

AT&T VOIP
Nortel BCM 200/400 (Release 4.0.2.03a)
Configuration Guide
For Use with AT&T
IP Flexible Reach Service

Issue 1.2
3/02/2007



BCM400



BCM200

TABLE OF CONTENTS

1	Introduction.....	4
1.1	Document Change History.....	4
2	Special Notes	5
3	Overview.....	6
4	Configuration Guide	8
4.1	Nortel BCM Version and Feature Requirements.....	8
4.2	VOIP Gateway Trunks.....	10
4.3	H.323 Gateway Parameters.....	15
4.4	Media Parameters.....	16
4.5	Port Ranges	17
4.6	Configuring Outgoing Calls from BCM to AT&T IP Flex Reach	18
4.7	Configuring Incoming Calls from AT&T IP Flex Reach to BCM	19
4.8	Configuring IP Phone LCD Screen to Display DID Number.....	20
5	Troubleshooting.....	21
5.1	System Monitoring with BCM Monitor	21
5.2	Real-time BCM System Status LED Displays.....	24
5.3	Real-time BCM Fault/Alarms Management.....	25
5.4	BCM Service Management System.....	26
5.5	BCM Log Management	28

TABLE OF FIGURES

Figure 1: AT&T IP Flexible Reach Network	6
Figure 2: BCM 200/400 software version	8
Figure 3: Software Management Menu	9
Figure 4: Patch List.....	9
Figure 5: Available VOIP Gateway Trunks.....	11
Figure 6: Assigning DN numbers to Line Pool	12
Figure 7: Defining Route for VOIP Trunks.....	13
Figure 8: Assign Destination Code to Route Numbers.....	14
Figure 9: H.323 Gateway Parameters	15
Figure 10: Media Parameters	16
Figure 11: Media Gateway Port Range.....	17
Figure 12: Configuring DID for Outgoing Calls	18
Figure 13: Configuring DID for Incoming Calls	19
Figure 14: Displaying DID Number on IP Set LCD.....	20
Figure 15: System Monitoring Example.....	21
Figure 16: IP Device Listing.....	22
Figure 17: RTP Session Information	22
Figure 18: Line Monitor Information	23
Figure 19: System Resources.....	23
Figure 20: Front Panel LED Display	24
Figure 21: Real-time BCM 200/400 Alarm Display.....	25
Figure 22: BCM Service Manager Screen.....	26
Figure 23: Log Management Screen.....	29

1 Introduction

This document provides a configuration guide to assist Nortel Networks BCM administrators in connecting to AT&T IP Flexible Reach service.

1.1 Document Change History

Issue 1.0	01-03-2007; first general release
Issue 1.1	02-05-2007; 1) modified section 4.2 for clarity of IP trunks and line pool configuration. 2) Added CCG disclaimer statement at end of document. 3) Modified cover page.

2 Special Notes

Emergency 911/E911 Services Limitations

While AT&T IP Flexible Reach services support E911/911 calling capabilities in certain circumstances, there are significant limitations on how these capabilities are delivered. Please review the AT&T IP Flexible Reach Service Guide in detail to understand these limitations and restrictions.

Failover to an Alternate AT&T Border Element Not Supported

BCM does not support failover to an alternate AT&T Border Element. BCM must be configured to send to one specific border element.

Unattended Call Transfers are not supported

An unattended transfer is one in which the recipient of the transfer has not answered the phone prior to the transfer. This type of transfer is not supported with BCM and the AT&T Network. For example, if a call with the AT&T network is transferred by BCM phone 1 to BCM phone 2, phone 2 must answer prior to the completion of the transfer by phone 1.

Fax Limitations

- T.38 fax is not currently supported with the IP Flexible Reach service
- IP Flexible Reach service supports fax using G.711; however, this is not supported by the BCM 200/400 today when configured to use G.729 as the first preferred codec. There is an issue where the BCM does not automatically detect fax/modem tones and switching the call to G.711.
- To work-around this limitation; the BCM supports fax by using analog/POTS lines to the PSTN. BCM-GATM-8 or BCM-GATM-4 media bay modules are required to interface with analog/POTS lines.

3 Overview

This section provides a service overview of the Nortel Business Communication Manager 200/400 (BCM 200/400) IP PBX integration with AT&T IP Flexible Reach service. For an overview of Nortel BCM 50 for IP Flexible Reach; please reference a separate document named “Nortel BCM 50 Configuration Guide.”

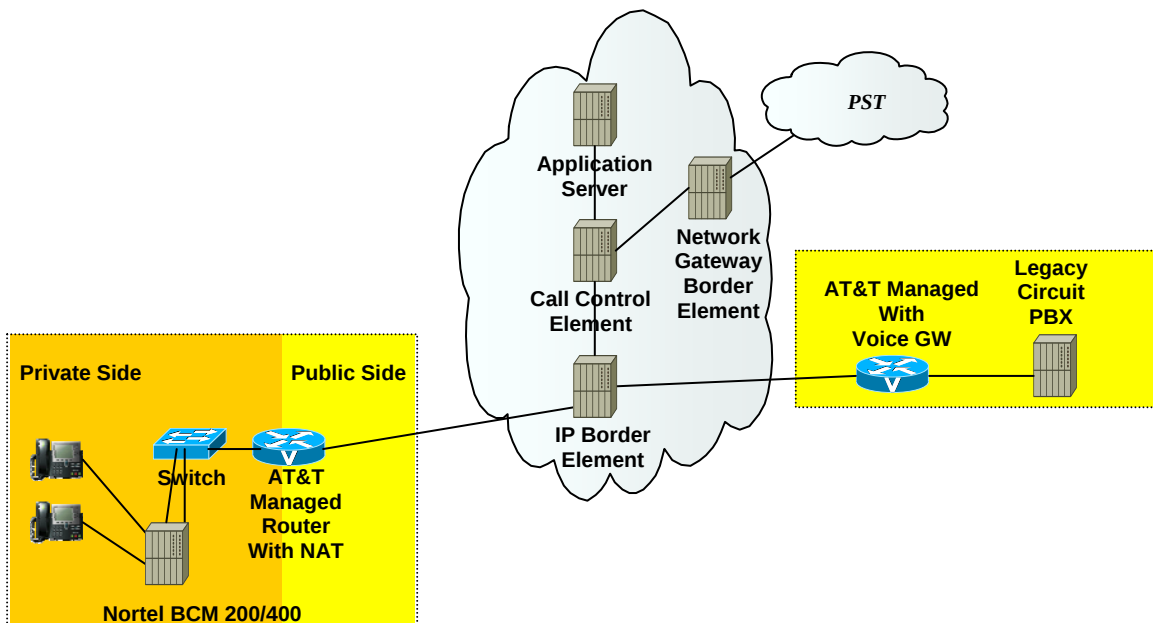


Figure 1: AT&T IP Flexible Reach Network

The Nortel BCM customer premises site shall consist of the following components.

- Nortel IP 2004 or IP 2002 phones – These phones use the Nortel proprietary UNISTim signaling protocol to communicate to the Nortel BCM 200/400 IP PBX for call feature and routing support. These phones can be connected to a Nortel Ethernet switch (ES 470, ERS 5520, etc.) that supplies in-line power (IEEE 802.3af) to the phones.

