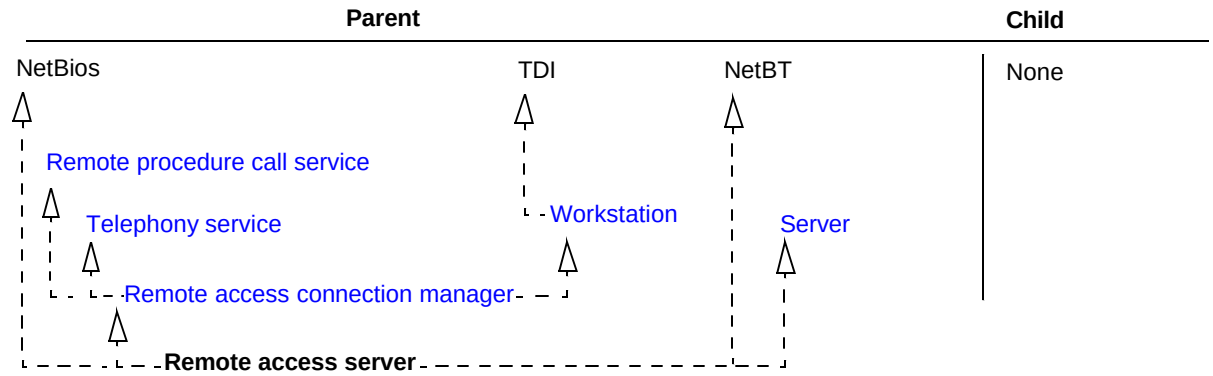
Remote access connection manager - service structure



Remote access server

Remote access server	The Remote access server manages dial-in and dial-out connections.
Type	System-level services
Service name:	RemoteAccess
Default status:	Stopped
Default startup:	Manual
Alarms:	None

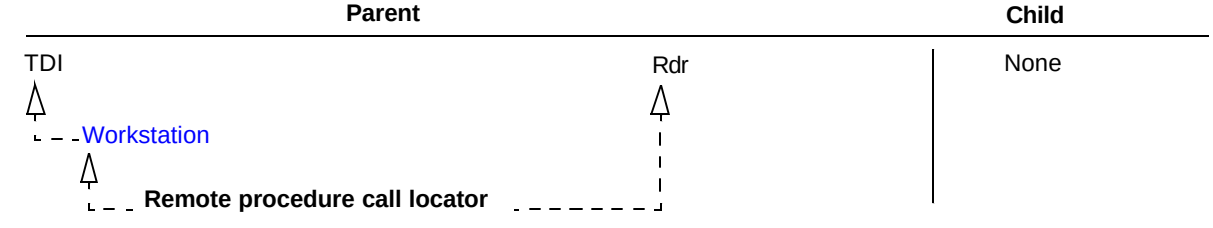
Remote access server - service structure



Remote procedure call locator

Remote procedure call locator	The Remote procedure call (RPC) locator service is a protocol used to encapsulate function calls over a network. Features like LAN CTE require the RPC locator service. In a distributed network, the server partially registers its status with the RPC name server database. Clients query the database to locate available server applications. The service maintains the RPC name server database, and requires the RPC service to be started. Nortel Networks recommends that you do not disable this service.
Type	System-level services
Service name:	RPCLOCATOR
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Remote procedure call locator server - service structure



Remote procedure call service

Remote procedure call service	The Remote procedure call (RPC) service enables function calls over a network and operates in tandem with the Remote procedure call (RPC) locator service. The RPC service is fundamental to the operations of any RPC system activities. Nortel Networks recommends that you do not disable this service.
Type	System-level services
Service name:	RpcSs
Default status:	Running
Default startup:	Automatic
Alarms:	None

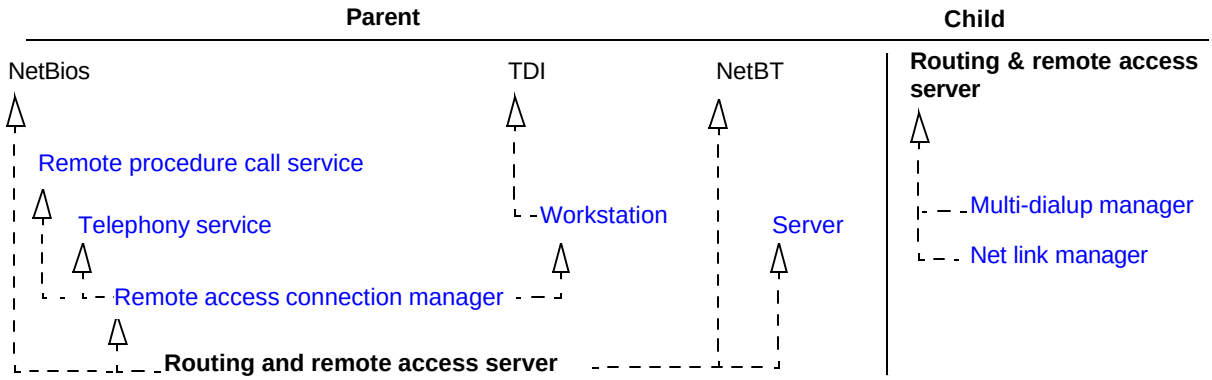
Remote procedure call service - service structure

Parent	Child
None	**Remote procedure call service** Alarm service Protected storage RDS self-certifying Task scheduler TIntsvr Qos_flt_init Windows management Remote access connection manager Remote access autodial manager Remote access server Routing and remote access service Multi-dialup manager Net link manager World wide web publishing service FTP Publishing service Windows internet name service Microsoft DNS server Voice Net QoS monitor VoIP Gateway VoIP SIP Gateway Microsoft DHCP server COM + Event System System event notification Policy service System status monitor Voice management subsystem

Routing and remote access service

Routing and remote access service	The Routing and remote access service manages the IP/IPX routing in the BCM as well as dial-in connections. All the routing & dial-up connections rely on this service.
Type	System-level services
Service name:	Router
Default status:	Running
Default startup:	Automatic
Alarms:	• IPXRouterManager • Router

Routing and remote access server - service structure



Serial port manager

Serial port manager	The Serial port manager service controls the telnet session environment (interfaces with a PC). Use this service to initiate a telnet session for startup or maintenance purposes.
Type	System-level services
Service name:	CMDRMT
Default status:	Running
Default startup:	Automatic
Alarms:	Standard NT alarm event?

Serial port manager - service structure:

Parent	Child
None	None

Server

Server	The Server service acts as the key to all server-side NetBIOS applications and provides support for print, file, and named pipe sharing through the SMB services. The service is a subsystem for NT sharing (directories and printers). Network level inbound communication logon services are affected. Backup services are affected.
Type	System-level services
Service name:	LanmanServer
Default status:	Running
Default startup:	Automatic
Alarms:	None

Server - service structure

Parent	Child
TDI **Server**	**Server** Computer Browser Routing and remote access service Net link manager Multi-dialup manager Remote access server

Services Monitor

Services Monitor	The Services monitors service monitors the services status and logs information.
Type	System-level services
Service name:	ServicesMon
Default status:	Running
Default startup:	Automatic
Alarms:	None

Services Monitor - service structure

Parent	Child
None	None

Spooler

Spooler	The Spooler service is the NT printing subsystem and lets the local system spool jobs to a network printer. The service accepts client print requests, stores and sends print tasks (one at a time) to the specified print devices. Nortel Networks recommends this service be set to automatic.
Type	System-level services
Service name:	Spooler
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Spooler - service structure

Parent	Child
None	None

SQLServerAgent

SQLServerAgent	The SQLServerAgent service is a database used for Call Centre components.
Type	System-level services
Service name:	SQLServerAgent
Default status:	Stopped
Default startup:	Manual
Alarms:	None

SQLServerAgent - service structure

Parent	Child
None	None

SSH Secure Shell 2

SSH Secure Shell 2	The SSH Secure Shell 2 service provides an SSH Shell into BCM.
Type	System-level services
Service name:	SSHSecureShell2Server
Default status:	Running
Default startup:	Automatic
Alarms:	None

SSH Secure Shell 2 - service structure

Parent	Child
None	None

Survivable remote gateway

Survivable remote gateway	The survivable remote gateway service provides the SRG mode.
Type	System-level services
Service name:	SRG
Default status:	Running
Default startup:	Automatic
Alarms:	None

Survivable remote gateway - service structure

Parent	Child
None	**SRG** UNISTIM Terminal proxy server HotDesking

System event notification

System event notification	The System event notification (SENS) service tracks system events such as Windows logon network and power. This service provides notification of such events to COM+ Event System subscribers. SENS is an AutoStarted service. This service is critical to alarm and event notification on the BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	SENS
Default status:	Stopped
Default startup:	Manual
Alarms:	None

System event notification - service structure

Parent	Child
Remote procedure call service △ └ – – COM + Event System △ └ – – **System event notification**	None

Task scheduler

Task scheduler	The Task scheduler service executes an application at a specified time and date.
Type	System-level services
Service name:	Schedule
Default status:	Running
Default startup:	Automatic
Alarms:	Service Control Manager

Task scheduler - service structure

Parent	Child
Remote procedure call service △ └ – – **Task scheduler**	None

TCP/IP NetBIOS helper

TCP/IP NetBIOS helper	The TCP/IP NetBIOS helper service enhances NetBT and the Net Logon service.This service is an alternative to the DNS lookup. The service performs a lookup of the LMHosts file and matches an alias (NetBios name) to an IP address. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	LmHosts
Default status:	Running
Default startup:	Automatic
Alarms:	None

TCP/IP NetBIOS Helper - service structure

Parent	Child
NetworkProvider └ – - **TCP/IP NetBIOS helper**	**TCP/IP NetBIOS helper** └ – - Net logon └ – - Computer Browser

Tomcat

Tomcat	The Tomcat service provides Java servlet capabilities on the BCM.
Type	System-level services
Service name:	Tomcat
Default status:	Stopped
Default startup:	Automatic
Alarms:	None

Tomcat - service structure

Parent	Child
None	None

UPS - APC Powerchute plus

UPS - APC Powerchute Plus	The UPS service provides for the support and management of the Uninterruptable Power Supply (UPS). The UPS is physically connected (local) to the machine.
Type	System-level services
Service name:	UPS
Default status:	Stopped
Default startup:	Manual
Alarms:	UPS

UPS APC Powerchute Plus - service structure

Parent	Child
None	None

UPS Console Toggle

UPS Console Toggle	The UPS Console Toggle service turns the UPS serial port off for 15 minutes to allow for serial configuration (occurs upon system reboot).
Type	System-level services
Service name:	UPSConsoleToggle
Default status:	Running
Default startup:	Automatic
Alarms:	None

UPS Console Toggle - service structure

Parent	Child
None	None

VNC server

VNC server	The Virtual network computing (VNC) diagnostic tool is used by Nortel Network support teams to assist in remote system detection.
Type	System-level services
Service name:	winvnc
Default status:	Stopped
Default startup:	Disabled
Alarms:	VNC Service

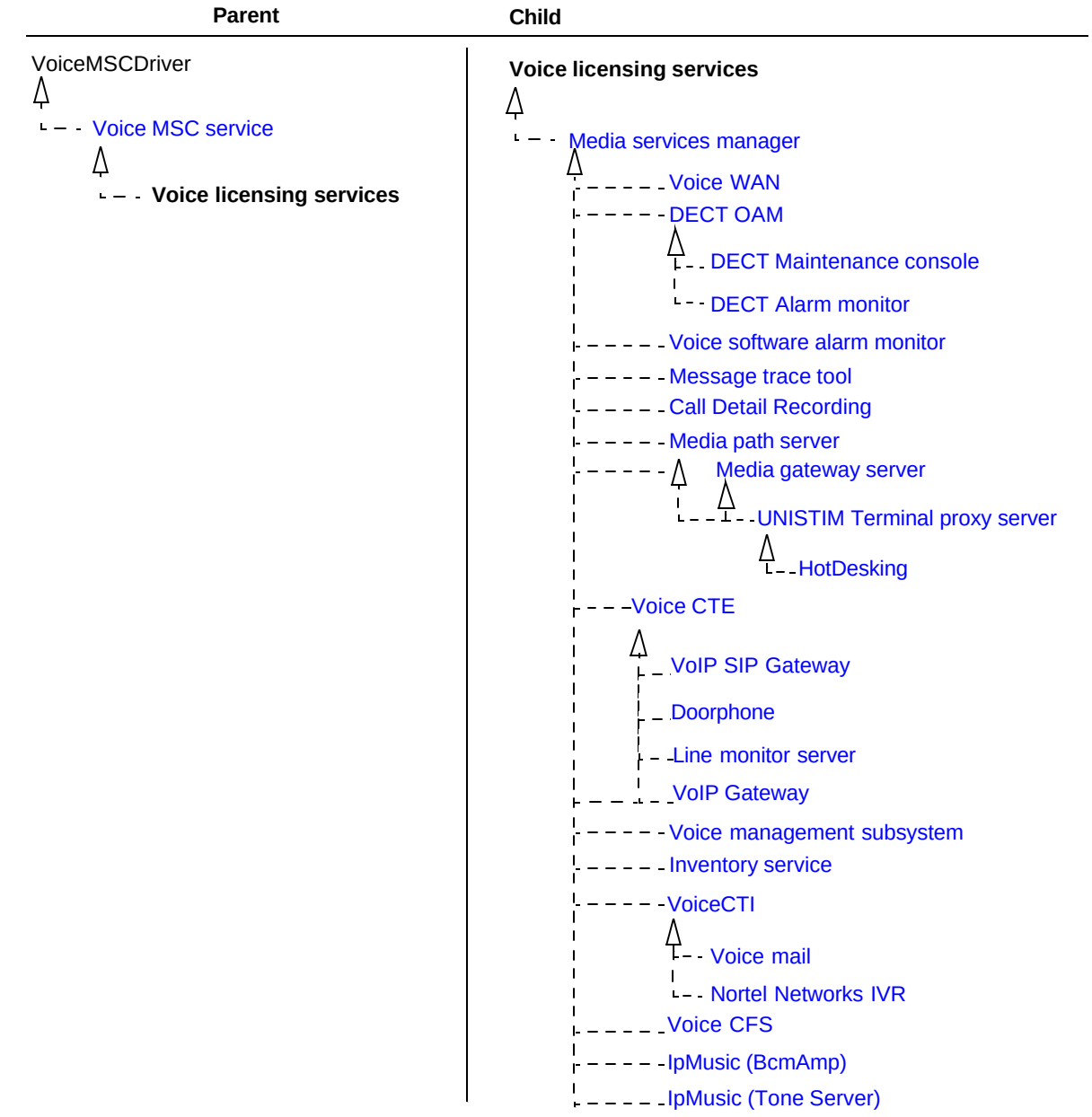
VNC server - service structure

Parent	Child
None	None

Voice Licensing services

Voice Licensing services	The Voice licensing services enables the ability to enter keycodes to the core telephony area of the BCM. If keycode entry doesn't function correctly, check the status of this service.
Type	System-level services
Service name:	LSManager
Default status:	Running
Default startup:	Automatic
Alarms:	cfsServr

Voice Licensing services - service structure



Windows installer

Windows installer	The Windows installer service manages application installations. Little to no impact on BCM.
Type	System-level services
Service name:	MSIServer
Default status:	Stopped
Default startup:	Manual

Alarms: None

Windows Installer - service structure

Parent	Child
None	None

Windows internet name service

Windows internet name service	Windows Internet Naming Service, a system that determines the IP address associated with a particular network computer, also called name resolution.
Type	System-level services
Service name:	Wins
Default status:	Stopped
Default startup:	Manual
Alarms:	Wins

Windows internet name service - service structure

Parent	Child
Remote procedure call service NT LM Security support provider **Windows internet name service**	None

Windows management

Windows management	The Windows Management service is the operating system component that contains the WMI repository.
Type	System-level services
Service name:	WinMgmt
Default status:	Running
Default startup:	Automatic
Alarms:	None

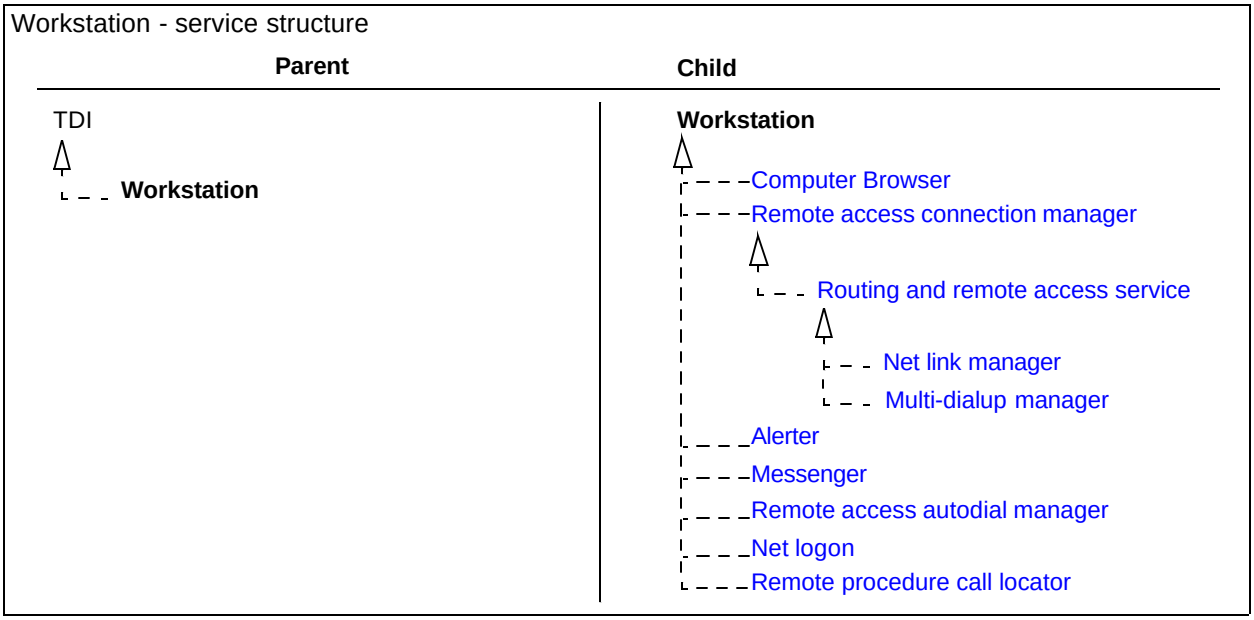
Windows management - service structure

Parent	Child
Remote procedure call service **Windows management**	None

Workstation

Workstation	The Workstation service is needed for communications and network connections and allows for outbound NetBIOS connections. See also the Server service description. Nortel Networks recommends careful consideration when configuring the system name. The system notifies you of duplicate names and fails to start the service.
Type	System-level services
Service name:	LanmanWorkstation
Default status:	Running
Default startup:	Automatic
Alarms:	None

Workstation - service structure



World wide web publishing service

World wide web publishing service	The World wide web publishing service provides HTTP services for Windows platform applications. When disabled, the operating system no longer acts as a Web server. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	System-level services
Service name:	W3SVC
Default status:	Stopped
Default startup:	Manual
Alarms:	None

World wide web publishing service - service structure

Parent	Child
Remote procedure call service NT LM Security support provider **World wide web publishing service**	None

Nortel Networks Configurable Services

Nortel Networks configurable services are software processes that are critical to Business Communications Manager software. Modify the services only when troubleshooting or performing maintenance on Business Communications Manager.

Modify a service only under the direction or guidance of Nortel Networks support. Improper service modification can adversely affect the normal operation of Business Communications Manager.

Warning:
Ensure you understand the implications of any modifications before you change service settings on your system. Call Nortel Networks Support before you modify any service.

See Nortel Networks configurable services for a summary of the Nortel Networks configurable services. Select a Display name from the table to display the full service description.

See System-level services for a summary of the System level services.

Table 16 Nortel Networks configurable services

Display name (Service name)	Default startup/status
Alarm service **(AlarmSvc)**	Stopped/Manual
BCMUpgrade (BCMUpgrade)	Running/Automatic
Call Detail Recording **(VoiceRecord)**	Running/Automatic
Doorphone **(CTEDP)**	Running/Automatic
DECT Alarm monitor **(DECTAlarms)**	Running/Automatic
DECT Maintenance console **(DECTMtce)**	Running/Automatic
DECT OAM **(DECTOAM)**	Running/Automatic
FTP Publishing service **(MSFTPSVC)**	Stopped/Manual

Display name (Service name)	Default startup/status
Policy service **(pep)**	Running/Automatic
PPPoE service **(PPPoEService)**	Stopped/Disabled
SNMP **(Simple network messaging protocol))**	Running/Automatic
SNMP Trap service **(SNMPTRAP)**	Stopped/Manual
System status monitor **(SSM)**	Running/Automatic
Telephony service **T(apiSrv)**	Running/Manual
Tlntsvr **(tlntsvr)**	Running/Automatic
UNISTIM Terminal proxy server **(UTPS)**	Running/Automatic

Table 16 Nortel Networks configurable services

Display name (Service name)	Default startup/status	Display name (Service name)	Default startup/status
HotDesking **(HotDesking)**	Running/Automatic	VBMain **(VBMain)**	Running/Automatic
Inventory service **(InventorySvc)**	Running/Automatic	Voice CFS **(CfsServer)**	Running/Automatic
IpMusic (BcmAmp) (BcmAmp)	Stopped/Manual	Voice CTE **(CTEngine)**	Running/Automatic
IpMusic (Tone Server) (Tone Srvr)	Stopped/Manual	VoiceCTI **(VoiceCTI)**	Running/Manual
IPSecIKE service **(IPSecIKE)**	Running/Automatic	Voice mail **(VoiceMail)**	Running/Automatic
Line monitor server (LMS)	Running/Automatic	Voice management subsystem **(VoiceManagementSubsystem)**	Running/Automatic
Media gateway server **(MGS)**	Running/Automatic	Voice MSC service **(VoiceMSCService)**	Running/Automatic
Media path server **(MPS)**	Running/Automatic	Voice Net QoS monitor **(VoiceNetQoSMonitor)**	Running/Automatic
Media services manager **(EmsManager)**	Running/Manual	Voice NNU diagnostics **(NnuDiagLogger)**	Running/Automatic
Message trace tool **(MTT)**	Running/Automatic	Voice software alarm monitor **(VoiceSW)**	Running/Automatic
Microsoft DHCP server **(DhcpServer)**	Stopped/Manual	Voice time synch **(VoiceTimeSynch)**	Stopped/Manual
Microsoft DNS server **(DNS)**	Running/Automatic	Voice WAN **(VoiceWAN)**	Stopped/Automatic
		Voice watchdog **(voicewatchdog)**	Running/Automatic
Net link manager **(NetLinkManager)**	Running/Automatic	VoIP Gateway **(VoiceNetVoIPGateway)**	Running/Automatic
Nortel Networks IVR **(Nortel Networks startup service)**	Stopped/Manual	VoIP SIP Gateway **(VoIPSIPGateway)**	Running/Automatic
Nortel Networks license service **(Nortel Networks license service)**	Running/Automatic		

Alarm service

Alarm service	The Alarm service provides alarm reporting capability through the local system interface. This service requires you to enable remote procedure call service (RpcSs) first. The Alarm service filters alarms and events from the NT event viewer and categorizes them in the BCM alarm database.
Type	Nortel Networks configurable services
Service name:	AlarmSvc
Default status:	Stopped
Default startup:	Manual
Alarms:	None

Alarm service - service structure

Parent	Child
Remote procedure call service ↑ └ – - **Alarm Service**	None

BCMUpgrade

BCMUpgrade	The BCM Upgrade service checks to see if an upgrade is present or started. If the upgrade exists, the service performs the upgrade.
Type	Nortel Networks configurable services
Service name:	BCMUpgrade
Default status:	Running
Default startup:	Automatic
Alarms:	None

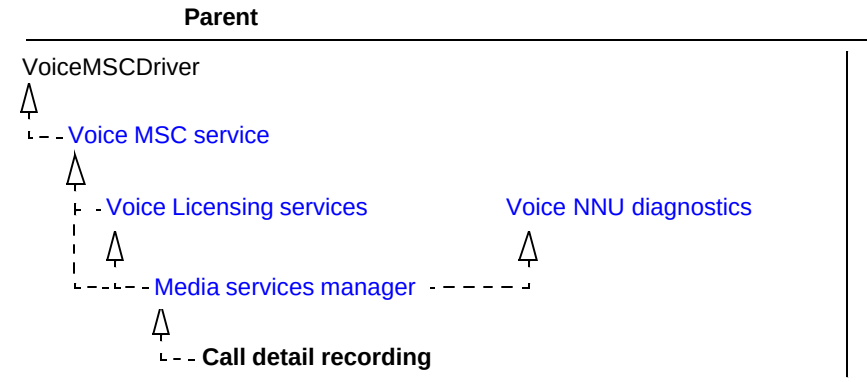
BCM Upgrade service - service structure

Parent	Child
None	None

Call Detail Recording

Call Detail Recording	Call Detail Recording provides CDR information from the core telephony to CDR or 3rd-party call accounting applications. CDR information contains detailed statistical information about calls. such as. length of time and who was on the phone. For more information on CDR see the *CDR Guide* in the documentation.
Type	Nortel Networks configurable services
Service name:	VoiceRecord
Default status:	Running
Default startup:	Automatic
Alarms:	• VoiceRecord • Service Control Manager

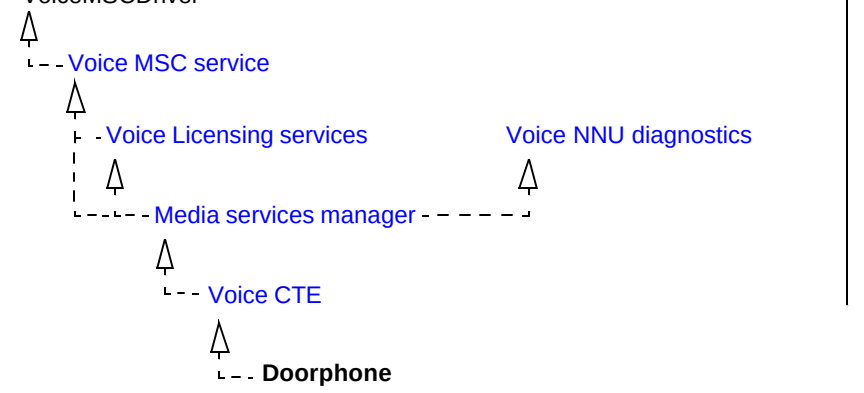
Call detail recording - service structure



Doorphone

Doorphone	The Doorphone service provides doorphone functionality.
Type	Nortel Networks configurable services
Service name:	CTEDP
Default status:	Running
Default startup:	Automatic
Alarms:	None

Doorphone - service structure

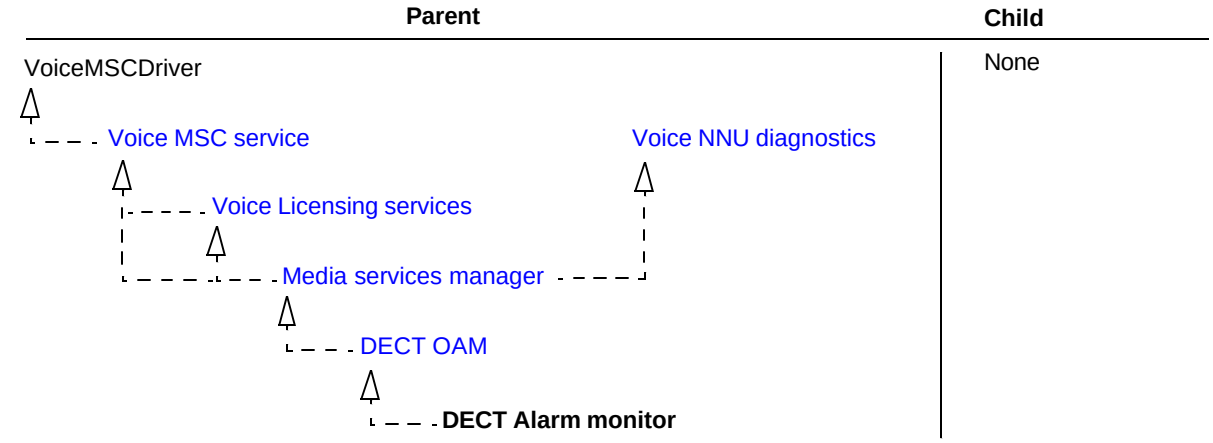


DECT Alarm monitor

DECT Alarm monitor	The DECT alarm monitor service monitors DECT alarms from the DECT media bay module. Any significant events trigger an alarm to the management applications. If you are not receiving alarms from the DECT module, verify the status of this service.
Type	Nortel Networks configurable services

Service name:	DECTAlarms
Default status:	Running
Default startup:	Automatic
Alarms:	• DECTAlarms • Service Control Manager

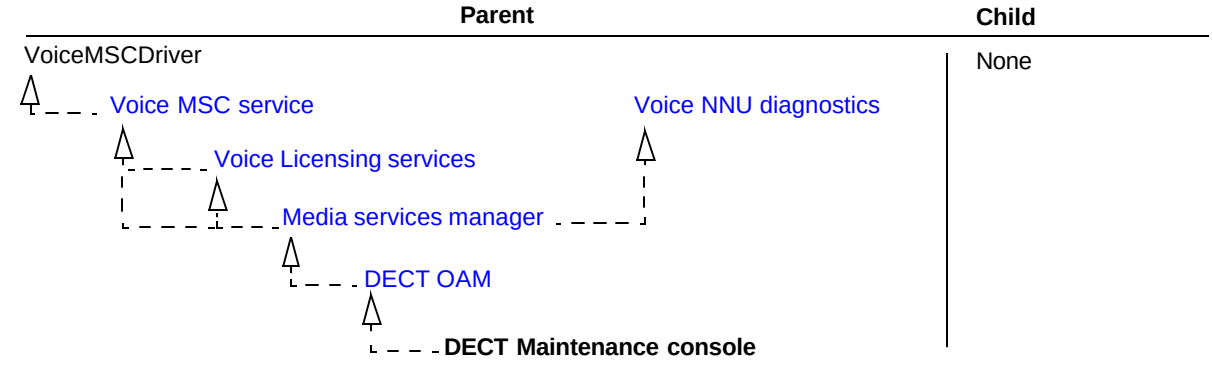
DECT alarm monitor - service structure



DECT Maintenance console

DECT Maintenance console	The DECT maintenance console service enables the maintenance console on the DECT media bay modules. If the management from Unified Manager or the wizards doesn't function correctly, verify the status of this service.
Type	Nortel Networks configurable services
Service name:	DECTMtce
Default status:	Running
Default startup:	Automatic
Alarms:	DECTMtce

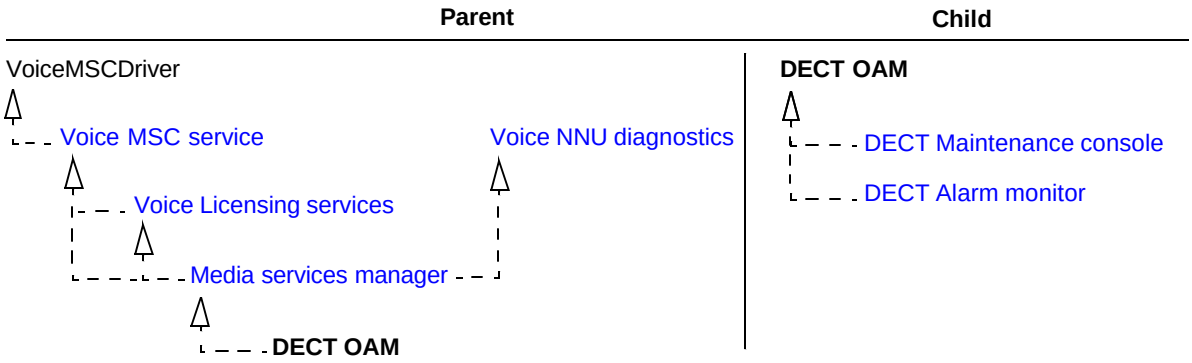
DECT Maintenance console - service structure



DECT OAM

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 Unified Manager. If the management function from Unified Manager or the wizards does not function correctly, verify the status of this service.
Type	Nortel Networks configurable services
Service name:	DECTOAM
Default status:	Running
Default startup:	Automatic
Alarms:	Service Control Manager

DECT OAM - service structure



FTP Publishing service

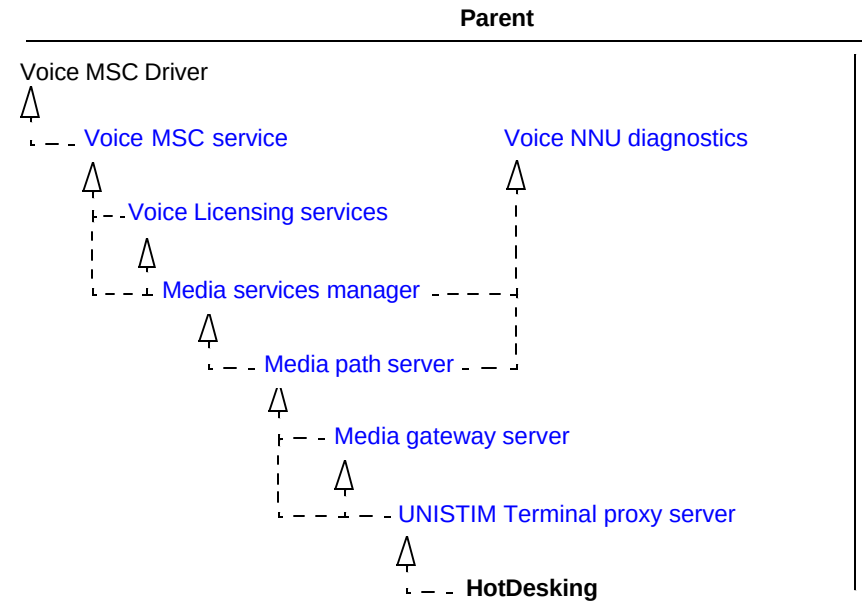
FTP Publishing service	The FTP (file transfer protocol) publishing service provides FTP connectivity and administration through the Internet Information Service (IIS) snap-in. Features include bandwidth throttling, security accounts, and extensible logging. This service is not critical to normal operation of BCM. Nortel Networks recommends you do not change the default status and startup values.
Type	Nortel Networks configurable services
Service name:	MSFTPSVC
Default status:	Stopped
Default startup:	Manual
Alarms:	None

FTP publishing service - service structure

HotDesking

HotDesking	The Hotdesking service lets IP sets use the hot desking feature.
Type	Nortel Networks configurable services
Service name:	HotDesking
Default status:	Running
Default startup:	Automatic
Alarms:	HotDesking

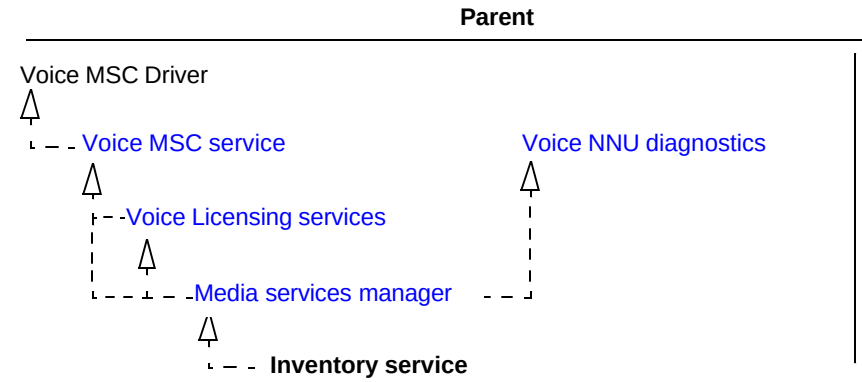
HotDesking - service structure



Inventory service

Inventory service	The Inventory service performs an inventory of system functions and reports information back to Unified Manager.
Type	Nortel Networks configurable services
Service name:	InventorySvc
Default status:	Running
Default startup:	Automatic
Alarms:	Inventory Service

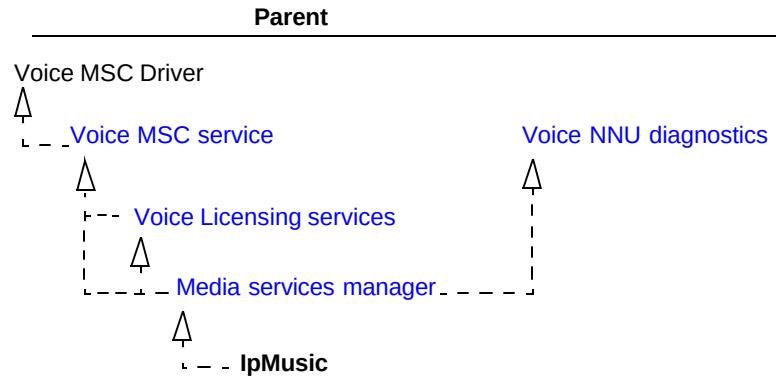
Inventory service - service structure



IpMusic (BcmAmp)

IpMusic	The IpMusic (BcmAmp) service provides an on-board, on-hold music player.
Type	Nortel Networks configurable services
Service name:	BcmAmp
Default status:	Stopped
Default startup:	Manual
Alarms:	BcmAmp

IpMusic (BcmAmp) - service structure



IpMusic (Tone Server)

IpMusic (Tone Server)	The IpMusic (BcmAmp) service provides an on-board, on-hold music to the network or BCMAmp.
Type	Nortel Networks configurable services
Service name:	ToneSrvr
Default status:	Stopped
Default startup:	Manual

Alarms: ToneSrvr

IpMusic (ToneSrvr) - service structure

Parent	Child
Voice MSC Driver Voice MSC service Voice NNU diagnostics Voice Licensing services Media services manager **IpMusic (ToneSrvr)**	None

IPSecIKE service

IPSecIKE service	The Internet protocol security - Internet key exchange (IPSecIKE) service manages the IPSec Internet Key Exchange (IKE) for the BCM IPSec security function. If IPSec clients or tunnels do not initiate or function correctly, check the status of this service.
Type	Nortel Networks configurable services
Service name:	IPSecIKE
Default status:	Running
Default startup:	Automatic
Alarms:	IPSecIKE

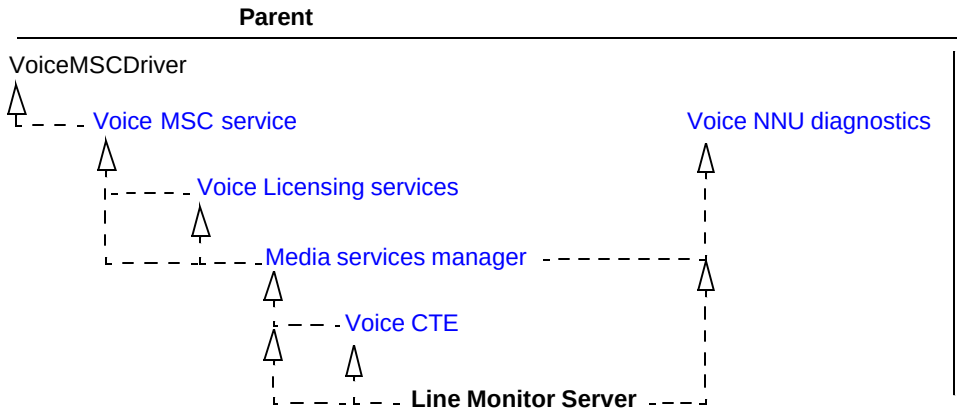
IPSecIKE Service - service structure

Parent	Child
None	None

Line monitor server

Line Monitor Server	The Line Monitor Server service provides line status information to BCM monitor.
Type	Nortel Networks configurable services
Service name:	LMS
Default status:	Running
Default startup:	Automatic
Alarms:	None

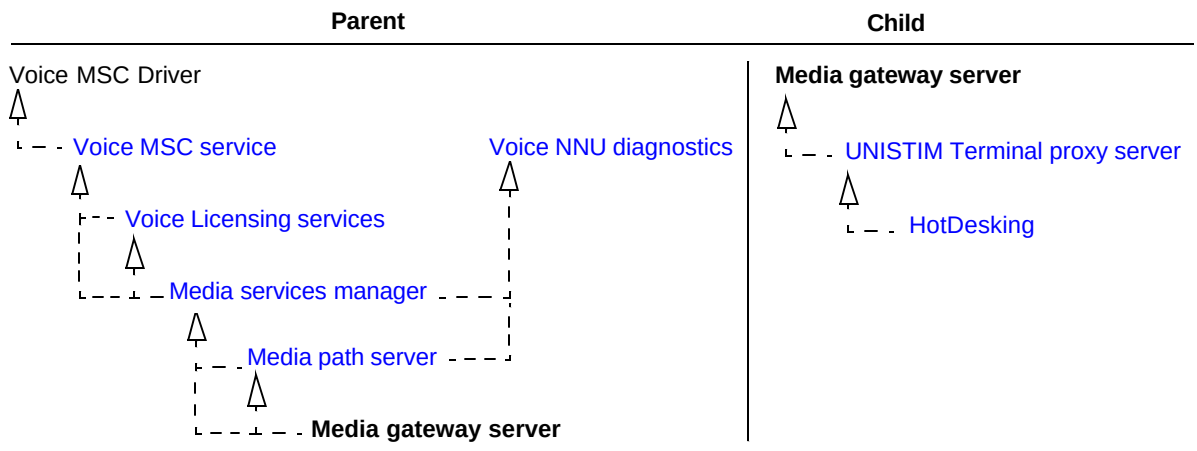
Line Monitor Server - service structure



Media gateway server

Media gateway server	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.
Type	Nortel Networks configurable services
Service name:	MGS
Default status:	Running
Default startup:	Automatic
Alarms:	• MGS • Service Control Manager

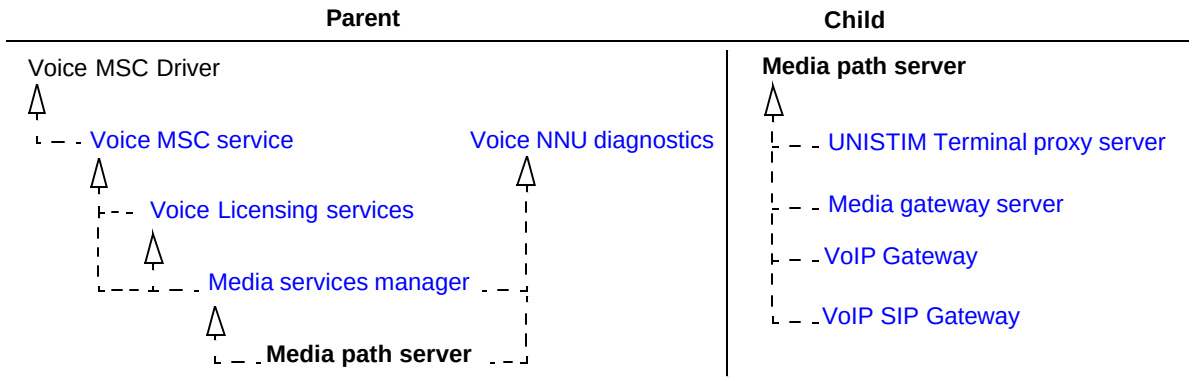
Media gateway server - service structure



Media path server

Media path server	The Media path server is an NT service that manages the allocation of media paths over the IP network.
Type	Nortel Networks configurable services
Service name:	MPS
Default status:	Running
Default startup:	Automatic
Alarms:	• MPS • Service Control Manager

Media path server - service structure



Media services manager

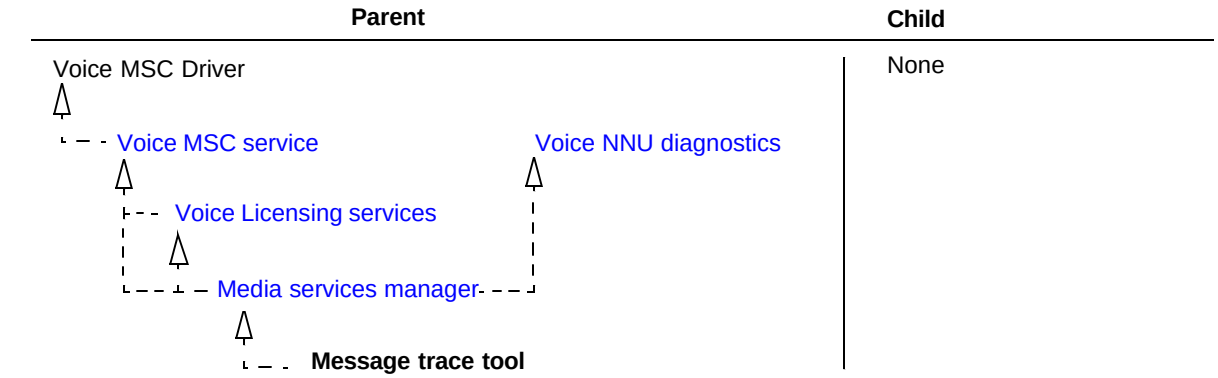
Media services manager	The Media services manager is responsible for management of resources (signaling channels, media channels, DSP tasks, application identifiers): • allocation of resources to applications • configuration of media transport driver modules • transport of signaling data and application related tasks
Type	Nortel Networks configurable services
Service name:	EmsManager
Default status:	Running
Default startup:	Manual
Alarms:	• emsManager • Service Control Manager

Media services manager - service structure

Message trace tool

Message trace tool	The Message trace tool service is a logging utility that records all telephony traffic information. The service is primarily used for problem diagnosis by support staff and designers.
Type	Nortel Networks configurable services
Service name:	MTT
Default status:	Running
Default startup:	Automatic
Alarms:	Service Control Manager

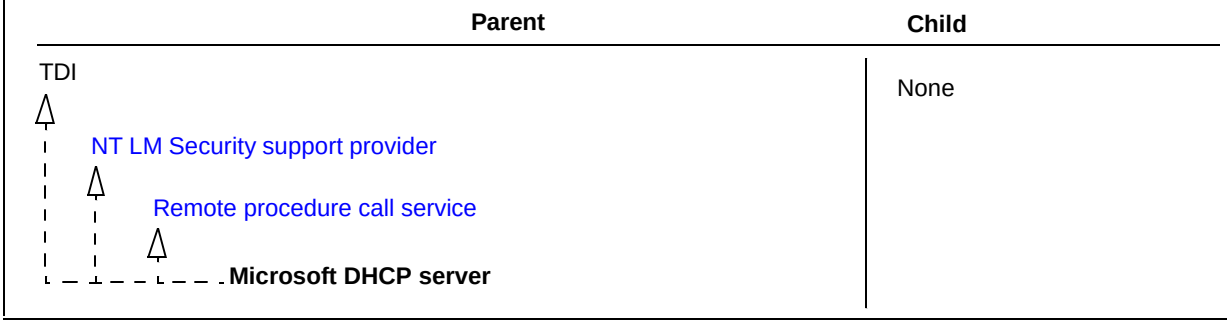
Message trace tool - service structure



Microsoft DHCP server

Microsoft DHCP server	The Microsoft DHCP (Dynamic Host Configuration Protocol) service enables DHCP capability on BCM and is used to assign dynamic IP addresses to devices on a network.
Type	Nortel Networks configurable services
Service name:	DhcpServer
Default status:	Stopped
Default startup:	Manual
Alarms:	DhcpServer

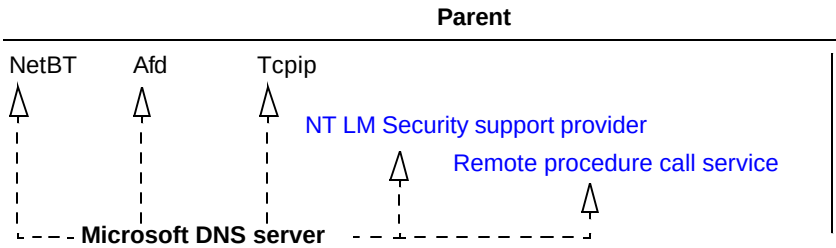
Microsoft DHCP server - service structure



Microsoft DNS server

Microsoft DNS server	The Microsoft (Domain Name System) server is a BCM service that translates domain names into IP addresses.
Type	Nortel Networks configurable services
Service name:	DNS
Default status:	Running
Default startup:	Automatic
Alarms:	DNS

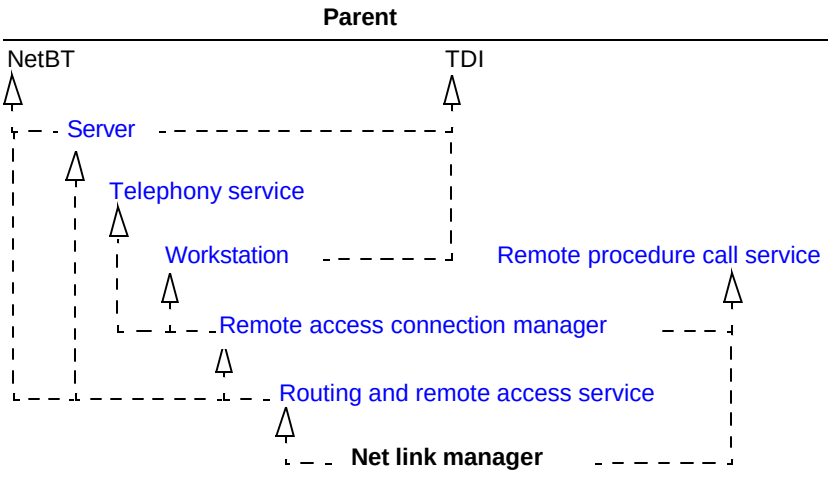
Microsoft DNS server - service structure:



Net link manager

Net link manager	The Net link manager service manages the default route and backup dialup connections switch-over process.
Type	Nortel Networks configurable services
Service name:	NetLinkManager
Default status:	Running
Default startup:	Automatic
Alarms:	NetLinkManager

Net link manager - service structure



Nortel Networks IVR

Nortel Networks IVR	The Nortel Networks IVR service starts the IVR service on Business Communications Manager.
Type	Nortel Networks configurable services
Service name:	Nortel Networks startup service
Default status:	Stopped

Default startup: Manual

Alarms: IVR

Nortel Networks IVR - service structure

Parent	Child
VoiceMSCDriver Voice MSC service Voice NNU diagnostics Voice Licensing services Media services manager VoiceCTI **Nortel Networks IVR**	None

Nortel Networks license service

Nortel Networks license service: The Nortel Networks licence service enables you to enter keycodes and verify licensing on BCM. If keycode entry does not function correctly, verify the status of this service.

Type: Nortel Networks configurable services

Service name: Nortel Networks license service

Default status: Running

Default startup: Automatic

Alarms: None

Nortel Networks license - service structure

Parent	Child
None	None

Policy service

Policy service: The Policy service provides Quality of Service (QoS) policy information base support, COPS protocol support, and policy rules implementation/installation/removal for policy enforcement.

Type: Nortel Networks configurable services

Service name: pep

Default status: Running

Default startup: Automatic

Alarms: Policy Services

Policy service- service structure

Parent	Child
Remote procedure call service ↑ **Policy service**	None

PPPoE service

PPPoE service	The PPPoE (Point to Point Protocol over Ethernet) service enables connectivity to networks that require PPPoE for authentication and access to the network. This service is enabled by keycode.
Type	Nortel Networks configurable services
Service name:	PPPoEService
Default status:	Stopped
Default startup:	Disabled
Alarms:	None

PPPoE service - service structure

Parent	Child
None	None

SNMP

SNMP	The SNMP (simple network messaging protocol) service manages the SNMP capabilities on BCM. The service allows inbound SNMP requests to be serviced by BCM. If the service is disabled, BCM does not respond to SNMP requests. If BCM is monitored by network management tools, the tools cannot collect data from BCM or control functionality via SNMP.
Type	Nortel Networks configurable services
Service name:	SNMP
Default status:	Running
Default startup:	Automatic
Alarms:	SNMP

SNMP - service structure

Parent	Child
Tcpip ↑ EventLog ↑ **SNMP**	None

SNMP Trap service

SNMP Trap service	The SNMP ((simple network messaging protocol) trap service receives trap messages generated by the BCM SNMP agent. The service forwards the messages to SNMP management programs in the network. If the service is disabled, SNMP applications that are registered to receive SNMP messages cannot receive SNMP traps.If the service is disabled, and if BCM is monitoring network devices or server applications using SNMP traps, significant system events are missed.
Type	Nortel Networks configurable services
Service name:	SNMPTRAP
Default status:	Stopped
Default startup:	Manual
Alarms:	SNMP Trap Agent

SNMP Trap service - service structure

Parent	Child
Tcpip EventLog **SNMP Trap service**	None

System status monitor

System status monitor	The system status monitor service associates the BCM front panel LEDs to the Unified Manager GUI. This module tracks system status and can reboot if WinNT hangs.
Type	Nortel Networks configurable services
Service name:	SSM
Default status:	Running
Default startup:	Automatic
Alarms:	System Status Monitor

System status monitor - service structure

Parent	Child
Remote procedure call service **System status monitor**	None

Telephony service

Telephony service	The Telephony service manages TAPI connection from the operating system to the Nortel Networks driver. This service is a requirement for all unimodem modems.
Type	Nortel Networks configurable services
Service name:	TapiSrv

Default status:	Running
Default startup:	Automatic
Alarms:	None

Telephony service - service structure

Parent	Child
None	**Telephony service** Remote access connection manager Remote access autodial manager Routing and remote access service Multi-dialup manager Net link manager Remote access server

TIntsvr

TIntsvr	The TIntsvr (Telnet service) lets a remote user log on to the system and run console programs using the command line. When enabled, the service supports connections from various TCP/IP Telnet clients. This service is used for configuration purposes. When disabled, remote users cannot connect to BCM using telnet clients. This service is disabled by default in BCM version 3.5.
Type	Nortel Networks configurable services
Service name:	tlntsvr
Default status:	Stopped
Default startup:	Disabled
Alarms:	TlntSvr

TIntsvr - service structure:

Parent	Child
Remote procedure call service **TIntsvr**	None

UNISTIM Terminal proxy server

UNISTIM Terminal proxy server	The UNISTIM terminal proxy server services enables IP clients (I2002, I2004, I2050 Softclient) on BCM.
Type	Nortel Networks configurable services

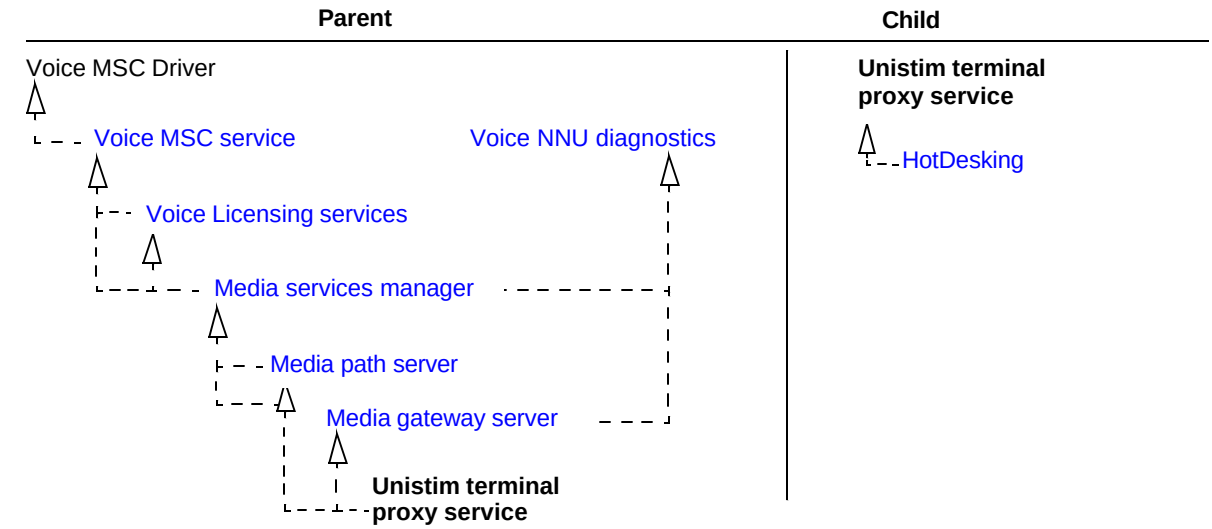
Service name: UTPS

Default status: Running

Default startup: Automatic

Alarms: Service Control Manager

UNISTIM Terminal proxy server - service structure:



VBMain

VBMain The VBMain service controls Multimedia Call Center on BCM. For more information about Multimedia Call Center see the *Multimedia Call Center Set Up and Operation Guide*.

Type Nortel Networks configurable services

Service name: VBMain

Default status: Running

Default startup: Automatic

Alarms: VBMain

VBMain - service structure

Parent	Child
None	None

Voice CFS

Voice CFS The Voice Component Feature Service processes the keycodes and licensing information for the BCM system.

Type Nortel Networks configurable services

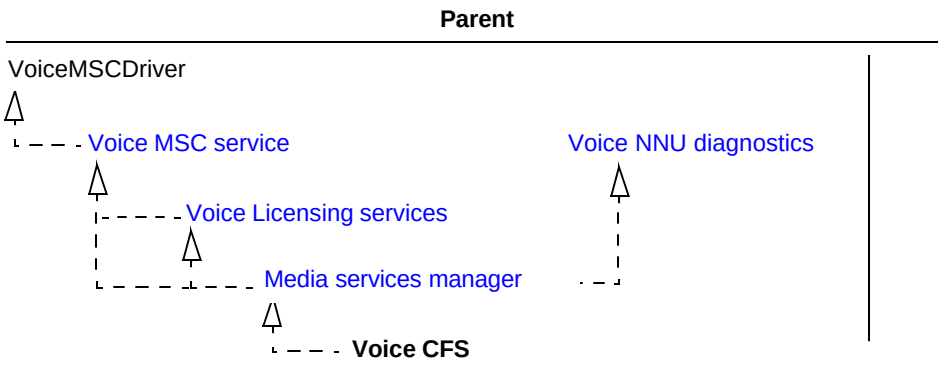
Service name: CfsServer

Default status: Running

Default startup: Automatic

Alarms: cfsServr

Voice CFS - service structure



Voice CTE

Voice CTE: Computer Telephony Engine - A middleware toolkit that provides interfaces for call control access to telephony devices on BCM.

Type: Nortel Networks configurable services

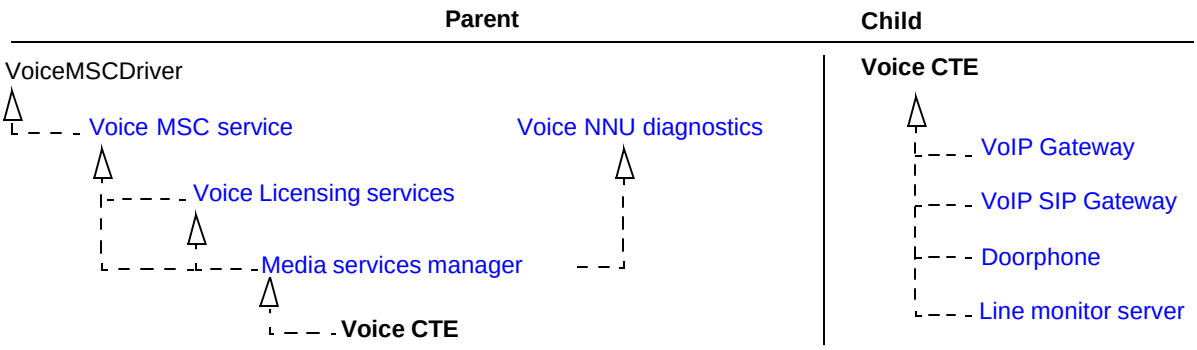
Service name: CTEngine

Default status: Running

Default startup: Automatic

Alarms:
- CTE
- Voice CTE
- Service Control Manager

Voice CTE - service structure



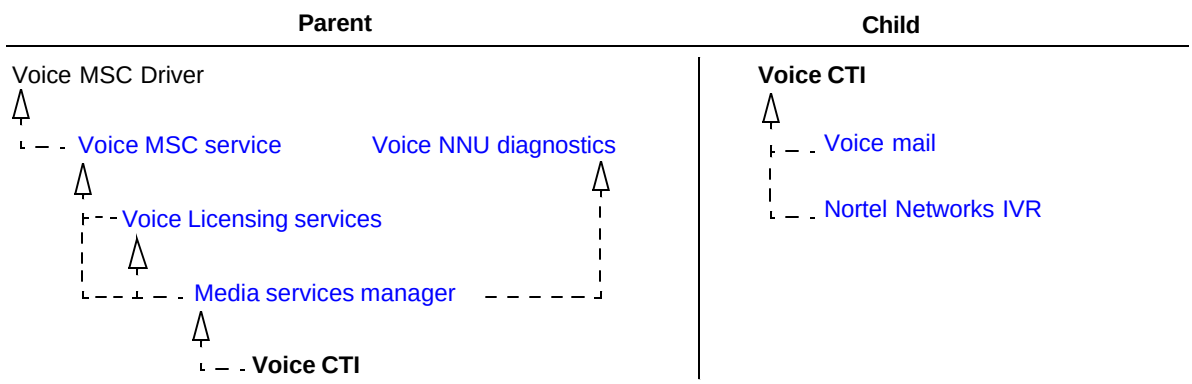
VoiceCTI

VoiceCTI: Middleware Service which provides an interface to CallPilot and Call Center on BCM for their call control and media requirements.

Type: Nortel Networks configurable services

Service name:	VoiceCTI
Default status:	Running
Default startup:	Manual
Alarms:	• VoiceCTI • Service Control Manager

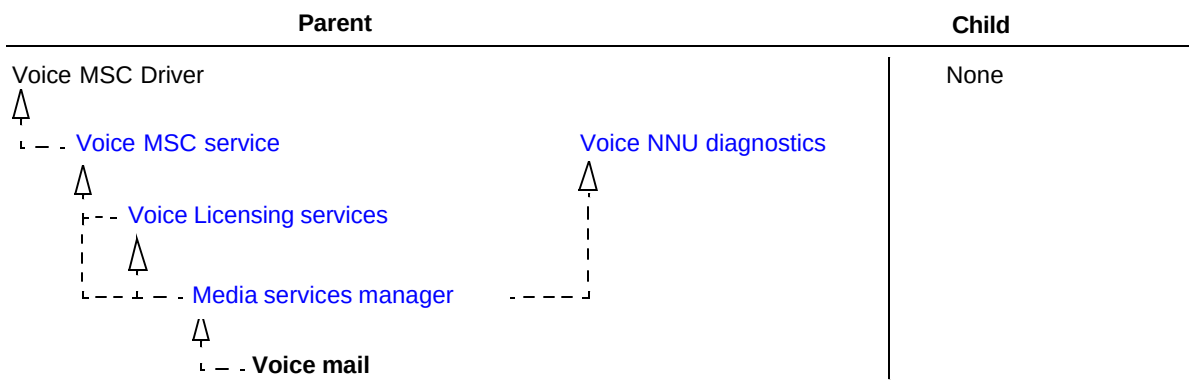
Voice CTI - service structure



Voice mail

Voice mail	This is the Voice mail and Call Center component of BCM.
Type	Nortel Networks configurable services
Service name:	VoiceMail
Default status:	Running
Default startup:	Automatic
Alarms:	• NVM • Service Control Manager

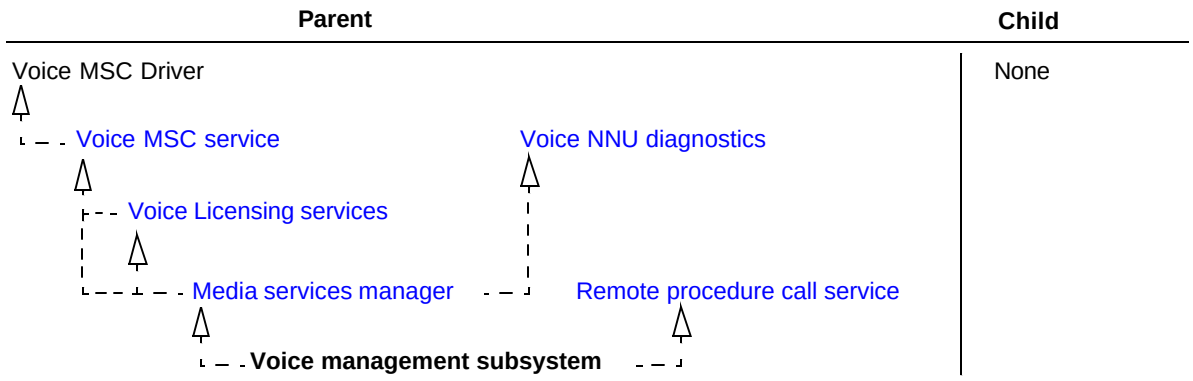
Voice mail - service structure



Voice management subsystem

Voice management subsystem	The Voice management subsystem is the Telephony administration area in Unified Manager.
Type	Nortel Networks configurable services
Service name:	VoiceManagementSubsystem
Default status:	Running
Default startup:	Automatic
Alarms:	• VoiceManagementSubsystem • Service Control Manager

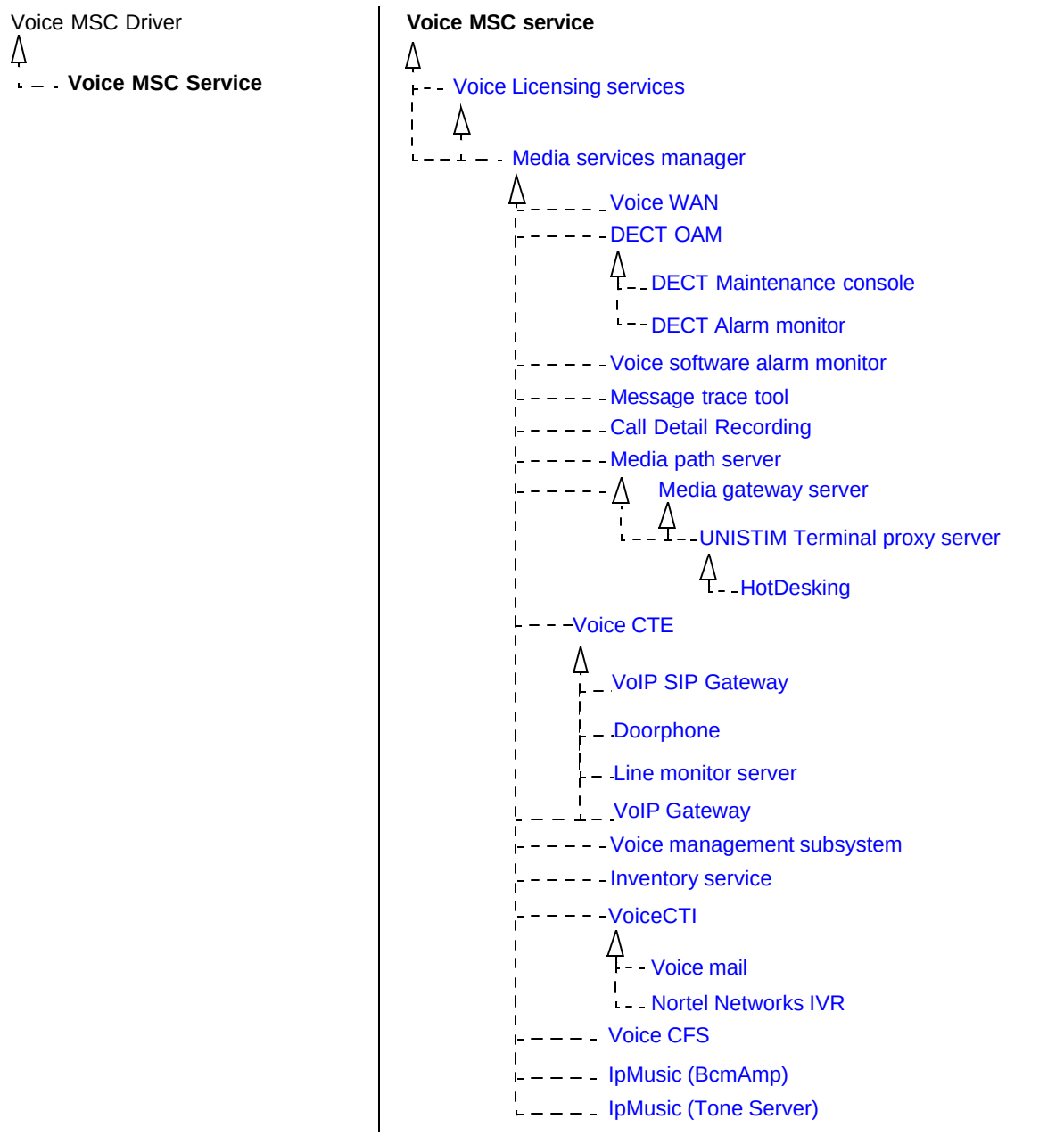
Voice management subsystem - service structure



Voice MSC service

Voice MSC service	The Voice MSC (Media Services Card) service provides the driver for the MSC hardware to the operating system on BCM. This service is critical for all Nortel Networks services running on BCM. If this service fails, the Watchdog attempts a restart. If the Watchdog restart fails, a reboot is required.
Type	Nortel Networks configurable services
Service name:	VoiceMSCService
Default status:	Running
Default startup:	Automatic
Alarms:	• VoiceMSCService • Service Control Manager

Voice MSC service - service structure



Voice Net QoS monitor

Voice Net QoS monitor	The Voice Net QoS monitor service monitors the QoS (quality of service) level of the data connections between BCMs, then sends the results to the VoIP gateways of the BCMs for determination of whether to fallback to PSTN for the voice calls between them.
Type	Nortel Networks configurable services

Service name:	VoiceNetQoSMonitor
Default status:	Running
Default startup:	Automatic
Alarms:	VNetQosMonitor

Voice Net QoS monitor - service structure

Voice NNU diagnostics

Voice NNU diagnostics	The Voice NNU (Nortel Network Utilities) diagnostics service is a library of interfaces provided to higher level applications for message logging, registry manipulation and other operating system functions.
Type	Nortel Networks configurable services
Service name:	NnuDiagLogger
Default status:	Running
Default startup:	Automatic
Alarms:	Nnu

Voice NNU diagnostics - service structure

Parent	Child
None	Media services manager **Voice NNU diagnostics** Voice WAN DECT OAM DECT Maintenance console DECT Alarm monitor Voice software alarm monitor Message trace tool Call Detail Recording Media path server Media gateway server UNISTIM Terminal proxy server HotDesking Voice management subsystem Inventory service VoiceCTI Voice mail Nortel Networks IVR Voice CFS IpMusic (BcmAmp) IpMusic (Tone Server) Voice CTE VoIP Gateway Line monitor server

Voice software alarm monitor

Voice software alarm monitor	The Voice software alarm monitor service monitors the telephony component for alarms that are set or cleared, and records them in the Windows NT Event Log. The service also does time synchronization between Windows NT and the MSC Telephony.
Type	Nortel Networks configurable services
Service name:	VoiceSW
Default status:	Running
Default startup:	Automatic

Alarms:
- Voice software
- Service Control Manager

Voice software alarm monitor - service structure:

Parent	Child
VoiceMSCDriver └ Voice MSC service └ Voice Licensing services └ Media services manager └ **Voice software alarm monitor** Voice NNU diagnostics	None

Voice time synch

Voice time synch	The Voice time synch service is an industry-standard NTP client for BCM, which synchronizes time of core telephony with NT operating system.
Type	Nortel Networks configurable services
Service name:	VoiceTimeSynch
Default status:	Stopped
Default startup:	Disabled
Alarms:	VoiceTimeSynch

Voice time synch - service structure

Parent	Child
None	None

Voice WAN

Voice WAN	The Voice WAN service manages the ISDN interface to the core telephony.
Type	Nortel Networks configurable services
Service name:	VoiceWAN
Default status:	Stopped
Default startup:	Automatic
Alarms:	Service Control Manager

Voice WAN - service structure:

Parent	Child
VoiceMSCDriver Voice MSC service Voice Licensing services Voice NNU diagnostics Media services manager **Voice WAN**	None

Voice watchdog

Voice watchdog	This service monitors the status of services that are based on the Media Services Card, and can restart them if they shutdown inadvertently.
Type	Nortel Networks configurable services
Service name:	voicewatchdog
Default status:	Running
Default startup:	Automatic
Alarms:	VoiceWatchdog

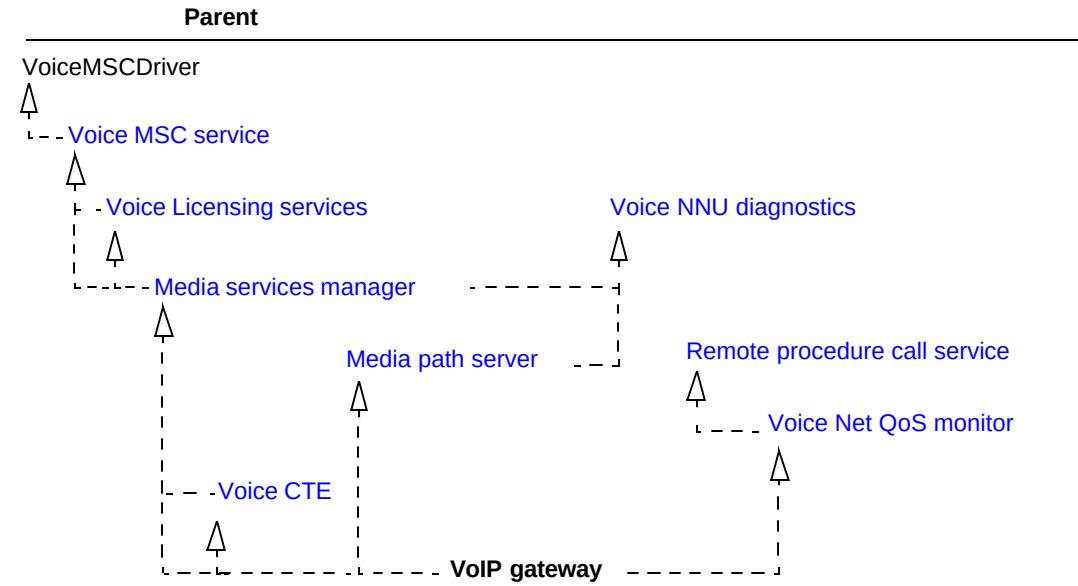
Voice watchdog - service structure

Parent	Child
None	None

VoIP Gateway

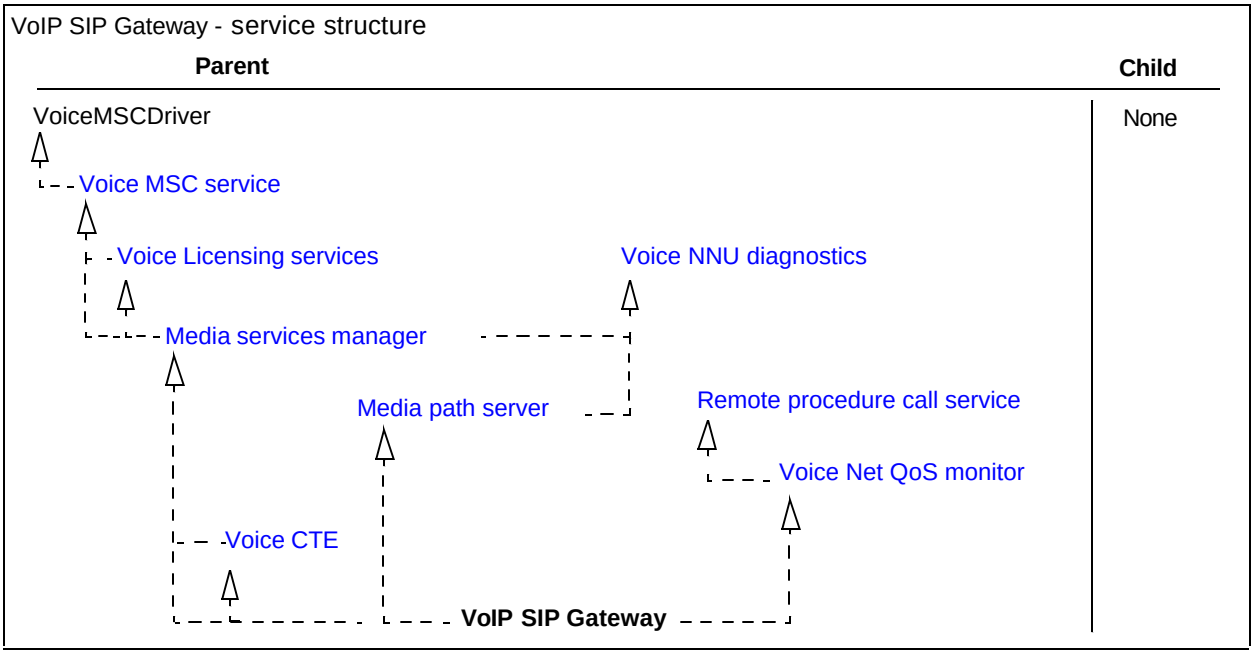
VoIP Gateway	The Voice over IP Gateway service provides voice over a packet network.
Type	Nortel Networks configurable services
Service name:	VoiceNetVoIPGateway
Default status:	Running
Default startup:	Automatic
Alarms:	VNetVoIPGtwy

VoIP gateway - service structure



VoIP SIP Gateway

VoIP SIP Gateway	The Voice over IP SIP Gateway service provides voice over a SIP packet network.
Type	Nortel Networks configurable services
Service name:	VoIPSIPGateway
Default status:	Running
Default startup:	Automatic
Alarms:	VoIPSipGateway



Watchdog Service

The Watchdog service runs continuously to monitor the state of all services. Activate service logging to generate logs that provide a history of changes to service status. The service log records manual or automatic service starts, and whether it was stopped manually. If a service stops running, Watchdog automatically attempts to restart the service. If the service fails to restart after 5 attempts, the Watchdog generates an event (trap type “error”) indicating the service has reached the restart attempt limit and must be started manually.

System service status reports are generated from the Unified Manager Maintenance page. Reports can be created for subsets of the services and drivers. These reports are grouped by the operational status of the service or driver.

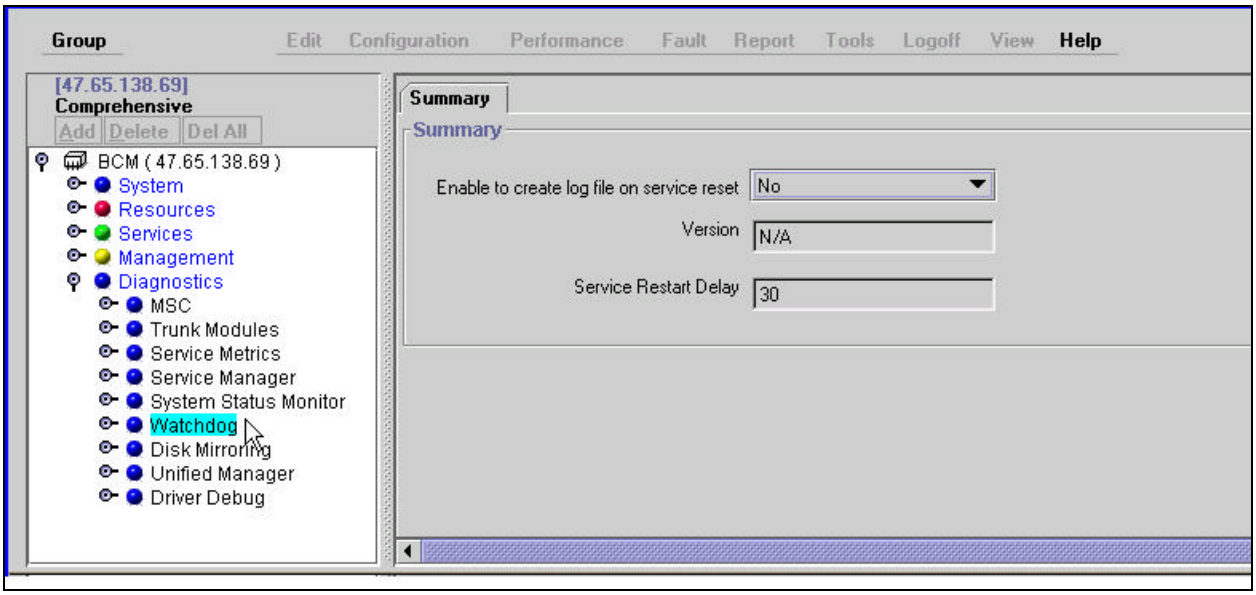
Using Watchdog with Service Manager

Use the Watchdog setting to activate service logging or to delay the start of services. This setting affects all services on your system.

To activate Watchdog service

1 On the Unified Manager navigation tree click the **Diagnostics** key and click the **Watchdog** heading.
On the Watchdog summary page you can enable or disable log reporting upon system reset, and specify the period of time (seconds) between service activation attempts.

Figure 34 Select Watchdog from the Unified Manager



2 From the **Enable to create file on service reset** list box select **Yes** to create a log file for each service reset
or
select **No** to disable log reporting.

3 Enter the time delay, in seconds, between service restart attempts (Service Restart Delay).

Chapter 4
Log Management

Log Managenent topics

Business Communications Manager Logs

Every component of Business Communications Manager is logged, so the system generates a large number of logs for a variety of purposes. In the case of faults, consult the logs to assist in the diagnosis and correction of the problem.

Some of the logs run continuously and collect information to help you troubleshoot in the event of system problems. You can disable some logs if the information collected is not of immediate or critical interest to maintain the health of the system.

Each event requires a unique maintenance activity. Determine the appropriate activity based on your level of administrator privileges.

Media service card (core telephony) logs

These are a set of event logs is maintained on the telephony side of the Business Communications Manager system.

MSC logs contain

- **MSC System Test Log**: contains diagnostic test results, telephony events and alarms, audits. It has a maximum size of 20 items, after which events are aged out to make room for new events.
- **MSC System Administration Log**: contains log-in, log-out information. Has a maximum of 10 entries. The 11th entry overwrites the 1st entry regardless of severity level.
- **MSC Network Event log**: contains T1 / PRI network interface events and alarms. This log has a maximum size of 10 events.

The System Test Log, System Administration Log, and Network Event log capture all the MSC (core telephony) system events (including alarms). These logs are viewed from the \Unified Manager \Configure\Diagnostics\MSC menu. The information in these logs can only be displayed and erased.

Core telephony alarms are sent to the MSC (core telephony) and the NT Event log systems. The Business Communications Manager generates NT event alarms that relate to events that occur in the voice software component. Use the log descriptions in conjunction with the voice software component alarms to resolve events with a severity level of P5 and above. For more information about alarms see Chapter2, "Fault Management System. For specific information about the voice software component alarms, see "Voice software" on page 219.

Information in the logs

- Description (MSC event or alarm number)
- Severity (1 - 9)
- Repeats (number of occurrences for this event)
- Time (format: yyyymmddhhmmss, e.g. 20030627135318)
- Parameters (report this information to Nortel Network support for debugging purposes - the field displays information on port numbers, internal software variables, buffer numbers)

MSC System test log

The System Test log keeps a record of events that occurr in the system related to diagnostic test results, telephony events and alarms, audits. Use the System Test log to check the frequency of log events and the number of consecutive occurrences of an event or an alarm.

Note: The System test log holds a maximum of 20 items. Check and record these items at regular intervals.

Erase the log after you correct all faults or ensure that the log items do not indicate a problem with system operation. For more information about how to display the system test log, see "Displaying the MSC log information" on page 317.

MSC System administration log

The System Administration log keeps a record of administrative events such as sessions in which a change was made, invalid password attempts, and password changes. You can check the items in the log, check when each item in the log occurred and you can erase the log.

Note: The System administration log holds a maximum of ten items. Check and record these items at regular intervals.

Erase the log after you correct all faults or ensure that the log items do not indicate a problem with system operation. For more information about how to display the System Administration log, see "Displaying the MSC log information" on page 317.

MSC Network event log

The Network event log keeps a record of events and alarms that are specific to the T1/PRI network interface. You can check the items in the log, check when each item in the log occurred and you can erase the log.

Note: The Network Event log holds a maximum of ten items. Check and record these items at regular intervals.

The Network Event log holds a maximum of 20 items. Erase the log after dealing with all the items. For more information about how to display the Network event log, see "Displaying the MSC log information" on page 317.

Displaying the MSC log information

Use the procedure in this section to display information on any item in the System Test, System Administration or Network Event logs.

To display the MSC log information:

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation tree click the **Diagnostics** and **MSC** keys. and click either the **System test log**, **System admin log** or **Network admin log** keys. If there are no log entries, no entries appear under the headings.
3. Select a numbered log item under the log key. Information about the log item appears in the information frame. The description attribute indicates if the item is an event or alarm and includes the associated code.

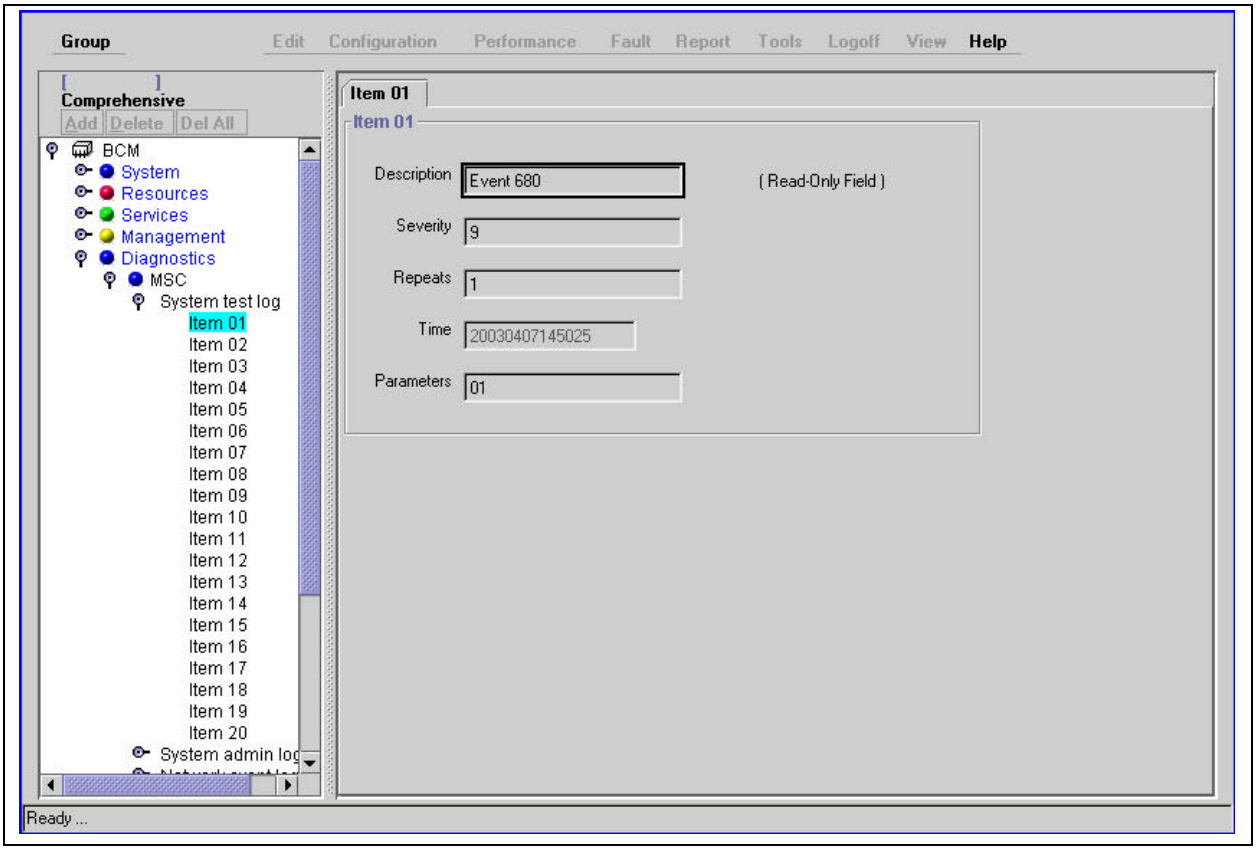
   The severity, frequency, time and parameters of the event or alarm are displayed. For more information about the event or alarm, see "Component ID (alarm) summary information" on page 92 or "MSC System test log" on page 316, "MSC System administration log" on page 316 or "MSC Network event log" on page 317.

Note: Alarms also appear in the Windows NT event log and the Alarm Database. You must configure the alarm database before alarms are stored in the database. For information about how to configure the Alarm Database, see the *Programming and Operations Guide.*

If the alarm service is not active, NT event logs accumulate to a maximum of 3MB. After the number of records reaches the 3MB threshold, the system overwrites the original files (starting with the oldest). If the alarm service is active, the NT event logs are cleared on reboots or if the Alarm Backup batch is run. When the alarms are clipped either through a reboot or the alarm backup batch, the files are time/date stamped.

Any information sent to the Windows NT event log can generate an SNMP trap.

Figure 35 System test log screen



4 Record the system test log item on the System administration log sheet. Repeat the steps in this procedure until you record all the items.