- Nortel BCM 200/400 IP PBX – This unit consists of the following.
 - o Media Service Card (MCS) Processor
 - o Two ports Ethernet / IP card
 - o Integrated CallPilot voice mail system
 - o Analog station ports for connection to fax machines.
 - o Digital station ports for Norstar digital phones
 - o T1 voice card for connection to the local PSTN.
 - o GATM-8 analog trunk to PSTN for inbound/outbound fax

The following routing scenarios are supported by the Nortel BCM IP PBX and **DO NOT** use the AT&T Call Control.

- Local Nortel BCM phone to local Nortel BCM phone
- Local fax machine to other fax machine via PSTN

The following routing scenarios are supported by the BCM IP PBX and **DO** use the AT&T Call Control. For voice calls, the G.729 codec shall be used.

- Nortel BCM phones to PSTN (domestic US and international).
- Nortel BCM phones to legacy PBX site with Cisco gateway.
- Legacy PBX site with Cisco gateway to Nortel BCM phones.
- Nortel BCM phones at one Nortel BCM IP PBX site to Nortel BCM phones at another Nortel BCM IP PBX site.

If the customer has subscribed to Calling Plans B and C (Local), then the following routing scenarios are supported by the BCM IP PBX and **DO** use the AT&T Call Control. For voice calls, the G.729 or G.711 codec may be used. BCM selects G.729 as the highest priority codec.

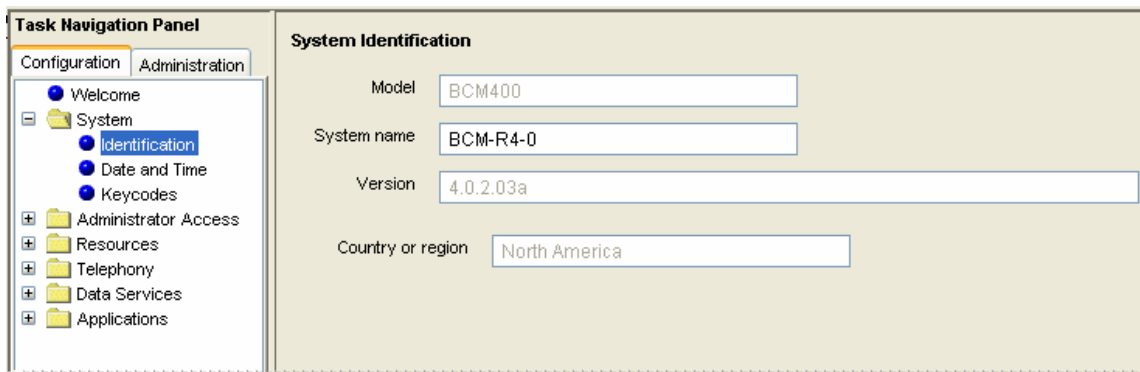
- Inbound PSTN to BCM phone
- Outbound local PSTN calls from the BCM phones.
- Outbound local N11 (i.e. 411, 911) calls from the BCM phones.

4 Configuration Guide

This configuration guide specifies the Nortel BCM 200/400 screens that must be configured and updated to support the AT&T IP Flexible Reach service.

4.1 Nortel BCM Version and Feature Requirements

The Nortel Networks BCM must be running release 4.0.2.03a. You can check the version of BCM by viewing the following screen.



The screenshot shows the 'System Identification' page in the Nortel BCM configuration interface. On the left is a 'Task Navigation Panel' with a tree view containing 'Welcome', 'System' (expanded), 'Identification' (selected), 'Date and Time', 'Keycodes', 'Administrator Access', 'Resources', 'Telephony', 'Data Services', and 'Applications'. The main content area has a title 'System Identification' and four input fields: 'Model' with the value 'BCM400', 'System name' with 'BCM-R4-0', 'Version' with '4.0.2.03a', and 'Country or region' with 'North America'.

Figure 2: BCM 200/400 software version

Ensure that the System Identification page specifies **Version 4.0.2.03a**. This is the supported release that is required for AT&T IP Flexible Reach service.

The following BCM 4.0 patches must be applied. To verify installed/applied patches; from the BCM Element Manager's main menu, select "**Administration**" then: ***Software Management→ Software Update History***

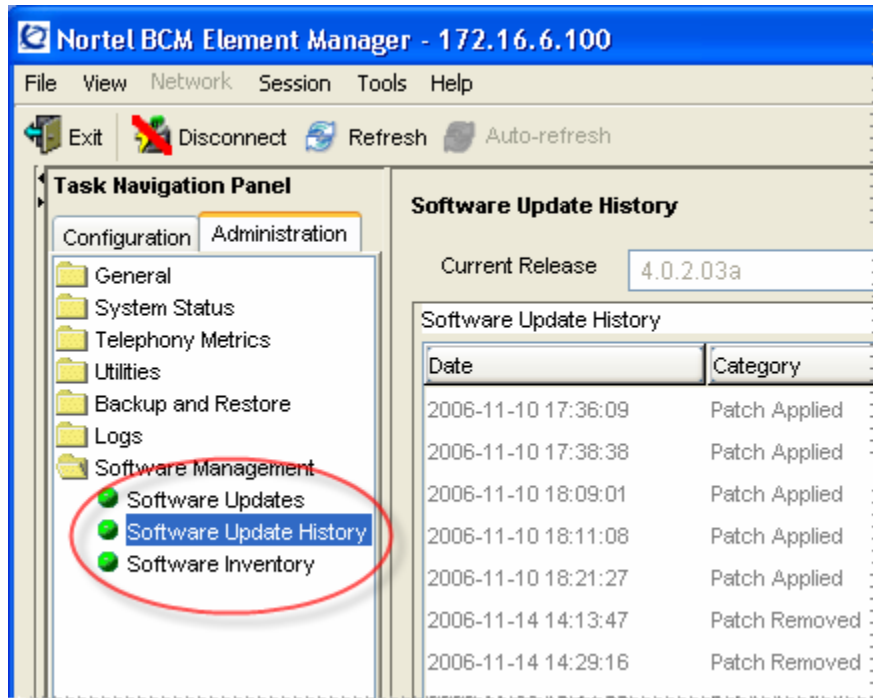


Figure 3: Software Management Menu

Patch Name	Version	Description
BCM.R400.027-IVR	1.0-1.3	IVR Provider Update
BCM040.025-CTE-CTI	1.0-1.0	LAN CTE Client Update
BCM.R400.034-IPTEL	1.1-1.0	IPTEL Provider Agent and FEPS Update
BCM.R400.035-CTI	1.1-1.2	CTI Update
BCM.R400.036-ElementManager	1.1-1.0	Element Manager Update
BCM.R400.032-PSM	1.0-1.0	PSM Update

Figure 4: Patch List

4.2 VOIP Gateway Trunks

Voice over IP (VoIP) lines are signaling channels that simulate how CO lines work. However, VoIP lines transmit data to the IP network over a LAN or IP network rather than over physical lines. Once the VoIP trunks are set up, you can assign them to line pools, and program their behavior in the same way you would PRI lines.

VoIP trunks use line numbers 001 to 060. To view these line records select Configuration --> Telephony --> Lines --> Active VoIP Lines. To access VoIP lines, you need to enter software keycodes. Each keycode supports a specific number of trunks. The H.323 trunks start numbering up from 001. No entries appear in the Enabled VoIP lines field until you complete the IP Trunks Settings field, which displays when you select IP Trunks under Configuration --> Resources --> Telephony Resources --> IP trunks.