5 Perform appropriate maintenance activities based on the event notification type.

Erasing the MSC log information

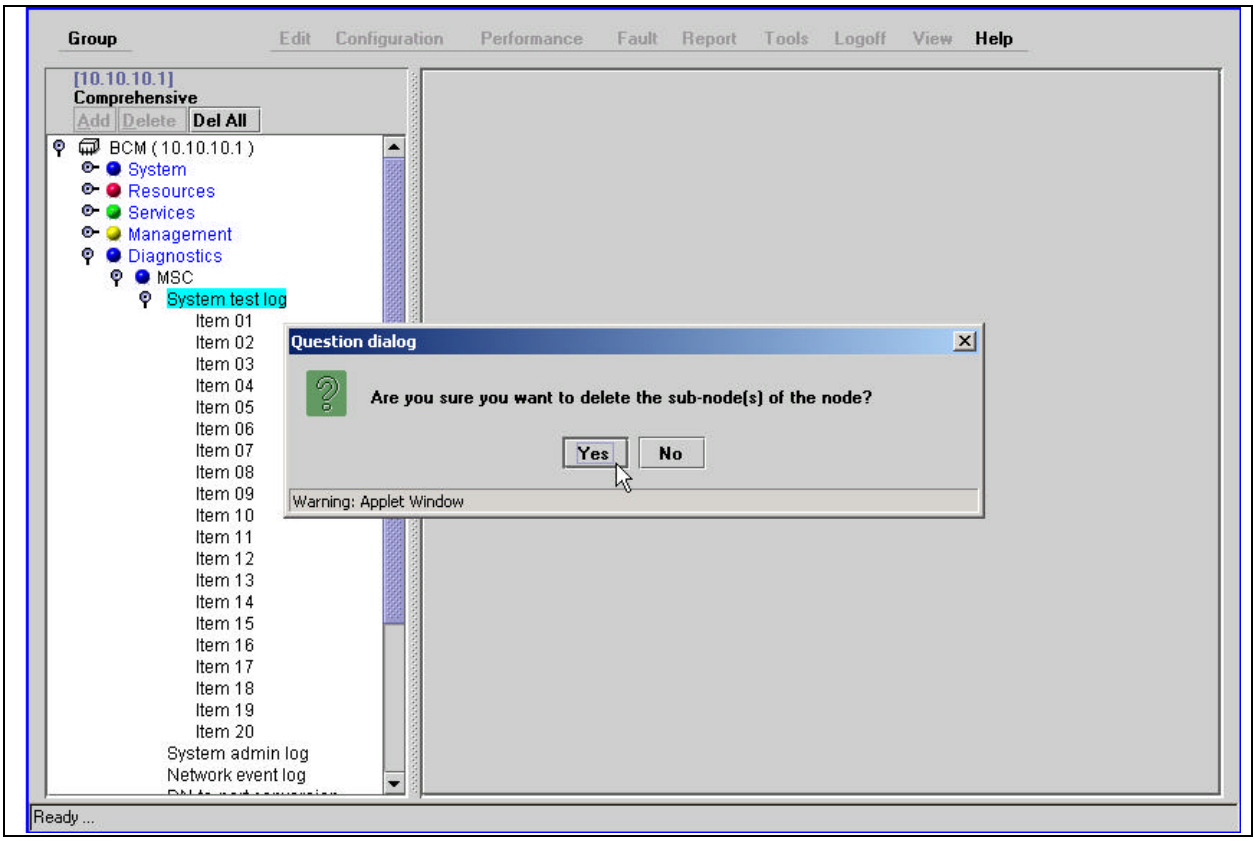
Use the procedure in this section to erase log items from the System Test, System Administration or Network Event logs.

Note: You only have the option of removing all the log items.

To erase log information

1. Access the correct Business Communications Manager in your network from the Unified Manager workstation browser.
2. On the Unified Manager navigation frame click the Diagnostics and MSC keys.
3. Right-click either the **System test log**, **System admin log** or **Network admin log** heading and click **Delete All**.
   If there are no log entries, no entries appear under the headings.
4. A message appears that asks you to confirm the deletion.

Figure 36 Delete the log dialog box



5. Select **Yes** to continue. If new items have been added since the log items were displayed, the new items are not erased.

Archlogs

Access the archlog management system from the Maintenance page. Archlog selections are:

Report-a-problem wizard

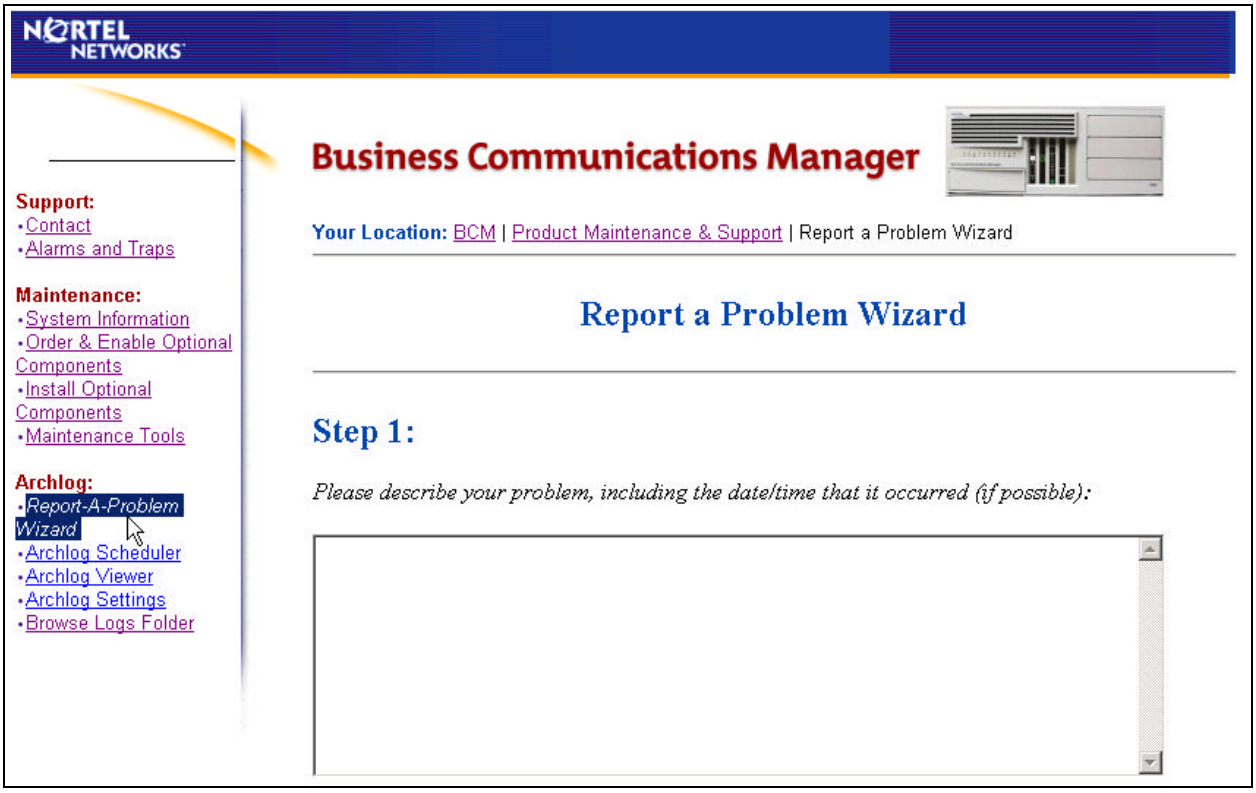
The Report-a-problem wizard selection displays a form for you to write a description of the problem you are experiencing. The form is recorded and stored in the archlog package.

Using the Report-a-problem wizard

Use this procedure to complete a support request form.

1. On the Unified Manager main page, click the **Maintenance** icon and log on with your user name and password.
   The Product Maintenance & Support Website appears.
2. In the left frame, under the **Archlog** heading, click the **Report-A-Problem Wizard** link.
   The Report-A-Problem input screen appears.

Figure 37 Report-a-problem input screen



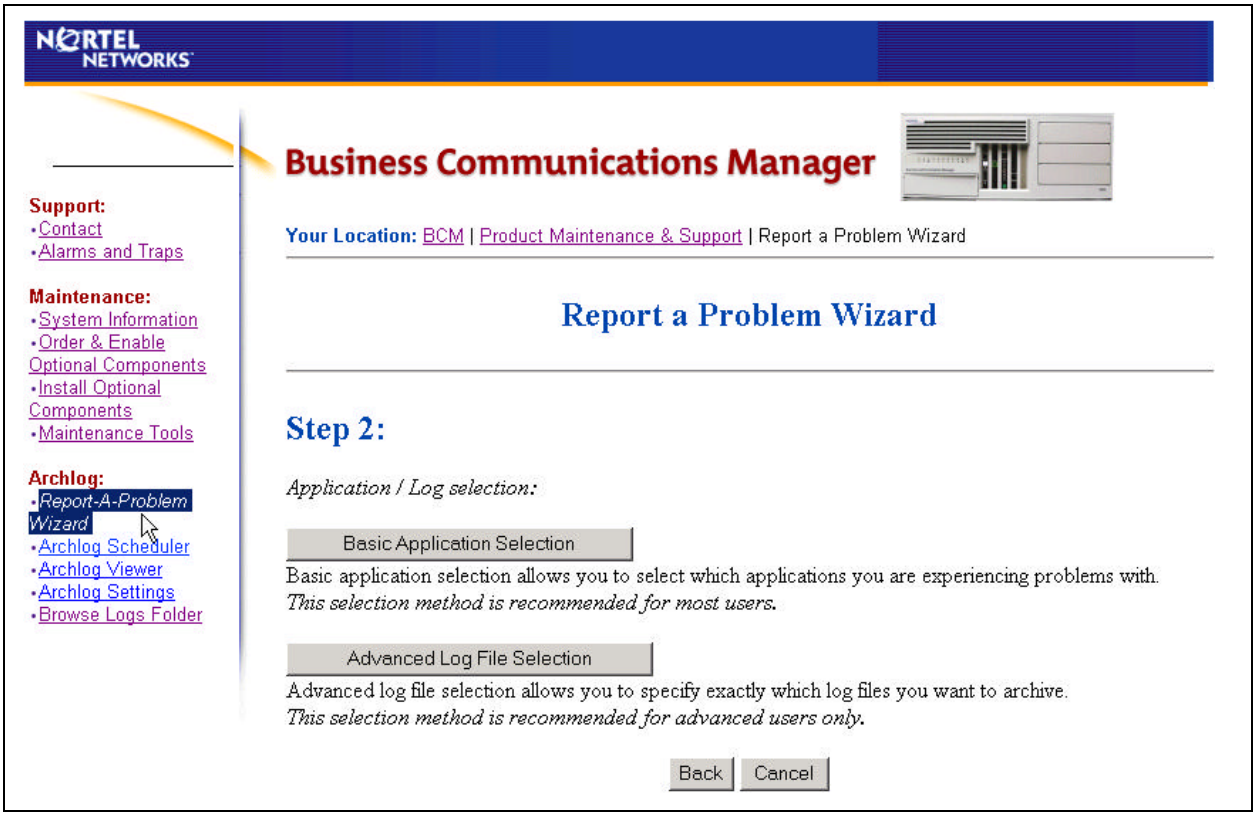
3 Type a description of the problem and click the **Next** button when you are finished.

4 Click either the **Basic Application Selection** or **Advanced Log File Selection** buttons.

From the basic pplication selection you can select the applications you are having problems with. This selection method is recommended for most users. Go to step 5.

From the advanced log file selection you can specify which log files you want to archive. This selection method is recommended for advanced users only. Go to step 6.

Figure 38 Report-a-problem application selection screen (step 2)



5 If you select Basic application, select the application that requires support.

Note: Unless support requests you to select specific application or log files, the standard practice is to select ALL log files. This insures all relevant files are captured.

- To return to the previous screen click **Back**.
- To cancel the operation and continue to Archlog Scheduler, click **Cancel**.
- To complete the Report-a-problem wizard form, click **Finish**.

Figure 39 Basic application selection screen

The table Report-a-problem wizard application selections lists the report-a-problem wizard applications.

Table 17 Report-a-problem wizard application selections

Logs Applications	System Services	Data	IP Telephony	Digital Telephony	Admin & Setup
Call Center	Apache Web Server	Firewall	IP Sets (i2004)	Analog Sets	Backup and Restore
Call Detail Recording	DHCP	IP SEC	IP Sets (i2002)	Analog Trunks	Key Codes
Call Center Reporting	DNS	IP Routing	IP Soft Client (i2050)	DECT	Patch Installation / System Upgrade
Desktop Assistant	Voice Time Synchronization	IPX Routing	IP Trunks	Digital Sets	Programming Wizards
FAX	NCM	Network Address Translation	Symbol	ISDN Networking	Unified Manager
Interactive Voice Response	System Status Monitor	Networking (LAN, WAN, etc)			

Table 17 Report-a-problem wizard application selections

Logs Applications	System Services	Data	IP Telephony	Digital Telephony	Admin & Setup
Personal Call Manager	Uninterruptable Power Source	Policy Services			
TAPI Applications	Voice Watchdog	v.90 Modem			
Unified Messaging	Services Monitor	Web Caching / Web Access			
Voice Mail / Call Pilot					

6 If you select Advanced Log File Selection, the Advanced application selection screen appears. Select the applications or log files that require support.

Figure 40 Advanced application selection screen

The table Report-a-problem wizard advanced application selections provides information on the report-a-problem wizard advanced application selections (application files, logs and filepaths).

Table 18 Report-a-problem wizard advanced application selections

Application / Log	File / Filepath
Application exception handler log	E:\Nortel Networks\Logs\drwtsn32.log
BRU Logs	F:\Program Files\Nortel Networks\BRU\Working*.*
Call Center Logs	• E:\Nortel Networks\Logs\CallPilot\CallCenter*.* • D:\St\Acdagent.out • D:\St\Acdcall.out • D:\St\acdcdn.out • D:\St\PMPORTUSAGE.out • D:\St\Vbsm.out
Detailed WinNT system report	None
Interactive Voice Response files	E:\NortelNetworks\logs\IVR*.*
NCM Logs	E:\NortelNetworks\logs*.log
DHCP	C:\Winnt\System32\Dhcp\DhcpSrvLog.*
DNS	C:\Winnt\System32\Dns\dns.log
Drive C: D: E: F: & I: Content Listings	None
Firewall report logs	F:\Program Files\Nortel Networks\Unified Manager\log*Report.txt
IP routing tables	None
IPX routing tables	None
Media Services Manager logs	• E:\Nortel Networks\Log\NNU\EmsManager.log • E:\Nortel Networks\Log\NNU\EmsManager.bak
MSC Core Upload log	F:\Program Files\Nortel Networks\Voice Solution\upload.log
MSC Service and CTI logs	F:\Program Files\Nortel Networks\Voice CTI untime*.log
MTT logs	E:\Nortel Networks\Logs\MTT Logs*.*
NNU logs	• E:\Nortel Networks\Logs\NNU*.log • E:\Nortel Networks\Logs\NNU*.bak
Programming Wizards logs	F:\Program Files\Nortel Networks\Unified Manager\wizardresults*.*
SEKUR keycode information file	D:\Data Files\Nortel Networks\Voice CTI\SEKUR
System Inventory	F:\Program Files\Nortel Networks\Voice Platform\wwwroot\inventory.xml
Telephony OAM interface logs	D:\Data Files\Nortel Networks\Voice Solution\logs*.log
Unified Manager logs	E:\Nortel Networks\Logs\Unified Manager*.*

Table 18 Report-a-problem wizard advanced application selections

Application / Log	File / Filepath
V.90 Modem	• F:\Program Files\Nortel Networks\Voice Platform\logs\mdetect.log • F:\Program Files\Nortel Networks\Voice Platform\logs\modbackup.log • F:\Program Files\Nortel Networks\Voice Platform\logs\modemInst.log • F:\Program Files\Nortel Networks\Voice Platform\logs ras_config.log • F:\Program Files\Nortel Networks\Voice CTI untime\Servutil.log
Multimedia Call Center	E:\Nortel Networks\Logs\Multimedia Call Center\logs*.*
Voice Mail logs	• D:\st\Stlog.out • D:\st\Stdbg.out • D:\st\sysdir.wlt • D:\st vmsffax.log • D:\st\f982wui.log
Voice Platform maintenance logs	F:\Program Files\Nortel Networks\Voice Platform\logs*.*
VoIP Gateway diagnostic logs	F:\Program Files\Nortel Networks\VoIP Gateway*Diagnostics.log
Watchdog	F:\Program Files\Nortel Networks\Voice CTI untime\Watchdog.log
WinNT system event logs	*D:\Data Files\Nortel Networks\Unified Manager\archive*.evt*

Archlog scheduler

Use the Archlog scheduler to enter the time to run an archlog batch file job. The scheduling information that you enter instructs the system when to compile and save archlog files to the BCM hard drive. An archlog batch job demands CPU processing time, so schedule the archlog to run during hours of low call traffic.

Scheduling an archlog batch job

Use this procedure to instruct the BCM system on the time and frequency to record and store log information into archlog file. This procedure also prompts you to select the applications on which to record and store the log information.

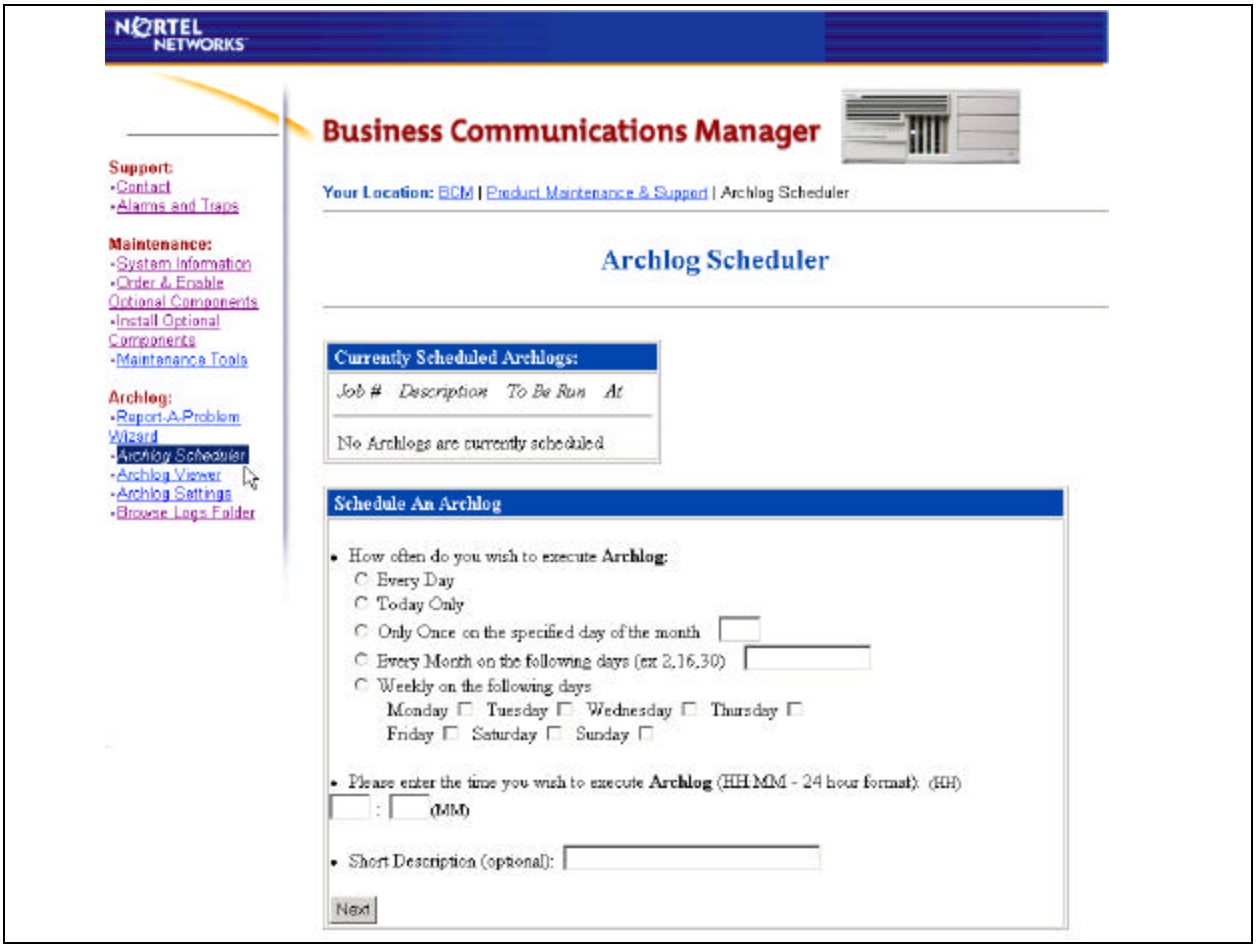
Note: An archlog batch job affects CPU processing efficiency. This can result in IP telephone outages, slower voice mail performance or an overall reduction in system performance. Schedule the archlog to run during hours of low call traffic unless otherwise instructed by Nortel Networks support teams.

Note: Ensure to schedule an Archlog batch job so that it does not conflict with other scheduled activities such as BRU backups.

1 On the Unified Manager main page, click the **Maintenance** icon and log on with your user name and password.
The Product Maintenance & Support Website appears.

2 In the left frame, under the **Archlog** heading, click the Archlog Scheduler heading.
The Archlog Scheduler screen appears.

Figure 41 Archlog schedule screen (page 1)



3 Enter the time and frequency to perform an archlog batch job:

- Everyday
- Today only
- Once on a specified day (enter a number value, e.g. 12 - instructs the system to perform an archlog on the 12th day the current month. Valid values are 1 - 31).
- Every month on one or more days (separate multiple values by a comma. Valid values are 1 - 31. Maximum number of characters is 14 - including commas).
- Weekly (select the day of the week).
- Enter the time of day to perform an archlog (24 hour clock format, HH:MM).
- Enter a short description of the archlog. Enter unique system information, e.g. “daily archlog of System B”.

4 Click the **Next** button to display the next pageof the archlog scheduler.

Note: If you enter invalid values from step 1 of this procedure, the system displays page 2, but prompts you to return to page 1 and enter the correct values. When you have entered valid values, continue to the next page.

5 Select from a list of applications. Select the application you require log files for.

6 Click the **Schedule New Archlog Now** button to save the archlog scheduling information. A summary of the archlog schedule information is displayed.

7 You can click the **Details** link to review the archlog schedule and application information, or
click the **Delete Scheduled Archlog** link to delete the archlog schedule information.

Archlog viewer

From the Archlog viewer you can access all the archlogs batch files created by the Archlog scheduler (see "Archlog scheduler" on page 326). Archlog files are stored in a directory on the Business Communications Manager hard drive. The archlog files, or packages, are compressed (.zip) files. The viewer displays links to the archlog files saved on the Business Communications Manager hard drive.

With the Archlog viewer you can download, view or delete archlog packages (zip file). Select the link to download the archlog file (package) and save it to the hard drive of your PC.

Viewing archlog files

Use this procedure to download, view or delete archlog packages (zip file).

1 On the Unified Manager main page, click the **Maintenance** icon and log on with your user name and password.
The Product Maintenance & Support Website appears.

2 In the left frame, under the **Archlog** heading, click the **Archlog Viewer** link.
The Archlog viewer screen appears. The Archlog viewer screen lists the Archlog files stored on the BCM hard drive.

3 Click the **Download Archlog Package** button to access the required Archlog files.
The system prompts you to:

- open the .zip file package and display the archlog files
- save the .zip archlog file package to your PC (save the files to a unique directory)
- cancel the download operation

4 Click the **Delete Archlog Package** button to delete the archlog file package from the BCM hard drive.

Figure 42 Archlog viewer screen

Archlog settings

You can use Archlog settings to configure archlog batch file process to:

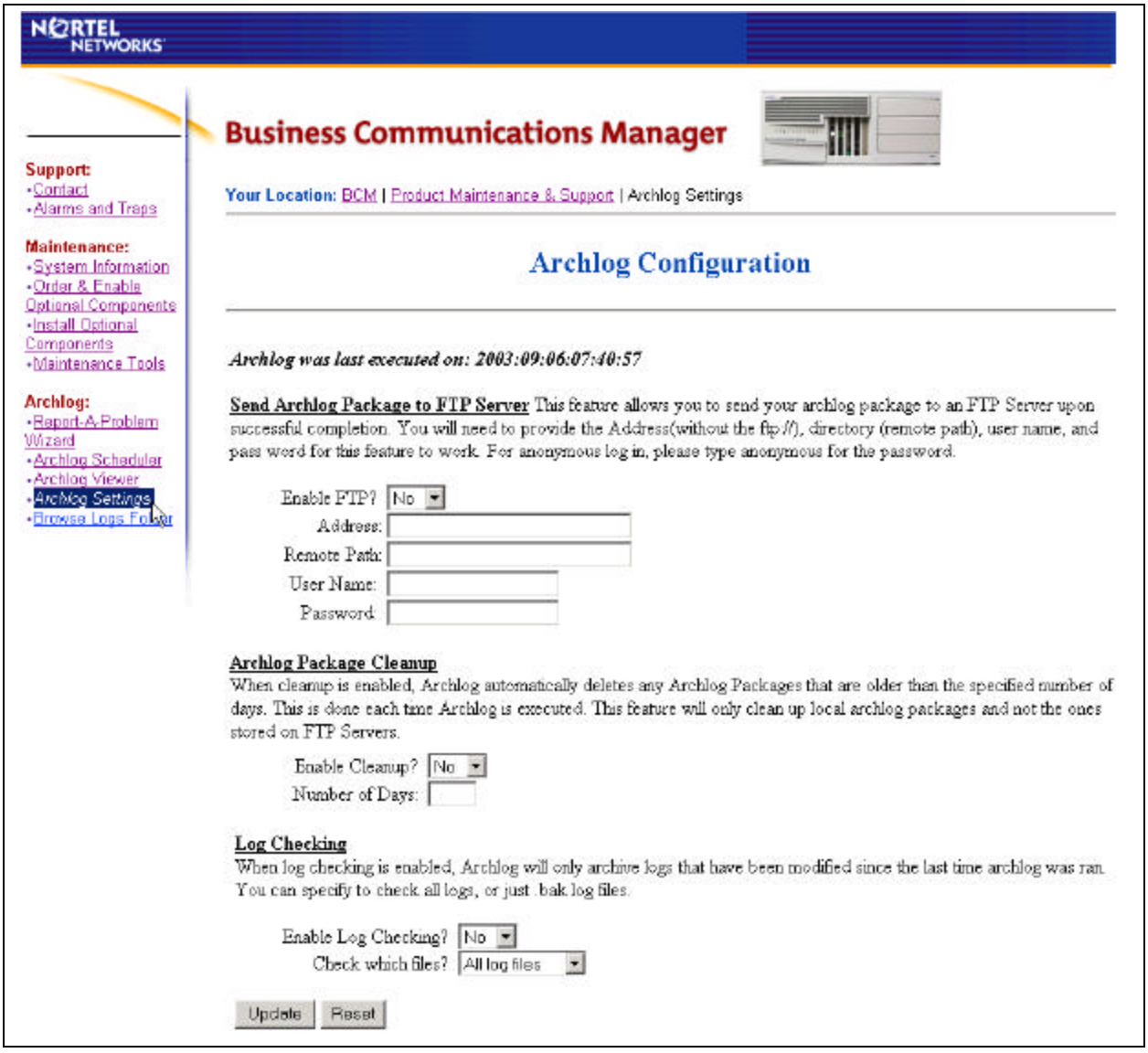
- **Send Archlog Package to FTP Server**: After the archlog package compiles, you can send your archlog package to an FTP server.
- **Archlog Package Cleanup**: When cleanup is enabled, Archlog automatically deletes any archlog packages that are older than the specified number of days. Cleanup is done each time Archlog is executed. This feature only deletes local archlog packages and not the ones stored on FTP Servers.
- **Log Checking**: When log checking is enabled, Archlog archives only those logs that have been modified since the last time archlog was ran. You can specify to check all logs, or just .bak log files.

To configure the Archlog process

1. On the Unified Manager main page, click the **Maintenance** icon and log on with your user name and password.
   The Product Maintenance & Support Website appears.
2. In the left frame, under the **Archlog** heading, click the **Archlog Settings** link category on the maintenance page. The system displays the Archlog configuration screen. The Archlog configuration screen lists of all Archlog files stored on the BCM hard drive.
3. Enable the system to send Archlog Package to FTP Server:
   a. From the list box select **Yes** to enable the archlog FTP process.
   b. Enter the FTP address (without the ftp://), directory (remote path), username, and password. For anonymous log in, enter: “anonymous” in the password field.

4. Enable the Archlog Package cleanup process:
   a. From the list box select **Yes** to enable the archlog cleanup process.
   b. Enter the number of days. The system automatically deletes any archlog packages that are older than the specified number of days.
5. Enable the log checking process:
   a. From the list box select **Yes** to enable the log checking process.
   b. From the list box select **All log files** or **.bak files only**. The system archives only the logs that have been modified since the last time archlog ran.
6. Click **Update** to save the archlog configuration settings
   or
   click **Reset** to clear your configuration settings and use the system defaults.

Figure 43 Archlog configuration screen



Browse logs folder

Use the Browse logs folder selection to display the log directories and log files stored on Business Communications Manager.

Browsing archlog files

Use this procedure to display, examine and select for viewing, archlog directories and log files.

1 On the Unified Manager main page, click the **Maintenance** icon and log on with your user name and password.
The Product Maintenance & Support Website appears.

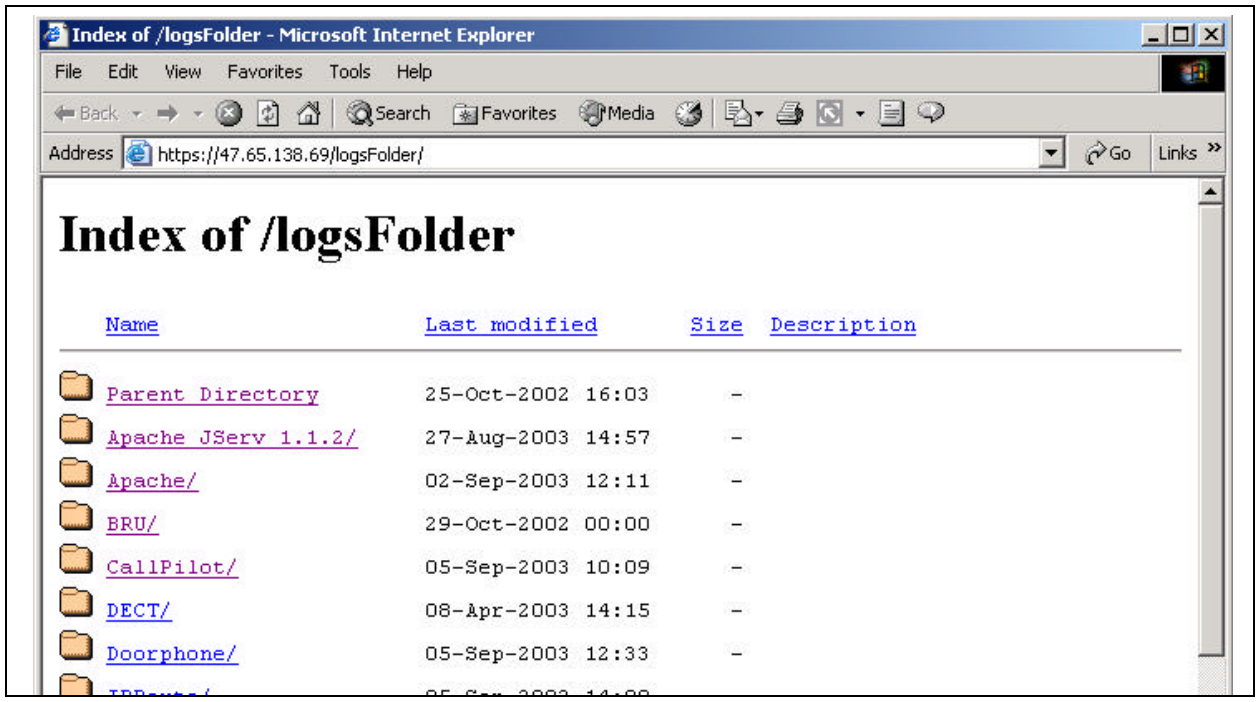
2 In the left frame, under the **Archlog** heading, click the Browse Logs Folder link.
A new browser window opens that lists the archlog directories and log files stored on the BCM hard drive.

3 Select a folder to display the directory file contents. Log files use various file extensions, depending on the log.

4 Select a log file to display the log contents.
You can open the file in Notepad or save the log file to your PC.

5 Close the browser window when you are done.

Figure 44 Archlog browse logs folder screen



Obtaining NT Event Logs from Archlog

After you enable the Alarm Service, the Business Communications Manager system automatically archives the event logs. Whenever Business Communications Manager is rebooted, the event logs are copied to an archive directory and the event logs are erased.

Business Communications Manager stores the event log archives in the directory D:\Data Files\Nortel Networks\Unified Manager\archive

Filename conventions for the event log archives

- SystemLogYYMMDDhhmm.evs
- ApplicationLogYYMMDDhhmm.evs

- SecurityLogYYMMDDhhmm.evs

  Where:

  — YY is the year the log was created
  — MM is the month the log was created
  — DD is the day the log was created
  — hh is the hour the log was created
  — mm is the minute the log was created

Use the procedure in this section to download and review NT Event logs using the Archlog application. These files can aid in problem resolution because they contain the alarms displayed within alarm banner.

Download archlogs after completing the report a problem wizard or use archlog viewer to obtain the latest package. The files are listed in chronological order from top to bottom.

The events at the bottom are the most recent. Each of the files is laid out into 9 columns:

Date | Time | N/A | N/A | Event ID | Component ID | User | BCM System Name | Problem Description

1. Unzip the archlog package to an empty directory on your client PC.
2. From the unzipped contents navigate to "nortel networks\logs\system"
   In this directory contains the 3 event log files:
   - AppEvent.txt - application event log
   - SecEvent.txt - security event log
   - SysEvent.txt - system event log
3. From the client PC, open the appropriate log with a text editor such as notepad.

Chapter 5
BCM Monitor

BCM Monitor topics

For more information about BCM monitor, consult the online help.

Starting BCM Monitor

BCM Monitor is an optional, standalone application you can use to view system and IP telephony information for each Business Communications Manager. Open several instances of the BCM Monitor on a single PC to monitor the corresponding Business Communications Manager systems.

Topics in this section

Installing BCM Monitor on your computer

1. On the Unified Manager main page, click the **Install Clients** icon.
   The Download Client Applications page appears.

2. In the left frame, under the **Administrative Tools** heading, click the **BCM Monitor** link.
   The BCM Monitor page appears.
3. Click the **Download BCM Monitor** icon.

4. Enter the System Administrator user name and password and click the **OK** button.
5. Select the **Save this program to disk** option and select the **OK** button.
6. Select a folder where you want to store the BCM Monitor install file and select the **Save** button.

7 From your desktop, move to the folder where you saved the install file and double click the **BCMMonitor.exe** icon

8 Follow the instructions provided by the installation wizard to install the application.

Starting BCM Monitor

1 Select the application icon on your desktop or find **BCM Monitor** on your **Start/Programs** menu.

2 Enter the IP address or system name of the Business Communications Manager you want to monitor in the **System Name or IP Address** box.

3 Enter your Business Communications Manager Unified Manager user name in the **Connect As** box.

4 Enter your Business Communications Manager Unified Manager password in the **Password** box.

Note: For some platforms, such as Windows 95, you may need to enter your network user name into the Unified Manager to allow access.

See the User Manager section of the *Business Communications Manager Programming Operations Guide* for information about user name and password formats.

5 Select the **Connect** button.
The first BCM Monitor screen appears.

Saving your logon information

With the BCM Monitor you can save your log on information on your computer. After you save your log on information, whenever you start BCM Monitor your log on information is automatically entered in the log on screen.

1 To save your logon information, select the **Save Information** check box before you click the Connect button when you log on.

Note: To prevent unauthorized access to your logon information, the saved logon information is encrypted.

The encryption of the logon information relies on features provided by the operating system you are using on your computer. For this reason, the Save Information check box is not available if you are using Windows 95, Windows 98, or Windows Me.

Using BCM Monitor to analyze your system status

BCM Monitor supports real time troubleshooting and report generation. System administrators and support personnel can use BCM Monitor to obtain key, real-time troubleshooting information and save information to generate system utilization and traffic reports.

The BCM Monitor screens provide information about:

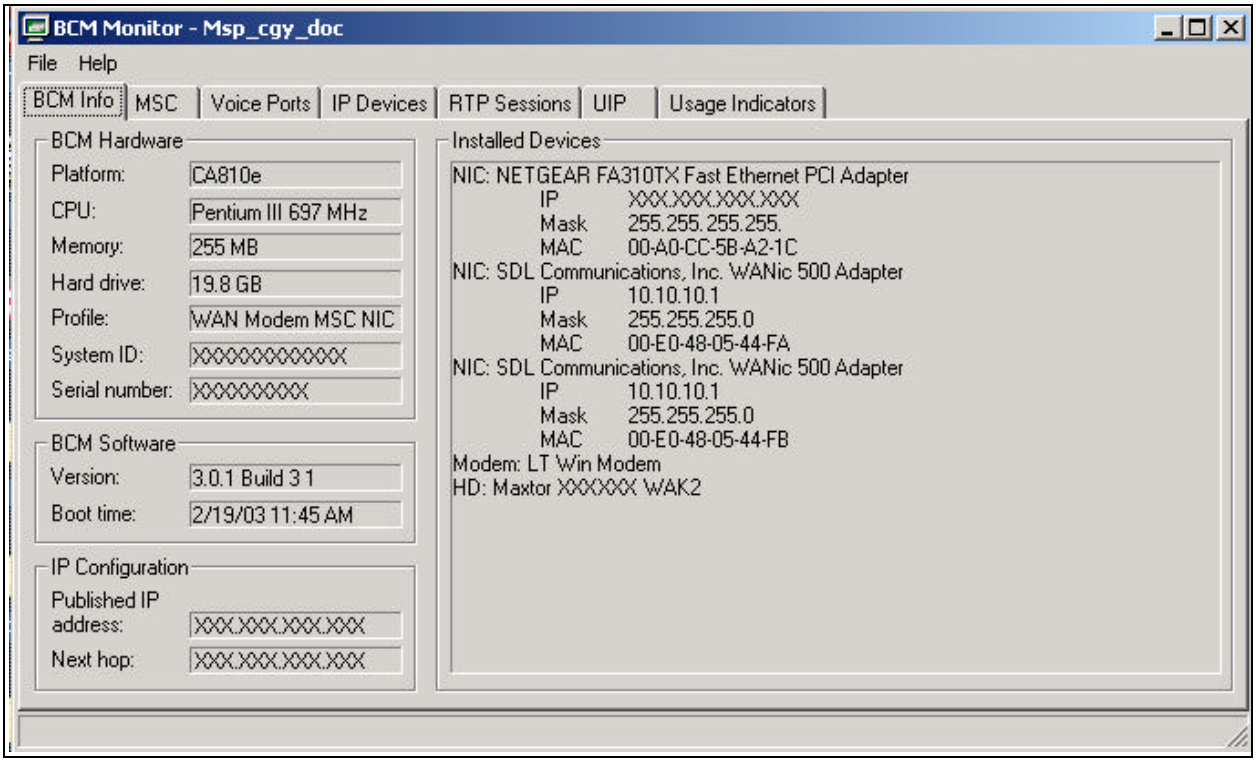
- system status
- utilization of resources in the Media Services Card
- operation of telephony applications such as Voice Mail or Call Center
- IP telephony activity

Topics in this section

BCM Info screen

Displays BCM system hardware, software and IP information. This information is useful for the static report format.

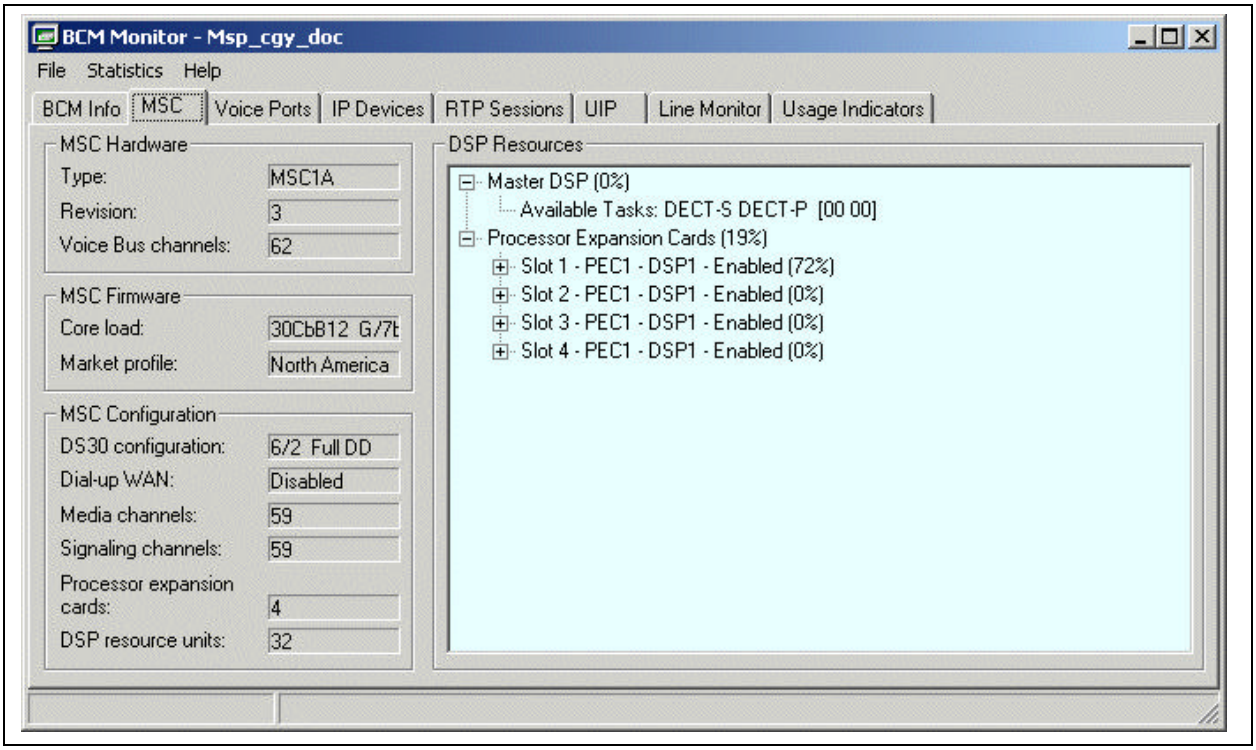
Figure 45 BCM Monitor info screen



MSC (Media Services Card) screen

- hardware information about the MSC, including type and revision, and MSC firmware load and market profile
- MSC configuration information such as DS30 configuration including split mode (6/2 or 5/3 split), and density mode (partial double density, full double density)
- indication of whether the dial-up WAN interface is in use
- how many signaling channels (D channels) and media channels (64 kbps B channels) are available
- processor expansion cards (PEC) in use on the MSC, and the total number of logical DSP resource units provided by all installed processor expansion cards. The available tasks and tasks in service are also shown per PEC, for example the types of codecs that each PEC can support

Figure 46 BCM Monitor MSC screen

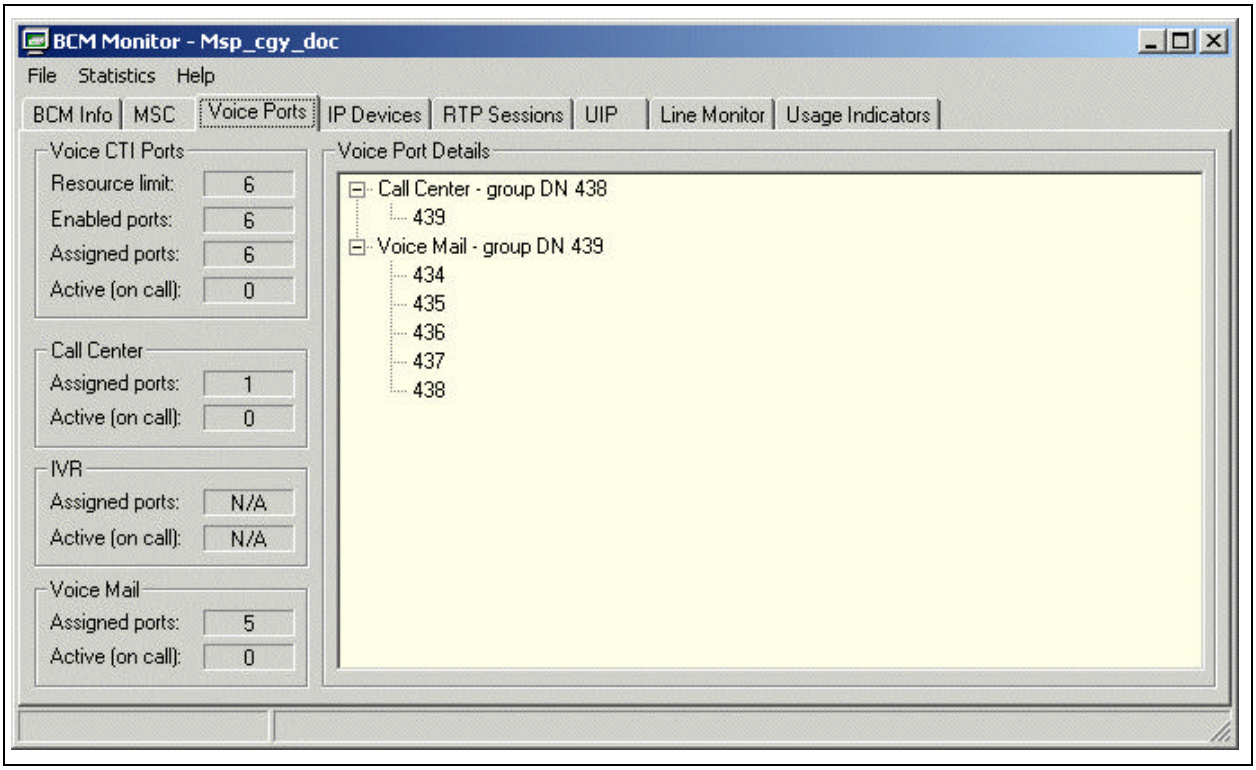


Voice Ports screen

This screen displays real time information about the configured voice ports. A configured voice port is a logical device used for Voice Mail, Call Center and IVR. As these values change with the usage of the switch, this tab is well suited for dynamic logging to view trends on system activity. Details about voice ports used by the Voice CTI services include:

- how many resources (ports) are configured for use by Voice CTI
- how many Voice CTI ports have been enabled
- how many Voice CTI ports are assigned to each of Call Center, Voice Mail and IVR
- how many of the assigned ports are currently active. The DN number of the user is given. The DNs reserved for voicemail are shown.

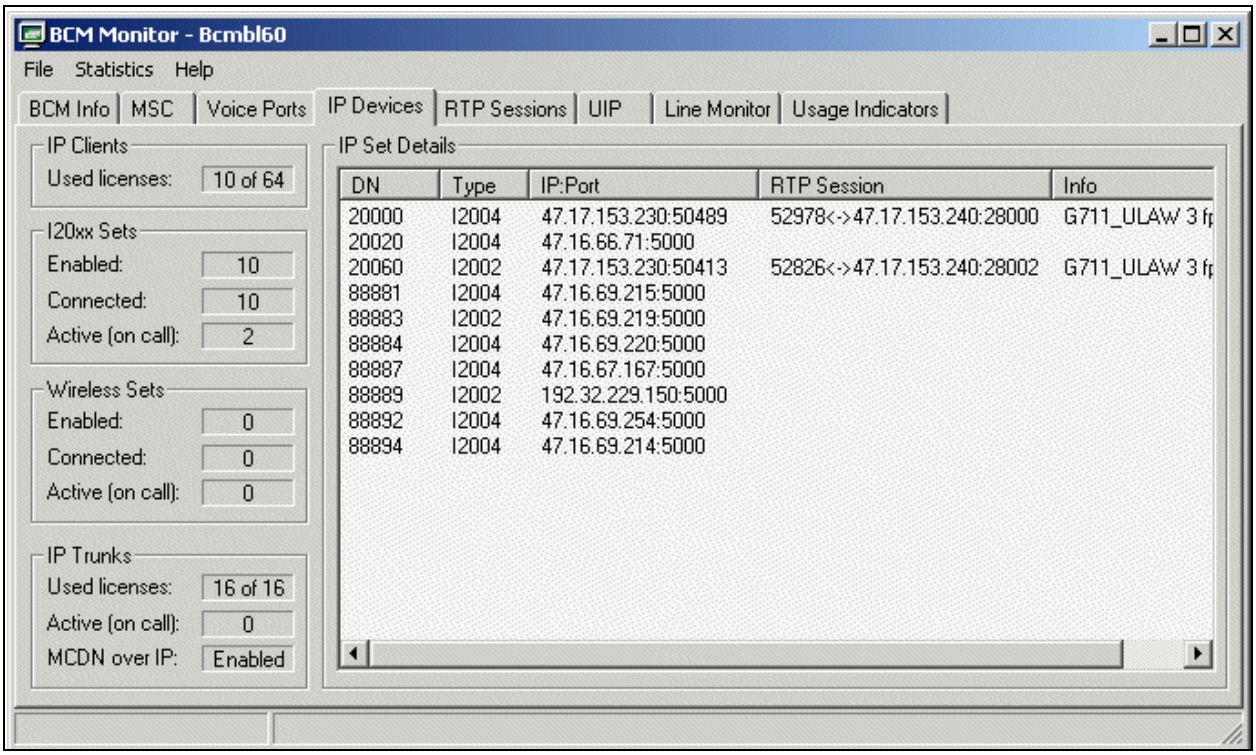
Figure 47 BCM Monitor voice ports screen



IP Devices screen

This screen displays information about the call activity of IP sets, wireless sets, and IP trunks. IP sets includes IP clients (e.g. i2050 softphone), i200x IP sets, and wireless sets. This tab shows how many sets in each category are enabled, connected, and active. For each active call, the DN, IP address and type of set is shown.

Figure 48 BCM Monitor IP devices screen

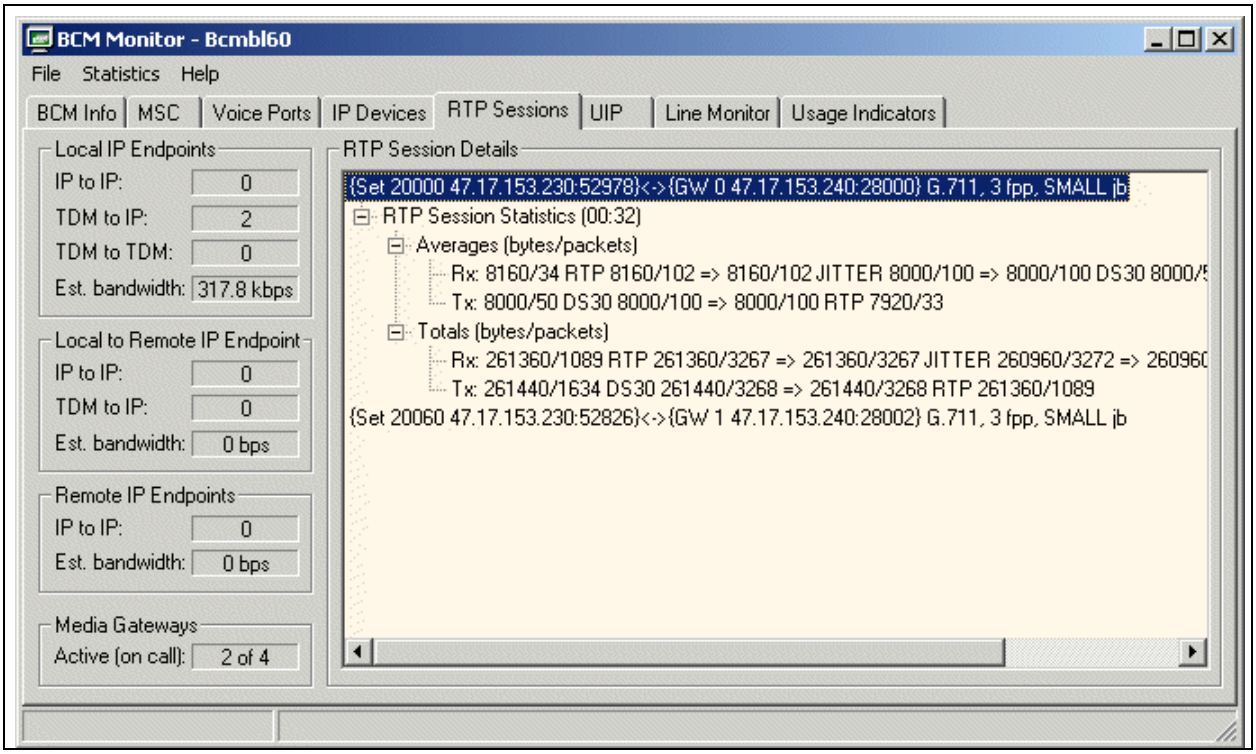


Real time Protocol over UDP (RTP) session screen

RTP session details are provided for each active VoIP session. The information displayed includes IP endpoints and trunks, stream information, and codec information between:

- local IP endpoints (two sets both connected to the local Business Communications Manager; combinations of IP to IP, TDM to IP, and TDM to TDM; estimate of bandwidth used by local IP endpoints). The protocol in use is shown. Can be used to trouble shoot one way speech traffic issues. You can see that set 1 is talking to set 2, but set 2 is not talking to set 1. This tool provides a way to monitor the direct path between the two IP sets. Jitter buffer setting is given (e.g. high, medium, low JB), and whether echo cancellation is enabled. NLP – allows echo canceller to detect far end and adjust echo. Can have echo canceller turned on.
- local to Remote IP Endpoints (IP to IP and TDM to IP)
- Remote IP endpoints (IP to IP)
- allocated Media Gateways for providing a connection between a TDM device and an IP endpoint

Figure 49 BCM Monitor RTP session screen

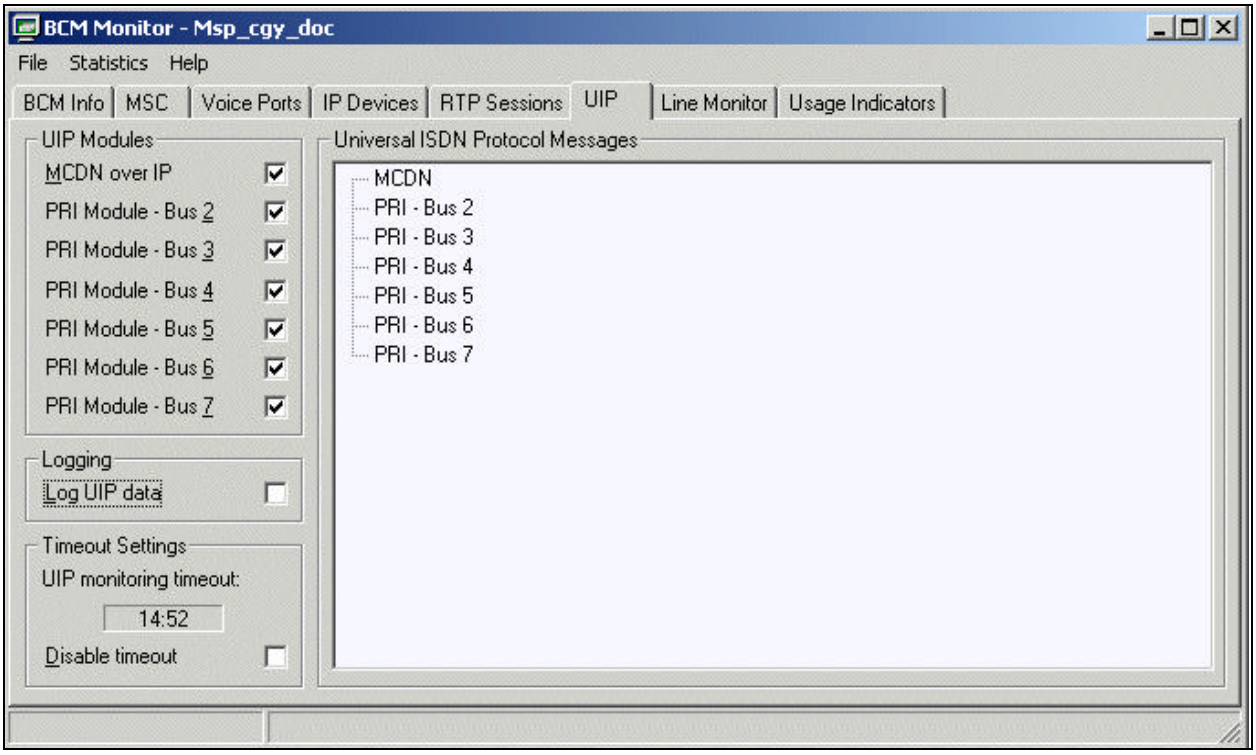


Universal ISDN Protocol (UIP) screen

This tab displays monitoring of Universal ISDN Protocol activity associated with IP trunks and PRI modules. This screen captures real time D channel signaling, showing the progression of a call through the stages through call setup to call teardown. This can be a very important troubleshooting tool for many types of call issues such as dialing plan or routing issues, as detailed called information is provided without requiring the use of protocol analyzers.

You can use this screen to track how long each session was, which digits were dialed and other call attributes. UIP can be logged to track the most recent 20 UIP messages. The UIP messages that contain at least one Information Element can be expanded to show the information element, which can be expanded to show the data portion of the Information Element.

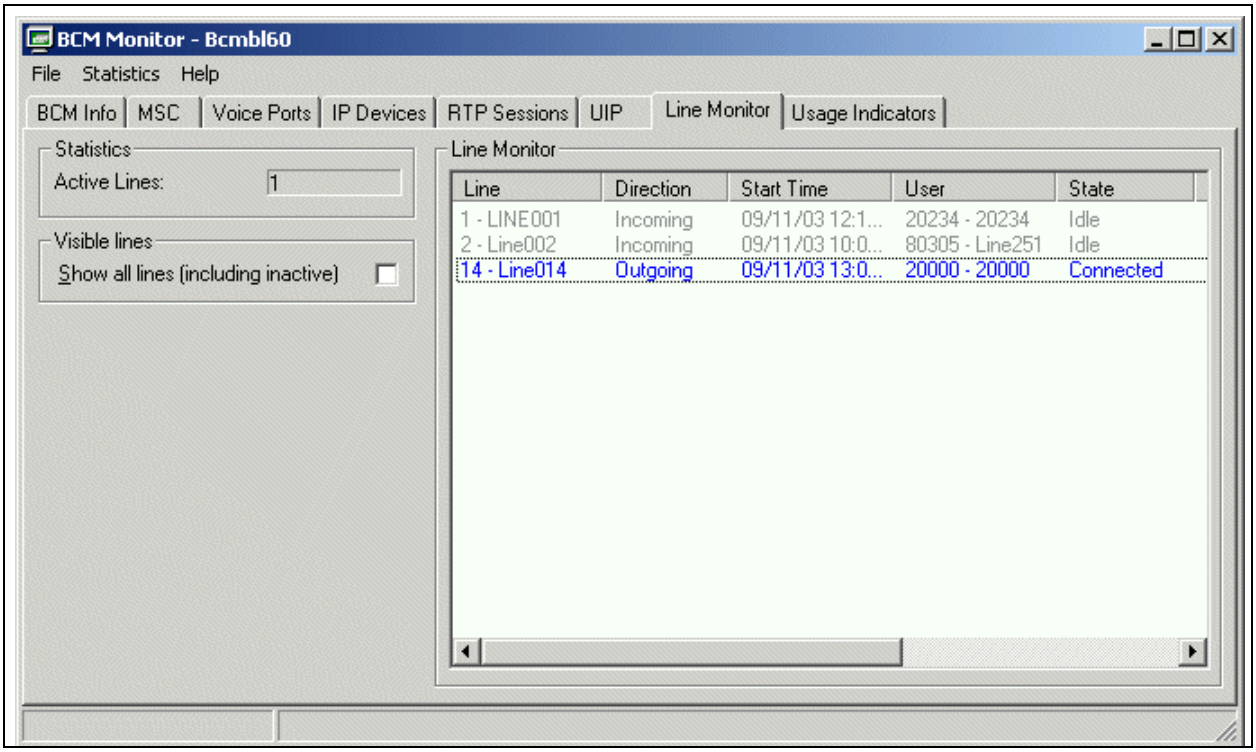
Figure 50 BCM Monitor UIP screen



Line monitor screen

The Line Monitor screen shows the status of the lines on Business Communications Manager.

Figure 51 BCM Monitor line monitor screen

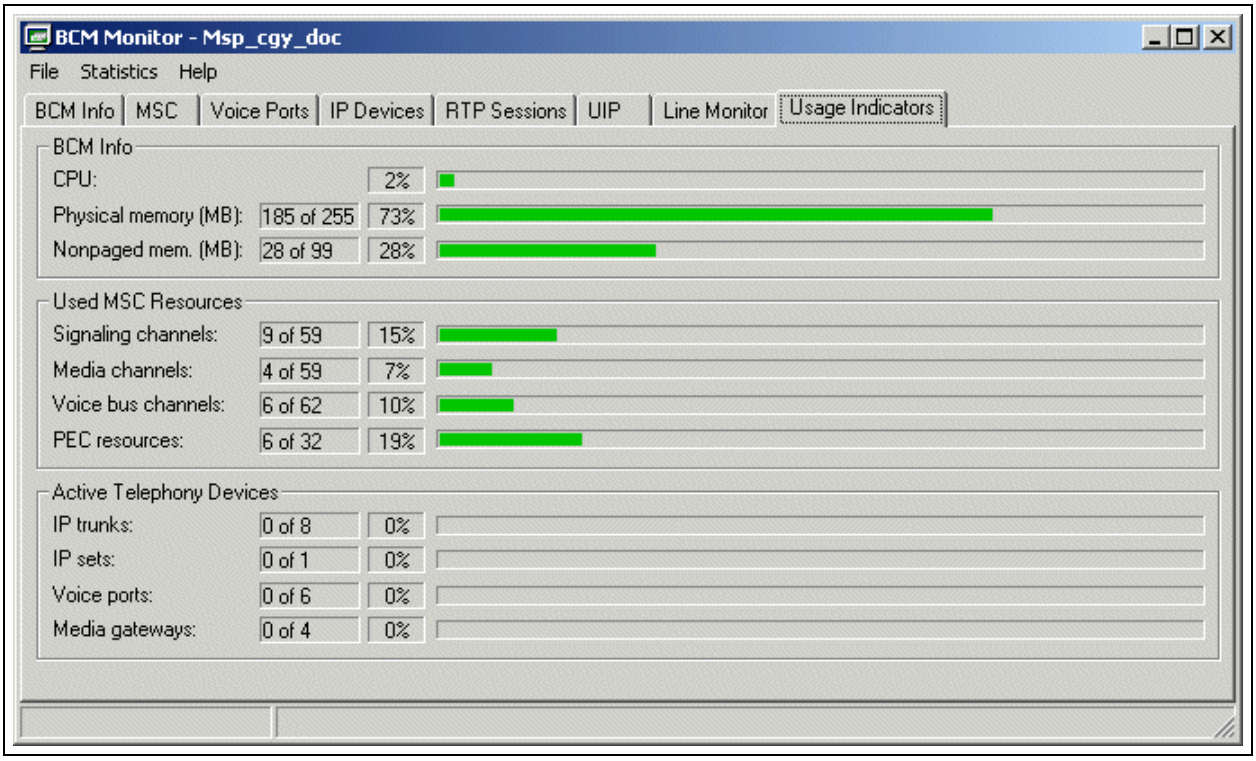


Usage indicators screen

This screen displays real time information about the BCM system's CPU and memory use, use of MSC resources and active IP telephony devices. This information can be statically captured for an on-demand view of the system, or can be dynamically logged.

- System status includes absolute and statistical view of CPU usage and memory usage.
- MSC resource information includes active signaling channels, media channels, voice bus channels, and PEC resources. MSC resource usage is reported as an absolute figure (for example: "Signalling channels: 29 of 59) as well as presented as a % of resource used.
- Active Telephony Devices reports on the number of active IP trunks, IP sets, voice ports, and media gateways.

Figure 52 BCM Monitor usage indicator tab screen display



BCM Monitor statistical values (minimum and maximums)

BCM Monitor stores the minimum and maximum values for many of the statistics that appear on BCM Monitor screens. For BCM Monitor to store the minimum and maximum values, the statistic must be a numeric value and must change over time. 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 (not a numeric value) and Serial Number (does not change).

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 quit BCM Monitor.

Topics in this section

Viewing minimum and maximum values

1. Click the value on the BCM Monitor screen 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 screen.

   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 screen while you are viewing the information on another screen.

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 occurr. To view the date and time:

1. Select the value for which you want to view the minimum or maximum value.
2. From the **Statistics** menu select **Show Min/Max Times**.
   A dialog box appears with the date and time when the minimum and maximum values occurred.
3. Select 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. On the **Statistics** menu, click **Reset Current Min/Max**
   or
   to reset the minimum and maximum values for all statistics: from the **Statistics** menu select **Reset All Min/Max**.

BCM Monitor information capture

You can information capture an instantaneous snapshot of the information into a text file (“static snapshot”). This is done by pre-selecting which of the BCM Monitor screens you want to capture, and invoking a “save” function to capture the required information into a static snapshot .txt file. The file name embeds time, date and Business Communications Manager name information to make it easy to view using MS Word or other program at a later time.

You can also do dynamic logging, in which BCM Monitor records snapshots at a user-specified frequency. This information is written into a file that is recognized by spreadsheet applications such as Excel. You can specify which information you want dynamically logged, and enable the automated dynamic snapshots to begin. The interval of time between successive snapshots can be specified in units of seconds. A maximum number of snapshots can be specified, or infinite logging. Once enabled, BCM Monitor dynamic logging writes the periodic snapshot information into a file on your workstation using the comma separated value (csv) file format.

Configuring the static snapshot settings

1. On the **File** menu, click **Snapshot Settings**.
   The Snapshot Settings screen appears.
2. Click the **Static snapshot settings** tab.
3. In the **Output filename** box, enter the filename for the static snapshot.
   You can also add additional information to the filename by selecting one or more of the options on the drop down list beside the Output filename box. The additional information available is:
   Auto-increment Counter — This option adds a series number to the filename. This number starts at 0000 and is incremented every time you take a static snapshot of this Business Communications Manager system.
   BCM name — This option adds the System Name of the Business Communications Manager

system to the filename.
Time — This options adds the time that the static snapshot was saved.
Date — This options adds the date that the static snapshot was saved.
When you select one of these options, a marker is added to the filename at the spot where the cursor is located. The actual information is not generated until you save the static snapshot.

4 In the **Output folder** box, enter the path of the folder where you want to store the static snapshots. To browse for the correct folder, click the button beside Output Folder box.

5 Ensure that all of the BCM Monitor tabs that have information you want included in the snapshot appear in the **Tabs saved in snapshot** box. For example, if you want the snapshot to include the statistic Active Lines which appears on the Line Monitor tab, ensure the Line Monitor tab is included in the Tabs saved in snapshot box.

6 Click the **OK** button.

Saving a static snapshot

1 Configure the static snapshot settings to ensure that information you want is stored in the static snapshot.

2 On the **File** menu, click **Save Static Snapshot**.
The information is stored in a file located in the folder you specified on the Static snapshot settings screen.

Configuring the dynamic snapshot settings

1 On the **File** menu, click **Snapshot Settings**.
The Snapshot Settings screen appears.

2 Click the **Dynamic snapshot settings** tab.

3 In the **Output filename** box, enter the filename for the dynamic snapshot.
You can also add additional information to the filename by selecting one or more of the options on the drop down list beside the Output filename box. The additional information available is:
Auto-increment Counter — This option adds a series number to the filename. This number starts at 0001 and is incremented every time you take a dynamic snapshot of this Business Communications Manager system.
BCM name — This option adds the System Name of the Business Communications Manager system to the filename.
Time — This options adds the time that the dynamic snapshot was started.
Date — This options adds the date that the dynamic snapshot was started.
When you select one of these options, a marker is added to the filename at the spot where the cursor is located. The actual information is not generated until you start the dynamic snapshot.

4 In the **Output folder** box, enter the path of the folder where you want to store the dynamic snapshots. To browse for the correct folder, click the button beside Output Folder box.

5 Ensure that all of the BCM Monitor tabs that have information you want included in the snapshot appear in the **Tabs saved in snapshot** box. For example, if you want the snapshot to include the statistic Active Lines which appears on the Line Monitor tab, ensure the Line Monitor tab is included in the Tabs saved in snapshot box.

6 Select the **Enable automatic snapshot** check box.
The **Automatic snapshot interval** and **Number of snapshots** boxes become available.
If you clear the **Enable automatic snapshot** check box, a single snapshot is taken when you start this dynamic snapshot instead of a series of snapshots.

7 In the **Automatic snapshot interval** box, use the arrow buttons to select the amount of time in seconds that you want BCM Monitor to wait between taking snapshots.

8 In the **Number of snapshots** box, use the arrows buttons to select the number of snapshots that you want BCM Monitor to take before stopping. If you want BCM monitor to continue taking snapshots until you stop the dynamic snapshot, select **Infinite**.

9 Click the **OK** button.

Starting a dynamic snapshot

1 Configure the dynamic snapshot settings to ensure that information you want is stored in the series of snapshots.

2 On the **File** menu, click **Dynamic Snapshot** and then click **Start**.
BCM Monitor starts taking snapshots and stores the resulting snapshots in a file located in the folder you specified on the Dynamic snapshot settings screen.

BCM Monitor continues taking snapshots until it reaches the number of snapshots specified in the **Number of snapshots** box, or until you stop the dynamic snapshot.

Stopping a dynamic snapshot

1 On the **File** menu, click **Dynamic Snapshot** and then click **Stop**.

Chapter 6
Performance Management

This section has information about managing the performance of the Business Communications Manager network.

Performance Management topics

System Performance tools and services

The Business Communications Manager network uses these software applications to monitor system performance:

- **Unified Manager**: A web-based configuration and maintenance application bundled with Business Communications Manager software. Unified Manager is the single point of access for managing programming for individual BCM systems. Access to the Unified Manager is password protected, and is secure for both enterprise customers and small to medium-sized businesses. Administrators use Unified Manager to set up BCM telephony and data functions, users, mailboxes, and directory numbers.
- **BCM Monitor**: A standalone diagnostic tool you can use to view system and IP telephony information on individual Business Communications Manager units. Open several instances of BCM Monitor to monitor several remote BCMs on a single PC simultaneously. This tool supports real-time debugging. You can also save and process data at a later time to generate system utilization and traffic reports. For more information about BCM Monitor, see Chapter 5, "BCM Monitor.
- **MIB II and MS Windows NT Performance MIBs**: With these MIB, you can query BCM performance and usage information using SNMP.

Unified Manager Performance Monitor

The Unified Manager performance monitor tool provides detailed performance information for the system and the system resources. The statistics are shown in charts or table format. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

Performance monitor is available for these Unified Manager navigation tree selections:

- System (see "System Performance Monitor" on page 352).
- Resources (see "Resources Performance Monitor" on page 355)

Use the statistical information to determine the most appropriate time for maintenance activities such as backups, system tests, batch jobs or archlogs.

Note: Generating statistics puts an additional workload on the Business Communications Manager server CPU, connecting network, and web client. Exercise caution when running statistics.

System Performance Monitor

With the system performance monitor you can access performance measurement graphical tools that display overall system performance metrics. Business Communications Manager provides statistical information on system throughput and other performance-related information.

System performance information includes:

- System CPU Usage Graph (see "To access the System CPU Usage Graph" on page 353)
- System CPU Usage Table (see "To access the System CPU Usage Table" on page 353)
- Memory Usage Graph (see "To access the Memory Usage Graph" on page 354)
- Memory Usage Table (see "To access the Memory Usage Table" on page 354)

Accessing the System CPU Usage Graph and Table

The System CPU Usage Graph displays real-time statistical information on processing activity levels.

The system samples CPU processing activity and presents the information in a graph format. The graph displays the percentage of CPU processing resources consumed over a period of time. The *x*-axis indicates the polling intervals. The *y*-axis indicates the percentage of CPU computing resources used at a point in time. The graph shows measurements over several intervals.

The graph also displays the minimum, average and peak CPU usage percentage for each second.

To access the System CPU Usage Graph

1 On the Unified Manager navigation tree click the **System** heading.

2 On the top menu click **Performance** and select **System CPU Usage Graph**.

- To pause the sampling, click the **Paused** button.
  To resume sampling, click **Paused** again.
- To reset the CPU usage values to zero, click the **Reset** button.
  The CPU usage values are reset and the system continues to display statistics.
- You can select a polling interval from the **Polling Interval** list box.
  The polling intervals range from 200 -10,000 ms.

To access the System CPU Usage Table

The System CPU Usage Table displays real-time statistical information on processing activity load.

The system samples CPU processing activity and presents the information in a table format. The table displays the percentage of CPU processing resources consumed over a period of time. The table updates the information in accordance with the polling interval selected. The table also displays the minimum, average and peak CPU usage percentage for each interval.

1 On the Unified Manager navigation tree click the **System** heading.

2 On the top menu click **Performance** and select **System CPU Usage Table**.

3 Select a polling interval.
The polling intervals are 200, 500, 1000, 2000 or 5000 ms.

Accessing the Memory Usage Graph and Table

The Memory Usage Graph displays real-time statistical information on computing memory consumption or availability. The system samples CPU memory availability and presents the information in a graph.

The *x*-axis indicates the polling intervals. The *y*-axis indicates the amount of CPU memory consumed (bytes) used at a point in time. The graph shows measurements over several intervals.

The graph displays either:

- percentage of CPU memory required over a period of time (committed bytes)
  or
- percentage of CPU memory available over a period of time (available bytes)

The system updates the information displayed in the graph according to the polling interval you select. The graph also displays the last reported, average and peak CPU memory for each interval.

The Memory Usage Table displays real-time statistical information on computing memory consumption or availability in a table.

The Memory Usage Table displays:

- percentage of CPU memory required over a period of time (committed bytes)
- percentage of CPU memory available over a period of time (available bytes)

The table updates the information according to the polling interval you select. The table also displays the minimum, average and peak CPU usage percentage for each interval.

To access the Memory Usage Graph

1. On the Unified Manager navigation tree click the **System** heading.
2. On the top menu click **Performance** and select **Memory Usage Graph**.
   - To pause the sampling, click the **Paused** button.
     To resume sampling, click the Paused button again.
   - To reset the memory values to zero, click the **Reset** button.
     The memory values are reset and the system continues to display statistics.
   - You can select a polling interval from the **Polling Interval** list box.
     The polling intervals range from 200 -10,000 ms.

To access the Memory Usage Table

1. On the Unified Manager navigation tree click the **System** heading.
2. On the top menu click **Performance** and select **Memory Usage Table**.
3. Select a polling interval.
   The polling intervals are 200, 500, 1000, 2000 or 5000 ms.

Memory usage counter types

The memory usage graph and table selections display system and operational statistics. When you display the memory usage graph, you can select and display statistics for one of these counter types:

- **Committed bytes**: The ratio of the Committed Bytes to the Commit Limit. This represents the amount of available virtual memory in use. Note that the Commit Limit may change if the paging file is extended. This is an instantaneous value, not an average.
- **Available bytes**: The size of the virtual memory currently on the Zeroed, Free, and Standby lists. Zeroed and Free memory is ready for use, with Zeroed memory cleared to zeros. Standby memory is memory removed from a process's Working Set but still available. Notice that this is an instantaneous count, not an average over the time interval.

Resources Performance Monitor

With the system resources performance monitor you can access performance measurement graphical tools that display performance metrics on these system resources:

Business Communications Manager provides statistical information on system throughput and other performance-related information. For information on how to configure and optimize network traffic and communications devices, see the *Programming Operations Guide*.

Accessing the Resources Performance Monitor

This section contains topics about using the performance monitor to observe packet-based activity on Business Communications Manager:

Accessing the IP Packets graph and table

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file, such as an e-mail message, HTML file, GIF file, URL request, and so forth, is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file.

To access the IP Packets Graph and Table

1 On the Unified Manager navigation tree click the **Resources** heading.

2 On the top menu click **Performance** and select **IP Packets Graph or IP Packets Table**.

IP Packet counter types

The IP Packets graph and table selections display IP-related network traffic statistics. When you display the IP Packets graph, you can select and display statistics for one of these counter types.

Table 19 IP Packet counter types

IP Packets Forwarded	Rate of input datagrams for this entity that was not their final IP destination, as a result of which an attempt was made to find a route to forward them to the final destination. In entities that do not act as IP Gateways, this rate includes only packets that were source-routed via this entity, and the source-route option processing was successful.
Outbound discarded	Output IP datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space.) This counter includes datagrams counted in datagrams forwarded if any packets met this (discretionary) discard criterion.
Outbound - no route	IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in datagrams forwarded that meet this `no route' criterion.
Received address errors	Input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0. 0.0) and addresses of unsupported classes (e.g., Class E). For entities that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received delivered	Rate that input datagrams are successfully delivered to IP user-protocols (including ICMP).
Received discarded	Input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for lack of buffer space, for example). This counter does not include any datagrams discarded while awaiting re-assembly.

Table 19 IP Packet counter types

Received header errors	Input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Received unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received	Rate that IP datagrams are received from the interfaces, including those received in error.
Sent	Rate that IP datagrams are supplied to IP for transmission by local IP user-protocols (including ICMP). This counter does not include any datagrams counted in datagrams forwarded.
Datagrams	Rate that IP datagrams are received from or sent to the interfaces, including those received or sent in error. Forwarded datagrams are not included in this rate.
Fragment re-assembly errors	Number of failures detected by the IP re-assembly algorithm for whatever reason, such as timed out, errors, etc.
Fragmentation failures	Number of IP datagrams discarded because they needed to be fragmented at this entity but could not be, for example because their Don't Fragment flag was set.
Fragmented datagrams	Rate that datagrams were fragmented at this entity.
Fragments created	Rate that IP datagram fragments were generated because of fragmentation at this entity.
Fragments re-assembled	Rate that IP fragments are re-assembled.
Fragments received	Rate that IP fragments that need to be re-assembled at this entity are received.

Accessing the ICMP Packets graph and table

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams and are processed by the TCP/IP software.

To access the ICMP Packets Graph and Table

1 On the Unified Manager navigation tree click the **Resources** heading.

2 On the top menu click **Performance** and select **ICMP Packets Graph** or **ICMP Packets Table**.

ICMP Packet counter types

The ICMP Packets graph and table selections display ICMP-related network traffic statistics. When you display the ICMP Packets graph, you can select one of these counter types:

Table 20 ICMP Packet counter types

Messages outbound errors	ICMP messages that this entity did not send due to problems in ICMP such as lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there can be no types of error that contribute to this counter's value.
Messages received errors	ICMP messages that the entity received but determined as having errors such as bad ICMP checksums, bad length.
Messages received	Rate that ICMP messages are received by the entity including messages received in error.
Messages sent	Rate that ICMP messages are attempted to be sent by the entity including messages sent in error.
Messages	Total rate that ICMP messages are received and sent by the entity including messages received or sent in error.
Received address mask	ICMP Address Mask Request messages received.
Received address mask reply	ICMP Address Mask Reply messages received.
Received destination unreachable	ICMP Destination Unreachable messages received.
Received echo reply	Rate of ICMP Echo Reply messages received.
Received echo	Rate of ICMP Echo messages received.

Table 20 ICMP Packet counter types

Received parameter problem	ICMP Parameter Problem messages received.
Received redirect	Rate of ICMP Redirect messages received.
Received source quench	ICMP Source Quench messages received.
Received time exceeded	ICMP Time Exceeded messages received.
Received timestamp reply	Rate of ICMP Timestamp Reply messages received.
Received timestamp	Rate of ICMP Timestamp (request) messages received.
Sent address mask	ICMP Address Mask Request messages sent.
Sent address mask reply	ICMP Address Mask Reply messages sent.
Sent destination unreachable	ICMP Destination Unreachable messages sent.
Sent echo reply	Rate of ICMP Echo Reply messages sent.
Sent echo	Rate of ICMP Echo messages sent.
Sent parameter problem	ICMP Parameter Problem messages sent.
Sent redirect	Rate of ICMP Redirect messages sent.
Sent source quench	ICMP Source Quench messages sent.
Sent time exceeded	ICMP Time Exceeded messages sent.
Sent timestamp reply	Rate of ICMP Timestamp Reply messages sent.
Sent timestamp	Rate of ICMP Timestamp (request) messages sent.

Accessing the UDP Packets graph and table

User Datagram Protocol (UDP) is a transport layer protocol designed to improve performance of message transfer between a host server and a gateway to the Internet. UDP uses IP for data transfer and as a result, relies on a best effort delivery strategy. UDP establishes a host-to-host communication channel to deliver packets between processes running on two different Business Communications Manager systems. The MSC, for example, uses the UDP protocol to enable the T.38 fax feature.

To access the UDP Packets Graph and Table

1. On the Unified Manager navigation tree click the **Resources** heading.
2. On the top menu click **Performance** and select **UDP Packets Graph** or **UDP Packets Table**.

UDP Packet counter types

The UDP Packets graph and table selections display UDP-related network traffic statistics. When you display the UDP Packets graph, you can select a counter type:

Table 21 UDP Packet counter types

Datagrams no port	Rate of received UDP datagrams for which there was no application at the destination port.
Datagrams received errors	Received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Datagrams received	Rate that UDP datagrams are delivered to UDP users.
Datagrams sent	Rate that UDP datagrams are sent from the entity.
Datagrams	Rate that UDP datagrams are sent or received by the entity.

Accessing the TCP Packets graph and table

Transport Control Protocol (TCP) is transport layer component that provides the connection point through which applications access network services. TCP use IP, and as a result, uses a best effort delivery strategy. IP encapsulates TCP information in datagrams and delivers the data across router-connected internetworks.

To access the TCP Packets Graph and Table

1. On the Unified Manager navigation tree click the **Resources** heading.
2. On the top menu click **Performance** and select **TCP Packets Graph or TCP Packets Table**.

TCP Packet counter types

The TCP Packets graph and table selections display TCP-related network traffic statistics. When you display the TCP Packets graph, you can select a counter type.

Table 22 TCP Packet counter types

Connection failures	Rate that TCP segments are sent or received using the TCP protocol.
Connections archive	Number of times TCP connections made a direct transition to the syn-sent state from the closed state.
Connections established	TCP connections for which the current state is either established or close-wait.
Connections passive	Number of times TCP connections made a direct transition to the syn-rcvd state from the listen state.
Connections reset	Number of times TCP connections made a direct transition to the closed state from either the established state or the close-wait state.
Segments received	Rate that segments are received, including those received in error and segments received on currently established connections.
Segments retransmitted	Rate that segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes.
Segments sent	Rate that segments are sent, including those on current connections, but excluding those containing only retransmitted bytes.
Segments	Rate that TCP segments are sent or received using the TCP protocol.

Accessing the LAN performance monitor

This section describes how to access and use the LAN performance monitor to analyze LAN traffic characteristics.

- "Accessing the QoS Graph and Table" on page 368)
- "Accessing the QoS Queue 1-5 Graph and Table" on page 369)
- "Accessing the QoS Queue 6-9 Graph and Table" on page 370)

Accessing the LAN graph and table

The statistics compiled by the system indicate packet traffic over the LAN. A packet is the unit of data that is routed between an origin and a destination over the LAN.

Each packet is separately numbered and includes the LAN IP address of the destination. When the packets have all arrived, they are reassembled into the original file.

To access the LAN Graph and Table

1. On the Unified Manager navigation tree click the **Resources** and **LAN** keys, and click the heading for the LAN resource you want to see the performance for, for example LAN 1. The LAN summary page appears.
2. On the top menu click **Performance** and select a LAN performance monitor selection:
   - LAN Graph
   - LAN Table
   - QoS Graph (see "Accessing the QoS Graph and Table)
   - QoS Table (see "Accessing the QoS Graph and Table)
   - QoS Queue 1-5 Graph (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 1-5 Table (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 6-9 Graph (see "Accessing the QoS Queue 6-9 Graph and Table)
   - QoS Queue 6-9 Table (see "Accessing the QoS Queue 6-9 Graph and Table)

LAN counter types

The LAN graph and table selections display LAN-related network traffic statistics. When you display the LAN graph, you can select a counter type:

Table 23 LAN counter types

Byte received/sec	Rate that bytes are received on the interface, including framing characters.
Byte sent/sec	Rate that bytes are sent on the interface, including framing characters.

Table 23 LAN counter types

Byte total/sec	Rate that bytes are sent and received on the interface, including framing characters.
Current bandwidth	Estimate of the interface's current bandwidth in bits per second (bps). For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.
Output queue length	Length of the output packet queue in packets. If this is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible. Since the requests are queued by NDIS in this implementations, this will always be 0.
Packets outbound discarded	Outbound packets discarded even though no errors were detected to prevent their being transmitted. A possible reason for discarding a packet is to free up buffer space.
Packets outbound errors	Outbound packets that could not be transmitted because of errors.
Packets received discarded	Inbound packets chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet is to free up buffer space.
Packets received errors	Inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets received non-unicast/sec	Rate that non-unicast (that is, subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.
Packets received unicast/ sec	Rate that (subnet) unicast packets are delivered to a higher-layer protocol.
Packets received unknown	Packets received via the interface that were discarded because of an unknown or unsupported protocol.
Packets received/sec	Rate that packets are received on the network interface.
Packets sent non-unicast/ sec	Rate that packets are requested to be transmitted to non-unicast (that is, subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets sent unicast/sec	Rate that packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets sent/sec	Rate that packets are sent on the network interface.
Packets/sec	Rate that packets are sent and received on the network interface.

Accessing the WAN performance monitor

This section describes how to access and use the WAN performance monitor to analyze WAN traffic characteristics and also contains these topics:

Accessing the WAN graph and table

The statistics compiled by the system indicate packet traffic over the WAN. A packet is the unit of data that is routed between an origin and a destination over the WAN.

Each packet is separately numbered and includes the WAN IP address of the destination. When the packets have all arrived, they are reassembled into the original file.

To access the WAN Graph and Table

1. On the Unified Manager navigation tree click the **Resources** and **WAN** keys, and click the heading for the WAN resource you want to see the performance for, for example WAN 1. The WAN summary page appears.
2. On the top menu click **Performance** and select a WAN performance monitor selection:
   - WAN Graph
   - WAN Table
   - QoS Graph (see "Accessing the QoS Graph and Table)
   - QoS Table (see "Accessing the QoS Graph and Table)
   - QoS Queue 1-5 Graph (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 1-5 Table (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 6-9 Graph (see "Accessing the QoS Queue 6-9 Graph and Table)
   - QoS Queue 6-9 Table (see "Accessing the QoS Queue 6-9 Graph and Table)

WAN counter types

The WAN graph and table selections display WAN-related network traffic statistics. When you display the WAN graph, you can select a counter type.

Byte received/sec	Rate that bytes are received on the interface, including framing characters.
Byte sent/sec	Rate that bytes are sent on the interface, including framing characters.
Byte total/sec	Rate that bytes are sent and received on the interface, including framing characters.

Current bandwidth	Estimate of the interface's current bandwidth in bits per second (bps). For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.
Output queue length	Length of the output packet queue (in packets.) If this is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible. Since the requests are queued by NDIS in this implementations, this will always be 0.
Packets outbound discarded	Outbound packets discarded even though no errors were detected to prevent their being transmitted. A reason for discarding a packet is to free up buffer space.
Packets outbound errors	Outbound packets that could not be transmitted because of errors.
Packets received discarded	Inbound packets discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. A reason for discarding a packet is to free up buffer space.
Packets received errors	Inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets received non-unicast/sec	Rate that non-unicast (that is, subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.
Packets received unicast/ sec	Rate that (subnet) unicast packets are delivered to a higher-layer protocol.
Packets received unknown	Packets received via the interface that were discarded because of an unknown or unsupported protocol.
Packets received/sec	Rate that packets are received on the network interface.
Packets sent non-unicast/ sec	Rate that packets are requested to be transmitted to non-unicast (that is, subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets sent unicast/sec	Rate that packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes packets that were discarded or not sent.
Packets sent/sec	Rate that packets are sent on the network interface.
Packets/sec	Rate that packets are sent and received on the network interface.

Accessing the Dial Up performance monitor

This section describes how to access and use the Dial Up performance monitor to analyze dialup traffic characteristics. The statistics compiled by the system indicate packet traffic over the dial up connection. A packet is the unit of data that is routed between an origin and a destination over the dial up connection.

Each packet is separately numbered and includes the IP address of the dial up destination. When the packets have all arrived, they are reassembled into the original file.

This section contains these topics:

To access the dialup performance manager

1 On the Unified Manager navigation tree click the **Resources** key and the **Dial Up** heading.

2 On the top menu click **Performance** and select a performance monitor selection:

- **Qos Graph (**see "Accessing the QoS Graph and Table)
- QoS Table (see "Accessing the QoS Graph and Table)
- QoS Queue 1-5 Graph (see "Accessing the QoS Queue 1-5 Graph and Table)
- QoS Queue 1-5 Table (see "Accessing the QoS Queue 1-5 Graph and Table)
- QoS Queue 6-9 Graph (see "Accessing the QoS Queue 6-9 Graph and Table)
- QoS Queue 6-9 Table (see "Accessing the QoS Queue 6-9 Graph and Table)

Accessing the UTWAN performance monitor

This section describes how to access and use the UTWAN performance monitor to analyze dialup traffic characteristics. The statistics compiled by the system indicate packet traffic over the UTWAN. A packet is the unit of data that is routed between an origin and a destination over the UTWAN.

Each packet is separately numbered and includes the IP address of the destination over the UTWAN. When the packets have all arrived, they are reassembled into the original file.

Accessing the WAN graph and table

The statistics compiled by the system show packet traffic over the WAN. A packet is the unit of data that is routed between an origin and a destination over the WAN.

Each packet is separately numbered and includes the WAN IP address of the destination. When the packets have all arrived, they are reassembled into the original file.

To access the WAN Graph and Table

1. On the Unified Manager navigation tree click the **Resources** and **WAN** keys, and click the heading of the WAN resource you want to see.
2. On the top menu click **Performance** and select an item:
   - UTWAN Graph
   - UTWAN Table
   - QoS Graph (see "Accessing the QoS Graph and Table)
   - QoS Table (see "Accessing the QoS Graph and Table)
   - QoS Queue 1-5 Graph (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 1-5 Table (see "Accessing the QoS Queue 1-5 Graph and Table)
   - QoS Queue 6-9 Graph (see "Accessing the QoS Queue 6-9 Graph and Table)
   - QoS Queue 6-9 Table (see "Accessing the QoS Queue 6-9 Graph and Table)

The performance statistics are the same as those measured for a UTWAN. For more information, see:

- "Accessing the QoS Graph and Table" on page 368)
- "Accessing the QoS Queue 1-5 Graph and Table" on page 369)
- "Accessing the QoS Queue 6-9 Graph and Table" on page 370)

Accessing the QoS Graph and Table

QoS (Quality of Service), refers to guaranteed throughput level. QoS lets a server 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 uses high bandwidth.

The QoS monitor gathers information on the volume of data associated with maintaining QoS. Use the Quality of Service (QoS) monitor to observe the QoS system performance.