VoIP trunks should be configured to use a single line pool per VoIP trunk type. Do not mix other trunk types on the same line pool. The VoIP line pools are assigned to routes, which in turn, are configured with destination codes that route calls to the AT&T IP Flex Reach network.

You can also create a fallback for the trunk. This is a situation where the system reroutes the call to a PSTN line pool if the primary route is not available or the call quality is not suitable. If you do not configure your network for fallback and the call quality is below threshold, the IP call fails.

Check under **Configurations -> Lines -> Active VOIP Lines** to see if Trunks have been allocated (See Figure 5 below). You should have a number of VOIP gateway trunks displayed. The total number of lines indicated corresponds to the number of IP trunks licensed by Nortel for your BCM. In this case we show eight active trunks.

The screenshot displays the Nortel BCM configuration interface. On the left is the 'Task Navigation Panel' with a tree view. Under 'Telephony', 'Lines' is expanded, and 'Active VOIP Lines' is selected. The main area is titled 'Active VOIP Lines' (circled in red) and contains a table with 8 rows of active trunks. Below the table are 'Copy' and 'Paste' buttons. At the bottom, the 'Details for Line: 002' panel is shown with tabs for 'Parameters', 'Preferences', 'Restrictions', and 'Assigned DNS'. The 'Parameters' tab is active, showing 'Name' as 'Line002', 'Line Type' as 'Pool:O' (circled in red), and 'Distinct Ring' as 'None'.

Line	Trunk Type	Control Set	Prime Set
001	VoIP	3000	3000
002	VoIP	3000	3000
003	VoIP	3000	3000
004	VoIP	3000	3000
005	VoIP	3000	3000
006	VoIP	3000	3000
007	VoIP	3000	3000
008	VoIP	3000	3000

Details for Line: 002

Parameters Preferences Restrictions Assigned DNS

Name: Line002

Line Type: Pool:O

Distinct Ring: None

Figure 5: Available VOIP Gateway Trunks

For each IP trunk you must select a Line Pool in the “**Details**” tab at the bottom of the page (See Figure 6 below). Available Pool codes start at A to O. In this case we selected “**Pool O.**” Additionally, the Line Pool needs to be associated with all DN's that require access to the VOIP trunks. Go to **Configurations** → **Telephony** → **Dialing Plan** → **Line Pools** to perform this configuration.

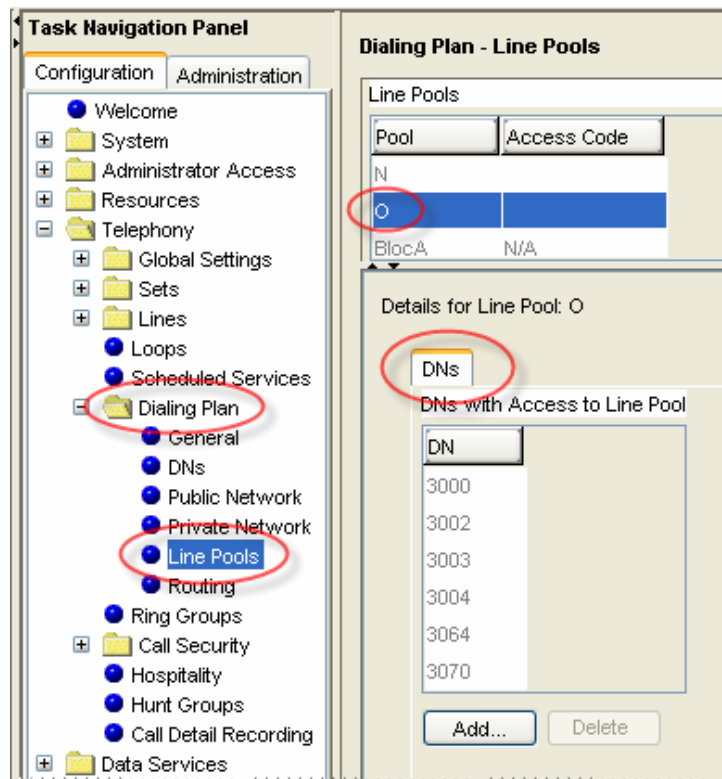


Figure 6: Assigning DN numbers to Line Pool

Under **Configuration → Telephony → Dialing Plan → Routing → Routes** tab we need to define a “Route” for each pool (See Figure 7 below). In our case we defined Route 001. We also need to assign “Pool O” to this particular route and configure the route for “National” numbering dial plan type.

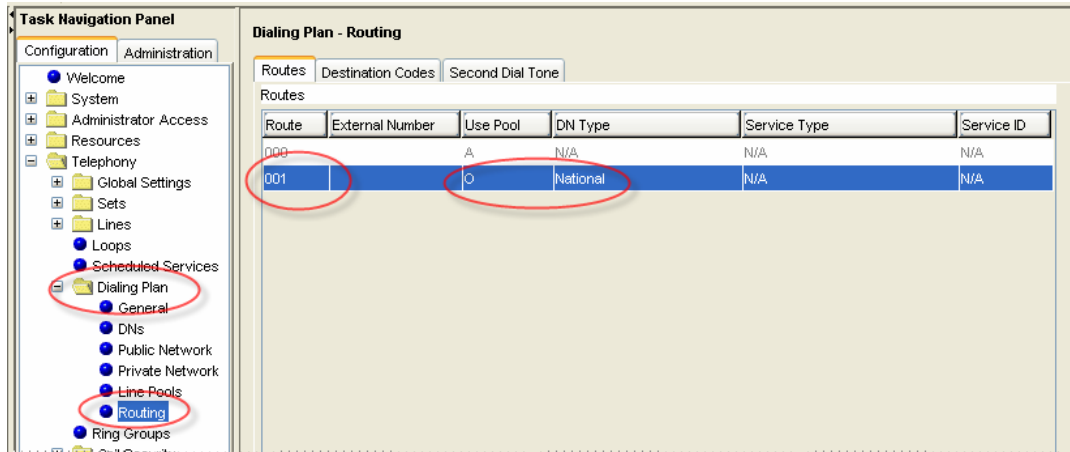


Figure 7: Defining Route for VOIP Trunks

Under **Configuration → Telephony → Dialing Plan → Routing** (See Figure 8 below), under the “Destination Codes” tab we need to associate the Route to the desired access code. Configure this to access code “9” or to whatever code you want to access for outside (IP off-net) call that will be presented to the AT&T service for routing. In this case, when “9” is dialed we wish to push the dialed string to the IP trunk for routing.