To access the QoS Graph and Table

1 On the Unified Manager navigation tree click the **Resources** and **LAN** keys, and click the heading of the LAN resource you want to see.

2 On the top menu click **Performance** and select an item:

- QoS Graph
- QoS Table
- QoS Queue 1-5 Graph
- QoS Queue 1-5 Table
- QoS Queue 6-9 Graph
- QoS Queue 6-9 Table

QoS counter types

The QoS graph and table selections display quality of service related network traffic statistics.

Table 24 QoS counter types

Priority sessions not served	Priority sessions not served.
Priority sessions requested	Priority sessions requested.
Priority sessions served	Priority sessions served.
Total best-effort octets	Best-effort queues octets since system reboot.
Total best-effort packets	Best-effort queues packets since system reboot.
Total dropped octets	Octets dropped since system reboot.
Total dropped packets	Packets dropped since system reboot.

Table 24 QoS counter types

Total octets	Octets since system reboot.
Total packets	Packets since system reboot.
Total priority packets	Priority queue octets since system reboot.

Accessing the QoS Queue 1-5 Graph and Table

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.

Use the Quality of Service (QoS) monitor to observe the system performance for queued octets, packets and packets dropped (range 1 - 5).

To access the QoS Queue 1-5 Graph and Table

1. On the Unified Manager navigation tree click the **Resources** and **LAN** keys, and click the heading of the LAN resource you want to see.
2. On the top menu click **Performance** and select **QoS Queue 1-5 Graph** or **QoS Queue 1-5 Table**.

QoS Queue 1-5 counter types

The QoS 1-5 graph and table selections display quality of service related network traffic statistics.

Table 25 Qos Queue 1-5 counter types

Total queue 1 octets	Queue 1 octets since system reboot.
Total queue 1 packets	Queue 1 packets since system reboot.
Total queue 1 packets dropped	Queue 1 packets dropped since system reboot.
Total queue 2 octets	Queue 2 octets since system reboot.
Total queue 2 packets	Queue 2 packets since system reboot.

Table 25 Qos Queue 1-5 counter types

Total queue 2 packets dropped	Queue 2 packets dropped since system reboot.
Total queue 3 octets	Queue 3 octets since system reboot.
Total queue 3 packets	Queue 3 packets since system reboot.
Total queue 3 packets dropped	Queue 3 packets dropped since system reboot.
Total queue 4 octets	Queue 4 octets since system reboot.
Total queue 4 packets	Queue 4 packets since system reboot.
Total queue 4 packets dropped	Queue 4 packets dropped since system reboot.
Total queue 5 octets	Queue 5 octets since system reboot.
Total queue 5 packets	Queue 5 packets since system reboot.
Total queue 5 packets dropped	Queue 4 packets dropped since system reboot.

Accessing the QoS Queue 6-9 Graph and Table

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.

Use the Quality of Service (QoS) monitor to observe the system performance for queued octets, packets and packets dropped (range 6 - 9).

To access the QoS Queue 6-9 Graph and Table

1. On the Unified Manager navigation tree click the **Resources** and **LAN** keys, and click the heading of the LAN resource you want to see.
2. On the top menu click **Performance** and select **QoS Queue 6-9 Graph** or **QoS Queue 6-9 Table**.

QoS Queue 6-9 counter types

The QoS 6-9 graph and table selections display quality of service related network traffic statistics.

Table 26 Qos Queue 6-9 counter types

Total queue 6 octets	Queue 6 octets since system reboot.
Total queue 6 packets	Queue 6 packets since system reboot.
Total queue 6 packets dropped	Queue 6 packets dropped since system reboot.
Total queue 7 octets	Queue 7 octets since system reboot.
Total queue 7 packets	Queue 7 packets since system reboot.
Total queue 7 packets dropped	Queue 7 packets dropped since system reboot.
Total queue 8 octets	Queue 8 octets since system reboot.
Total queue 8 packets	Queue 8 packets since system reboot.
Total queue 8 packets dropped	Queue 8 packets dropped since system reboot.
Total queue 9 octets	Queue 9 octets since system reboot.
Total queue 9 packets	Queue 9 packets since system reboot.
Total queue 9 packets dropped	Queue 8 packets dropped since system reboot.

SNMP Performance Management

MIB II

Business Communications Manager supports MIB II (RFC1213), providing access to MIB II performance and platform information. This information can be polled from an SNMP-capable management framework. MIB II information, relevant to the BCM, includes availability and status of data LAN and WAN interfaces (including dial-up V.90 and ISDN interfaces) (for example, interface type, interface bandwidth, interface status, interface packet counts) and router performance data (if the BCM router is enabled) including packet throughput, packets dropped or forwarded. For more information about BCM MIBs see AppendixA, “Management Information Base (MIB) System.

MIB II information is about these WAN/LAN interface counters

- bytes received
- bytes sent
- bytes total
- current bandwidth
- output queue length
- packets outbound discarded
- packets outbound errors
- packets received discarded
- packets received errors
- packets received non-unicast
- packets received unicast
- packets received unknown
- packets received
- packets sent non-unicast
- packets sent unicast
- packets sent
- packets

MS Windows NT Performance MIBs

Use the MS Windows NT Performancs MIB to monitor some BCM performance statistics, including Memory, Processor, Network Interface, Physical Disk, Locgical Disk, Paging FIle, Process, TCP, IP, and UDP. The MS Windows NT Performancs MIB defines these perfomance counters.

Table 27 MS Windows NT Performance MIBs

MIB group name	Group objects
memory	Available Bytes, Committed Bytes, Commit Limit, Page Faults Per Sec, Write Copies Per Sec, Transition Faults Per Sec, Cache Faults Per Sec, Demand Zero Faults Per Sec, Pages Per sec, Pages Input Per Sec, Page Reads Per Sec, Pages Output Per Sec, Page Writes Per Sec, Pool Paged Bytes, Pool Nonpaged Bytes, Pool Paged Allocs, Pool Nonpaged Allocs, Free System Page Table Entries, Cache Bytes, Cache Bytes Peak, Pool Paged Resident Bytes, System Code Total Bytes, System Code Resident Bytes, System Driver Total Bytes, System Driver Resident Bytes, System Cache Resident Bytes, Committed Bytes In Use (%)
processor	**cpuprocessTable** Instance Name, Processor Time (%), User Time (%), Privileged Time (%), Interrupts Per Sec, DPC Time (%), Interrupt Time (%), DPCs Queued Per Sec, DPC Rate, DPC Bypasses Per Sec, APC Bypasses Per Sec
network interface	**network-InterfaceTable** Instance Name, Bytes Total Per Sec, Packets Per Sec, Packets Received Per Sec, Packets Sent Per Sec, Current Bandwidth, Bytes Received Per Sec, Packets Received Unicast Per Sec, Packets Received Non-Unicast Per Sec, Packets Received Discarded, Packets Received Errors, Packets Received Unknown, Bytes Sent Per Sec, Packets Sent Unicast Per Sec, Packets Sent Non-Unicast Per Sec, Packets Outbound Discarded, Packets Outbound Errors, Output Queue Length
physicalDisk	**pdiskphysicalDiskTable** Instance Name, Current Disk Queue Length, Disk Time (%), Avg. Disk Queue Length, Disk Read Time (%), Avg. Disk Read Queue Length, Disk Write Time (%), Avg. Disk Write Queue Length, Avg. Disk sec Per Transfer, Avg. Disk sec Per Read, Avg. Disk sec Per Write, Disk Transfers Per sec, Disk Reads Per Sec, Disk Writes Per Sec, Disk Bytes Per Sec, Disk Read Bytes Per Sec, Disk Write Bytes Per Sec
logicalDisk	**ldisklogicalDiskTable** Instance Name, Free Space (%), Free Megabytes, Current Disk Queue Length, Disk Time (%), Avg. Disk Queue Length, Disk Read Time (%), Avg. Disk Read Queue Length, Disk Write Time (%), Avg. Disk Write Queue Length, Avg. Disk sec Per Transfer, Avg. Disk sec Per Read, Avg. Disk sec Per Write, Disk Transfers Per sec, Disk Reads Per sec, Disk Writes Per sec, Disk Bytes Per sec, Disk Read Bytes Per sec, Disk Write Bytes Per sec
pagingFile	**pagefilepaging-FileTable** Instance Name, Usage (%), Usage Peak (%)

Table 27 MS Windows NT Performance MIBs

MIB group name	Group objects
process	**processprocessTable** Instance Name, Processor Time (%), User Time (%), Privileged Time (%), Virtual Bytes Peak, Virtual Bytes, Page Faults Per sec, Working Set Peak, Working Set, Page File Bytes Peak, Page File Bytes, Private Bytes, Thread Count, Priority Base, Elapsed Time, ID Process, Pool Paged Bytes, Pool Nonpaged Bytes, Handle Count
tCP	Segments Per sec, Connections Established, Connections Active, Connections Passive, Connection Failures, Connections Reset, Segments Received Per sec, Segments Sent Per sec, Segments Retransmitted Per sec
iP	Datagrams Per sec, Datagrams Received Per sec, Datagrams Received Header Errors, Datagrams Received Address Errors, Datagrams Forwarded Per sec, Datagrams Received Unknown Protocol, Datagrams Received Discarded, Datagrams Received Delivered Per sec, Datagrams Sent Per sec, Datagrams Outbound Discarded, Datagrams Outbound No Route, Fragments Received Per sec, Fragments Re-assembled Per sec, Fragment Re-assembly Failures, Fragmented Datagrams Per sec, Fragmentation Failures, Fragments Created Per sec
uDP	Datagrams Per sec, Datagrams Received Per sec, Datagrams No Port Per sec, Datagrams Received Errors, Datagrams Sent Per sec

Chapter 7
Performance Management Using NetIQ

This section has information about the third-party NetIQ performance management solution for Business Communications Manager.

Performance Management using NetIQ topics

The Vivinet Manager Suite from NetIQ is a robust platform and suite of modules that provides monitoring, management, and reporting for Nortel VoIP solutions. With Vivinet Manager you can proactively manage BCM system health, call quality, and network performance from a single console. Vivinet Manager ensures that service levels can be maintained through automated problem management, and lowers support costs by identifying and resolving potential problems before end users are affected.

Knowledge Scripts (KS) are provided with the Vivinet Manager solution, to manage availability and performance of IP Telephony systems and networks. These scripts use business or system management rules to collect data, monitor systems and/or respond with one or more actions.

NetIQ Vivinet Manager support for BCM delivers Knowledge Scripts, which monitor many aspects of BCM such as Voice over IP quality, CPU use, memory use, interface metrics, and others. This information is reported back to a centralized Vivinet Manager Server for display and reporting.

The NetIQ BCM solution requires NetIQ Vivinet Manager software which is sold, installed and supported by NetIQ, and a no-charge BCM NetIQ Agent Keycode to enable the feature on the BCMs under NetIQ management.

Note: Enabling the NetIQ feature causes QoS Monitor Logging to be enabled. If you are using H.323 VoIP trunking and QoS Monitor is enabled in support of that service, then having QoS Monitor Logging automatically enabled by the NetIQ feature ensures that MOS scores are automatically logged for use by the NetIQ Knowledge Scripts.

For more information about NetIQ Vivinet Manager support for BCM, go to http://www.netiq.com/products/vm/modules/nortel.asp

For details on how to use Vivinet Manager to support BCM performance monitoring, see "Working Smarter with Vivivnet Manager for Nortel Networks Business Communications Manager", available from NetIQ.

NetIQ feature overview

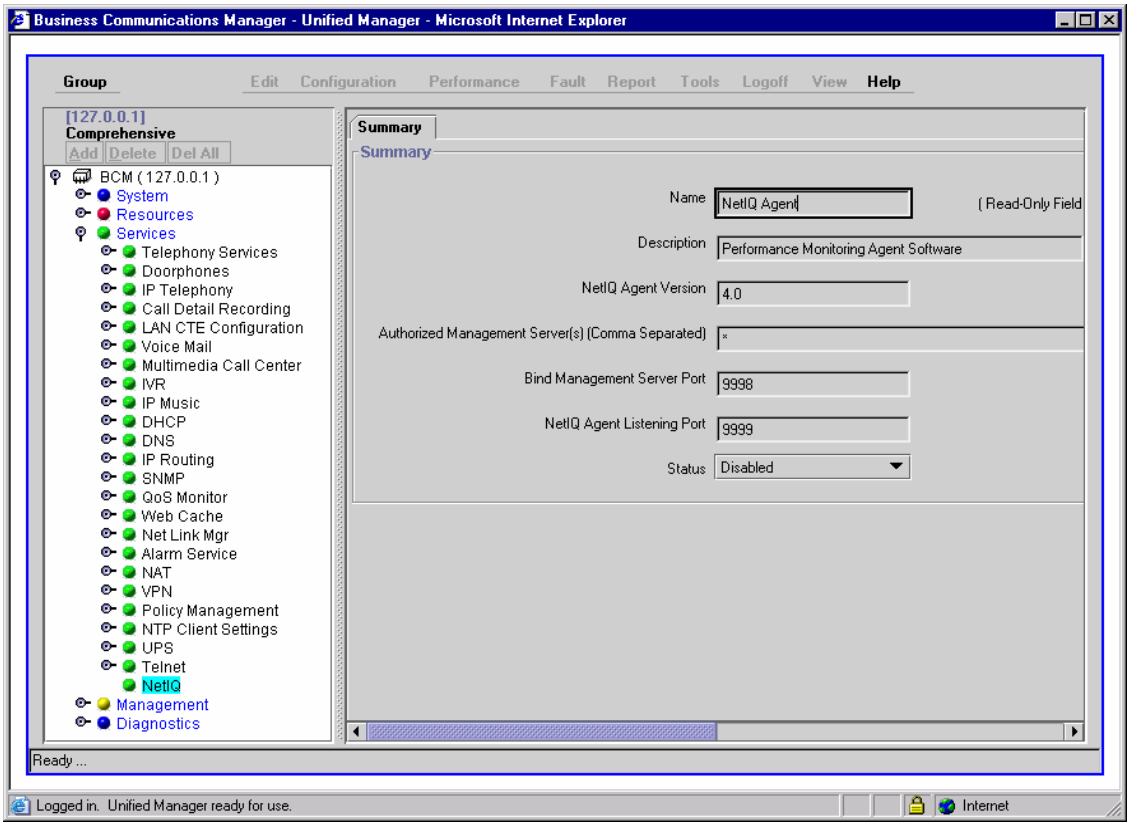
For a centralized NetIQ Vivinet Manager server to monitor the BCM, you must apply the NetIQ keycode on BCM and enable the feature. This enables the NetIQ agent software on Business Communications Manager. BCM can then be discovered by the NetIQ Vivinet Manager server, which directs the NetIQ agent on BCM to execute the Knowledge Scripts and forward data from BCM back to the Vivinet Manager server.

The IP address of the NetIQ Vivinet Manager and the ports used for communication between Vivinet Manager and the BCM can be configured through the Unified Manager NetIQ screen.

Use the NetIQ Feature

Use the NetIQ page, found under the Services heading in the Unified Manager (see Figure 53), to enable and configure the NetIQ feature.

Figure 53 NetIQ summary tab



Applying the NetIQ keycode

Before you configure the NetIQ feature to enable management of BCM by the NetIQ Vivinet Manager server, obtain and apply the NetIQ agent software authorization keycode. Go to **System -->Licensing-- >Keycode Files** in Unified Manager and use the Keycode File Location Information screen. For more information about using keycodes with the BCM, see the *Software Keycode Installation Guide*.

Field descriptions

This section provides detailed description of individual fields with their possible values.

Field name	Description
Name	Read-only name of the NetIQ agent.
Description	Read-only description of the NetIQ agent; this is a read-only field.
NetIQ Agent Version	Read-only version of the NetIQ agent you are using.

Field name	Description
Authorized Management Server(s) (comma separated)	IP addresses of the NetIQ management servers that the NetIQ agent running on BCM can communicate with. Valid values are comma-separated IP addresses or an asterisk (*). IP addresses identify the specific management servers to which the NetIQ agent allows communication. An asterisk (*) means the NetIQ agent allows communication with all NetIQ management servers. A blank field means the agent does not allow communication with any NetIQ management servers and is not permitted on BCM if the NetIQ feature is enabled.
Bind Management Server Port	RPC port number on the NetIQ management server that the NetIQ agent running on BCM uses to communicate with the server. Valid port range is 1 to 65535. Default port is 9999. If you change the port number, you must change the corresponding NetIQ management server port number to the same value.
NetIQ Agent Listening Port	RPD port number on BCM that the NetIQ agent uses to communicate with the NetIQ management server. Valid port range is 1 to 65535. Default port is 9998. If you change the port number, you must change the corresponding NetIQ management server port number to the same value.
Status	Shows whether the NetIQ agent is enabled. Values for this field are Enabled and Disabled.

Enabling the NetIQ feature

1. On the Unified Manager navigation tree, click the **System** key and the **Licensing** heading. The Licensing Setting screen appears.
2. On the top menu, click **Configuration** and select **Add a Keycode**. The Applied Keycodes dialog box appears.
3. Enter the NetIQ keycode and click the **Save** button.
4. In the Authorized Management Server(s) field, enter a list (separated by commas) of IP addresses of the Vivinet Manager servers to which you want to restrict access by the BCM. For example, enter 10.41.6.17, 10.41.7.18.

Note: Whether you enter one IP address or a list, you are restricting the BCM to respond only to the specified Vivinet Manager servers. To allow the BCM to respond to any Vivinet Manager server, enter an asterisk (*).

For the BCM to be managed by a Vivinet Manager server, this field must have a value in it and cannot be left blank.

5. Select **Enabled** in the Status field to enable the NetIQ agent.

Note: If required, you can configure the ports used in the agent and server communication, by setting the bind management server port, and NetIQ agent listening port fields.

Chapter 8
System Backup and Restore (BRU)

This section has information about how to manage the Business Communications Manager Backup and Restore Utility (BRU).

Backup and restore procedures:

BRU Overview

BRU provides a way to preserve the integrity of your Business Communications Manager operating system software and configuration data. With BRU you can perform a backup or restore via a web connection. BRU is a single-user application.

Before you perform any substantial maintenance on Business Communications Manager, save your data to a safe storage module location elsewhere in the network. After hardware maintenance is complete, restore the data to your Business Communications Manager. You access BRU through the Unified Manager main page.

When you run or schedule a backup or restore, make sure there are no conflicts between BRU processes. If a conflict occurs the processes terminate and result in a failure. The conflict error is not written to the event log.

Error Messages

Most errors originate with the mapping of a network resource for the purpose of the backup and restore scripts. Errors are usually about permissions and security settings of the network resource. Ensure the username you provide has full-control sharing access to the network resource and full-control security permissions. Other errors can originate from the XML file function. In this case the exact error is stored in a log file on the destination of the backup data.

Volume Administration

With BRU you can save information about the most used network targets, called Volumes. You do not need to type the remote path and user name every time you want to run a script requiring access to a remote resource.

Note: This feature can not be accessed during a process execution. You must complete all the information to be able to save a volume.

Table 28 Volume administration information

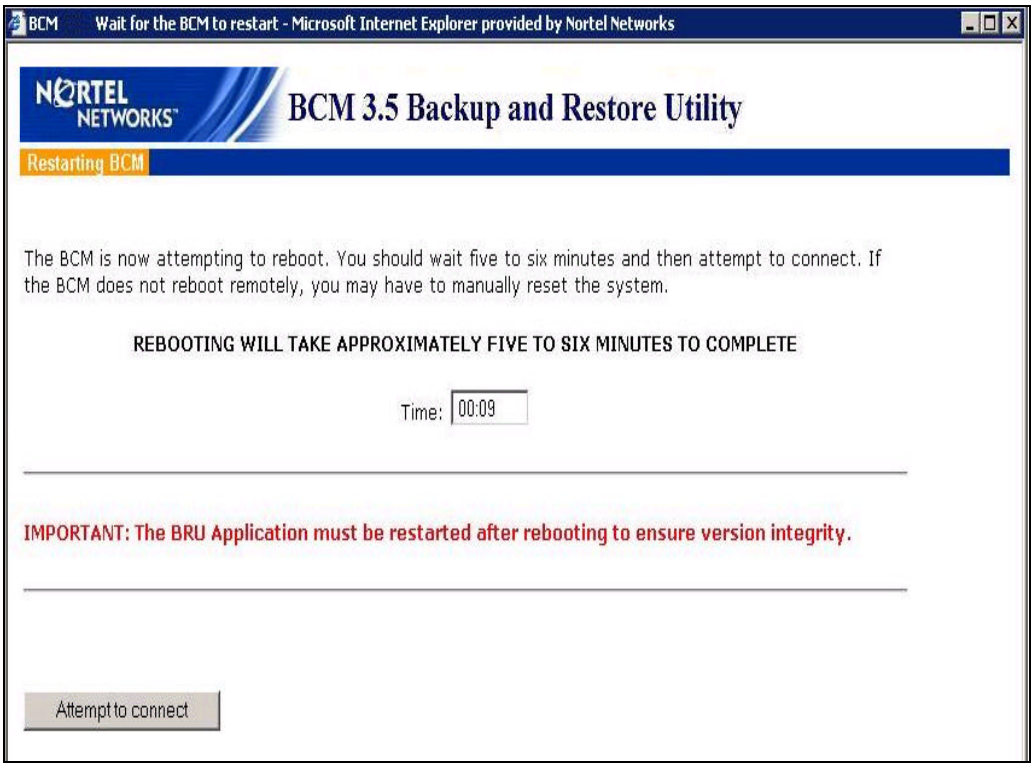
Data	Description
Volume ID	Identification number for each of the Volumes saved
Type	Whether the volume refers to a remote, a local folder or FTP server
Logical name	A logical name for the volume. You can enter any desired name.
Location	Path to access the local folder or remote network resource or FTP server.
User name	User name that allows the connection into the UNC path.
ADD	Lets the user add a new volume with parameters in the five fields described above.
Modify	Lets the user make changes on the corresponding volume.
Delete	Lets the user delete the corresponding volume.

BCM Reboot

With the reboot feature you can restart the BCM server from the client machine. BRU sends the reboot command to BCM and the system displays the reboot screen.

Note: Reboot can not be accessed during a process execution.

Figure 54 Reboot screen display



About button

Use this to verify the BRU version installed on Business Communications Manager. Information about the connection and the XML files in the XMLFolder are also displayed.

Note: You cannot access this feature during a process execution.

Backup Mode

To back up Business Communications Manager, you must have a shared resource prepared to store the data. See "Destination Drive" on page 384 for details. The shared resource must have the permissions set so the user name has full access to the folder. Business Communications Manager must be allowed to see this destination folder and be able to map to the shared resource.

After you ensure that Business Communications Manager has full access to the desired shared resource, you select the components to be backed-up. You can schedule a backup to run in interactive mode, or to run on a specific date, time and frequency.

Note: Voice mail is unavailable during the Voice Applications backup (or restore).

Destination Drive

Local Drive*:* To back up Business Communications Manager to a Local Drive (E:), you must be aware that the space available might not be enough and the backup will not be completed. The default space available for backup to the E: drive should not exceed 1 gigabyte.

Remote Drive*:* To back up Business Communications Manager to a Remote Drive, you must have a destination shared network resource prepared to store the data. The shared resource must have the permissions set so that the specific user has full control, and Business Communications Manager must be must be able to map to this shared resource.

FTP Server*:* To back up Business Communications Manager to a FTP Server, you must have a destination folder prepared to store the data. The folder must have its permissions set so the specific user has full control, and Business Communications Manager must be must be able to find this FTP Server.

Note: You are responsible for managing the shared network resource and the FTP Sever. Data already on the destination will be overwritten with new data on consequent executions of the backup and restore script. If you want to save different versions of backed-up data, you must manage the volumes and shared resources.

For example, you can decide to schedule a backup every day; however a safer way to do this is to have two or more backup volumes. Each backup can be backed up to a different volume, on different days, so that at least two full backups are available to choose from. For added safety, you can back up the volumes are to different servers, so that a second copy of the backup is always available.

To save the information about the most used destination drives, see the section on “Volume Administration” on page 382.

Scheduled backup

The backup process can be scheduled to run on a specific date, time and frequency.

To schedule a backup, follow the steps to configure a backup and select the specific date, time, and frequency. Be aware that the selected time starts the process according to the date and time on Business Communications Manager. Be aware of time differences, especially if you schedule a backup on a Business Communications Manager at a different time zone. The time on the Business Communications Manager is shown, although this is an approximation. The time is normally within a few minutes of the actual time set on the target BCM.

After you enter all the data, press the Start Backup button to load the task into the scheduler on Business Communications Manager. After you press the Start Backup button, you are asked to enter some extra information that must be provided to ensure that the backup runs with no configuration errors. The backup runs as a background task. While BRU is running, do not schedule a second backup on the same Business Communications Manager at the same time as errors may occur.

Note: BRU is not a multi-user application. When you run or schedule a backup or restore, make sure that there is no conflict in between one or more BRU processes. If a conflict occurs the BRU will not complete and can fail unexpectedly. The error will not be registered on the eventlog.

Voice mail is unavailable during the Voice Applications backup (or restore).

Backup components

The Backup and Restore script makes most data required for BCM applications available as a component. The separation of components lets you back up or restore any combination of components at any time.

Components you can back up

- Apache Configuration
- Archlog Settings
- Backup and Restore Utility
- DECT OAM
- Interactive Voice Response
- Licensing
- Multimedia Call Center
- Registry
- Unified Manager
- Voice applications
- Telephony

Apache Configuration

If you select Apache Configuration in the BCM Component list, configuration changes in the Unified Manager, under the Services, Web Cache section, are saved. A reference to the primary LAN address is also saved in the Apache settings, so we suggest that you back up this component with Unified Manager so that conflicting IP address information is not preserved. The table below lists Apache configuration data that is saved

Table 29 Apache configuration data

Sub component	Configuration location
None	Unified Manager ->Resources ->LAN ->LAN (IP Address)
	Unified Manager ->Services ->Web Cache
	SSL Certificate file (Source unknown)

Archlog Settings

If you selecting Archlog Settings in the BCM Component list, Archlog settings set in the Product Support and Maintenance Pages, under Archlog Settings, are saved. Any scheduled Archlog executions in the Archlog Explorer are also saved. The table below lists Archlog configuration data that is saved

Table 30 Archlog configuration data

Sub component	Configuration location
None	Maintenance ->Archlog Settings
	Maintenance ->Archlog Explorer ->Show Archlog Execution

Backup and Restore Utility

If you select Backup and Restore Utility in the BCM Component list, scheduled BRU jobs and volume information in the BRU Schedule and Volume Administration interfaces is saved. The table below lists the BRU configuration data that is saved

Table 31 BRU configuration data

Sub component	Configuration location
None	BRU ->Schedule Tab
	BRU ->Volume Admin

DECT OAM (Operations Administration and Maintenance)

For information about the DECT backup procedure see Performing a backup using BRU on page 399. The table below lists the DECT configuration data that is saved

Table 32 DECT configuration data

Sub component	Configuration location
None	Wizards ->DECT Configuration
	Wizards ->DECT Mobile Recording
	Unified Manager ->Services ->DECT

IVR

The IVR component backs up all the files related to the Interactive Voice Response. The files are stored in the backup folder at the backup location.

The table below lists the IVR configuration data that is saved

Table 33 IVR configuration data

Sub component	Configuration location
None	All IVR prompts uploaded through the Unified Manager -> Services -> IVR -> IVR Prompts

Licensing

If you select Licensing in the BCM Component list, keycodes entered through the Unified Manager Licensing section or a keycode file are saved. You can restore any keycodes viewable in Unified Manager, as long as the restore occurs on the same system. The table below lists the Licensing configuration data that is saved

Table 34 Licensing configuration data

Sub component	Configuration location
None	Unified Manager ->System Licensing ->Apply Keycodes
	Unified Manager ->System Licensing ->Keycode FIles

Multimedia Call Center

If you select Multimedia Call Center in the BCM Component list, configuration entered through the Multimedia Call Center Admin web tool is saved. The table below lists the Multimedia Call Center configuration data that is saved

Table 35 Multimedia Call Center configuration data

Sub component	Configuration location
None	Unified Manager ->Services ->Multimedia Call Center ->Tools (on menu bar) ->MMCC Admin

Registry

A Registry backup backs up the Business Communications Manager registry files. The files are be saved into the file Backup\SysReg folder, compressed to a .bru file, and transferred to the backup location. The table below lists the Registry configuration data that is saved

Table 36 Registry configuration data

Sub component	Configuration location
None	HKEY_LOCAL_MACHINE and HKEY_USERS

Unified Manager

The Unified Manager component in the BCM Component list encompasses a number of BCM components that have interdependencies and interrelated data. The table below lists the Unified Manager configuration data that is saved

Table 37 Unified Manager subcomponents and configuration data

Sub component	Configuration location
General	Unified Manager ->Diagnostics ->Unified Manager ->Recording
	Unified Manager ->System ->Identification (System name & Time zone only)
Wizard	Wizards -> Edit DN Record Template
Policy Service	Unified Manager ->Services ->Policy Management ->Policy Agent
ISDN	Unified Manager ->Resources ->Dial-Up ->ISDN
PPTP	Unified Manager ->Services ->VPN ->PPTP
QoS	Unified Manager ->Services ->QoS Monitor ->Mean Option Score
	Unified Manager ->Services ->Policy Management ->QoS
NAT	Unified Manager ->Services ->NAT
IPSec	Unified Manager ->Services ->VPN ->IPSec*
Firewall filter	Unified Manager ->Services ->Policy Management ->IP Firewall Filters
LAN	Unified Manager ->Resources ->LAN

Table 37 Unified Manager subcomponents and configuration data

Sub component	Configuration location
UT1	Unified Manager ->Resources ->UTWAN
Router	Unified Manager ->Services ->IP Routing
DNS	Unified Manager ->Services ->DNS
MSM	Published IP Address (determined from IP Telephony Published IP address: Unified Manager ->Resources ->LAN (or WAN) LANx (or WANx)
NTP	Unified Manager ->Services ->NTP Client Settings*
DHCP	Unified Manager ->Services ->DHCP
SNMP	Unified Manager ->Services ->SNMP (except Summary ->Status)
IPX	Unified Manager ->Services ->IPX Routing
UPS	Unified Manager ->Services ->UPS
SSM	Unified Manager ->Diagnostics ->System Status Monitor ->SSM Settings
User Manager	Unified Manager ->Management ->UserManager
Alarm Service	Unified Manager ->Management ->AlarmManager*

Voice Application

The Voice Applications component in the BCM Component list encompasses a number of BCM components that have interdependencies and interrelated data. Below is a listing of the subcomponent and the configuration data that is saved for it.

Note: Voice mail and IVR are unavailable during a Voice Applications backup or restore.

The table below lists the voice application subcomponents and configuration data that is saved.

Table 38 Voice application sub-components and configuration data

Sub-component	Configuration location
CDR	Unified Manager ->Services ->Call detail recording
	All CDR records
Call pilot	Unified Manager ->System ->Identification (Call pilot region only)
UTPS & Hot desking	Unified Manager ->Services ->IP Telephony ->Nortel IP terminals
VoIP Gateway	Unified Manager ->Services ->IP Telephony ->H.323 terminals
	Unified Manager ->Services ->IP Telephony ->IP Trunks ->H.323 Trunks
SIP Gateway	Unified Manager ->Services ->IP Telephony ->IP Trunks ->SIP Trunks
MSM	Unified Manager ->Resources ->Media Services Card ->MSC Configuration
Voicemail	Call Pilot (external)
CTE	Unified Manager ->Services ->LAN CTE Configuration
Doorphones	Unified Manager ->Services ->Doorphones

Table 38 Voice application sub-components and configuration data

Sub-component	Configuration location
BcmAmp	Unified Manager ->Services ->IP Music (music source = BcmAmp)
IP Music	Unified Manager ->Services ->IP Music
CTI	None (see Voicemail & IVR) - All voicemail messages and all created mailboxes are backed up

Telephony

The Telephony Backup backs up Telephony Application files. The data is saved to TelephonyData.bru in the backup folder on the destination drive. This file contains files from the folder defined in registry key "HKLM\SOFTWARE\Nortel Networks\Voice Solution\FTMSS\MSC-1\BackupDir". This backup directory is defined and can be changed from the Unified Manager System directory. We recommend you do not change this directory from its default location.

The table below lists the telephony configuration data that is saved.

Table 39 Telephony components

Sub-component	Configuration location
None	Unified Manager ->Services ->Telephony services
None	Unified Manager ->Diagnostics ->MSC
None	Unified Manager ->Diagnostics ->Trunk modules
None	Unified Manager ->Diagnostics ->Service metrics ->Telephony services

Restore Mode

To restore components to Business Communications Manager, you must have a valid local, ftp or network resource location to get the data from. This source location must be shared and have the security set to full control for the user specified in the volume table, and must contain the valid backed-up data. Business Communications Manager must be able to access this source location and be able to map to this resource.

After you ensure that Business Communications Manager has full access to the desired source location, select the components to be restored. Note: BRU queries all the backup report files on the backup resource, if local or network, and highlights the components that have been successfully backed up.

Note: Voice mail is unavailable during the restore.

Whether all components were successfully restored or not, you must reboot Business Communications Manager when restore process is finished. A reboot is required in order to use the restored data and re-start stopped services

Source Drive

Local Drive*:* To restore Business Communications Manager data from a Local Drive (E:), be aware that the space available might not be enough and the restore will not be completed. The total space used for backup/restore on the E: drive should not exceed 1 gigabyte.

Remote Drive*:* To restore component data to Business Communications Manager, you must have a local source or shared network resource to get the data from. This shared resource must have permissions set so the specific user has access to the resource at read/write permission level. Check the documentation of the system you want to back up for how to set the security and share level. Business Communications Manager must be able to map to this shared resource.

FTP Server*:* To restore Business Communications Manager data from a FTP Server, you must have a source folder to store the data. The folder must have its permissions set so the specific user has full control. Business Communications Manager must be able to find this FTP Server.

After you make sure that Business Communications Manager has full access to the desired source drive, select the components to be restored.

Restore Options

BRU offers two restore options that let you run the restore with version compare or not.

1. **Restore only if the bcm version and the backup version are the same** runs the script that compares the BCM version with the backup version and if they are different, cancels the restore.
2. **Restore even if the bcm version and the backup version are different**: does not run the script that compares the BCM version with the backup version. and if they are different, the restore can cause serious and irreversible problems. This action must be performed with caution.

Restore Components

The Backup and Restore script makes most data required for Business Communications Manager applications available as a component. This separation lets you back up or restore any combination of components at any time.

Restore components available

- Apache Configuration
- Archlog Settings
- Backup and Restore Utility
- DECT OAM
- IVR
- Licensing

- Multimedia Call Center
- Registry
- Unified Manager
- Voice Applications
- Telephony

Apache

The Apache restore restores the files related to Apache configuration. The files are restored from the C_ApacheConfigData.bru file in the Backup folder.

See "Apache Configuration" on page 386 for details of the contents of the backup.

Archlog

The Archlog Settings restore restores Archlog information. The data is restored from the ArchlogData.bru and ArchlogData_E.bru files in the Backup folder. See "Archlog Settings" on page 386 for details of the backed up data.

BRU

Selecting BRU in the component list saves all scheduled BRU jobs and Volume information located in the BRU Schedule and Volume Administration interfaces.

DECT OAM

The DECT OAM restore process takes about 26 minutes. During this time the main BRU window displays a message that says a script is being processed. When the restore is complete, a message appears that says the restore is completed. See "Performing a restore using BRU" on page 404.

IVR

The IVR Data Restore restores files for Interactive Voice Response. The files are restored from the Backup folder at the backup location. See "IVR" on page 387 for a description of the data that is backed up.

License Restore

The License Restore restores Business Communications Manager Licensing data. The data is restored from the VoiceLicenseData.bru file in the Backup folder. See "Licensing" on page 387 for details of the backed up data.

Note: You cannot copy keycode-purchased functionality from one system to another by doing NVRAM restores.

Multimedia Call Center

The Multimedia Call Center restore restores data for Multimedia Call Center. The files are restored from the CallCenterData.bru file in the Backup folder.

See the "Multimedia Call Center" on page 388 for details of the data backed up.

Registry

The Registry Data restore restores the saved registry database. **This registry data overrides any other registry information from other components.** The files are restored from the Backup\SysReg folder on the source resource.

Note: You restore the registry, you must restart BRU after the reboot. Choose the registry only if you are restoring the information to a replacement Business Communications Manager or a replacement hard drive on the same Business Communications Manager. as BCM-specific WindowsNT security information is also transferred using the registry.

Unified Manager

The Unified Manager restore restores files for Unified Manager. The files are restored from the C_UnifiedMgrData.bru and D_UnifiedMgrData.bru files in the Backup folder. See "Unified Manager" on page 388 for details of data that is contained in the backup files.

Note: If the file "D_UnifiedMgrData.bru" is not created during the Backup process, the error *"Could not find the file"* occurs during the Unified Manager restore. This error is be displayed as a warning and does not affect the restored data.

Voice Application

The Voice Application restore restores files for voice applications. The files are restored from the VoiceAppsData.bru file in the Backup folder. See "Voice Application" on page 389 for a description of the data that is backed up.

Telephony

The Telephony Restore restores telephony data to the Business Communications Manager and uploads this data onto the Media Services Card. The data is restored from the TelephonyData.bru file in the Backup folder. See "Telephony" on page 390 for the location and contents of the backup file.

Schedule

The schedule link on the Main Menu displays the scheduled processes for BRU on the connected Business Communications Manager. See also "Scheduled backup" on page 384 and "Scheduling a backup" on page 402.

Note: This feature can not be accessed during a process execution.

When the scheduled processes page is open, this table appears:

Table 40 Scheduled backup job information

Field name	Description
Action	Delete and Log links for the scheduled job. Click the DELETE link to delete the scheduled job. Click the LOG link to view the report generated the last time this scheduled job was run.
Status	Status of the scheduled job.
Schedule Information	Time and date the job is scheduled to start, and whether the job is scheduled to run once or is repeated.
Last Date Performed	Time and date the scheduled job was last run.
Location	Volume where the backup information is stored.
Components - Status	List of the components included in the backup, and if the backup has previously been run, the status of each of the components as of the last backup event. PASS | WARN | Fail

User Name and Password

The user name and password is required for access to the destination or source network resource entered in the Volume table.

Report File

The report file is generated for two purposes:

1. It provides a record of the pass or failure of each component that was run in a script.
2. In the case of the backup and restore script, BRU reads these files to determine which backups are valid so that you have an indication of which backup can be restored, if necessary.

The report file is displayed on the BRU status window after the script is finished processing, but only in interactive (non-scheduled) mode.

Note: You specify the report file name before the script execution starts, except for a restore process where it inherits the automatically generated script file name, for example BRUXXDDMMYYYY.rep.txt for rstore on the source folder and <report_name>.rep for backup on the destination folder.

Start Backup|Restore Button

To start the script process, click the "START BACKUP" or "START RESTORE" button. This Start Backup/Restore action is dependant on the mode selected. The table below shows what to expect.

Mode	Information required
Backup to a remote drive	1. user name and password for the remote drive 2. report file name 3. dect password (if dect oam has been selected)
Backup to a local drive	1. report file name 2. dect password (if dect oam has been selected)
Backup to a ftp server	1. user name and password for the ftp server 2. report file name 3. dect password (if dect oam has been selected)
Restore from a remote drive	1. user name and password for the remote drive 2. dect password (if dect oam has been selected)
Restore from a local drive	1. dect password (if dectoam has been selected)
Restore from a ftp server	1. user name and password for the ftp server 2. dect password (if dectoam has been selected)

Note: When the backup or restore is complete, some files that were created during the process are deleted. If the process is successful, the .log file and the .cmd file corresponding to process are deleted. Otherwise, if the backup or restore end with errors or warnings, only the .cmd file is deleted.

Accessing BRU

1 On The Unified Manager main page click the **BRU** icon.
The BRU screen appears (see "Performing a backup using BRU" on page 399).

Exiting from the backup and restore utility

Use this procedure to exit from the backup and restore utility.

1 Select the **Exit** link.
A message appears that asks you to confirm that you want to exit.

2 Click the **Confirm** button.
The BRU utility main page closes.

Resetting the BRU screen

1 Select the **Home** link to reset the BRU screen. This reset the BRU screen and clear the current BRU settings.

Note: If a BRU process is running when you select the **Home** link, a warning appears. You can choose to stop the process and continue resetting the BRU screen or you can cancel the reset and let the process continue.

Adding a new volume

Backup volumes are the locations where you store the backed up settings.
Use this procedure to add new volumes using the Volume Administration screen.

1 On the Unified Manager main page click the BRU icon.
The BRU screen appears with backup selected.

2 From the top menu, select **Volume Admin**.
The Volume Administration screen appears (see "Performing a backup using BRU" on page 399).

3 From the **Type** box select **Local**, **Remote or FTP**.

- Select **Local** if you want the backup stored in a volume on Business Communications Manager.
- Select **Remote** if you want the backup stored on a computer on the network.
- Select **FTP** if you want the backup stored on an FTP server.

4 In the **Logical Name** box enter the name of the backup volume. Use alphanumeric characters only (for example, Volume1). Do not use symbols or other special characters.

5 In the **Location** box enter the path name of the volume.

- If the volume is a local volume, enter the drive designation (for example, **`E:\`**).
- If the volume is a remote volume, enter the computer IP address or computer name and the path name of the directory. For example, \\<**IP_address**>**shared_folder or** \\<**computer_name**>**shared_folder**.
- If the volume is an FTP volume, enter FTP server IP address or node name and the path name of the directory. For example, <**IP_address**>/**path** or <**ftp node name**>/**path**.

6 In the User Name box enter the user name required to access the given path on the remote drive or FTP server. The user name must have full access control on the given path.

- When the domain name is required, enter **`domain_name\user_name`**.
- When the domain name is not required, enter **`user_name`**.

7 Click the **Add** button.
Repeat steps 3 to 7 for each volume you want to add.

8 Click the **Close** button to close the Volume Administration screen.

Modifying a volume

Backup volumes are the locations where you store the backed up settings. Use this procedure to modify volumes using the Volume Administration screen.

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with backup selected.
2. On the top menu, select **Volume Admin**.
   The Volume Administration screen appears.
3. Select the volume you want to modify.
   The volume information is displayed.
4. Change the volume information you want to modify.
5. Click the **Modify** button.
6. Click the **Close** button to close the Volume Administration screen.

Deleting a volume

Backup volumes are the locations where you store the backed up settings. Use this procedure to delete volumes using the Volume Administration screen.

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with backup selected.
2. On the top menu, select **Volume Admin**.
   The Volume Administration screen appears.
3. Select the volume you want to delete.
   The volume information appears on the screen.
4. Select the **Delete** button.
   A message appears that asks you to confirm the deletion.
5. Select the **OK** button.
6. Select the **Close** button to close the Volume Administration screen.

Performing a backup using BRU

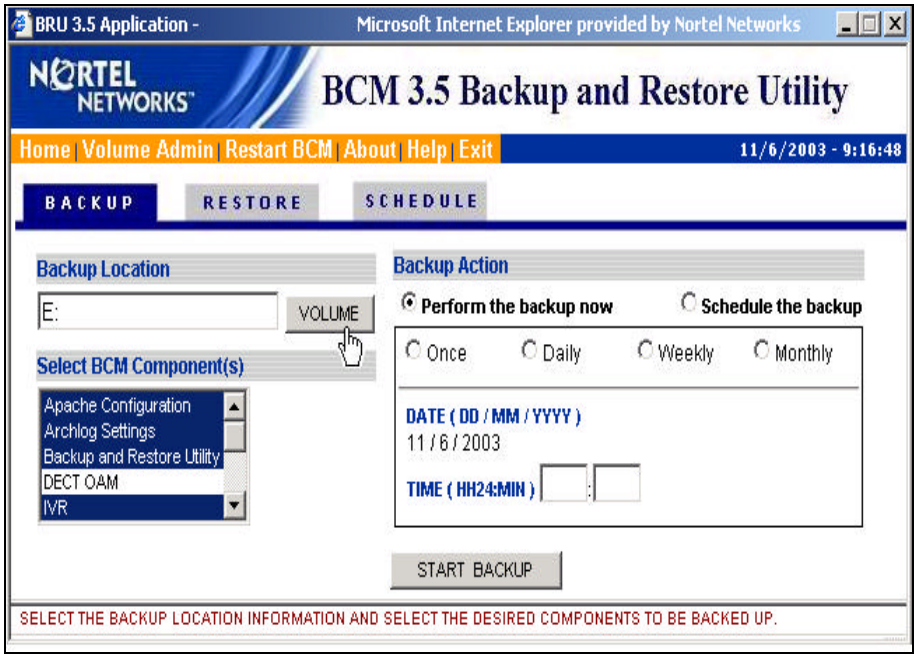
A backup saves your Business Communications Manager settings to a volume on the local hard drive or another computer on the network. Use this procedure to perform a backup to a local or remote hard drive.

Note: We recommend you back up your Business Communications Manager on a regular basis.

Note: IVR and CallPilot voicemail functionality is unavailable for a period of time while the Voice applications are backed up.