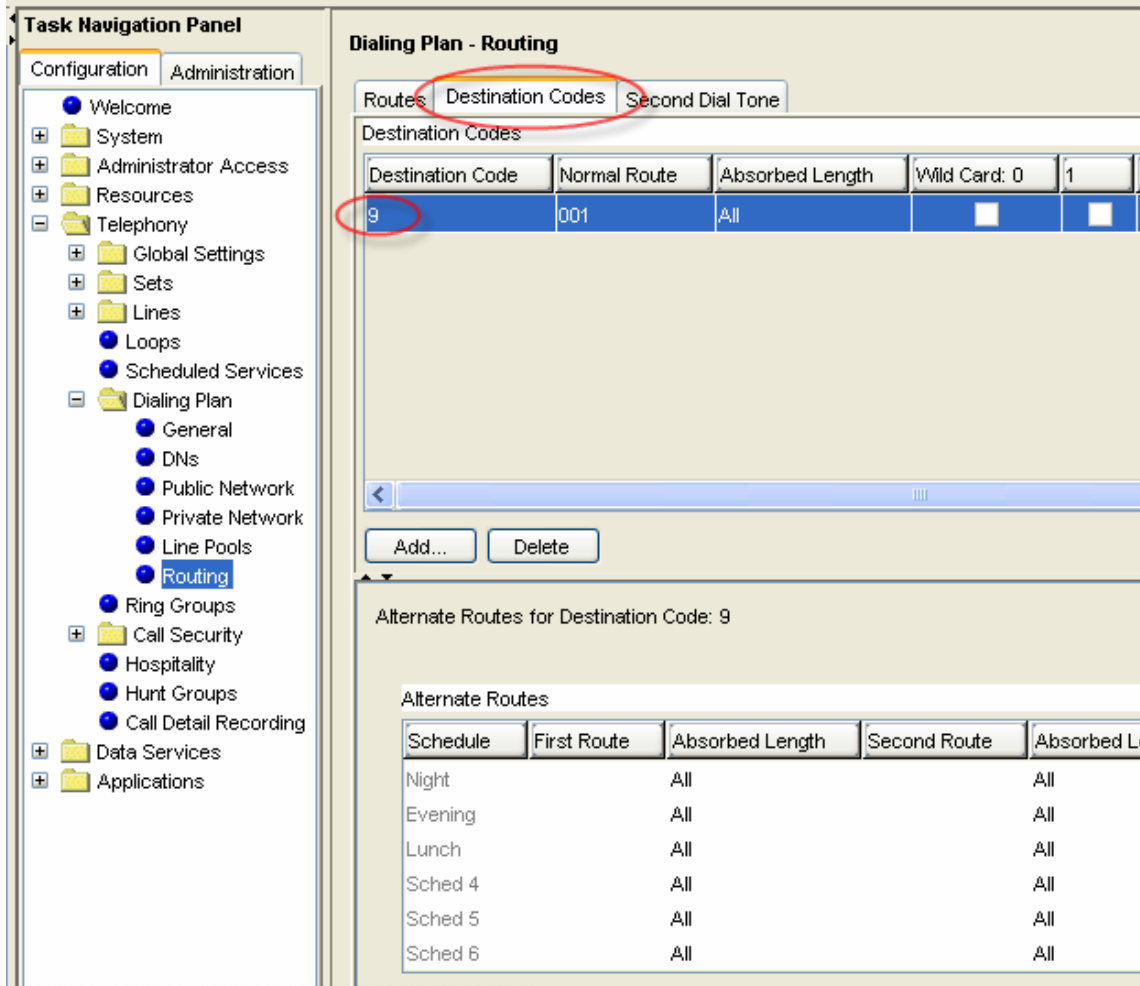


Figure 8: Assign Destination Code to Route Numbers

4.3 H.323 Gateway Parameters

Configuration → Telephony Resources → IP Trunks →

- On this screen we need to populate the **Call Signaling** as **“GatekeeperRoutedNoRAS”**
- **Alias Name:** The AT&T IP Flexible Reach service does not require a H.323 ID name. However, the BCM was tested with a H.323 ID name and Nortel recommends that the customer provides a meaningful name in this field.
- **H.245 tunneling** must be enabled.
- For the **Call Signaling Port** use **1720** as a value.
- Make sure the **Primary Gatekeeper IP** is populated with the correct AT&T IPBE IP address. Sample IP addresses are shown next.
 - Primary Gatekeeper – **(please contact your Customer Care Representative for the AT&T IP border element IP address)**
 - Backup Gatekeeper – 0.0.0.0*

Telephony Resources

Modules

Bus	Prog Type	Actual Type	Dip Sw	State	Devices	Low	High	Total	Busy
0	N/A	IP Trunks	N/A	N/A	Lines	1	60	N/A	N/A
1	N/A	IP & App Sets	N/A	Enabled	Sets	N/A	N/A	11	0
2	Trunk Mod	None	N/A	Unequipped	Lines	N/A	N/A	N/A	0
2.0	PRI	None	xxx111	N/A	Lines	211	233	N/A	0

Disable Enable

Details for Module: 0

Routing Table IP Trunk Settings **H323 Settings** H323 Media Parameters SIP Settings SIP Media Parameters SIP URI Map

Telephony Settings

Fallback to circuit-switched Disabled Gatekeeper digits

Gateway protocol None **Gatekeeper wildcard** ☒

Configuration

Call signaling **Gatekeeper Routed no RAS** Call signaling port 1720

Enable H245 tunneling ☒ RAS port 0

Primary Gatekeeper IP 12.176.183.132 Registration TTL (s) 60

Backup Gatekeeper(s) Gatekeeper TTL (s) 0

Alias names bcm_r4_0 Modify...

Status H323 Gateway is running in Direct mode

Figure 9: H.323 Gateway Parameters

*Note: the backup gatekeeper will not be supported on the current BCM 200/400 release. The Nortel backup implementation is not compatible with the IP Flexible

Reach service today. Nortel will provide support in a future release. In case of failure to the primary gatekeeper; the BCM will not be able to place any outgoing calls to the AT&T IP Flexible Reach service. The backup gatekeeper IP address (Please contact your Customer Care representative) must be manually configured in the “**Primary Gatekeeper IP**” field to restore outgoing calls. Additionally, the AT&T IP Flexible Reach service will send incoming calls to the BCM from multiple IP border elements. The BCM will accept calls from any border elements without additional configuration.

4.4 Media Parameters

Configuration → Resources → Telephony Resources → IP Terminal Global Settings

Within the Media Parameters tab; ensure that all values are exactly as the sample screen shot shown below:

- **1st Preferred Codec:** **G.729**
- **Silence Compression:** **Disabled**
- **Jitter Buffer – Voice:** **Auto**
- **T.38 Fax Support:** **Disabled**
- **G.729 Payload Size:** **20**

The screenshot displays the 'Telephony Resources' configuration window. At the top, a table lists modules. Module 1, 'IP & App Sets', is highlighted with a red circle. Below the table, the 'Details for Module: 1' section is shown. The 'IP Terminal Global Settings' tab is selected and circled in red. This tab contains several configuration options: 'Enable registration' (checked), 'Enable global registration password' (checked), 'Global password' (masked with asterisks), 'Auto-assign DNS' (unchecked), 'Advertisement/Logo' (set to 'BCM-r4'), 'Default codec' (set to 'G.729'), 'Default jitter buffer' (set to 'Auto'), 'G.729 payload size (ms)' (set to '20'), 'G.723 payload size (ms)' (set to '30'), and 'G.711 payload size (ms)' (set to '20').

Bus	Prog Type	Actual Type	Dip Sw	State	Devices	Low	High	Total	Busy
0	N/A	IP Trunks	N/A	N/A	Lines	1	60	N/A	N/A
1	N/A	IP & App Sets	N/A	Enabled	Sets	N/A	N/A	11	0
2	Trunk Mod	None	N/A	Unequipped	Lines	N/A	N/A	N/A	0
2.0	PRI	None	xxx111	N/A	Lines	211	233	N/A	0

Details for Module: 1

IP Terminal Global Settings | IP Terminal Details | Set Port Details

Enable registration ☒ Default codec: G.729

Enable global registration password ☒ Default jitter buffer: Auto

Global password: ***** G.729 payload size (ms): 20

Auto-assign DNS: ☐ G.723 payload size (ms): 30

Advertisement/Logo: BCM-r4 G.711 payload size (ms): 20

Figure 10: Media Parameters

4.5 Port Ranges

Configuration → Resources → Port Ranges →

Use the values shown below. The default ranges are from 28000 to 28511. This range is used for fax, digital phones and analog phones. The media gateway port ranges are configurable.

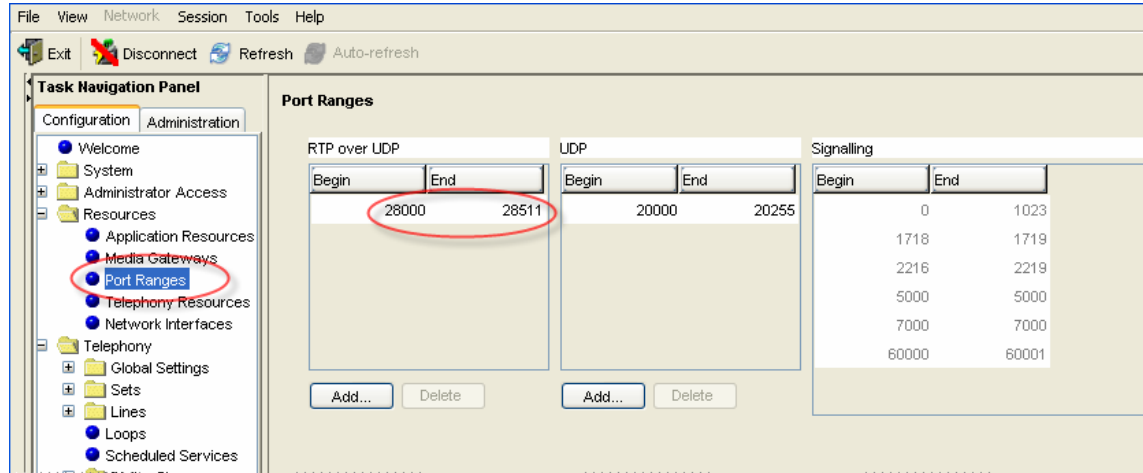


Figure 11: Media Gateway Port Range

The BCM IP phone's RTP and RTCP port range are 51000-51399. Each IP phone call uses two ports. The default port range for RTP and RTCP are not configurable.

4.6 Configuring Outgoing Calls from BCM to AT&T IP Flex Reach

Configuration → Telephony → Active Sets →

First locate the desired private DN number that you want to assign the public DID number under the “**Line Access**” tab. In this case we have selected “**DN 3000**”. At this point, select the “**Properties**” tab under the “Details” window. We will now associate the private DN number with the DID number. In the example below; 3000 is entered in the “**Private OLI**” field and 7323683476 is entered in the “**Public OLI**” field. This example enables “calling number translation” (outgoing) for this particular DN number.

Task Navigation Panel

- Configuration Administration
- Welcome
- System
- Administrator Access
- Resources
- Telephony
 - Global Settings
 - Sets
 - Active Sets
 - Active Application
 - Inactive DNs
 - All DNs
 - Lines
 - Active Physical Lin
 - Active VoIP Lines
 - Target Lines
 - Inactive Lines
 - All Lines
 - Loops
 - Scheduled Services
 - Dialing Plan
 - Ring Groups
 - Call Security
 - Hospitality
 - Hunt Groups
 - Call Detail Recording
 - Data Services
 - Applications

Active Sets

Line Access Capabilities and Preferences Restrictions

DN	Model	Name	Port
3000	1140E/2004/2007/2050	3000	0119
3002	1120E/2002	3002	0118
3003	1140E/2004/2007/2050	3003	0120

Copy Paste

Details for DN: 3000

Properties Line Assignment Line Pool Access Answer DNs

Pub. OLI 7323683476

Priv. OLI 3000

Fwd No Answer 3251

Fwd Delay 4

Fwd Busy

Fwd All

Figure 12: Configuring DID for Outgoing Calls

4.7 Configuring Incoming Calls from AT&T IP Flex Reach to BCM

Configuration → Telephony → Active Sets →

We will now configure the “called number translation” (incoming) for the DN number. First locate the desired private DN number that you want to assign the public DID number under the “**Line Access**” tab. In this case we have selected “**DN 3000**”. At this point, select the “**Line Assignment**” tab under the “Details” window. Enter 3000 in the “**Private Received**” number field; then enter the 10 digit DID (Public number) in the “**Public Received**” number field. With the BCM 4.0 release; incoming DID calls will be routed to telephones, based on all 10 digits received by the network. For example, Incoming calls from the AT&T IP Flexible Reach network will deliver a ten digit DID number, e.g. 7323683476. The BCM will route the call using all ten digits, e.g. 7323683476.

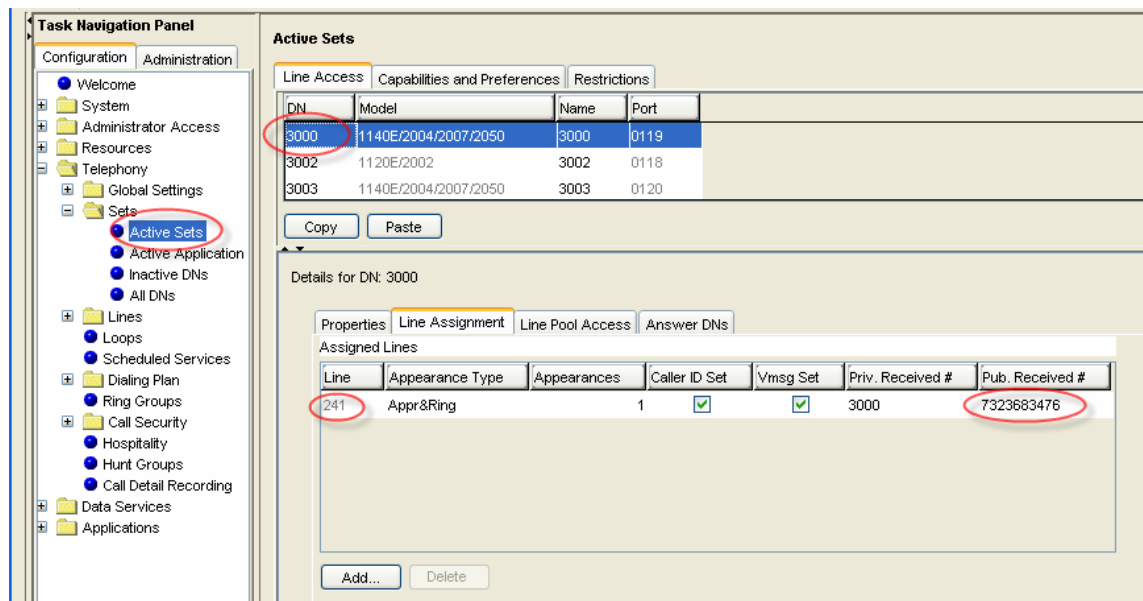


Figure 13: Configuring DID for Incoming Calls

4.8 Configuring IP Phone LCD Screen to Display DID Number

Configuration → Telephony → Lines → Target Lines → Line 241

To display the DID number on the IP phone LCD screen; select Line 241 than go to the “Parameters” tab. In our example below, enter 3683476 in the “Name” field and then select “public” as the line type from the drop down menu.