1 On the Unified Manager main page click the BRU icon.
The BRU screen appears with backup selected.

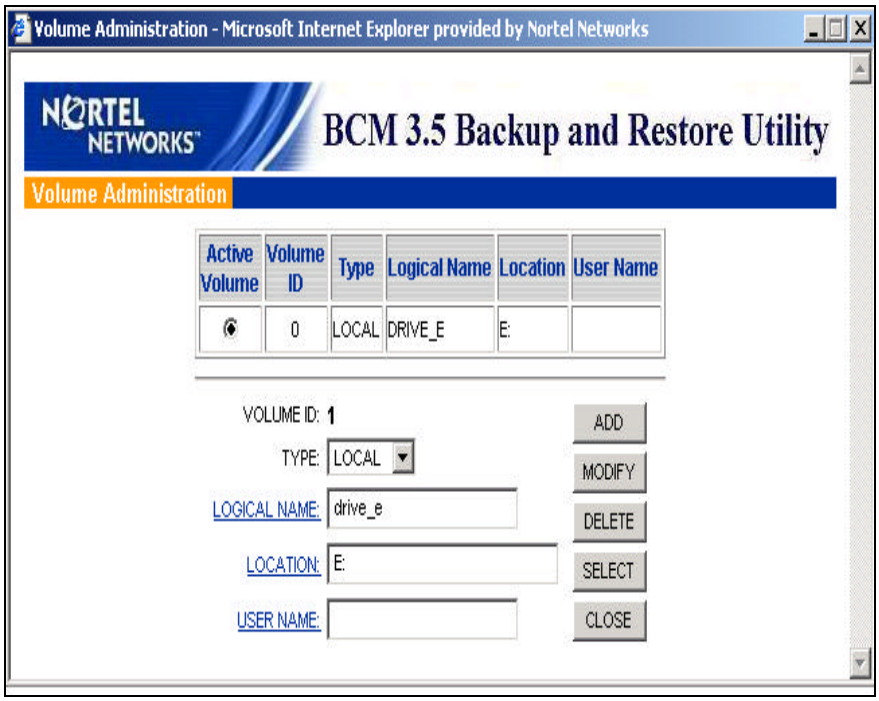
Figure 55 Backup and restore main page screen display



2 Click the **Volume** button.
The BRU Volume administration screen appears.

3 Select the volume where you want to store the backup. If you want to store the backup in a volume that does not appear on the list, see "Adding a new volume" on page 397 for more information.

Figure 56 BRU Volume administration screen display



- The Logical Name box displays the name of the volume.
- The Location box displays the path to either a remote drive, Unix FTP server or WindowsNT FTP server as shown in the table below:

Remote Drive:	Format for static IP address: \\<IP_address>\shared_folder	Format for computer using DHCP server (must): \\<computer_name>\shared_folder
UNIX FTP Server:	Format for static IP address: <IP_address>/path_folder	Domain name: <domain_name>/shared_folder
WindowsNT FTP Server:	Format for static IP address: <IP_address>/<root_drive>:/path_folder	Domain name: <domain_name>/<root_drive>:/ shared_folder

- In the User Name box you can access the path for the Remote drive or FTP server.

4 Click the **SELECT** button.
The Backup and Restore main page appears. The selected volume appears in the backup location box.

5 From the **Select BCM Component(s)** list select the components you want to back up. By default, all of the components except DECT OAM are selected.

- To clear highlighted components, click anywhere on the list.
- To select more than one component, hold the CTRL key and select from the list.

6 On the BRU Report filename entry screen, click the **Start Backup** button from the to run the backup job. If you chose to backup the DECT OAM component, the DECT OAM Password screen appears. If you are not performing a backup on the DECT OAM component, continue to the next step in this procedure.

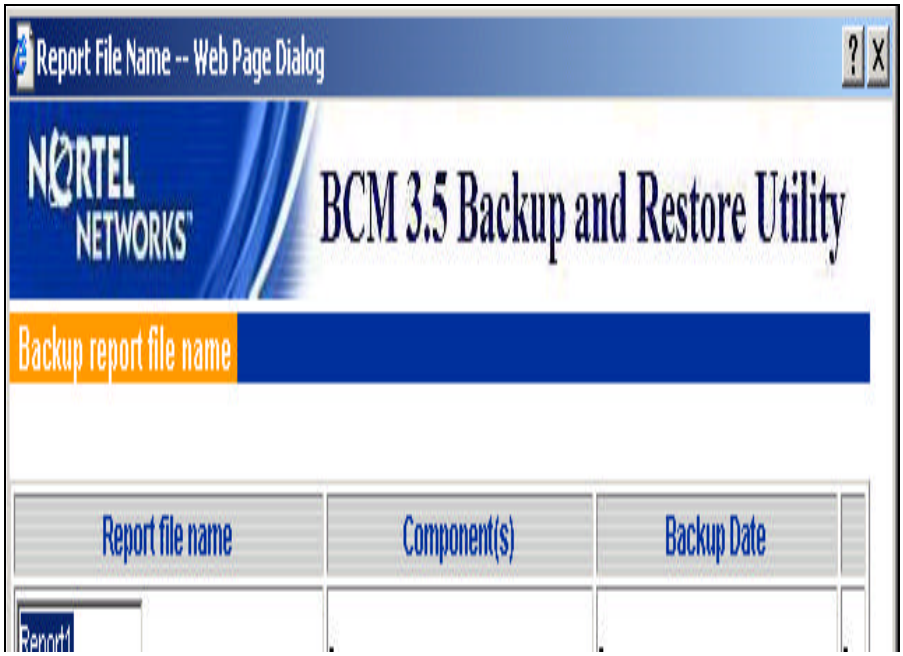
- Enter the DECT OAM installer password in the **Password** field, and select **Submit**. The default DECT OAM Installer password is: **insta**.

7 Enter your user name and password if prompted (for remote backups only). If you are backing up the file to a Local volume, the User Name and Password screen does not appear. Continue to the next step in this procedure.

- Enter the user name in the **Username** box to access the remote volume. Use a domain name qualifier if required.
- Enter the password in the **Password** box to access the remote volume.
- Select the **Submit** button.

8 The BRU Report file name entry screen appears.

Figure 57 BRU Report filename entry screen display



9 In the Report filename box enter a name for the backup report.
The backup report contains the results of the backup process and is stored in the same folder as the backup.

10 On the BRU Report filename entry screen, click the **Next** button.
When the backup is complete, a message appears that indicates the backup is a success or failure.

- If the backup is successful, click the **OK** button and continue to the next step in this procedure.
- If the backup is not successful, click the **OK** button and check the log file for errors. Correct the cause of the errors and run the backup again.

Scheduling a backup

With a scheduled backup you perform a backup at the time and date of your choosing. You can do the backup at a convenient time or when there is less network traffic.

You can also schedule the backup to repeat on a regular basis. Nortel Networks recommends that you do backups on a regular basis to capture changes to the Business Communications Manager settings and data.

Note: IVR and voicemail are unavailable while the Voicemail applications are backed up.

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with the Backup tab selected.
2. Click the **Volume** button.
   The Volume Administration screen appears.
3. Select the volume where you want to store the backup. If you want to store the backup in a volume that does not appear on the list, see "Adding a new volume" on page 397.
   - The Logical Name field displays the name of the volume
   - The Location field displays the path to either a remote drive, Unix FTP server or WindowsNT FTP server as shown in the table below:

Remote Drive:	Format for static IP address: \\<IP_address>\shared_folder	Format for computer using DHCP server (must): \\<computer_name>\shared_folder
UNIX FTP Server:	Format for static IP address: <IP_address>/path_folder	Domain name: <domain_name>/shared_folder
WindowsNT FTP Server:	Format for static IP address: <IP_address>/<root_drive>:/path_folder	Domain name: <domain_name>/<root_drive>:/ shared_folder

   - From the User Name field you can access the path for the Remote drive or FTP server.
4. Click the **SELECT** button.
   The selected volume appears in the Backup Location box.
5. From the **Select BCM Component(s)** list select the components you want to back up.
   By default, all of the components except DECT OAM are selected.
   - To clear the highlighted components, click anywhere on the list.
   - To select more than one component, hold the CTRL key and select from the list.
6. Under the **Backup Action** heading, select the **Schedule the backup** option.

Caution: Do not schedule BRU and NCM backups/restores within an hour of each other. Doing so can cause the processes to overlap, which terminates both processes.

7 Select the frequency of the scheduled backup:

- Select **Once** to perform the backup one time at the time and date specified.
- Select **Daily** to perform the backup every day at the time specified.
- Select **Weekly** to perform the backup on the same day and time every week (for example, Monday at 4:00 am).
- Select **Monthly** to perform the backup on the same date and time every month (for example, the 15th of the month at 4:00 am).

8 Select the day on which to perform the backup:

- If you selected **Once** (from the previous step), select **Today** or select **Specific Day** and enter the date when you want the backup to run.
- If you selected **Daily** (from the previous step), you do not need to enter a date.
- If you selected **Weekly** (from the previous step), select the day of the week you want the backup to run.
- If you selected **Monthly** (from the previous step), enter the date you want the backup to run.

9 Enter the hours and minutes when you want the backup to run:

- Enter the information in the two **Time** fields in 24 hour format (HH:MM).
- Select the **AM** or **PM** option.
- If you chose Daily, Weekly or Monthly for the frequency, this is the time when all subsequent backups will run.

10 Click the **Execute** button.
The User Name and Password prompt appears. If you are backing up the file to a local volume, the User Name and Password screen does not appear, and continue to the next step in this procedure.

- Enter the user name in the **Username** box to access the remote volume.
Use a domain name qualifier if required.
- Enter the password in the **Password** box to access the remote volume.
- Select the **Submit** button.

11 Enter a name for the report for this backup job in the **Report File Name** box. This report contains the results of the backup process and is stored in the same folder as the backup.

12 Click the **Submit** button.

13 If you chose to back up the DECT OAM component, the DECT OAM Password screen appears. If you are not performing a backup on the DECT OAM component, continue to the next step in this procedure.

- Enter the DECT OAM installer password in the **Password** box, and click the **Submit** button. The default DECT OAM Installer password is: *insta*.

Viewing scheduled backups

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with the Backup tab selected.
2. Click the **Schedule** tab.
   he Scheduled Backups screen appears and displays the scheduled backups scheduled.
3. Click the **Close** button to close the Scheduled Backups screen.

Viewing a scheduled backup report

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with the Backup tab selected.
2. Click the **Schedule** tab.
   The Scheduled Backups screen appears and displays the scheduled backups.
3. Select the **Log** link for the scheduled backup.
4. Select the **Open this file from its current location** option to view the report on your computer.
5. Select the **Save this file to disk** option to save the report on your computer.

Deleting a scheduled backup

1. On the Unified Manager main page click the BRU icon.
   The BRU screen appears with the Backup tab selected.
2. Click the **Schedule** tab menu.
   The Scheduled Backups screen appears.
3. Click the **Delete** button for the scheduled backup you want to delete.

Performing a restore using BRU

A restore copies the Business Communications Manager settings from a backup volume to the local hard disk of Business Communications Manager.

The Business Communications system must be operational and you must be able to access it using Unified Manager before you can restore the settings.

If you replace a component and all programming is set to default, perform the component-specific initialization procedure before performing the restore procedure described in this section.

Note: If you replace the MSC, you must obtain and install new software keycodes before you can restore the settings. Your old software keycodes will not work with the new MSC.

The new software keycodes can be regenerated using your existing software keycodes. To regenerate the software keycodes, use the Nortel Networks Keycode Retrieval System website at http://www.nortelnetworks.com/servsup/krs/.

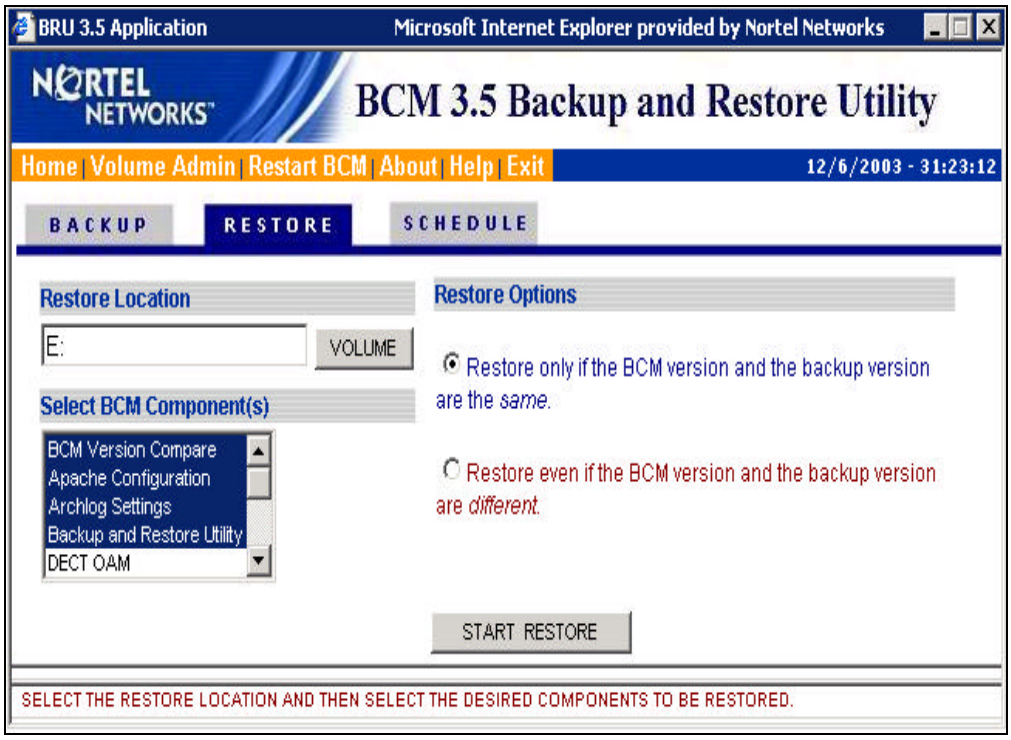
Note: If you restore programming to a different system than the system from which the backup was created, you must set the time zone on the restored system using Unified Manager.

Note: The restore process terminates the services associated with the chosen components and sub-components.

1 On the Unified Manager main page click the BRU icon.
The BRU screen appears with the Backup tab selected.

2 Select the **Restore** tab.
The BRU screen displays the restore options.

Figure 58 BRU Restore screen display



3 Click the **Volume** button.
The Volume Administration screen appears.

4 Select the volume from which you want to restore the backup.
aIf you want to restore the backup from a volume that does not appear on the list, see "Adding a new volume" on page 397.

- The Logical Name field displays the name of the volume
- The Location field displays the path to either a remote drive, Unix FTP server or WindowsNT FTP server as shown in the table below:

Remote Drive:	Format for static IP address: \\<IP_address>\shared_folder	Format for computer using DHCP server (must): \\<computer_name>\shared_folder
UNIX FTP Server:	Format for static IP address: <IP_address>/path_folder	Domain name: <domain_name>/shared_folder
WindowsNT FTP Server:	Format for static IP address: <IP_address>/<root_drive>:/path_folder	Domain name: <domain_name>/<root_drive>:/ shared_folder

- From the User Name field you can access the path for the Remote drive or FTP server.

5 Click the **SELECT** button.
The selected volume appears in the Restore Location field.

6 From the **Select BCM Component(s)** list select the components you want to restore.
By default, all of the components available for restore are selected.
If you are using FTP to restore the data, none of the components are selected.

- To clear all highlighted components, click anywhere on the list.
- To select more than one component, hold the CTRL key and select from the list.

7 Click the **Start Restore** button.

8 Enter your user name and password if prompted (for remote restore only). If you are restoring the file to a Local volume, the User Name and Password screen prompt does not appear. Continue to the next step in this procedure.

- Enter the user name in the **Username** box to access the remote volume. Use a domain name qualifier if required.
- Enter the password in the **Password** box to access the remote volume.
- Select the **Submit** button.

9 When the restore is complete, a message appears that says whether the restore is a success or failure.

- If the restore is successful, click the **OK** button and continue to the next step in this procedure.
- If there is an error, click the **OK** button and check the log file for errors.
Correct the cause of the errors and retry the restore.

10 A message appears that prompts you to reboot Business Communications Manager.
Click the **OK** button to reboot your system.

Chapter 9
Security Management

This section contains information on how to manage security for the Business Communications Manager network.

Security Management topics

Computer requirements

To run the Unified Manager, you require:

- a 133 MHz Pentium CPU or higher (or compatible)
- 64 MB RAM
- a minimum of 10 MB of available disk space
- a minimum screen resolution of 1024 x 768
- a web browser

Browser requirements

To use Unified Manager, you require:

- Java Virtual Machine (JVM) 5.0 (build 5.00.3805 or greater), or Sun Java JRE 1.4.1_02 or greater (for Windows versions that do not have JVM installed)
- Microsoft Internet Explorer 5.X (excluding 5.00) or 6.X, or Netscape Communicator 4.8, 6.X or 7.X.

Note: Browser restrictions and limitations

- BRU and upgrades: Only Internet Explorer will work when using the backup/restore utility (BRU) or when performing an upgrade procedure.
- The Business Communications Manager upgrade wizard will not work with IE 5.00.

If you are using Netscape Communicator, set the following parameters:

- Enable Java: On
- Cached document comparison: Every time

If you are using Microsoft Internet Explorer, set the following parameters:

- Check for newer versions: Every visit to the page
- Java JIT compiler enabled: On

For information about setting these parameters, check the documentation that came with your web browser.

You can access the Business Communications Manager system from another computer through a WAN/Internet connection or a dialup connection. The dialup connection uses either the internal V.90 modem (North America only) or an ISDN dialup. Both access methods create an IP connection that enables all IP-based management tools. For more information on remote connections, refer to "Dial Up" on page 621.

Using a HTTP Proxy server

Unified Manager does not work properly if you use a HTTP Proxy server to connect to the Internet. If you use an HTTP Proxy server, you must change your web browser settings so you can bypass the Proxy Server when connecting to Business Communications Manager.

Bypassing the HTTP Proxy on Microsoft Internet Explorer 5.0

This procedure is based on the user interface for Microsoft Internet Explorer 5.0. If you have a newer version, some steps may be different.

1. On the menu bar, click the **Tools** menu and click **Internet Options**.
2. Click the **Connections** tab and click the **LAN Settings** button.
3. Click the **Advanced** button.
4. In the **Exceptions** box, type the IP address of the Business Communications Manager system.
5. Click the **OK** button until the main browser page appears.

Bypassing the HTTP Proxy on Netscape Communicator 4.5

This procedure is based on the user interface for Netscape Communicator 4.5. If you have a newer version, some steps may be different.

1. On the menu bar, click the **Edit** menu and click **Preferences**.
2. Click the + symbol beside **Advanced**.
3. Click the **Proxies** heading.
4. Click the **View** button.

5 In the **Exceptions** box, type the IP address of the Business Communications Manager system.

6 Click the **OK** button until the main browser page appears.

Note: If the Business Communications Manager system is located outside of your network, or you have to use a proxy as a gateway proxy to communicate with Business Communications Manager, the procedures above may not work. For these procedure to work, the gateway proxy must be able to understand and pass distributed component object model (DCOM) calls between Business Communications Manager and the computer you are using to run Unified Manager.

Logging on to Unified Manager

Use the following procedure to log on to Business Communications Manager using the web browser:

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

Security note: The configuration section in the Unified Manager is not secured through SSL encryption. To provide security for this section, establish a VPN client tunnel. Refer to "IPSec Remote User configuration" on page 751.

1 Launch your web browser.

2 BCM 3.5 software provides secure server access to the Business Communications Manager.

- If you updated from a previous version of software, and you have the Business Communications Manager address (http://<*IP address*>:6800) bookmarked, you will find that the login is redirected to an https:// entry.
- If you have a new system, enter https//:<*IP Address*>.

Note: You must include **https://** with the address to access Unified Manager when you are using Internet Explorer as your browser.

Note: If your Business Communications Manager has a network Fully Qualified Domain Name (FQDN), you can access your system by pointing your browser to that name.

3 If the browser does not automatically launch, click on the Go tab beside the URL address field. A security dialog appears.

Security note: The default security certificate that comes with BCM 3.5 version software is a self-signed certificate that enables SSL encryption functionality. The default certificate does not address site authentication since site authentication requires site and system-specific information such as IP address, company name, and so on. Refer to "Understanding BCM SSL certificate properties" on page 410 for more information.

Figure 59 Security Alert dialog

4 Click **Yes**.
The first page of the Unified Manager appears.

Understanding BCM SSL certificate properties

When you first run BCM software, you will see that the default Web access to the Business Communications Manager now uses SSL encryption for system security. This includes the appearance of a security alert when you initiate a connection to the Unified Manager using SSL, which indicates site validation of the default certificate.

This security alert does not appear if you:

- add a site-specific certificate ("Uploading a certificate and a private security key" on page 411)
- suppress the message on your client browser ("Suppressing the security alert message" on page 413)
- use the non-SSL port (http:6800) ("Using the non-secure http:6800 port" on page 413)

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

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

Uploading a certificate and a private security key

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

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

1. Log on to the Business Communications Manager main screen.
2. Click the **Maintenance** icon.
   You are prompted to enter a system user name and password.
3. Click the **OK** button.
   The Product Maintenance and Support page appears.

Figure 60 Main Product Maintenance and Support web page

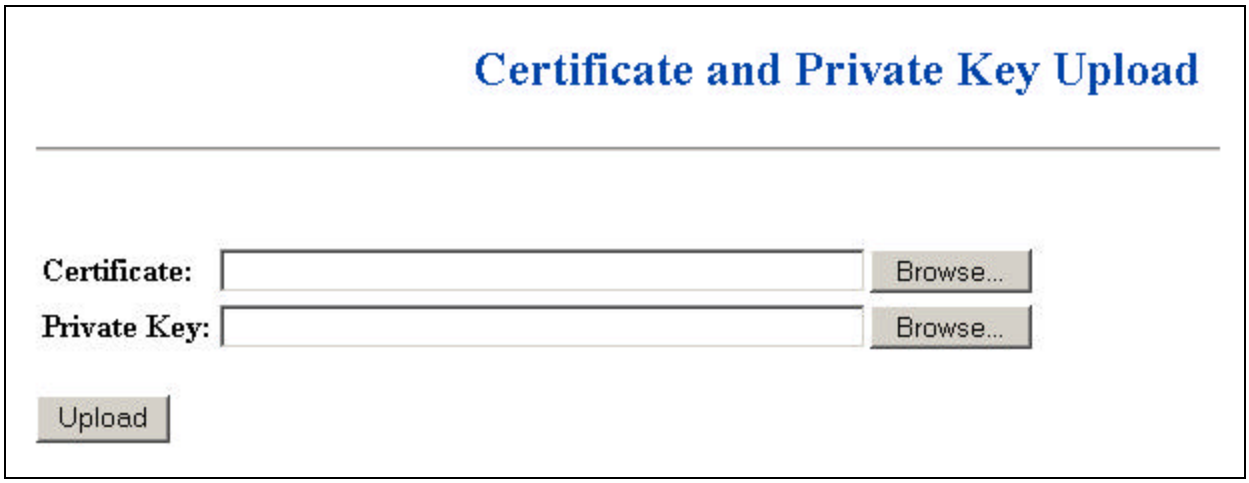
4. On the left frame, under the **Maintenance** heading, click the **Maintenance Tools** link.
   A web page showing a list of Maintenance Tools appears.

Figure 61 Maintenance Tools dialog web page

Maintenance Tools	
Application	**Tool(s)**
Shared Drive	• Attach to a shared volume • Detach a shared volume • Enable/Disable BCM Drive Shares
System Interaction	• Execute a command • Schedule a Command to Execute • Schedule a Restart • Telnet Session
Troubleshooting	• IP network troubleshooting • Services & driver troubleshooting
DECT	• Time Synchronisation • Backup Firmware • Restore Firmware • Firmware Upload • Restore Default Configuration • ALaw/muLaw Companding Scheme
Security	• Upload Certificate and Private Key
Miscellaneous	• Reset Unified Manager Server

5 In the **Security** row, click the **Upload Certificate and Private Key** link. The Certificate and Private Key page appears.

Figure 62 Main Product Maintenance and Support web page



6 Use the **Browse** button beside each field to locate the certificate and private key files. Both files must be uploaded at the same time.

7 Click the **Upload** button.
Upload messages:

- If the upload is successful:
```
Certificate and Private Key Upload Was Successful!
You must restart the Apache Service or Restart the BCM before the
Settings will take Effect.
```
- If the upload is unsuccessful:
```
Certificate and Private Key Upload Was NOT Successful!
The Certificate and Private Key do not match.
Please upload a VALID Certificate and Private Key Combination!
```

8 Beside **Your Location**, click the **BCM** link to exit the maintenance pages.

9 To replace the default certificate with the new certificate and private key, exit Unified Manager and then log back on.

Troubleshooting: Restoring the default certificate

If something happens to your private security certificate file, you cannot access Unified Manager and you need to restore the default certificate. Contact your technical support team for assistance. See "Contact" on page 45 for Nortel Networks support contact numbers.

Suppressing the security alert message

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

1 Open Internet Explorer.

2 On the **Tools** menu select **Internet Options**.

3 Click the **Advanced** tab.

4 Scroll to **Warn about invalid site certificates** and make sure the check box is cleard.
Note: The location of this item can vary depending on your version of Internet Explorer.

5 Restart the browser.

Using the non-secure http:6800 port

If you choose not to use SSL on your system, you can disable the system prompt that forces secure web access. See "Setting system security compatibility levels" on page 416. On the Security screen described in that section, choose **Disabled** for the **Force Secure Web Access** field.

Security Management Tools

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

Security note: This symbol is used throughout this section to indicate areas of possible security concern, primarily about default settings that can be a security risk if they are not changed.

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

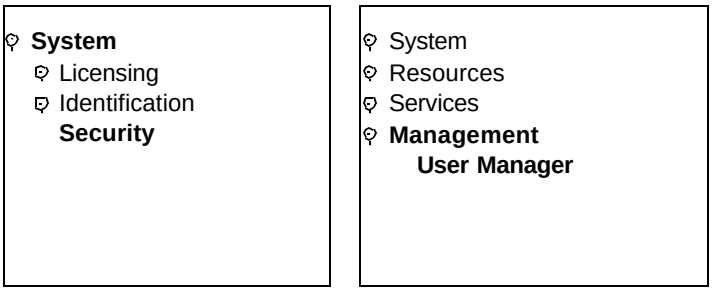
Security note: Minimum configuration should include changing all default system passwords.

Unified Manager security considerations

- How long you want the Unified Manager to remain open if there is no input from the user. See “Setting the Interface Timeout” on page 415.
- If you want to use secure web access to Unified Manager through SSL (Secure Sockets Layer). Note that SSL encryption does not secure the Configuration Menu. To secure communication with the Configuration Menu, a VPN client connection is required. See “Setting system security compatibility levels” on page 416 and the chapter that describes Virtual Private Networks (VPN) in the *Programming Operations Guide*.
- How much access to the Unified Manager interface users are allowed. Access is based on user privileges defined through user group membership.There are two default administrator accounts, *ee_admin* and *supervisor*, both of which have default dial-in access privileges. See “Managing access passwords” on page 417. This section also contains information about password policy.

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

Figure 63 Security and user access headings



Setting the Interface Timeout

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

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

To set the Interface Timeout

1 On the navigation tree, click the **Management** heading and click the **Unified Manager Management** tab.

Figure 64 Unified Manager Timeout setting

2 In the **Unified Manager Timeout** box, enter the period of inactivity the program allows before it closes the application and returns to the log on screen.

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

Setting system security compatibility levels

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

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

To set system security compatibility levels

1. On the navigation tree, click the **System** key and the **Security** heading. The Security screen appears in the right frame.
2. This table describes the fields. Set the fields to the values that best fit your system requirements and that accommodate compatibility issues with interconnecting users or services.

Attribute	Value	Description
Authentication Compatibility	LM&NTLM response - refuse NTLMv2 session security LM & NTLM response NTLM response only NTLMv2 response only NTLMv2 response only - refuse LM	Default: LM & NTLM response This setting determines the type of authentication protocol required by your system during interactions with client applications. The default, LM & NTLM response, maintains compatibility with all Windows OS versions. Any of the other settings enforce a more secure authentication protocol, and will prevent access from computers running Windows 95/98/Me, unless you install the directory services client on the client computer.
Clear Page File on Shutdown	Disabled Enabled	Default: Disabled If Enabled, this setting prompts the system to clear the virtual memory swap file on shutdown. When enabled, this option extends system shutdown by about two minutes.
SMB Client Signing	Allow Disabled Require	Default: Allow Determine what level of signing you require from SMB clients. Disabled: None required. Allow: Tries to perform the digital signature whenever a compatible client platform is detected. This setting also supports clients running with Windows 95/98/Me. Require: Always secures the connection with a digital signature. However, this setting prevents access from clients running with Windows 95/98/Me. Applicable applications: BRU and Archlog

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

3 Click outside the window to save the changes.

Managing access passwords

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

Security note: 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. See Chapter 21 in the *Programming Operations Guide*.

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

- "Viewing User Manager information" on page 418
- "Adding or modifying a user profile" on page 420
- "Adding or modifying a group profile" on page 424
- "Setting password lockout policy" on page 427
- "Setting password policy" on page 428

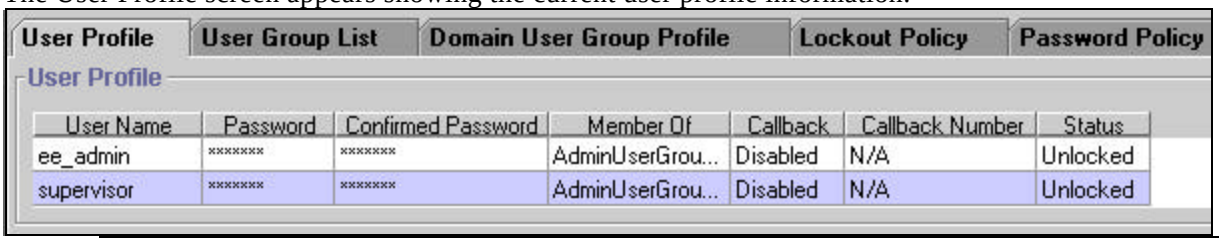
Security note: Callback security
If a user is connecting to the system using a V.90 modem, you can enhance your access security by assigning the person a specific user account that prompts the system to acknowledge the user, then hang up and dial back the user at a designated telephone number, before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

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

Viewing User Manager information

On the User Manager screens you can define user and group profiles, and the parameters that define security levels for user accounts.

On the navigation tree click the **Management** key and the **User Manager** heading.
The User Profile screen appears showing the current user profile information.



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

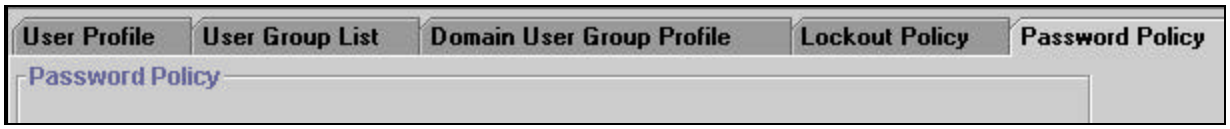
Remote support: In order for the Nortel Networks support organization to assist you, dial-in access has been granted to both default administrator accounts. If dial-in access is removed, then remote access by support organizations may be impacted. It is recommended that the administrator accounts and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

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

Table 41 User Manager screens

User Profile	Business Communications Manager comes with these user profiles: • **ee_admin (cannot be deleted)**: Default password: PlsChgMe!. Access privilege: Read-Write, dial-up access • **supervisor** (can be deleted): Default password: PlsChgMe!. Access privilege: Read-Write, dial-up access
User Group List	Shows the user groups defined in your system. The system comes with a set of default User Groups that have various access privileges.
The Domain User Group Profile	Lists the domains for the user group profiles.
 **The Lockout Policy**	Provides settings to determine the parameters for locking users out of the Unified Manager if the lockout policy is enabled.
Password Policy	Where you can define the complexity policies for your system passwords.

1



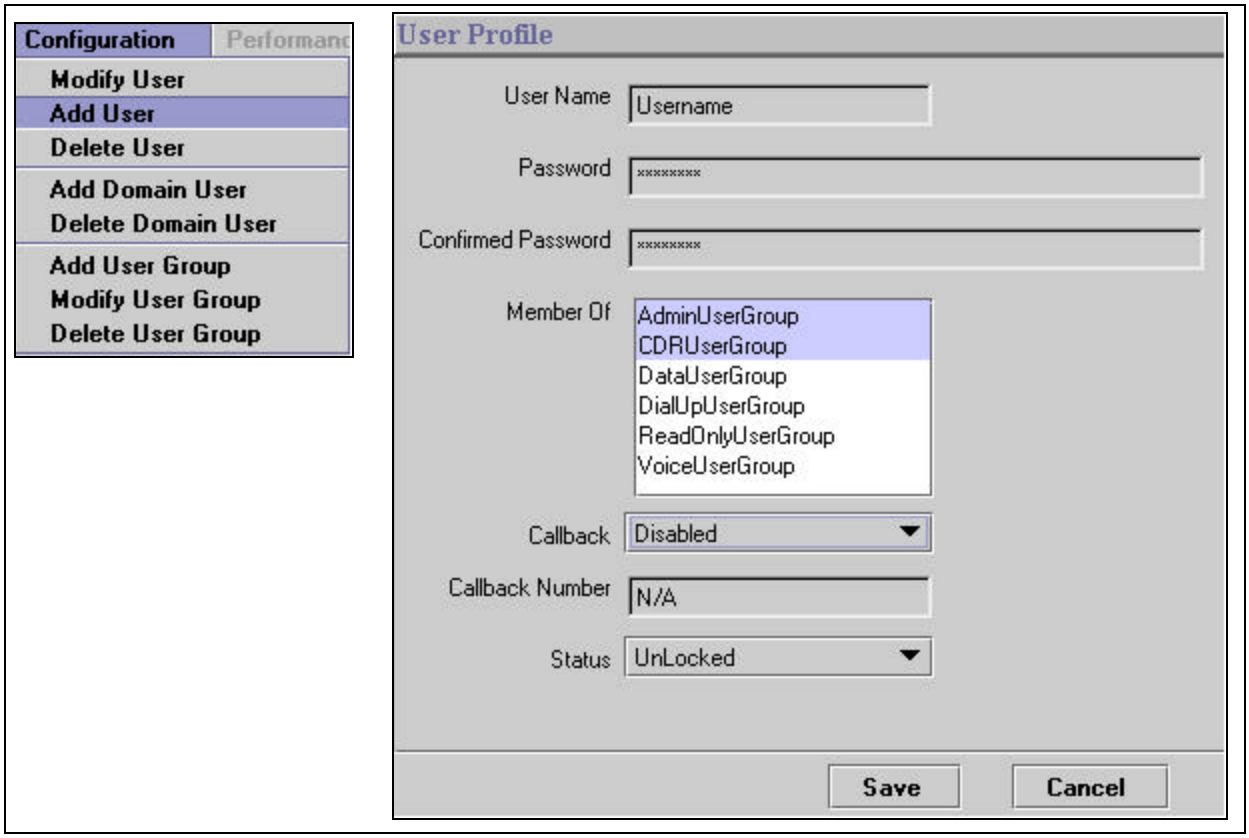
Adding or modifying a user profile

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

1 On the navigation tree, click the **Management** key and the **User Manager** heading.
The User Profile screen appears showing the current user profile information.

2 To add a new user, from the **Configuration** menu, select **Add User**.
To edit a user, select the user name on the list, and from the **Configuration** menu, select **Modify User**.
The User Profile dialog box appears.

Figure 65 User Profile Add/Modify screen



3 Use this table to determine what information you need to add or change.

Attribute	Value	Action
User Name	*<a maximum of 20 characters>*	Enter the user name. The User Name is case-sensitive and can be a maximum of 20 characters. **Note:** You cannot modify a user name. You must delete the complete User Profile row from the User Profile window and add a profile with the new name. **ISDN note:** When you enter an ISDN dialup user interface, the user name appears in this list. If you plan to use the secure callback properties for an ISDN user, you need to specify a static IP address for the interface. See "Configuring an ISDN interface" in the *Programming Operations Guide*.
Password	*<between 8 and 14 characters long>*	Assign a password to the user. The password is case-sensitive and can be a maximum of 14 characters. **Note:** • Password length is determined by the Minimum Password Length setting in the Password policy table. • Passwords must contain elements from three of these four character sets. This requirement can change, if you change the default password policy complexity setting ("Setting password policy" on page 428): — upper case alphabet — lower case alphabet — westernized Arabic numerals — nonalphanumeric characters ($, !, %, ^) • A user who fails to enter the correct password can be locked out of the system after a defined number of retries (account lockout threshold). For information about setting the lockout threshold, see "Setting password lockout policy" on page 427.
Confirmed Password		Requires you to enter the same password again to validate the new or modified password.
Member of	AdminUserGroup CDRUserGroup DATAUserGroup DialUpUserGroup ReadOnlyUserGroup VoiceUserGroup	Select the level of access associated with the user: **AdminUserGroup:** Can see and change any menu items (default). **CDRUser Group:** Can see everything but cannot make changes. This user is restricted to accessing the CDRs. **DATAUserGroup:** Can only configure pre-defined data fields (default). **DialUpUserGroup:** All menus are invisible, and no menus are configurable (default). This group lets the user access the system through a dialup connection. **ReadOnlyUserGroup:** Can see everything but cannot make changes (default). **VoiceUserGroup:** Can only configure pre-defined voice fields (default). Note: You cannot modify default user groups. **Dial-up note:** If any of the users will be using a dial-up connection to access the system, they must be assigned to the DialUpUserGroup.

Attribute	Value	Action
Callback	Disabled/Enabled	If this user is going to use a V.90 modem or an ISDN-BRI link to connect to the system and the user requires callback, ensure that Callback is enabled. If the user is configured as an ISDN interface, ensure that a static IP address has been specified for the interface. See “Configuring an ISDN interface” in the *Programming Operations Guide*. If this user is not using a V.90 modem or an ISDN-BRI link or does not require callback, set Callback to Disabled. Note: The system supports one dial-up connection at a time.
Callback Number		This is the number the system uses to call back to the external modem or ISDN-BRI link. Ensure that the appropriate routing codes are added to the dial string.
Status	Unlocked Unlock	Shows the current state of the user’s password. If the password becomes locked and the user does not want to wait the lockout time, you can unlock the user’s password record to release the password.

4 Click the **Save** button to save your settings.
The new user profile information is added to the User Profile list.

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

Setting up callback for a user

If the user will access the system through a dialup connection, you need to add that group to the user account. In this case, callback will be enabled to ensure that the system security is maintained.

1 On the navigation tree click the **Management** key and the **User Manager** heading.
The User Profile screen appears showing the current user profile information.

2 To add a new user account, on the **Configuration** menu select **Add User**.
To change an account, select the name on the list, then from the **Configuration** menu select **Modify User**.

3 Enter a User Name, if one does not already exist.

4 Enter and confirm a password, if one has not already been specified.

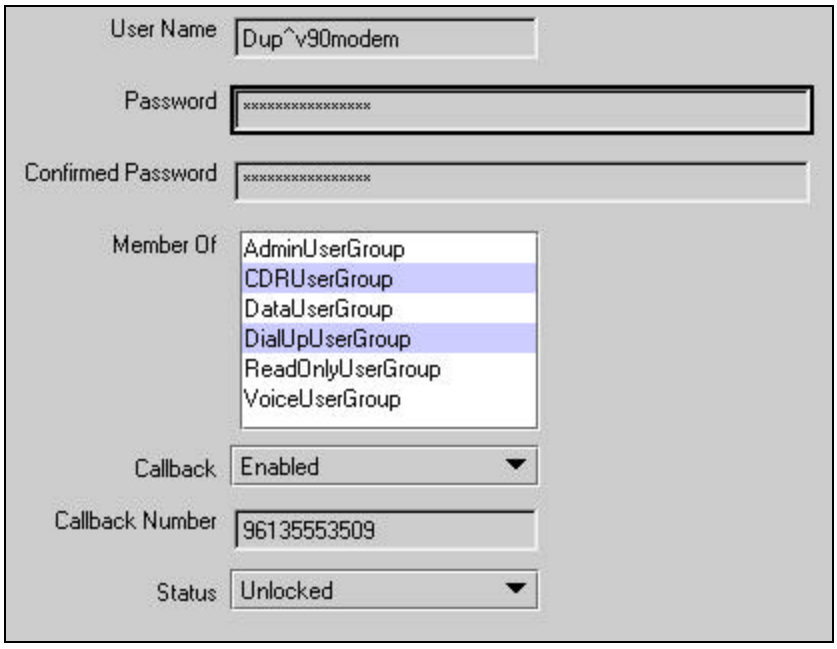
5 Click to highlight the DialUpUserGroup name. Then hold the **<Ctrl>** key down and click any other groups to which you want to assign the user.

6 From the **Callback** list box select **Enabled**.

7 Enter the number the system will dial to contact the client modem. Ensure you include the correct routing codes.

8 Click the **Save** button to save the settings.

Figure 66 User profile for dial-up user



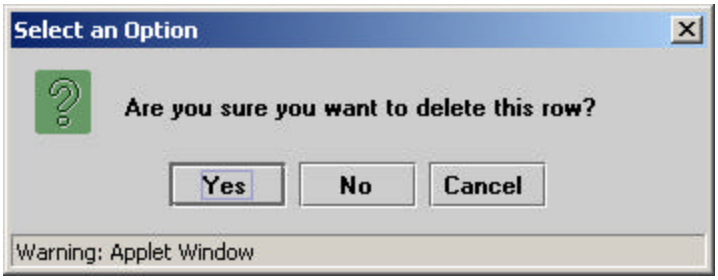
Deleting a user profile

1 On the navigation tree click the **Management** key and the **User Manager** heading. The User Profile screen appears showing the current user profile information.

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

3 From the **Configuration** menu, select **Delete User**. A message appears that asks you to confirm the deletion.

Figure 67 User Manager delete confirmation dialog



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

Security note: You cannot delete the ee_admin user.

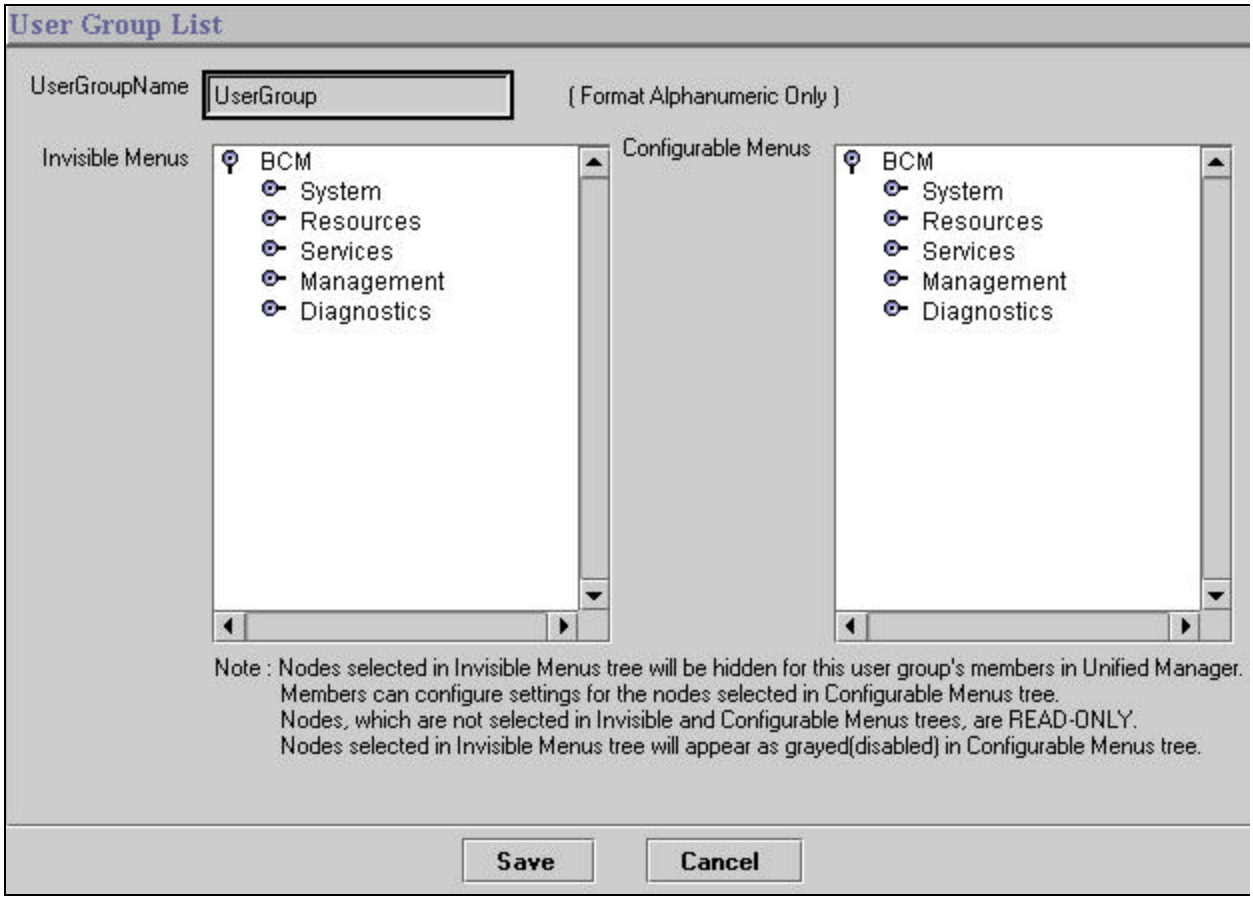
Adding or modifying a group profile

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

To add or modify the profile for a group

1. On the navigation tree click the **Management** key and the **User Manager** heading. The User Profile screen appears showing the current user profile information.
2. Click the **User Group List** tab to view the existing groups.
3. Add or change a user group:
   - To add a new group, from the **Configuration** menu, select **Add User Group**.
   - Tou edit a group, select the user group name on the list, then from the **Configuration** menu, select **Modify User Group**.
4. The User Group List dialog box appears.