The screenshot shows the 'Task Navigation Panel' on the left with the 'Telephony' folder expanded and 'Target Lines' selected. The 'Target Lines' table on the right lists three lines, with Line 241 highlighted. Below the table are 'Copy' and 'Paste' buttons. The 'Details for Line: 241' section shows the 'Parameters' tab with the 'Name' field set to '3683476', 'Line Type' set to 'Public', 'Pub. Received #' set to '7323683476', 'Priv. Received #' set to '3000', and 'Distinct Ring' set to 'Pattern 3'.

Line	Trunk Type	Control Set	Prime Set
241	Target line	3000	3000
242	Target line	3000	3000
243	Target line	3000	3000

Copy Paste

Details for Line: 241

Parameters Preferences Assigned DN's

Name: 3683476

Line Type: Public

Pub. Received #: 7323683476

Priv. Received #: 3000

Distinct Ring: Pattern 3

Figure 14: Displaying DID Number on IP Set LCD

5 Troubleshooting

This section provides some tips about troubleshooting problems

5.1 System Monitoring with BCM Monitor

A valuable application for performance monitoring is the BCM Monitor. It allows the BCM administrator to see the current status of various parts of the BCM system. Statistical information is provided on system throughput and other performance-related information, including system CPU usage (graph or table format) and memory usage (graph or table format).

If a performance display is active, it is automatically updated with real-time performance information in user-selectable time increments.

The focus of the real-time monitoring capabilities is:

- Overall system status
- Utilization of resources on the Media Services Card (e.g. signaling channel usage)
- Operation of telephony applications (e.g., Messaging, Call Center, etc.).
- IP telephony activity
- D-channel monitoring for PRI, BRI and VoIP trunks

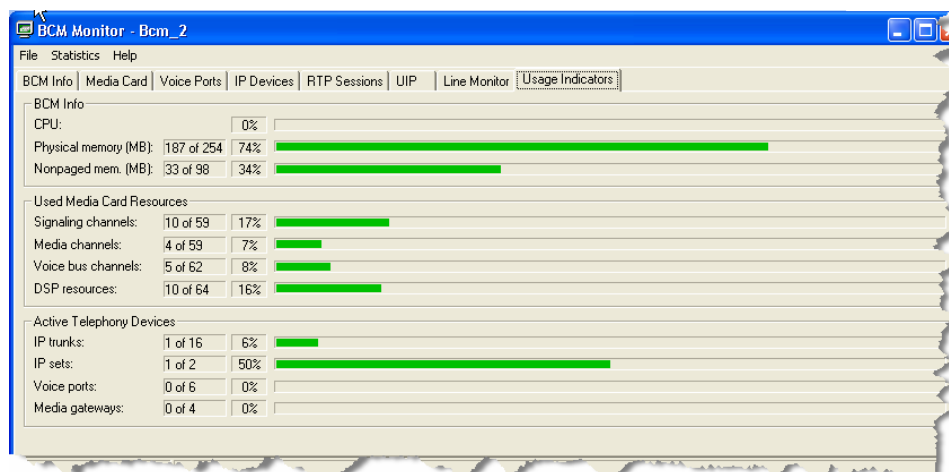


Figure 15: System Monitoring Example

The BCM Monitor application can be downloaded to an administrator's PC from the BCM and pointed at a specific BCM's IP address for monitoring. Multiple instances of the BCM Monitor application can be used on a single PC to monitor several remote BCM systems at the same time. Backward version compatibility is supported.

All of the registered IP devices can be viewed with the BCM Monitor. The screen shot below depicts IP Phone type, DN number and IP address of each registered IP phone. Additionally, if the device is active on a call the RTP session information is also displayed.

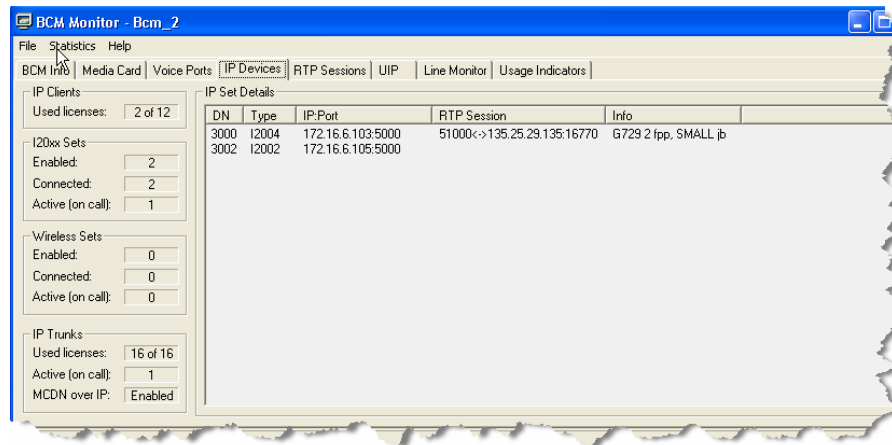


Figure 16: IP Device Listing

The end-to-end RTP sessions per IP call can also be displayed with the BCM Manager. The example below depicts an end-to-end call.

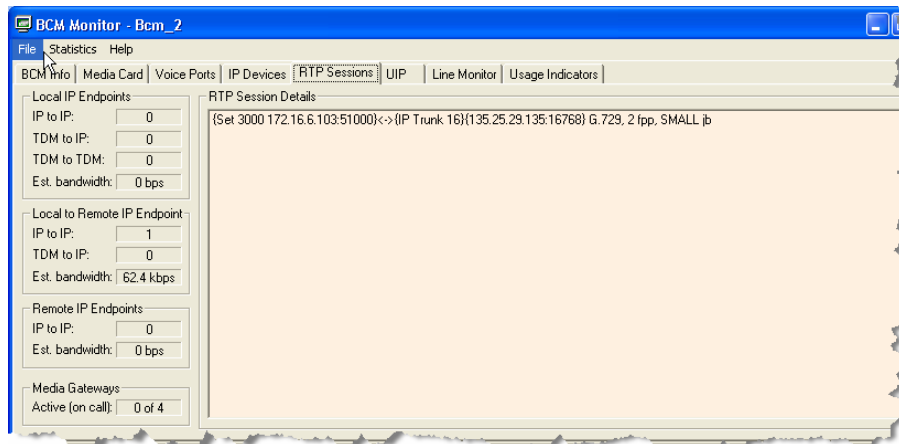


Figure 17: RTP Session Information

The BCM Monitor can be used to monitor incoming and outgoing trunks to determine if trunks are being busy or if they are idle. The example below depicts utilized lines used by local and remote telephone/DN numbers.

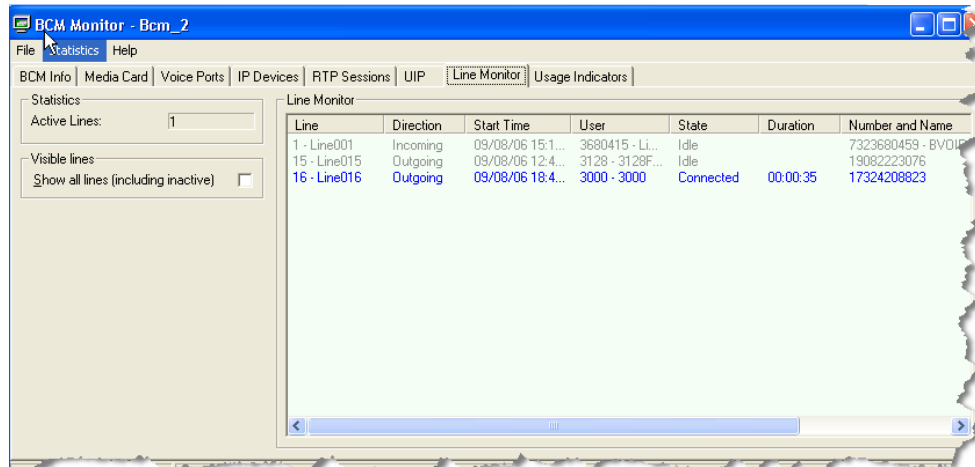


Figure 18: Line Monitor Information

The BCM Monitor can also be used to monitor all types of system usages. The following are some parameters that can be monitored:

- CPU utilization
- Physical memory
- Media card DSP utilization
- IP sets and IP Trunks
- Voice ports and media gateway usage

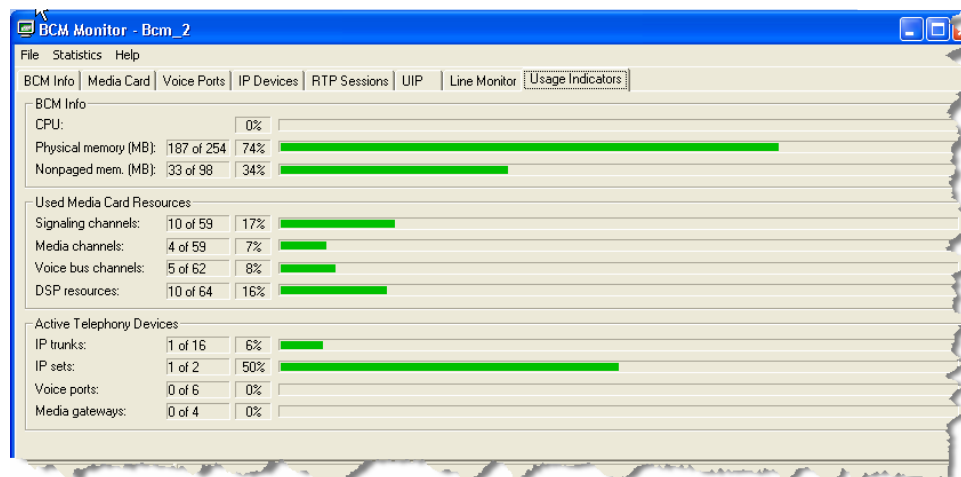


Figure 19: System Resources

5.2 Real-time BCM System Status LED Displays

Administration → System LED Status →

The BCM 200/400 front panel LED displays can be viewed remotely to determine certain critical components. The following are some LED indications that can be viewed remotely with the NCM Unified Manager:

- Power
- Hard drive (HDD)
- Multi-service Card (MSC)
- Modem
- Ethernet ports (NIC)
- System temperature
- Fan indications

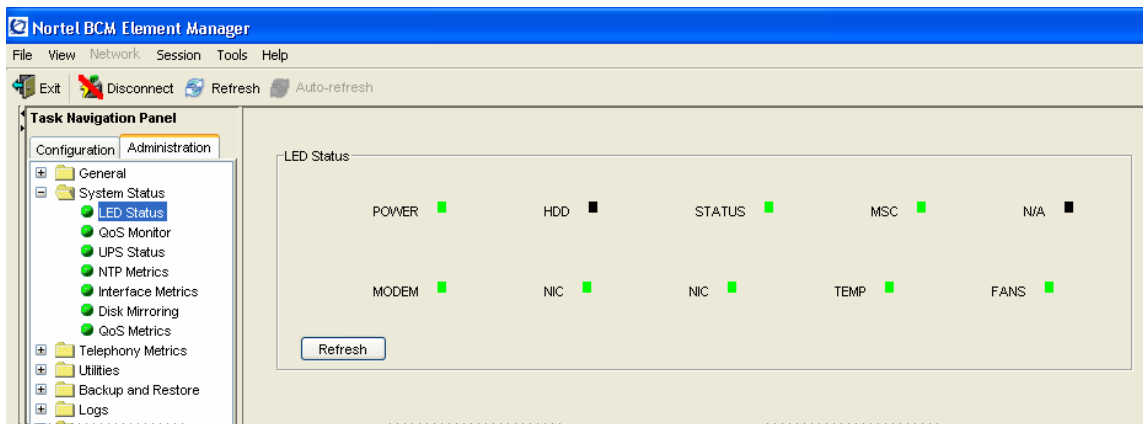


Figure 20: Front Panel LED Display

Using the Element Manager “System Status” tab, you can monitor overall system performance and other performance-related information. You monitor system status using the following tools:

- LED Status
- QoS Monitor
- UPS Status
- NTP Metrics
- Interface Metrics
- Disk Mirroring
- QoS Metrics

5.3 Real-time BCM Fault/Alarms Management

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

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

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

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

Below is an example of the BCM Alarms Panel in the BCM Element Manager:

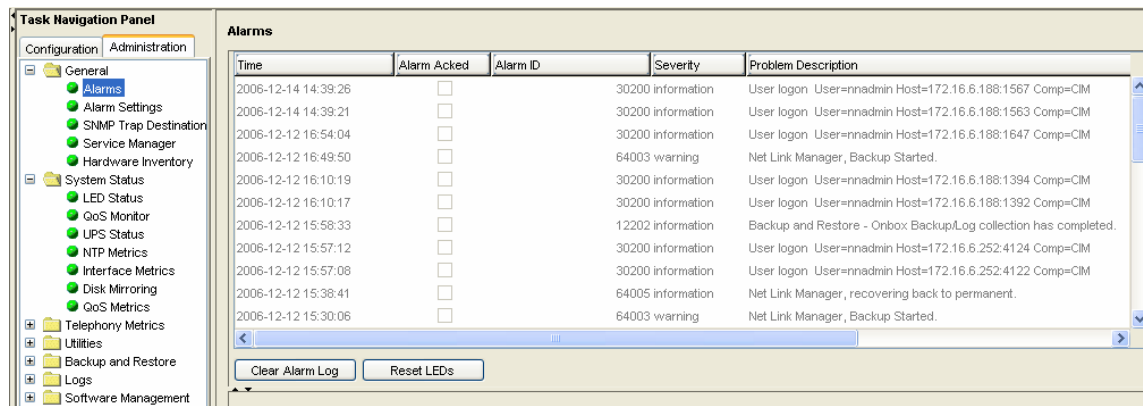


Figure 21: Real-time BCM 200/400 Alarm Display

You can manage alarms and alarm information by:

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

5.4 BCM Service Management System

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

- The name of a service
- Whether a service is enabled to automatically start up
- The status of the service running on the BCM