Figure 68 User Group List add/modify screen

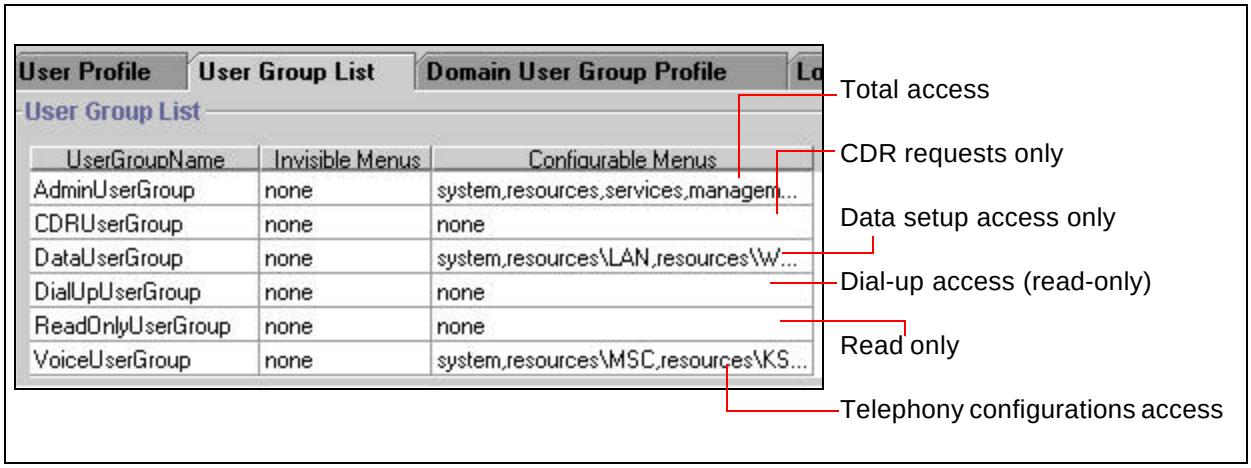


5 Use this table to determine the user group profile information that needs to be added or changed:

Attribute	Action
UserGroupName	View the name of the user group. If you are modifying an existing record, you will not be able to change this field.
Invisible menus	Choose which menus you want to keep hidden from the user group. The Configurable Menus box shows these fields covered by a grey box.
Configurable menus	Select the settings users are able to change. Headings that appear in white will appear on the menu, but will be read-only for this group.

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

Figure 69 Default user groups



Deleting a group profile

1 On the navigation tree click the **Management** key and the **User Manager** heading.
The User Profile screen appears showing the current user profile information.

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

3 From the **Configuration** menu, select **Delete User Group**.
A message appears that asks you to confirm the deletion.

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

Adding a Domain User Group profile

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

You can add only valid users currently assigned to CDR user groups. See "Adding or modifying a user profile" on page 420. When you add local users, the user name is automatically added to this list. If you are entering an external user, they must be members of a domain that recognizes this Business Communications Manager, and you add their user name.

1. On the navigation tree click the **Management** key and the **User Manager** heading.
   The User Profile screen appears showing the current user profile information.
2. Click the **Domain User Group Profile** tab to view the existing groups.
3. From the **Configuration** menu, select **Add Domain User**.
   The Domain User Group Profile dialog box appears.
4. Use this table to add the new Domain user Group profile name.

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

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

Deleting a Domain User Group profile

1. On the navigation tree click the **Management** key and the **User Manager** heading.
   The User Profile screen appears showing the current user profile information.
2. Click the **Domain User Group Profile** tab to view the existing groups.
3. From the **Configuration** menu, select **Delete Domain User**.
   A message appears that asks you to confirm the deletion.
4. Click the **Yes** button to delete the Domain User Group profile.

Setting password lockout policy

If you have Lockout Policy enabled, you can determine when a user is locked out of the system if they enter an incorrect password.

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

1. Select **Management, User Manager**.
   The User Profile screen appears showing the current user profile information.
2. Click the **Lockout Policy** tab.
   Lockout Policy is enabled by default.
3. Use the information provided in this table to determine the lockout policy for your system. The settings are effective as soon as they are entered.

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

Setting password policy

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

1. On the navigation tree click the **Management** key and the **User Manager** heading.
   The User Profile screen appears showing the current user profile information.
2. Click the **Password Policy** tab.
3. Use the information in this table to determine the lockout policy for your system.

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

Using the SSH client to access the text-based interface

Some operations for Business Communications Manager, such as initializing a new hard disk, use a text-based interface. In previous versions, Telnet was used to access Business Communications Manager text menus. BCM version 3.5 software introduces the ability to securely access Business Communications Manager through a network connection using SSH server software. SSH service software is from SSH Communications Security (www.ssh.com). You can download the SSH client application, called PuTTY, from the Business Communications Manager front page.

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

Security note: You can still use Telnet for direct connections through a crossover cable, since network security is not an issue in this case.
If you want to use Telnet over the network, you need to manually start the service.
See "Manually activating Telnet" on page 431.

Installing PuTTY

PuTTY is a desktop application tool that connects you to the text interface used by Business Communications Manager.

1 On the Unified Manager front page, click the **Install Clients** icon.
The Download Client Applications page appears.

2 In the left frame, under the **Administrative Tools** heading, click the **SSH client** link.

3 On the SSH Client page, click the **Download SSH Client** icon and download PuTTY to your computer.

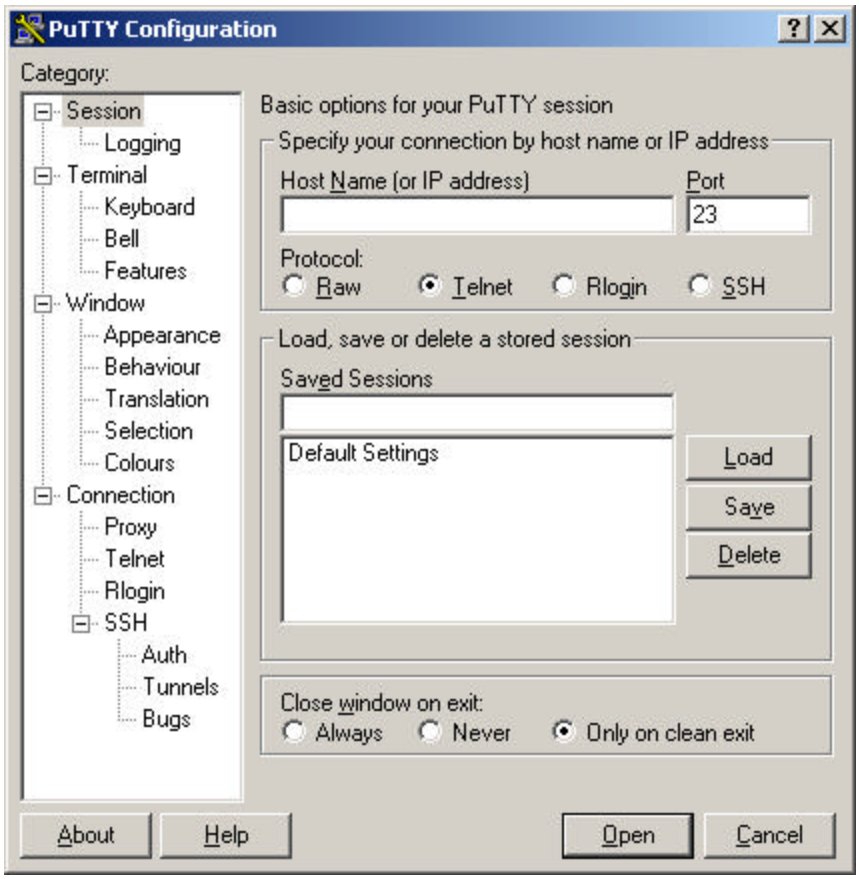
4 On your desktop, double click **Putty.exe**.

5 Follow the install wizard to install PuTTY.

Using PuTTY

1 Click the shortcut PuTTY icon.
The PuTTY Configuration screen appears.

Figure 70 PuTTY Configuration screen



2 Select the **SSH** option.

3 In the **Host Name (or IP address)** box enter the IP address or the Fully Qualified Domain Name for the Business Communications Manager you want to connect with and click the **Open** button.
The first time you start PuTTY you can receive a security notice.

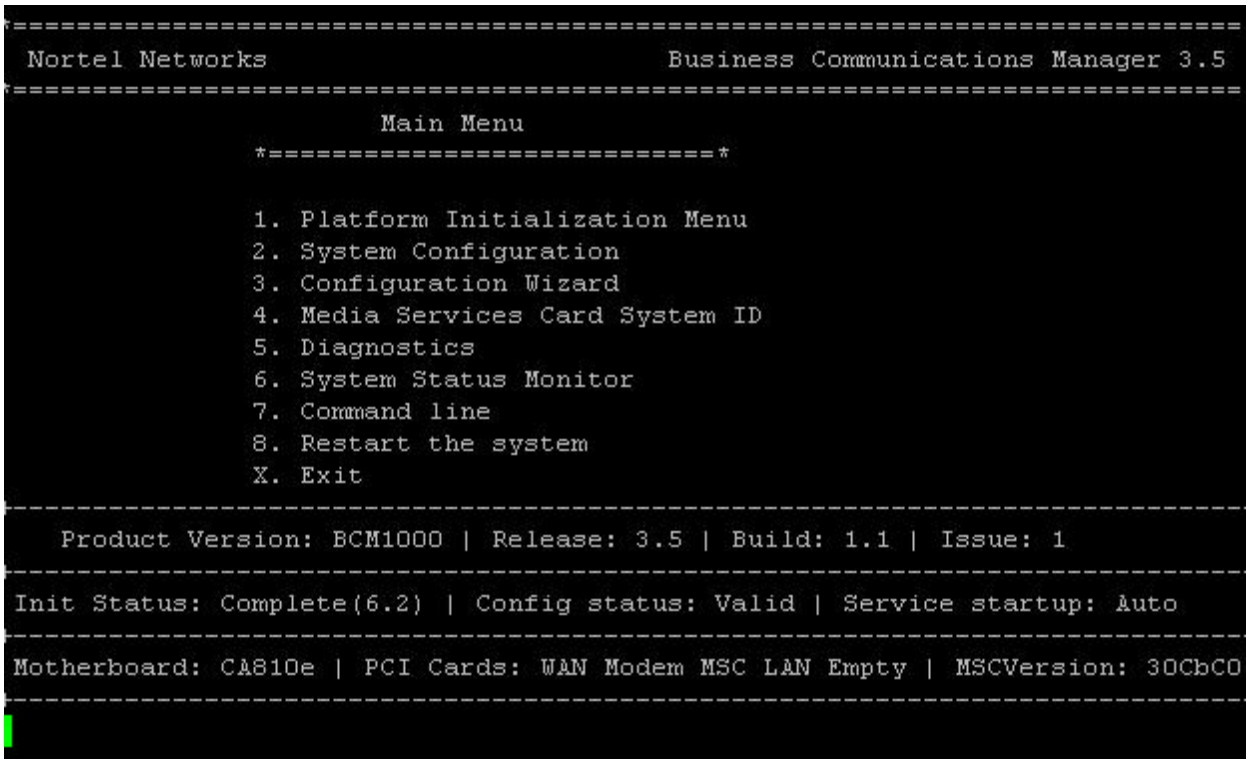
4 Click the **OK** button.
The PuTTY text screen appears.

5 At the login prompt, enter an administrator-level user name and press <**Enter**>.

6 At the next prompt, enter the corresponding password and press <**Enter**>.

7 The Business Communications Manager Main Menu appears.

Figure 71 Business Communications Manager Main Menu



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

Manually activating Telnet

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

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

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

1 In the Unified Manager navigation frame, click the **Services** key and click **Telnet** heading. The Telnet Summary screen appears.

2 From the Status list box, change **the status** to **Enabled**.

Accessing Unified Manager through the firewall

The Business Communications Manager IP Firewall Filters feature is one of the security features Business Communications Manager offers to protect your network against intruders. You can also use the security and firewall features to control what outside resources your users can access.

For more information about firewalls, see Chapter 33 in the *Programming Operations Guide*.

Dial up access

Through Business Communications Manager you can create and use dial up connections for Remote Access Service (RAS) or dial-on-demand network access.

With RAS you can access Business Communications Managers remotely by making an IP connection using PPPoE, an ISDN BRI/PRI line or the V.90 modem (North America only). After you connect to the Business Communications Manager system, you can access all IP-based system management operations.

Business Communications Manager also supports dial-on-demand for primary and backup WAN connections. Primary and backup WAN connections can use an ISDN BRI/PRI line or a V.90 modem (North America).

For more information about dial up access, see Chapter 21 in the *Programming Operations Guide.*

Using VPN

Business Communications Manager uses the Internet and tunneling protocols to create secure extranets. These secure extranets require a protocol for safe transport from the Business Communications Manager to another device through the Public Data Network (PDN).

Business Communications Manager uses the PPTP and IPSec tunneling protocols. Both of these protocols have encryption, but IPSec has a slightly more secure hashing algorithm for negotiating keys.

Extranets can connect:

- mobile users to a fixed private network at their office over the PDN
- private networks in the two branch offices of the same corporation over PDN
- two divisions of the same corporation over the corporate intranet

When connecting two branch offices, the use of a VPN over the public data network is very efficient if the connection is required only intermittently or a dedicated point-to-point link is considered too expensive. Also, with the advent of business-to-business solutions, VPNs can be deployed to provide secure connections between corporations.

For more information on creating and using a virtual private network, see Chapter 21 in the *Programming Operations Guide*.

Chapter 10
Testing, Troubleshooting, and Diagnostics

This section contains information about diagnosing module line performance issues and device line issues. This section also provides instructions on how to perform a system startup, set identification parameters and maintain telephony resources.

Testing, troubleshooting and diagnostics topics

Module Diagnostics

To perform troubleshooting diagnostics on your Business Communications Managers, you must know the system version and the status of each of the Media Bay Modules. For procedures on how to access this information, see:

To troubleshoot specific modules and lines, there are a number of tests you can perform;

For DTM modules:

- "Testing DTM Modules" on page 439.
- "DTM CSU statistics" on page 441

For device or station module issues:

- "Troubleshooting Telephone Connections" on page 448
- "Identify a device connected to the system" on page 448

System version

View the system version to can check the version number of the System Processor (SP) software that resides on the Media Services Card (MSC).

1 On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
The version number of the software appears in the System version box.

2 Write the version number on the appropriate Maintenance record.

Note: You can use the version number to determine the software release, which can be required by support staff if a software fault occurs.

Problems with module service

Check first for user problems, then wiring connections and programming errors before replacing Business Communications Manager equipment.

Warning: Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

1 Check that the module is properly inserted in the server or expansion cabinet.

2 Access **Resources** and then **Media Bay Modules**, to ensure that the module is not disabled. For more information, see the procedure, "Media Bay Module status" on page 437.

If the problem persists

If the AC power is present and the LED indicator on the module is off, contact your customer service representative. If AC power is present and the LED indicator on Business Communications Manager is off, replace the Business Communications Manager system.

Note: Before you replace the Business Communications Manager system, disconnect all central office and station lines from the Business Communications Manager system. Power down the system by unplugging it.

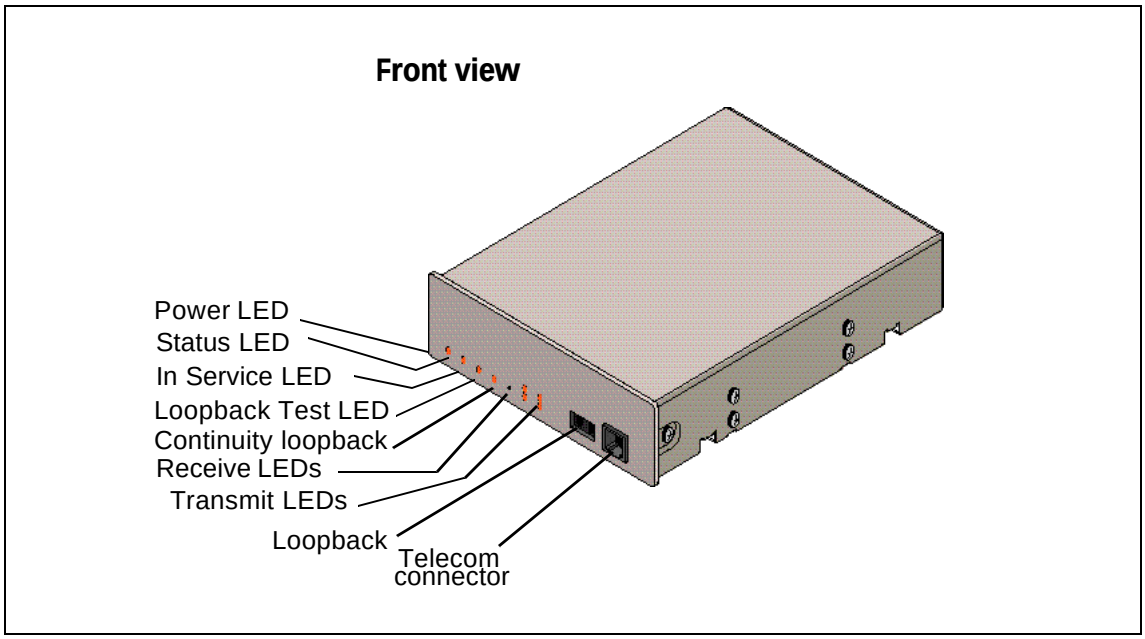
Refer to *Business Communications Manager Installation and Maintenance Guide* for information on replacing components. For more information see:

- "Digital trunk module problems" on page 435
- "Monitoring the T1 or PRI signal" on page 436

Digital trunk module problems

1 On the navigation page, click the **Resources** and **Media Bay Modules** key, and the bus that the module is on to verify that the DTM is enabled and that the lines are provisioned. For more information, see the procedure, "Media Bay Module status" on page 437.

Check the LEDs on the front of the DTM.



- **Receive Alarm**: yellow LED on indicates a problem with the digital transmission being received. This half-duplex link is unusable.
- **Receive Error**: yellow LED on indicates a minor error as a result of degraded digital transmission. Possible causes are an ohmic connection, water ingress, or too long a loop.
- **Transmit Alarm**: red LED on indicates an inability to transmit. Alarm indication signal (AIS) is being transmitted to the terminating switch. This half-duplex link in unusable.
- **Transmit Error**: yellow LED on indicates a remote alarm indication (RAI) carrier failure alarm (CFA) is being sent to the terminating switch. If the Transmit Alarm is not on, this indicates a far-end or cable problem.

- **In service**: flashing green LED indicates that the T1 or PRI trunks are out of service because of a running loopback test, or because the DTM is being initialized.
- **Loopback test**: red LED on indicates a continuity loopback test is running.
- **All LEDs flashing continuously**: the DTM is being initialized.

2 On the Unified Manager navigation tree, select **Resources, Telephony**, **Maintenance**, and **Tests** to run any loopback tests as appropriate.

3 Check the pinout of the cable that connects the DTM to the termination point from the T1 or PRI service provider or the external channel service unit, and check that the cable is properly connected.

4 Check with your T1 or PRI service provider to see if through-fed repeaters are used on the T1 or PRI span. The DTM does not provide the DC connection required for through-fed repeaters. If through-fed repeaters are used on the T1 span, disable the internal CSU and connect the DTM to an external CSU.

5 If the problem persists, replace the DTM.

Caution: Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

For information on how to replace system components, see the *Business Communications Manager Installation and Maintenance Guide*.

Monitoring the T1 or PRI signal

If you are finding minimal faults with the T1 or PRI signal, you can monitor the signal to try to isolate the problem. The monitor jack on the DTM faceplate provides non-intrusive, bridged in-service monitoring of the T1 or PRI signal. Connect a protocol analyzer or other test equipment into the monitor jack to monitor the signal received from the network, and the signal transmitted by Business Communications Manager.

Problems with trunk or station modules

1 On the navigation page, click the **Resources** and **Media Bay Modules** key, and the bus that the module is on to ensure that the module is not disabled. For more information, see the procedure, "Media Bay Module status" on page 437.

2 Disable the module using the procedure, "Disabling or enabling a single module" on page 438.

3 Enable the module using the procedure, "Disabling or enabling a single module" on page 438.

For an DTM, CTM or DSM:
Check the external line by terminating a single-line telephone directly on the distribution block, or equivalent, which connects to the Trunk Module.

For an ASM, if the ASM is still down, power down, and then power up Business Communications Manager.

If the problem persists

1 If AC power is present and the LED indicator on the module is off, replace the module.

2 Replace the link cable.

3 Replace the module.

For information about replacing components, see the *Business Communications Manager Installation and Maintenance Guide*.

Media Bay Module status

From the Media Bay Modules selection you can view the status of all the modules and identify any device or lines connected to the system so that you can isolate any malfunctioning part of the system. You can also use the Media Bay Module selection to disable and enable modules and devices. For more information, see the following procedures.

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

1 On the navigation tree, click the **Resources** and click **Media Bay Modules** keys and click the heading of the bus you want to view.
The information of the module associated with the bus appears.

Disabling/enabling a bus

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

1 On the navigation tree, click the **Resources** and **Media Bay Modules** keys and the bus number of the module you want to enable or disable.

2 On the top menu, click **Configuration**, and then, click **Enable** or **Disable**.
A message appears that asks you to confirm your request.

3 Click the **OK** button.

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

Disabling or enabling a single module

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

1. On the navigation tree, click the **Resources** and **Media Bay Modules** keys and the bus number of the module you want to enable or disable.
2. Click the module number of the media bay module you want to enable/disable.
3. On the top menu, click **Configuration**, and then click **Enable** or **Disable**.
   A message appears that asks you to confirm your request.
4. Click the **OK** button.

Tips: If your system has a 3/5 DS30 split, Bus 07 does not have a module assigned to it.

Disabling/enabling a port channel setting

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

To turn off a channel

1. On the navigation tree, click the **Resources** and **Media Bay Modules** keys and the bus number where the module is located.
2. Click the **Ports on bus** key and the key for the port that contains the channel you want to disable.
3. Click the **Channels** key and the B channel you want to disable (**B1** or **B2**).
4. On the top menu, click **Configuration** and select **Disable** or **Enable**.
   If you are disabling the channel, a message appears that asks you to confirm the deletion.
   The State field shows the mode of operation for the port. If the port is enabled, this field is blank unless a device is physically connected.

Testing DTM Modules

You can run tests on Business Communications Manager to verify the integrity of the installation wiring to DTM modules.

Warning: Choose an appropriate time to run tests, such as after office hours.

Table 42 Messages that can appear on the Alarm Telephone during Loopback tests

Message	Explanation
EVT: 210-YYYZ	Loopback test YYY on Trunk module Z has started
EVT: 211-YYYZ	Loopback test YYY on Trunk module Z has ended

You can start and stop Loopback tests under the Diagnostics section of Unified Manager. Run only one test at a time on a DTM. You can do other programming task while the loopback test is running. While the loopback test is running, the green “in Service” LED on the DTM flashes.

If you administer the internal CSU on a line loopback and payload loopback, the central office can also invoke and stop tests. To be able to run a payload loopback test, you must configure the DTM for extended superframe format.

Tests you can run on Business Communications Manager

- “Line loopback test” on page 439
- “Payload loopback test” on page 440
- “Card loopback test” on page 440
- “Continuity loopback test” on page 440

Use the procedure “Start a loopback test” on page 440, to run any of these tests.

Line loopback test

The line loopback test loops the full 1.544 Mbps signal received from the network back to the network. The looped signal regenerates without any change in the framing format and without the removal of any bipolar violations. The line loopback test can also be invoked and stopped remotely using the in-band signal or via the facility data link (FDL) in extended super frame (ESF) format.

The line loopback test must be run in coordination with the T1 or PRI service provider. Some test patterns can cause the DTM to reset. To avoid this, start the line loopback test from your system before the T1 or PRI service provider begins their test, and stop the line loopback test from your system after the T1 or PRI service provider ends their test.

Payload loopback test

The payload loopback test loops the received information bits (192 per frame) back to the network. You can also remotely invoke and stop the payload loopback test through the facility data link (FDL) in extended super frame (ESF) format.

The payload loopback test must be run in coordination with the T1 service provider. Some test patterns can cause the DTM to reset. To avoid this, start the payload loopback test from your system before the T1 service provider begins their test, and stop the payload loopback test from your system after the T1 service provider ends their test.

Card loopback test

The card edge loopback test loops the outgoing signal on the DTM back to its internal received signal path. The system disconnects signal paths to the external network.

Continuity loopback test

The continuity loopback test shorts the tip and ring pair of the receive signal path with the transmit signal path. Use this test to check the metallic continuity of the external wiring.

Start a loopback test

Warning: Give notice that you are running a loopback test.
Calls on all T1 or PRI lines on the DTM are automatically dropped when a loopback test is invoked. Use the Page feature to notify people using the system that a test is about to begin and that calls will be disconnected.

1 On the Unified Manager navigation frame click the **Diagnostics** and **Trunk Modules** keys, and click the keys for the bus that contains the card you want to test, and the module on the bus.

2 Click the **Loopback Tests** heading.
The Configuration menu is enabled. The loopback status box displays the type of test currently running.

Note: If there is an analog module in the media bay or the media is empty, the status is shown as Not equipped.

3 On the **Configuration** menu, click **Start loopback** to begin the test.
The Loopback type selection window appears.

4 Select the test you want to run and click the **OK** button.

Note: To end the test at any time, on the Configuration menu click Stop loopback.

DTM CSU statistics

Each DTM 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.

DTMs must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information see:

- "Statistics collected by the system" on page 441
- "Enabling the internal CSU" on page 442
- "Check the performance statistics" on page 442
- "Check the CSU alarms" on page 443
- "Check carrier failure alarms" on page 443
- "Check bipolar violations" on page 443
- "Check short term alarms" on page 443
- "Check Defects" on page 444
- "Reset all statistics" on page 444

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 as per 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:

- active carrier failure alarms (CFA) (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI)
- bipolar violations that occurred in the last minute
- defects (loss of signal LOS, out of frame OOF, alarm indication signal AIS) that occurred in the last minute
- milliseconds of short term alarms (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI) in the last minute. 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.

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

You can select the criteria for declaring and clearing the alarms to meet those in TIA-547A or TR64211.

Enabling the internal CSU

Use this procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

1. On the navigation tree, click the **Resources** and **Media Bay Modules** keys and the heading for the appropriate bus.
2. Click the **Modules on Bus** headingand the appropriate module.
3. Click the **T1 Parameters** heading and from the **Internal CSU** list box, select **On**. The module is temporarily disabled while the internal CSU is enabled.

Check the performance statistics

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.
2. Click the **Module**, **CSU statistics** and **Performance statistics** keys.
3. Click the **Current interval** heading to display 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).
4. Click the **15 min intervals** heading to display statistics for 15 minute intervals in the last 24 hours, numbered from the most recent (01) to the oldest (96). Click the most recent interval. The window shows the start time of the interval.
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.

Check the CSU alarms

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.

2. Click the **Module**, **CSU Statistics** and **Alarm statistics** keys, and click the **Active alarms** heading.
   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, see "Statistics collected by the system" on page 441.

Check carrier failure alarms

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.

2. Click the **Module**, **CSU Statistics** and **Alarm statistics** keys, and click the **CFA alarms** heading.
   The display shows LOS (loss of signal), OOF (out of Frame), AIS (Alarm indication signal), RAI (Remote alarm indicator), Short-term alarms and Defects. For more information on these types of transmission defects, see "Statistics collected by the system" on page 441.

3. Choose the type of alarm you wish to view, for example, LOS (Loss Of Signal).

4. Click the **Period #**.
   The Start time of the period is displayed.

Check bipolar violations

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.

2. Click the **Module**, **CSU Statistics** and **Alarm statistics** keys.
   The bipolar violations that occurred in the last minute are displayed.

Check short term alarms

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.

2. Click the **Module**, **CSU Statistics** and **Alarm statistics** keys, and click the **ShortTerm alarms** heading.
   The short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute are displayed.

Check Defects

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.
2. Click the **Module**, **CSU Statistics** and **Alarm statistics** keys, and click the **Defects** heading. The first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute are displayed.

Reset all statistics

1. On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that has the module that you want to check.
2. Click the **Module key and the CSU Statistics** heading.
3. On the **Configuration** menu, click **Clear CSU statistics.**
   A message appears that says that this action will remove all of the statistics.
4. Click the **OK** button to erase all the current statistics and begin collecting statistics again.

Testing the DDI Mux

Use loopback tests to check the DDI Mux data transfer capabilities. For loopback tests you must generate a test pattern or data traffic and provide a means to monitor the data path. The module provides two loopback tests:

- "DTE Loopback test" on page 444
- "DS30 Loopback test" on page 447

The following applies:

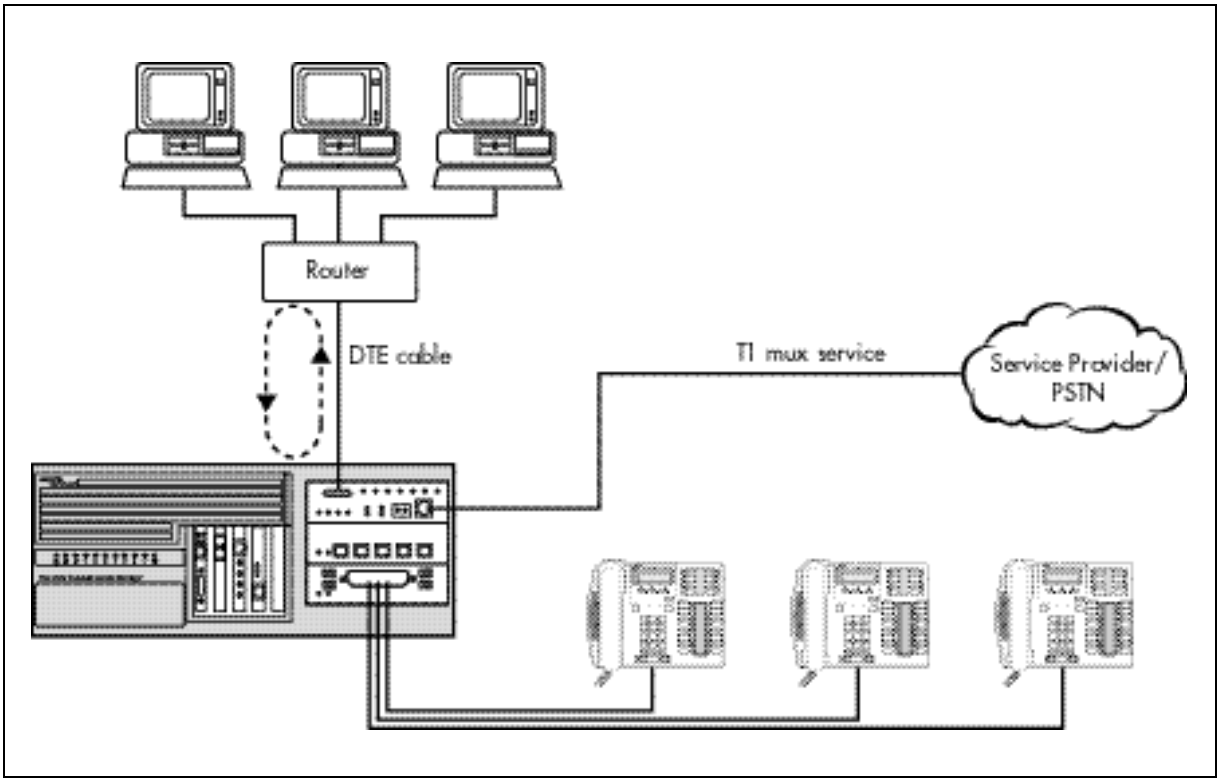
- activate one loopback at a time
- activation of a DTE loopback can be manual or automatic
- manual control over loopback state has priority over automatic
- manual capability of releasing all loopbacks

DTE Loopback test

The DTE Loopback test forwards data transmitted by the DTE (TxD) and loops the data back to the DTE (RxD). The DTE Loopback test establishes a data path from the DTE through the internal DDI Mux circuit and back to the DTE. Refer to Figure 59.

You must transmit a test pattern and monitor the received data at the DDI Mux data port. You can use a Bit Error Rate Tester to generate and monitor data traffic.

Figure 72 DTE Loopback Test



To begin a DTE Loopback test

1. On the navigation tree, click the **Diagnostics** and **Media Bay Modules** keys.
2. Click the key for the bus number assigned to the Data Module.
3. Click the **Data Module** key and then click the **Loopback status** heading.
4. From the **Loopback** listbox select **Manual DTE** or **Automatic DTE**.
   If you choose Manual DTE, the DDI Mux enters loopback mode with the DTE. Business Communications Manager takes any data it receives from the DTE and loops it back to the DTE.

   If you choose Automatic DTE, the DDI Mux enters the DTE loopback state when requested by the DTE. Use Automatic DTE only if this feature is supported by the DTE.
5. Exit the Unified Manager session. The TM LED lights to indicate the Loopback test has started.
6. View the TxD and RxD LEDs to make sure data is transmitted and received by the DTE. See "LED Indicator and Diagnostics" on page 446 for information about the LEDs.
7. When you are finished the loopback test, start a Unified Manager session.
8. Click the **Resources** and **Media Bay Modules** keys.

9 Click the key of the Bus number assigned to the Data Module.

10 Click the **Data Module** key and then click the **Loopback status** heading.

11 From the **Loopback** listbox select **Off**.

LED Indicator and Diagnostics

The DDI Mux has 15 LEDs that indicate current status or operating conditions:

Table 43 DDI Mux LED description

LED	Description
TxD (Transmit data)	The LED flashes at a rate equal to the number of zeros in the data received from the DTE and transmitted over the network. The speed of the flashes is an indication of the speed of the data sent over the network.
RxD (Receive data)	The LED flashes at a rate equal to the number of zeros in the data received from the network and transmitted to the DTE. The speed of the flashes is an indication of the speed of the data sent over the network.
RTS (Request to Send)	The LED lights when the DTE requests permission from the DDI Mux to send data.
CTS (Clear to Send)	The LED lights when the DDI Mux is signaling the DTE that it has permission to send data.
DCD (Data Carrier Detect)	The LED lights when Business Communications Manager is receiving a carrier signal.
DSR (Data Set Ready)	The LED lights when the DDI Mux is ready to communicate.
TM (Test Mode)	The LED lights when the DDI Mux is signaling to the DTE that it detects a test condition.
 (Power)	On indicates that the DTM is receiving +5 volts.
 (Status)	On indicates there is data communication between the DDI Mux and the MSC card.
In Service	Flashing indicates that the T1 trunks are out of service because a loopback test is running or the DDI Mux is initializing.
Loopback	On indicates a continuity loopback test is running on the T1 link.
Receive Alarm	On indicates a problem with the received digital transmission on the T1 link. This half-duplex link does not work.
Receive Error	On indicates a small error as a result of degraded digital transmission on the T1 link. Possible causes are an ohmic connection, water ingress, or too long a loop.
Transmit Alarm	On indicates the DDI Mux cannot transmit on the T1 link. The module sends an Alarm indication signal (AIS) to the terminating switch. This half-duplex link does not work.
Transmit Error	On indicates the DDI Mux is sending a remote alarm indication (RAI) carrier failure alarm (CFA) to the terminating switch. If the Transmit Alarm is not on, this error indicates a far-end or cable problem.

DS30 Loopback test

The DS30 Loopback test forwards data transmitted to the DTE (RxD) back to the MSC in Business Communications Manager. The DS30 Loopback establishes a data path from the MSC through internal DS256 bus and the internal DDI Mux circuit and back to the MSC.

You must generate a test pattern and provide a means to monitor the data path at the network connection. You can use a T1 Tester to generate and monitor data traffic. Connect the T1 Tester to the RJ48C connector on the module.

In a system where a T1 connects to a CSU/DSUs, the far end CSU/DSU can generate and monitor the network traffic while the local DDI Mux is in DS30 loopback tests.

To begin a DS30 Loopback test

1. On the Unified Manager navigation tree, click the **Resources** and **Media Bay Modules** keys.
2. Click the keys for the Bus number assigned to the Data Module and **Data Module**.
3. Click the **Loopback status** heading.
4. From the **Loopback** listbox, select **Manual DS30**.
   The DDI Mux enters loopback mode with the MSC. The module takes any data it receives from the MSC loops it back to the MSC.
5. Exit the Unified Manager session.
   The TM LED lights to indicate the Loopback test has started.
6. View the TxD and RxD LEDs to make sure data is transmitted and received by the MSC. See "LED Indicator and Diagnostics" on page 446 for information about the LEDs.
7. When you are finished the loopback test, start a Unified Manager session.
8. Click the **Resources** and **Media Bay Modules** keys.
9. Click the keys for the Bus number assigned to the Data Module and **Data Module**.
10. Click the **Loopback status** heading.
11. From the **Loopback** listbox, select **Off**.

Troubleshooting Telephone Connections

This section provides suggestions for ways of testing connections between devices and the system:

Check the port associated with a device DN

Before you run any tests, use this procedure to determine the port associated with a device DN.

1. Click the **Diagnostics and MSC** keys.
2. Click the **DN-to-port conversion** heading.
3. In the **DN to convert** box type the DN you want to check.
4. Click outside the window to refresh the screen.
   The values appear in the Device port and Device channel boxes. These ports and channels refer to the headings found under the Resources, Media Bay Modules, Bus ## headings that the device is wired to.

For how to perform a DN-to-port conversion test, see "DN-to-port conversion" on page 459.

Identify a device connected to the system

You can check a device version number for compatibility with the system. Use this procedure to display status information for any device connected to the system.

1. On the navigation tree, click the **Resources** and **Media Bay Modules** keys.
2. Click the key for the **Bus ##** for the station module the device is wired to.
3. Click the key for the **Port #** that you found when you ran the DN-to-port conversion.
4. Click the **Channels** key**.**
5. Click the **B1** heading to display the device connected to the B1 channel. (If your system is a Partial Double Density system (PDD), there will also be B2 headings for modules installed on Buses 06 and 07.)
   The device, its type, the version number of the device and its state is displayed.

6 If there is an add-on device attached to the telephone such as a central answering position module or a Busy Lamp Field, click the **B1** or **B2** key and click the **Addons** heading to display the add-on device.

This table lists some of the device types that can appear on the Business Communications Manager device identification display.

Display	Explanation
T7100	T7100 telephone
T7310	T7310 telephone
M7324	M7324 telephone
1: CAP1	First CAP module attached to an M7324 telephone
2: CAP2	Second CAP module attached to an M7324 telephone
Nortel Networks ATA 2	Analog Terminal Adapter

Disable a device

Warning: Give notice that you are disabling equipment.
Inform people that you are going to disable their devices.

Warning: Pick a suitable time to disable devices. Disabling a port will disconnect users from their calls.
Do not disable devices when many people are using the Business Communications Manager system. Wait until after regular office hours.

Warning: Do not enable or disable ports during the first two minutes after plugging in your system.
If you enable or disable ports in the first two minutes after powering up, incorrect ports may be enabled or disabled. To recover from this, disable, then enable the affected modules using the **Media Bay Modules** selection.

To disable a device

1 Identify the device you wish to disable. For information on how to do this procedure, see "Identify a device connected to the system" on page 448.

2 Click the device you want to disable.

3 On the **Configuration** menu, click **Disable**.
A warning appears that this action will disable the port.

4 Click the **OK** button
The system disables the device in one minute (or immediately, if the device is idle).

Enabling a disabled device

1 Identify the device you wish to disable.
For information on how to do this procedure, see "Identify a device connected to the system" on page 448.

2 Click the device you want to enable.

3 On the **Configuration** menu, click **Enable**.
A message indicating that the device is being enabled.

Performing a system startup and warm reset

A system startup replaces all existing telephony programming with the default programming.

1 On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
The Configuration menu is enabled.

2 From the **Configuration** menu, click **System startup**.
The system displays a dialog box with three parameters: Region, Template and Start DN.

3 From the **Region** list select a region.
Each region has a Market Profile associated with it.

Note: When you select a new region, the template list is read-only. The templates for the region apppear after you restart the system.

4 Type any valid value in the **Start DN** box.
The box displays the current value.

5 Click the **OK** button to apply these changes.
A warning appears that the system will restart and default programming values will be restored.

Note: After the system cold start is complete, you can use a different template than the default template. From Diagnostics, MSC, System startup and select a template from the template list. However, if you select a new template, you must perform another system restart.

Warm reset

A warm reset resets the telephony portion of the system but does not affect the current telephony programming.

1 On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
The Configuration menu option is enabled.

2 From the **Configuration** menu, click **Warm reset**.
The system displays a warning that all active calls will be dropped.

3 Click **OK** to continue.

Changing system identification parameters

Topics about changing your system identification parameters

Changing the system name

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

1 On the navigation tree, click the **System** key and click the **Identification** heading.
The Identification screen appears.

2 In the **System Name** box enter the new system name.

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

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

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

Changing the system domain

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

To change the system domain, add the Business Communications Manager system to a new domain. You can add the Business Communications Manager system to:

- a workgroup
- a domain
- a Windows 2000 domain

To add Business Communications Manager to a workgroup

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

To add Business Communications Manager to a domain

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

To add Business Communications Manager to a Windows 2000 domain

1. On the navigation tree, click the **System** key and click the **Identification** heading.
   The Identification screen appears.
2. Click the **Change Domain Membership** tab.
   The Change Domain Membership screen appears.
3. Click the **Add To** box and click **Win2000Domain**.
4. In the **Domain User ID** box enter the User ID that Business Communications Manager uses to access this domain.
5. In the **Password** box enter the password that Business Communications Manager uses to access this domain.
6. In the **New Win 2000 Domain** box enter the name of the domain to which you want to add Business Communications Manager.

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

8 Restart Business Communications Manager.

Changing the CallPilot region

The CallPilot region defines some call-management-related system defaults.

1 On the navigation tree, click the **System** key and click the **Identification** heading. The Identification screen appears.

2 Click the **CallPilot Region** box.

3 Click the region in which the Business Communications Manager system resides.

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

Changing the Business Communications Manager time and date

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

1 On the navigation tree, click the **System** key and click the **Identification** heading. The Identification screen appears.

2 In the **Date** box enter the current date.

3 In the **Time** box enter the current time at the site where Business Communications Manager is located.

4 In the **Time Zone** box select the time zone at the site where Business Communications Manager is located.

5 Press the **Tab** key to save your changes.

Maintenance programming for telephony resources

To perform maintenance on your Business Communications Manager, you must know the system version and the status of each of your Media Bay Modules. For how to access this information see:

- “System version” on page 454
- “Media Bay Module status” on page 454

If you want to run a line loopback, payload loopback, card loopback or continuity loopback test, see “Tests” on page 457.

For information on system statistics and metrics, see:

- “CSU statistics” on page 460

- "Link Status" on page 463
- "Metrics" on page 464

For information on physically moving an existing telephone, see "Moving telephones" on page 465.

System version

View the system version to check the version number of the System Processor (SP) software that resides on the Media Services Card (MSC).

1 On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
The version number of the software appears in the System version box.

2 Record the version number on the appropriate Maintenance record.

Note: You can use the version number to determine the software release and it may be required by support staff if a software fault occurs.

Media Bay Module status

With the Media Bay Modules selection you can view the status of all the modules and identify any device or lines connected to the system, to isolate any malfunctioning part of the system. You can also use the Media Bay Module selection to disable and enable modules and devices. For more information see:

- "Displaying the Media Bay Module status" on page 454
- "Disabling a module" on page 455
- "Enabling a disabled module" on page 455
- "Identifying a device connected to the system" on page 455
- "Disabling a device" on page 456
- "To enablie a disabled device" on page 457

Displaying the Media Bay Module status

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

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

2 Click heading of the Bus you want to view.
The Configuration menu is enabled and the status information of the module associated with the bus appears.

Disabling a module

You must disable a module before you replace it. In addition, you may be able to clear a hung line by disabling and enabling the affected module.

Warning: Use Page feature, on your system, prior to disabling.
Use the Page feature to inform users that you are about to disable a module. Indicate that they may experience delays in the performance of their devices.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the heading of the Bus you want to disable.
   The State boxshows that the module is enabled. The Configuration menu option is enabled.
3. On the **Configuration** menu, click **Disable**.
   A warning appears that this action will disable the module and all of its devices.
4. Click the **OK** button.
   The module is disabled in one minute, or immediately if the status is idle.

Enabling a disabled module

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the heading of the Bus associated with the module you want to enable.
   The State shows that the module is disabled and the Configuration menu is enabled.
3. On the **Configuration** menu, click **Enable**.
   A message appears saying that the module is being enabled.