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

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

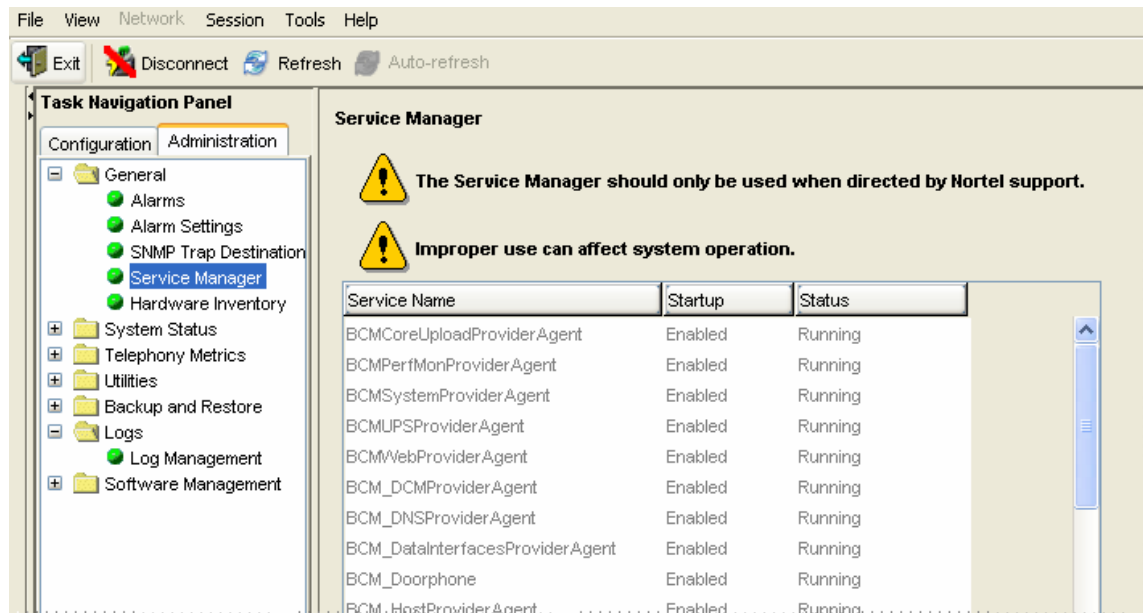


Figure 22: BCM Service Manager Screen

You can stop any of the services that are running on the BCM system.

To stop a service

- Click the **Administration** tab.
- Open the **General** folder, and then click the **Service Manager** task. The **Service Manager** page opens. Services are displayed in the Services table.
- In the Services table, select a service.

- Click the **Stop** button. A confirmation dialog box opens.
- Click **Yes**. In the Services table, Stopped is displayed in the Status column for the stopped service.

To restart a service

- Click the **Administration** tab.
- Open the **General** folder, and then click the **Service Manager** task. The **Service Manager** page opens. Services are displayed in the Services table.
- In the Services table, select a stopped service.
- Click the **Restart** button. A confirmation dialog box opens.
- Click **Yes**. In the Services table, **Running** is displayed in the **Status** column for the restarted service.

5.5 BCM Log Management

Another extremely useful tool is the “Log Management.” This allows you to quickly and easily collect all relevant logs files and other information to help the various support teams debug any problems you may have with your BCM 200/400. The entire log files required to diagnose a problem is consolidated into a single file.

A log file is a collection of individual log events generated by the BCM. An administrator can use log files to monitor and analyze system behavior, user sessions, and events. You manage log files by transferring selected BCM log archives from the BCM to a specified location, such as your personal computer. You can then view individual log events using the BCM Element Manager Log Browser or your usual text editor.

Note: Depending on the privileges assigned to you, you may or may not see all the log files or processes described in this section.

In addition to the log files generated by the BCM, the Element Manager itself generates a log file. This log is found under the Help selection of the BCM Element Manager Toolbar. This log contains diagnostic information.

The BCM manages log archives and maintains generations of information depending upon size or other criteria. Generations of log files have a numbered extension such as 3.gz.

A generation of the “alarms.systemlog” file is created each time the BCM is rebooted or when the log file reaches the 1 MB limit.

Transferring and Extracting Log Files

You use the BCM Element Manager to transfer log files from the BCM to an external location. You must transfer the log files to an external device before you can view them. If you are using the BCM Element Manager Log Browser to view the logs, you will also have to extract the log files from the log archive that is transferred from the BCM. The log archive contains a collection of log files.

When you transfer the log archives to another device, you can specify:

- The location to which you want to transfer log files, such as your personal computer or a network folder

- The category of logs you want to transfer, such as Sensitive Information logs
- A schedule for a log file transfer

You can also transfer log files using the BCM Web page if you cannot access the BCM Element Manager. After you transfer the log archives, several options are available to you for extracting the log file information and for viewing the log files. If you are using the BCM Element Manager (recommended), the Log Browser prompts you to extract the actual log files from the .tar file. If you prefer, you can use the WinZip application to expand the .tar file into its included log files. As an alternative to using the BCM Element Manager Log Browser, you can use an application such as WordPad to view the log files.

Using the BCM Element Manager Log Browser to view extracted log files gives you the ability to view information in a way that suits you; for example, you can filter and sort information according to priority, time, message, and so on.

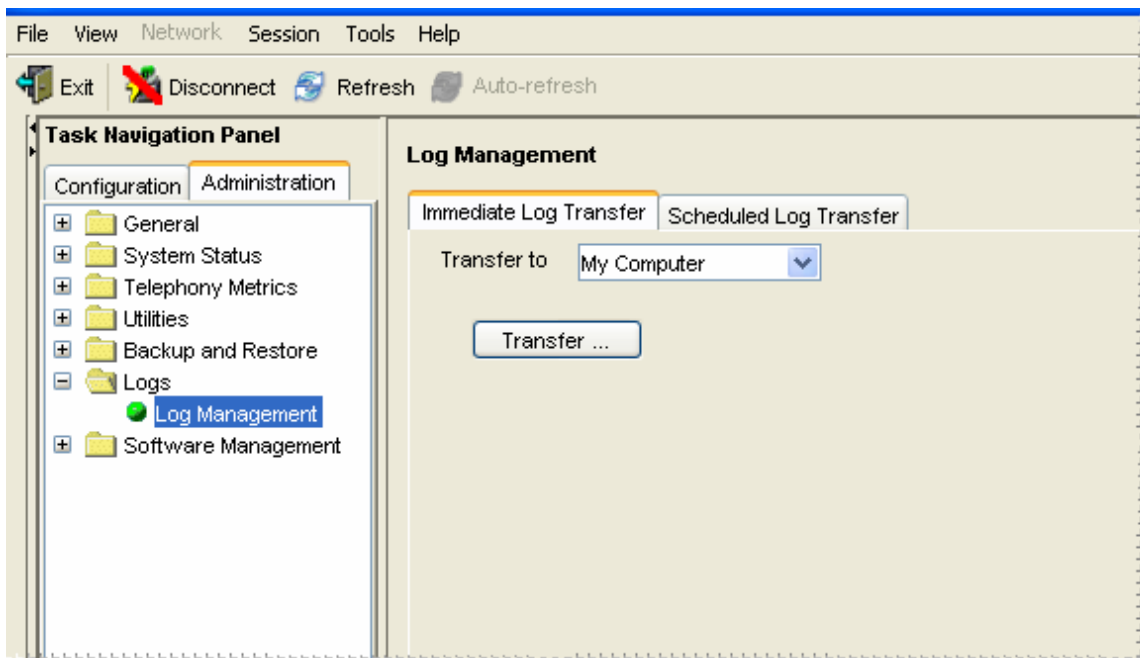


Figure 23: Log Management Screen

When you first suspect a problem with your BCM, it is important that you go into the “Log Management” screen and download the log file to your PC. Even if you end up resolving the issue, it is good to know that this information has been captured.

This Customer Configuration Guide ("CCG") is offered as a convenience to AT&T's customers. The specifications and information regarding the product in this CCG are subject to change without notice. All statements, information, and recommendations in this CCG are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this CCG.

In no event shall AT&T or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this CCG, even if AT&T or its suppliers have been advised of the possibility of such damage.

- End of Document -