Identifying a device connected to the system

You can check a device's version number for compatibility with the system. Use this procedure to display status information for any device connected to the system.

1. On the navigation tree, click the **Resources** and the **Media Bay Modules** keys.
2. Click the **Bus ##** and **Port #** keys.
3. Click the **Channels** key.
4. Click the **B1** or **B2** heading to display the device connected to those channels.
   The device, its type, the version number of the device and its state are displayed.
5. If there is an add-on device attached to the telephone such as a central answering position module or a Busy Lamp Field, click the **B1** or **B2** key and click the **Addons** heading to display the add-on device.

This table lists some of the device types that can appear in the Business Communications Manager device identification display.

Display	Explanation
T7100	T7100 telephone
T7310	T7310 telephone
M7324	M7324 telephone
1: CAP1	First CAP module attached to an M7324 telephone
2: CAP2	Second CAP module attached to an M7324 telephone
Nortel Networks ATA 2	Analog Terminal Adapter

Disabling a device

Warning: Give notice that you are disabling equipment.
Inform people that you are going to disable their devices.

Warning: Pick a suitable time to disable devices. Disabling a port will disconnect users from their calls.
Do not disable devices when many people are using the Business Communications Manager system. Wait until after regular office hours.

Warning: Do not enable or disable ports during the first two minutes after plugging in your system.
If you enable or disable ports in the first two minutes after powering up, incorrect ports may be enabled or disabled. To recover from this, disable, then enable the affected modules using the Media Bay Modules selection.

To disable a device

1. Identify the device you want to disable. For how to do this, see "Identifying a device connected to the system" on page 455.
2. Click the device you want to disable.
3. On the **Configuration** menu, click **Disable**.
   A warning appears that this action will disable the port.
4. Click the **OK** button.
   The device is disabled in one minute, or immediately if the device is idle.

To enablie a disabled device

1 Identify the device you want to disable. For how to do this, see "Identifying a device connected to the system" on page 455.

2 Click the device you want to enable.

3 On the **Configuration** menu, click **Enable**.
A message appears saying that the device is being enabled.

Tests

You can run tests on Business Communications Manager to verify the integrity of the installation wiring for the telephone sets. Before you run any tests, use the procedure, "DN-to-port conversion" on page 459, to determine the port associated with a particular DN.

Warning: Choose an appropriate time to run tests.
A good time to run tests is after office hours.

Messages that can appear on the Alarm Telephone during Loopback tests:

Message	Explanation
EVT: 210-YYYZ	Loopback test YYY on Trunk module Z has started
EVT: 211-YYYZ	Loopback test YYY on Trunk module Z has ended

You can start and stop Loopback tests under the Diagnostics heading. Run only one test at a time on an DTM. You can do other programming tasks while the loopback test is running. While the loopback test is running, the green "in Service" LED on the DTM flashes.

If you administer the internal CSU on a line loopback and payload loopback, the central office can also invoke and stop tests. To be able to run a payload loopback test, you must configure the DTM for extended superframe format.

Tests you can run on Business Communications Manager

- "Line loopback test" on page 458
- "Payload loopback test" on page 458
- "Card loopback test" on page 458
- "Continuity loopback test" on page 458

Use the procedure, "Starting a loopback test" on page 458, to run any of these tests.

Line loopback test

The line loopback test loops the full 1.544 Mbps signal received from the network back to the network. The looped signal regenerates without any change in the framing format and without the removal of any bipolar violations. The line loopback test can also be invoked and stopped remotely using the in-band signal or via the facility data link (FDL) in extended super frame (ESF) format.

The line loopback test must be run in coordination with the T1 or PRI service provider. Some test patterns can cause the DTM to reset. To avoid this, start the line loopback test from your system before the T1 or PRI service provider begins their test, and stop the line loopback test from your system after the T1 or PRI service provider ends their test.

Payload loopback test

The payload loopback test loops the received information bits (192 per frame) back to the network. You can also remotely invoke and stop the payload loopback test through the facility data link (FDL) in extended super frame (ESF) format.

The payload loopback test must be run in coordination with the T1 service provider. Some test patterns can cause the DTM to reset. To avoid this, start the payload loopback test from your system before the T1 service provider begins their test, and stop the payload loopback test from your system after the T1 service provider ends their test.

Card loopback test

The card edge loopback test loops the outgoing signal on the DTM back to its internal received signal path. The system disconnects signal paths to the external network.

Continuity loopback test

The continuity loopback test shorts the tip and ring pair of the receive signal path with the transmit signal path. Use this test to check the metallic continuity of the external wiring.

Starting a loopback test

Warning: Give notice that you are running a loopback test.
Calls on all T1 or PRI lines on the DTM are automatically dropped when a loopback test is invoked. Use the Page feature to notify people using the system that a test is about to begin and that calls will be disconnected.

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys, and the key for the bus that contains the card you want to test.

2 Click the key for the appropriate module on this bus.

3 Click the **Loopback Tests** heading.
The Configuration menu option is enabled. The loopback status box displays the type of test currently running.

Note: If there is an analog module in the media bay or the media is empty, the box displays Not equipped.

4 On the **Configuration** menu, click **Start loopback** to begin the test.
The Loopback type selection window appears.

5 From the list box, select the test you want to run and click the **OK** button.

Note: To end the test at any time, on the Configuration menu click Stop loopback.

DN-to-port conversion

If you know the DN of a telephone, you can determine the port associated with this DN using this procedure. See also "Troubleshooting Telephone Connections" on page 448.

1 Click the **Diagnostics and MSC** keys, and click the **DN-to-port conversion** heading.

2 In the **DN to convert** box type the DN and press **Enter**.
The values appear in the Device port and Device channel boxes.

Debug

Debug features are intended to be used with the assistance of your Business Communications Manager technical support team. You do not need the information provided by these features unless you are directed by a member of the technical support team. See also "Tests" on page 457.

To view the Restart info

1 Choose **Diagnostics**, **MSC**, **Debug**, and click the **Restart info** heading.
The **Restart info** summary screen appears.

2 On the **Configuration** menu click **Clear restart info** to clear the log.

To view the Registers information

1 Click the **Diagnostics and MSC** keys, and click **Debug**, **Restart info**.

2 Click the Registers heading.
The Registers summary screen appears.

Message monitoring

1 Click the **Diagnostics**, **MSC**, and **Debug** keys, and click the **Message monitoring** heading. The **Message monitoring** screen appears.

CSU statistics

Each DTM 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.

DTMs must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information, see:

- "Statistics collected by the Business Communications Manager system" on page 460
- "Enabling the internal CSU" on page 461
- "Checking the performance statistics" on page 461
- "Checking the CSU alarms" on page 462
- "Checking carrier failure alarms" on page 462
- "Checking bipolar violations" on page 462
- "Checking short term alarms" on page 462
- "Checking defects" on page 463
- "Resetting statistics" on page 463

Statistics collected by the Business Communications Manager system

The system accumulates three performance parameters:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined as per 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) (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI)
- the number of bipolar violations that occurred in the last minute
- any defects (loss of signal LOS, out of frame OOF, alarm indication signal AIS) that occurred in the last minute

- the number of milliseconds of short term alarms (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI) in the last minute. 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:

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.

Enabling the internal CSU

Use this procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

2 On the navigation tree, click the **Resources** and **Media Bay Modules** keys.

3 Click the key for the appropriate bus. and click the **Modules on Bus** key.
The modules on this bus appear.

4 Click the heading the appropriate module.

5 Click the **T1 Parameters** heading.

6 From the **Internal CSU** box, select **On**.
The module is temporarily disabled while the internal CSU is enabled.

Checking the performance statistics

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the key for the bus that contains the module that you want to check.

3 Click **Module #**, **CSU statistics**, **Performance statistics** keys.

4 Click the **Current interval** heading to display 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 **15 min intervals** heading to display statistics for 15 minute intervals in the last 24 hours, numbered from the most recent (01) to the oldest (96). Click the most recent interval. The window shows the start time of the interval.

6 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.

Checking the CSU alarms

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the key for the appropriate bus. and click the **Modules on Bus** key. The modules on this bus appear.

3 Click the **CSU Statistics** and **Alarm statistics** keys and click the **Active alarms** heading. The active alarms of the types LOS (loss of signal), OOF (out of Frame), RAI (Remote alarm indicator) or AIS (Alarm indication signal) are displayed. For more information on these types of transmission defects, see "Statistics collected by the Business Communications Manager system" on page 460.

Checking carrier failure alarms

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the key for the appropriate bus. and click the **Modules on Bus** key. The modules on this bus appear.

3 Click the **CSU Statistics** and **Alarm statistics** keys, and click the **CFA alarms** heading. TheLOS (loss of signal), OOF (out of Frame), AIS (Alarm indication signal), RAI (Remote alarm indicator), Short-term alarms and Defects are displayed. For more information on these types of transmission defects, see "Statistics collected by the Business Communications Manager system" on page 460.

4 Choose the type of alarm you wish to view and click the **Period #**. The start time of the period is displayed.

Checking bipolar violations

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the keys for the appropriate bus and modules.

3 Click the **CSU Statistics** and **Alarm statistics** keys. The bipolar violations that occurred in the last minute are displayed.

Checking short term alarms

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the keys for the appropriate bus and modules.

3 Click the **CSU Statistics** and **Alarm statistics** keys, and click the **ShortTerm alarms** heading.
The short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute are displayed.

Checking defects

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the keys for the appropriate bus and modules.

3 Click the **CSU Statistics** and **Alarm statistics** keys, and click the **Defects** heading.
The first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute are displayed.

Resetting statistics

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the keys for the appropriate bus and modules.

3 Click the **CSU Statistics** heading.

4 On the **Configuration** menu, click **Clear CSU statistics.**
A message appears saying that this will remove all of the statistics.

5 Click the **OK** button to erase all the current statistics and begin collecting statistics again.

Link Status

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

It is recommended that the number of lines that are deprovisioned on an DTM (configured as PRI) be the same as the number of b-channels that are disabled. For example, If the DTM is on bus 7, when b-channels 13-23 are disabled, you should deprovision lines 73 to 83.

1 On the navigation tree, click the **Diagnostics** and **Trunk Modules** keys.

2 Click the keys for the appropriate bus and modules.

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

4 Select a channel, for example B 01.
The status of the PRI channel is displayed.

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

Metrics

These usage metrics are available:

CbC limit metrics

You can view statistical information on call-by-call limit settings for PRI when the protocol is set to call-by-call routing.

1 On the navigation tree, click the **Diagnostics**, **Service Metrics**, **Telephony Services** and **CbC limit metrics** keys.
The pools that supports CbC routing are displayed.

2 Select a pool, for example Pool PRI-B.
The services in the pool are displayed. The services that appear depend upon the PRI protocol.

3 Select a service, for example Public.
The settings for the selected service are displayed.

To clear the settings for a selected service, on the **Configuration** menu click **Clear metrics**.

Hunt Group Metrics

This feature gives you statistical information on hunt group calls.

1 On the navigation tree, click the **Diagnostics**, **Service Metrics**, **Telephony Services**, **Hunt Group Metrics** keys.
All the Hunt Groups appear.

2 Click a Hunt Group.
The display shows all the statistical information for the selected hunt group.

To clear the hunt group metrics, click **Clear group** on the **Configuration** menu.

PSTN fallback metrics

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

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

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

Moving telephones

You can move a Business Communications Manager telephone to a new location in the system without losing its programmed settings. Set relocation (automatic telephone relocation) must be enabled in system programming. This makes the internal numbers, autodial settings, and personal speed dial codes remain with the telephone when it is unplugged.

Note: The set relocation feature applies to the digital telephones and ATAs only. IP telephones, such as the i2004, i2002, i2001, and i2050, always retain their programming regardless of where you move them on the LAN or WAN.

Automatic telephone relocation is disabled by default.

To enable set relocation.

1 On the navigation tree, click the **Services**, **Telephony Services** and **General settings** keys, and click the **Feature settings** heading.

2 In the **Set relocation** box, click **Y**.

After set relocation is enabled, unplug the telephone and plug it in again at another location. It may take up to 45 seconds for the system to recognize the telephone.

Tips

All telephones being moved should be relocated before new telephones are plugged into their place. This lets the moved telephones retain their programmed settings. If a new telephone is plugged into the system before the old telephone is reconnected at a new location, the system will give the old telephone information to the new telephone, and the old telephone will no longer be recognized by the system.

When changing a telephone internal number (in programming), wait one minute after Automatic Telephone Relocation.

When you relocate a telephone, the telephone must remain installed and connected in the new location for at least 3 minutes for the programming relocation to be complete. Moving the telephone again before the 3 minute period may result in losing the programming.

General Diagnostic Activities

Use the information in this section to monitor and diagnose general Business Communications Manager functions:

Service manager

You can monitor the state of your system services using Service Manager, located under Diagnostics in the Unified Manager. From the list you can choose a service and modify how the system interacts with the service. For more information on Service Manager, see "Service Manager" on page 251.

Watchdog with Service Manager

With the Watchdog setting you can activate service logging or to delay the start of services. This setting affects all services on your system.

For more information on Service Manager and watchdog, see "Voice watchdog" on page 311.

Base function tray system status display LEDs

As part of any general maintenance or troubleshooting procedure, you need to ensure that your hardware, and the firmware that runs that hardware, is operating as expected.

Methods of monitoring the system status monitor LEDs

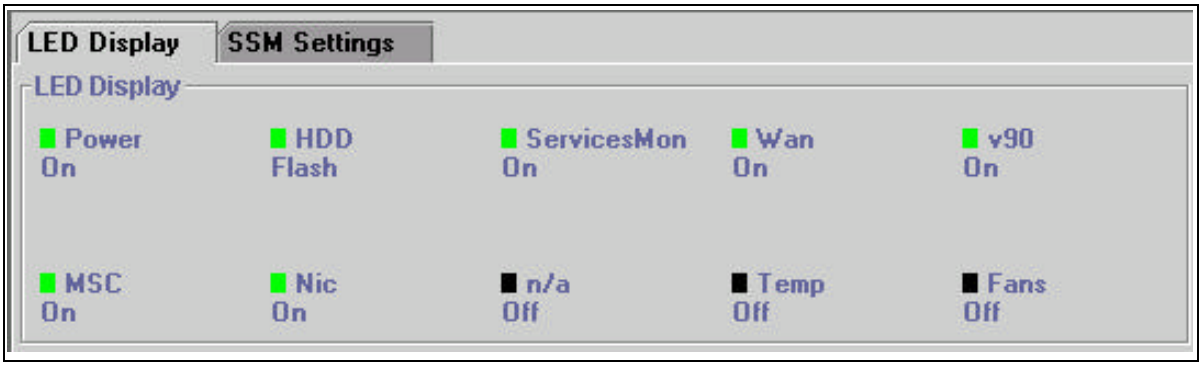
Using Unified Manager to monitor system hardware

With the System Status Monitor you can remotely view the status of the BCM LEDs on your PC. Monitor the LEDs through the Unified Manager to help you make preliminary decisions about maintenance actions.

To enter the System Status Monitor frm Unified Manager

1 On the Unified Manager navigation tree, click the **Diagnostics** key and click the **System Status Monitor** heading.
For systems using BCM400 or BCM200 hardware, the LED Display screen appears similar to the one shown in the below. The labels change, depending on which network cards are active loaded.

Figure 73 System Status Monitor LED Display screen for BCM400/BCM200 hardware



2 Use this table to interpret the LEDs shown on the system status monitor display.

Table 44 System Status Monitor LED descriptions

LED	Description
Power)	This indicator is green when all power components on your system are operating correcting. If one or more components fails, the LED turns red.
HDD	Indicates that the Primary hard disk is operating correctly.
Watchdog	This LED indicates the state of system status. The LED blinks when the system is functioning correctly.
WAN	Indicates the state of the WAN card functionality. The LED blinks when the card is functioning correctly.
MSC	Indicates the state of the MSC board functionality. The LED blinks when the board is functioning correctly.
v90	Indicates the state of the v90 modem board functionality. The LED blinks when the board is functioning correctly.
Nic (LAN)	Indicates the state of the LAN card functionality. The LED blinks when the card is functioning correctly.
Nic (LAN)	Indicates the state of the LAN card functionality. The LED blinks when the card is functioning correctly.
Temperature	The LED is green when the temperature in your system is within the accepted limits. If this changes, the LED turns red.
Fan	The LED is green when the fan, or fans, in your system are operating correctly. If one or more fans fail, or malfunction, the LED turns red.

3 To set the parameters for the System Status Sanity check, click the **LED Settings** tab.
The LED Settings record appears.

Figure 74 System Status Monitor LED (SSM) Settings record screen

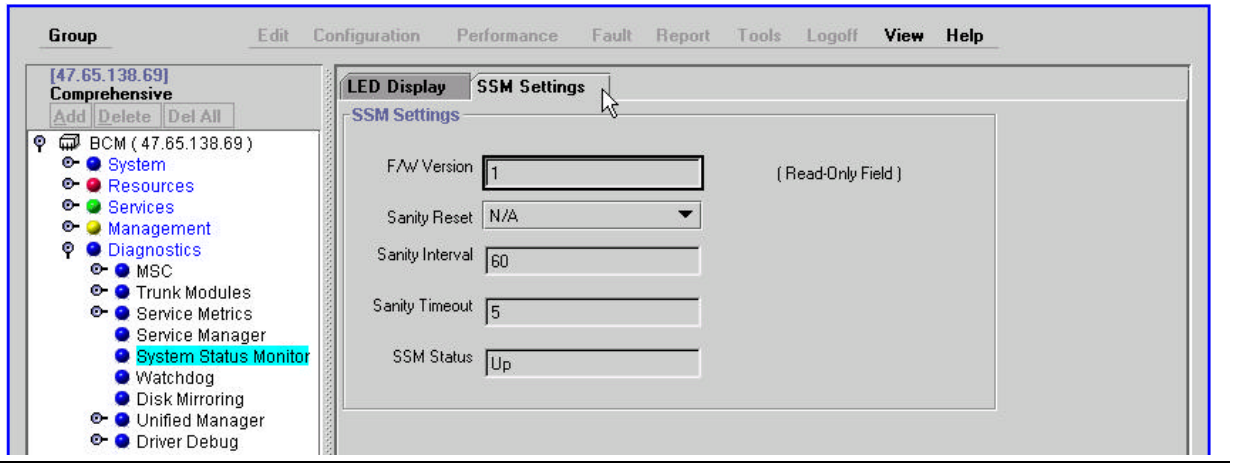


Table 45 LED Display screen settings

Attribute	Values	Description
F/W Version	Read only.	The current version of the LED monitoring application.
Sanity Reset	Enable Disable	Determine whether the system resets if communication between the System Status Monitor and the System Status Monitor Service is lost.
Sanity Interval	60-255 Default: 240	The time in seconds between sanity checks, before a timeout occurs.
Sanity Timeout	0-254 Default: 10	The number of timeouts before the system status monitor sends a reset signal to the computing platform.
SSM status	Read only	This field indicates the current status of the System Services Monitor itself. This field must be set to **Up** to show the current status of the equipment.

Note: If your Power or Fan LEDs are red:

If you have a BCM400 or BCM200 that does not have redundant power supplies or fans, you may notice that the Power and Fan LEDs are red even though the power module and fan appear to be working. Check to see if the jumper was installed across pins 2 & 3 on the PSU Status header, which is located on the interface card near the power supply connector. For Redundant systems this header is populated with a cable from the power supply. See the *Installation and Maintenance Guide* for details.

Using the system status display to monitor system hardware

A line of 10 LEDs display on the face of the Business Communications Manager (see Figure75). The LEDs show the current state of various hardware components. The Unified Manager contains a monitoring tool that helps you etermine the current condition of the LEDs from your computer. See the *Business Communications Manager Installation Guide* for more information.

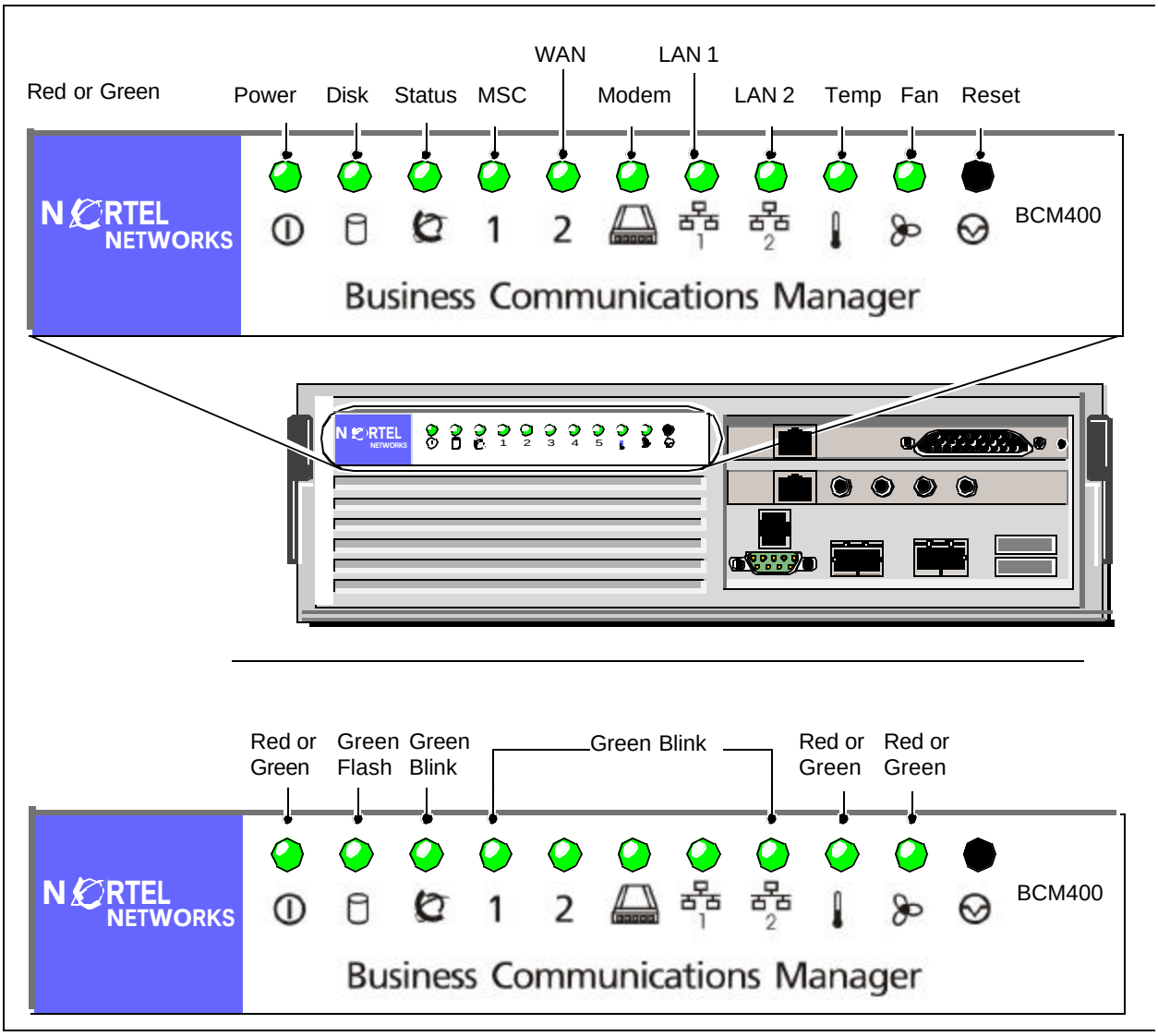
What system status LEDs indicate

- Power status (LED 1): Indicates the status of all power components. Green indicates normal status. Red indicates an excessive voltage deficiency or a component failure (such as a redundant power supply fan or module). An LED that monitors a component will also show a fault in combination with the Power LED.
- Hard disk activity (LED 2): Green indicates hard disk access.
- System status (LED 3): Solid green indicates the system is normal and operational. Green blink indicates one or more telephony services are not operational.[1]
- PCI device monitoring (LED 4-8): These LEDs monitor the peripheral components (2 x NICs, 1 x WAN, 1 x Modem, 1 x MSC). A steady green LED indicates the device is detected and operationally normal. A flashing green LED indicates that software detects the hardware, but there is no device driver. No color indicates the device is defective or missing.
  - LED 4: Monitors the MSC
  - LED 5: Monitors the WAN (if installed)
  - LED 6: Monitors the modem (if installed)
  - LED 7: Monitors the NIC 1 (LAN1)
  - LED 8: Monitors the NIC 2 (LAN2)
- Chassis/CPU temperature (LED 9): Green indicates a normal, operational temperature range for the chassis. Red indicates either a sensor is not operational or the chassis temperature is out of range.
- Fan activity (LED 10): Green indicates that all fans are operational. Red indicates that one (or more) fan is not operating correctly.
- Reset button: The reset button when depressed, restarts the system. The reset button is recessed to prevent an accidental reboot.

Note: The system status LEDs correspond to the devices, not to the PCI slots.

[1] Six, non-blinking LEDs in the center indicates monitoring software is not active.

Figure 75 Business communication manager base function tray system status display LEDs



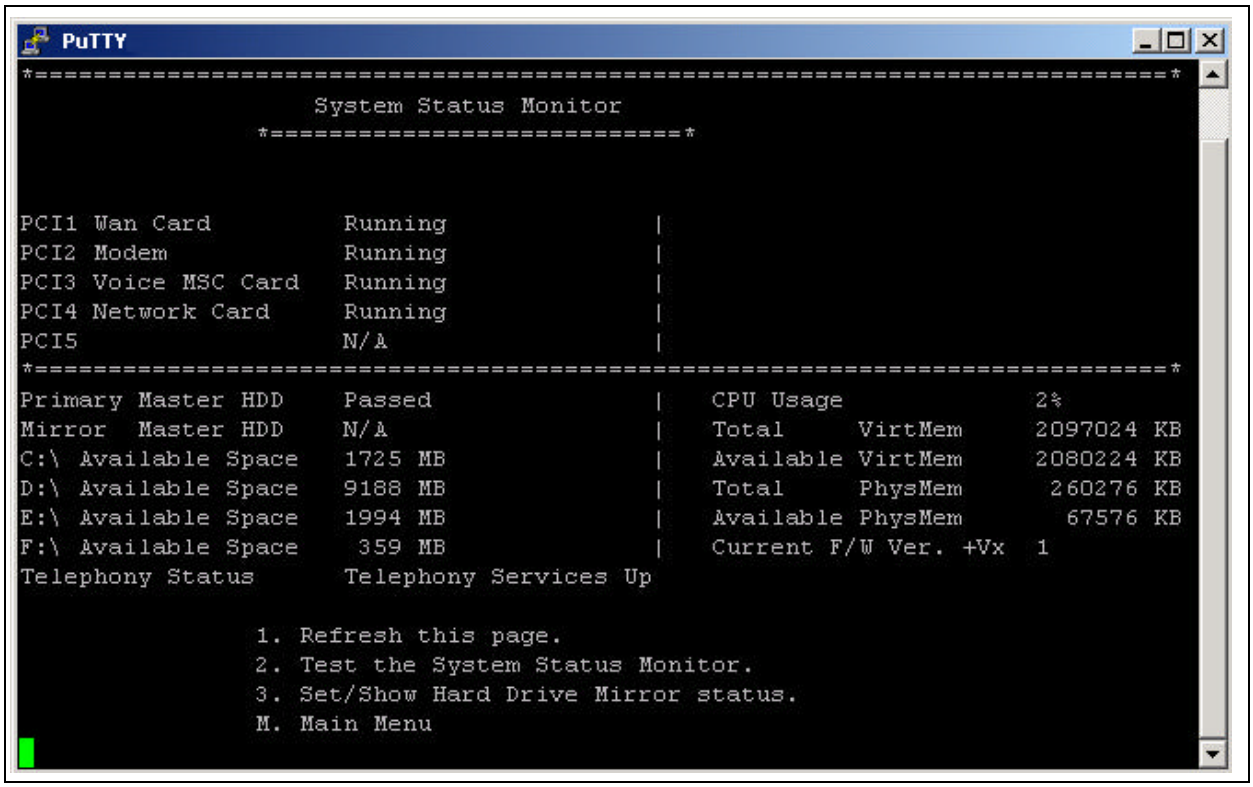
Using the Initialization menu to monitor system hardware

If you require a more detailed reading of what the SSM LEDs are reading, you can access another type of system status monitor by using PuTTY to access the Business Communications Manager Initialization menu.

1. Install the PuTTY as described in "Installing PuTTY" on page 429.
2. Access PuTTY as described in "Using PuTTY" on page 430.
3. When prompted, enter the user name (default: **`ee_admin`**).
4. When prompted, enter the password (default: **`PlsChgMe!`**).

5 When the Initialization screen appears, enter 6 on your keyboard.
The System Status Monitor screen appears.

Figure 76 PuTTY system status monitor screen



6 Type **M** and press **Enter** to return to the main menu.

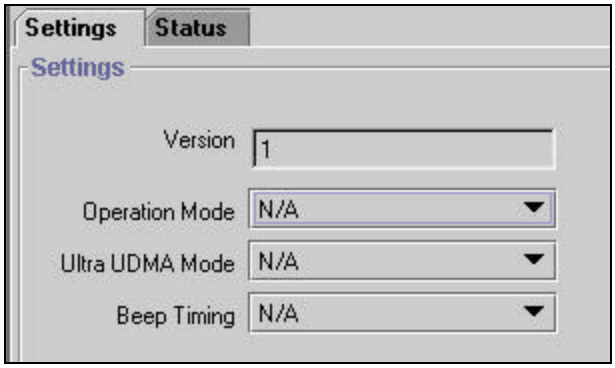
7 Type **X** and press **Enter** to exit PuTTY.

Disk mirroring function

If your system has a redundant hard disk RAID system installed, you may need to monitor the performance of either drive. Use the Disk Mirroring screens to view the current status of the drives as well as to reset modes, if required.

1 Click the **Diagnostics** key and click the **Disk Mirroring** heading.
The Disk Mirroring Settings screen appears.

Figure 77 Disk Mirroring Settings screen



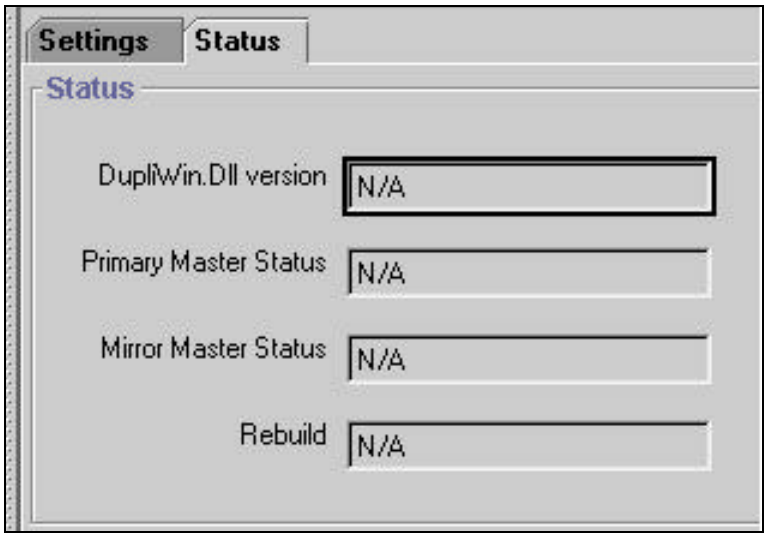
2 On this screen, you can change three of the settings. Version is a read-only field.

Table 46 LED Display screen settings

Attribute	Values	Description
Operation Mode	Primary Master, Mirror Master, Mirror Mode, N/A	
Ultra UDMA Mode	Disable, 0_16, 1_24, 2_33, 3_48, 4_66, Auto, N/A	
Beep Timing	Disable, Continuous, 5 seconds, 10 seconds, 15 seconds, 20 seconds, 30 seconds, 1 minute, 2 minutes,	Choose how long the beep will sound. To test the sound, choose one of the settings under the Tools menu.
Warning: Ensure you understand the implications of the changes before you change these settings on your system. Only the system administrator should have access to this screen.		

3 Click the **Status** tab to view the status of the disk mirror system. All the fields on this screen are read-only.

Figure 78 Disk Mirror Status screen



Emergency telephone does not function

If the emergency telephone is connected to the system

1. Check the power LED on the ASM 8 to check that the ASM 8 is receiving power.
2. Check that the emergency telephone has dial tone.
3. Check the external line and emergency telephone connections.
4. To avoid damage to the emergency telephone, connect the telephone directly to the external line and check for dial tone.
5. Replace the MSC.

If the emergency telephone is connected to the CTM

1. Check that the system has a CTM installed.
2. Check that there is no dial tone at the emergency telephone.
3. Replace the CTM.

ATA 2 does not function

If the Business Communications Manager ATA 2 does not function, follow these steps to troubleshoot the problem.

1. Make sure there is ac power connected to the ATA 2.
2. Make sure the ATA 2 is in the Tones OFF mode (for data applications only.)
3. Correctly configure the ATA 2 telephone port for data communication.
4. Allow sufficient start up time.
5. Assign the prime line.
6. Assign a ringing line if required, for example, auto-answer modems, FAX).

Checking the wiring

Check these connections:

- ATA 2 to terminal.
  The resistance must be 200 ohms or less for data applications and 1,300 ohms or less for voice applications.
- Business Communications Manager hardware to ATA 2.
  The wiring must be equivalent to 800 m of 0.5 mm wire (2,600 ft. of 24 AWG) or less. Do not use bridge taps and loading coils between the Business Communications Manager hardware and the ATA 2.
- External line to Business Communications Manager.
  Ensure the external line is correctly connected to the BCM1000 and make sure there is dial tone.

Checking for dial tone at the ATA 2

Check to ensure there is dial tone from the set and from the ATA 2.

1. If there is no dial tone, replace a single-line telephone for the data communication device.
2. If there is no dial tone at the ATA 2:
   a. Disconnect the line side of ATA 2. Connect a Business Communications Manager telephone to the ATA 2 port.
   b. Check that the connection from the ATA 2 to the Business Communications Manager hardware is functioning correctly (that is, that the telephone has dial tone).

Checking for trunk line dial tone to the ATA 2

1. Disconnect ATA 2 external line from the Business Communications Manager hardware and connect the data device directly to this external line.
2. Make a call.
3. If the problem continues, the device or the external line is possibly at fault.
4. Plug the device into a different line.
5. If the problem continues, the device is possibly at fault.

For more information about ATA 2, contact your customer service representative.

Unified Manager Diagnostics

The Unified Manager selection contains operations intended only for use by Nortel Networks technical support personnel.

Recording

The Recording selection contains operations intended only for use by Nortel Networks technical support personnel.

Playback

The Playback selection contains operations intended only for use by Nortel Networks technical support personnel.

Driver Debug diagnostics

The Driver Debug selection contains operations intended only for use by Nortel Networks technical support personnel.

WANExam

The WANExam selection contains operations intended only for use by Nortel Networks technical support personnel.

ISDN Monitor

The ISDN Monitor selection contains operations intended only for use by Nortel Networks technical support personnel.

QoS Debug

The QoS Debug selection contains operations intended only for use by Nortel Networks technical support personnel.

SDL Debugging

The SDL Debugging selection contains operations intended only for use by Nortel Networks technical support personnel.

WAN1

The WAN1 selection contains operations intended only for use by Nortel Networks technical support personnel.

WAN2

The WAN2 selection contains operations intended only for use by Nortel Networks technical support personnel.

Appendix A
Management Information Base (MIB) System

MIB is a virtual information store containing 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.

MIB topics

SNMP MIBs

MIB gives you access to the managed objects of a system through a virtual information store called the Management Information Base, or MIB. BCM supports a number of MIBs.

To access MIB files

1. On the Unified Manager navigation tree, click the **Services** key and the SNMP heading.
   The SNMP Summary screen appears.
2. On the **Tools** menu click **MIB download**.
   The MIB Files Download window appears. From here you can select which of the MIB files to download.

To access zipped MIB files from the Nortel Networks Customer Service site

1. Go to www.nortelnetworks.com. The direct link is http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp).
2. Click the **Business Series** link.
   The Products page appears.
3. Under the **Business Communications Manager (BCM)** heading click the **Software** link.

4 On the Business Communications Manager (BCM) screen, enter MIB in the by Title/Number Keyword and press the **Enter** key.

MIB Browsers allow the MIB information to be loaded so that the MIB structure can be browsed. An example of a utility is Microsoft MOM.

Third-Party Fault Management Systems

The BCM Small Site and BCM Small Site Event MIBs can be integrated into standards-based SNMP management frameworks in order to receive BCM alarms via SNMP.

MIB File Descriptions

The BCM MIBs are organized into three sections:

- Standard MIBs: includes SNMP Framework MIB (RFC2261) and INET-ADDRESS MIB (RFC2851)
- Nortel MIBS: includes BCM Small Site MIB and BCM Small Site Events MIB. The Events MIB defines the events (traps) which are usable by any SmallSite product or component.
- Microsoft MIBs: includes OSPF and RIP2 MIBs

Refer to Table 1, Table 2, and Table 3 for file names and files descriptions of each of the MIBs.

Table 1 Standard MIBs files descriptions

MIB	File name	Comments
RFC1354-MIB	Rfc1354.mib	This MIB defines the ipForwardTable. This standard MIB displays the IP routing table.
SNPM-FRAMEWORK-MIB	Rfc2261.mib	This is the SNMP Management Architecture MIB. This standard MIB displays parameters related to the SNMP Agent on the BCM.
INET-ADDRESS-MIB	Rfc2851.mib	This MIB defines textual conventions for representing Internet addresses. An internet address can be an IPv4 address, and IPv6 address, or a DNS domain name. This MIB defines IP addresses on the BCM in various formats.

Table 2 Nortel MIBs files descriptions

MIB	File name	Comments
Small Site MIB	Smallsite.mib	This MIB defines the upper-level hierarchy of an enterprise(1).nortel(562) sub-branch called smallsite. This Nortel Networks MIBN is the basis for several Nortel Networks smallsite products. In the BCM, this MIB is a prerequisite for the Small Sites Events MIB.

Table 2 Nortel MIBs files descriptions

MIB	File name	Comments
Small Site Events MIB	Smallsiteevents.mib	This MIB defines the events (traps) that can be used by the Small Site product or component. This MIB describes the events generated by the BCM. This MIB contains fields such as eventId, eventSource, eventTime, and EventDescr.
SYNOPTICS-ROOT-MIB	Synro**xxx**.mib	This MIB is the SynOptics root MIB. The policy object identifier is added for policy MIBs. This MIB is the root policy MIB in the BCM and is required by the PolicyFrameWorkPlb, QosPolicyIPPlb, and CopClient MIBs. (For OPS support.)
POLICY-FRAMEWORK-PIB	PibFramework.mib	This MIB is a policy information base (PIB) module that contains the base set of policy rule classes that are required to support all policies. This MIB falls under the Synoptics branch. (For OPS support.)
QOS-POLICY-IP-PIB	Piblp.mib	This PIB module contains an initial set of policy rule classes that describe the quality of service policies. This MIB includes the general classes that can be extended by other PIB specification and an initial set of PIC classes related to IP processing. This MIB falls under the Synoptics branch. (For OPS support.)
COPS-CLIENT-MIB	Copsclientmib.mib	The COPS Client MIB module is found under the Synoptics branch. For OPS support.

Table 3 Microsoft MIBs files descriptions

MIB	File name	Comments
OSPF MIBS	Wfospf.mib	This MIB defines the open shortest path first (OSPF) MIBs from Wellfleet. This Microsoft MIB is adopted and released as part of the Microsoft MIBs under the Wellfleet branch. This MIB defines the OSPF parameters that are needed by the network administrator. See “OSPF MIBs for a list of the parameters.
RIP2 MIBS	Msiprip2.mib	This MIB defines the RIP2 MIBs. This MIB defines RIP2 parameters that are required by the network administrator. See “RIP v2 MIBs for a list of the parameters.
Bootp MIBS	Msipbtp.mib	This MIB defines the BootP MIBs under the Microsoft branch. This MIB defines BOOTP parameters that are required by the network administrator. See “Bootp MIBs for a list of the parameters.
MS NT Performance MIBS	PERFMIB.mib	This MIB defines the Performance counter for Windows NT 4.0. Use this MIB to monitor some BCM performance statistics, including Memory, Processor, Network Interface, Physical Disk, Logical Disk, Paging FIle, Process, TCP, IP, and UDP. See “MS Windows NT Performance MIBs for a list of the parameters.

MIB File Compilation and Installation

Each MIB browser has its own MIB compilation tool. Complete the procedure and follow the order of the files in the following list.The Small Site MIBs have definitions for the binding values of the BCM SNMP traps. The Policy MIBs branch out from Synoptic and you must install synro123.mib before you can compile and install policy MIBs.

For Small Site MIBs:

- SmallSite.mib
- SmallSiteEvents.mib

For other MIBs:

- rfc1354.mib
- rfc2261.mib
- rfc2851.mib
- Synrol123.mib
- PibFramework.mib
- PibIp.mib
- Copsclientmib.mib
- Wfospf.mib
- Msiprip2.mib
- Msipbtp.mib
- PERFMIB.mib

Possible problems during compilation and installation

- BCM files are created and released in a MicroSoft Windows environment so that when these files are copied or 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”.
- If you have already installed the SYNOPTICS-ROOT-MIB for other MIBs, you must add the “policy OBJECT IDENTIFIER::={ synoptics 4}” in the synroxxx.mib. Recompile and reload the MIB for policy MIBs.

Small Site Event MIBs

The trap format is specified in the BCM Small Site Event MIB. BCM traps can be captured and viewed through any standard SNMP fault monitoring framework or trap watcher.

See “SNMP Trap Agent” on page 176 for information on how to enable SNMP traps.

BCM-specific SNMP trap fields for Small Site Event MIBs

- Enterprise: OID identifies the product (iso.org.dod.internet.private.enterprises.nortel.smallsite.common.events [1.3.6.1.4.1.562.37.3.1])
- Agent address: IP address of one of the BCM interfaces
- Generic trap type: 6, for Enterprise-specific traps
- Specific trap type:

  1 = eventInfo trap type

  2 = eventWarning trap type

  3 = eventError trap type
- Time stamp: system up time

BCM-specific SNMP variable bindings

- Binding #1 contains the corresponding Event ID (alarm)/eventID (trap)
- Binding #2 contains the Component ID (alarm)/eventSource (trap)
- Binding #3 contains the event Date and Time
- Binding #4 contains the Problem Description (alarm)/eventDescr (trap)

OSPF MIBs

An open shortest path first (OSPF) MIB is published in RFC1248. The MIBs defined in the BCM are from Microsoft, under the Wellfleet branch. The OSPF MIB is a subset of MIBs in RFC1248.

The MIB consists of nine parameters: a general variables group and eight tables.

Group	description
wfOspfGeneralGroup	General global variables
wfOspfAreaTable	Area descriptions
wfOspfLsdbTable	Link state database
wfOspfAreaRangeTable	Address range specifications
wfOspfIfTable	OSPF interface variables
wfOspfVirtIfTable	Virtual links
wfOspfNbrTable	(Non-virtual) OSPF neighbors
wfOspfVirtNbrTable	Virtual OSPF neighbors
wfOspfDynNbrTable	OSPF dynamic neighbor table

Section D.2 of the OSPF V2 specification (RFC 1247) lists a set of required statistics that implementation must maintain. These statistics are included in the OSPF MIB. The 13 counters and gauges of the MIB enable the evaluation of the performance of the OSPF protocol in an operational environment. Most of the remainder of the MIB variables parameterize the many features that OSPF provides the network administrator.

RIP v2 MIBs

This MIB defines the management information for the Routing Information Protocol Version 2 (RIP v2) MIB.

Global group	global information and statistics for the RIP. Information in this group is independent of the interfaces over which the protocol is enabled
Interface group	RIP configuration information and statistics specific to each interface
Peer group	statistics pertaining to RIP peers

Bootp MIBs

This MIB defines the management information for the BOOTP Protocol.

Global group	global information and statistics for the RIP. Information in this group is independent of the interfaces over which the protocol is enabled
Interface group	RIP configuration information and statistics specific to each interface

MS Windows NT Performance MIBs

The MS Windows NT Performance MIB defines these MIB groups.

Memory	Available Bytes, Committed Bytes, and Page Reads Per Sec group objects
Processor	cpuprocessTable and the Processor TIme (%), User Time, and Interrupts Per Sec group objects
Network interface	network-interfaceTable and the Current Bandwidth, Bytes Received Per Sec, and Packets Received Errors groups objects
Physical disk	pdiskphysicalDiskTable and the Current Disk Queue Length, Avg. Disk Queue Length, ad Disk Sec Per Write group objects
Logical disk	ldisklogicalDiskTable and the Free Space (%), Free Megabytes, and Current Disk Queue Length group objects
pagingFile	pagefilepagingFileTable and the Instance Name, Usage (%), and Usage Peak (%) group objects
Process	processprocessTable and the Processor Time (%), User Time (%), and Virtual Bytes group objects

iCP	onnections Established and Connections Active group objects
iP	Datagrams Per Sec, Datagrams Received Per Sec, and Datagrams Received Discarded group objects
uDP	Datagrams Per Sec and Datagrams Received Per Sec group objects

For more information on MS Windows NT Performance MIB group names and their related group objects, see "MS Windows NT Performance MIBs" on page 373.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W