555-7101-206

CallPilot

1002rp Server Maintenance and Diagnostics

Product release 3.0 Standard 1.0 November 2004

NORTEL NETWORKS™

P0949457

CallPilot

1002rp Server Maintenance and Diagnostics

Publication number:	555-7101-206
Product release:	3.0
Document release:	Standard 1.0
Date:	November 2004

Copyright © 2004 Nortel Networks, All Rights Reserved

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the CallPilot server and the switch or system is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

This page and the following page are considered the title page, and contain Nortel Networks and third-party trademarks.

Nortel Networks, the Nortel Networks logo, the Globemark, and Unified Networks, BNR, CallPilot, DMS, DMS-100, DMS-250, DMS-MTX, DMS-SCP, DPN, Dualmode, Helmsman, IVR, MAP, Meridian, Meridian 1, Meridian Link, Meridian Mail, Norstar, SL-1, SL-100, Succession, Supernode, Symposium, Telesis, and Unity are trademarks of Nortel Networks.

3COM is a trademark of 3Com Corporation.

ADOBE is a trademark of Adobe Systems Incorporated.

ATLAS is a trademark of Quantum Corporation.

BLACKBERRY is a trademark of Research in Motion Limited.

CRYSTAL REPORTS is a trademark of Seagate Software Inc.

EUDORA is a trademark of Qualcomm.

eTrust and InoculateIT are trademarks of Computer Associates Think Inc.

DIRECTX, EXCHANGE.NET, FRONTPAGE, INTERNET EXPLORER, LINKEXCHANGE, MICROSOFT, MICROSOFT EXCHANGE SERVER, MS-DOS, NETMEETING, OUTLOOK, POWERPOINT, VISUAL STUDIO, WINDOWS, WINDOWS MEDIA, and WINDOWS NT are trademarks of Microsoft Corporation.

GROUPWISE and NOVELL are trademarks of Novell Inc.

LOGITECH is a trademark of Logitech, Inc.

MCAFEE and NETSHIELD are trademarks of McAfee Associates, Inc.

MYLEX is a trademark of Mylex Corporation.

NETSCAPE COMMUNICATOR is a trademark of Netscape Communications Corporation.

NOTES is a trademark of Lotus Development Corporation.

NORTON ANTIVIRUS and PCANYWHERE are trademarks of Symantec Corporation.

QUICKTIME is a trademark of Apple Computer, In.

RADISYS is a trademark of Radisys Corporation.

SLR4, SLR5, and TANDBERG are trademarks of Tandberg Data ASA.

SYBASE is a trademark of Sybase, Inc.

TEAC is a trademark of TEAC Corporation

US ROBOTICS, the US ROBOTICS logo, and SPORTSTER are trademarks of US Robotics.

WINZIP is a trademark of Nico Mark Computing, Inc.

XEON is a trademark of Intel, Inc.

Publication history

November 2004	Release 3.0, Standard 1.0
September 2004	Release 3.0, Preliminary 2.0
July 2004	Release 3.0, Preliminary 1.0
May 2004	Release 3.0, Draft 0.01
April 2004	Release 2.5, Standard 2.0
October 2003	Release 2.5, Standard 1.0
June 2003	Release 2.5, Preliminary 1.0
April 2003	Release 2.5, Draft 2.0
October 2002	Standard 1.0 of *CallPilot Installation and Configuration, 1002rp Server Maintenance and Diagnostics* is issued for general release.

Contents

1 About this guide 11

Maintenance and diagnostics overview 12

2 Troubleshooting your CallPilot system 15

Startup diagnostics overview 16
Basic hardware check 17
Power-On Self-Test diagnostics 18
Interpreting POST diagnostics 19
Interpreting startup diagnostics from SCSI BIOS 21
What to do when the server fails to boot into service. 22

3 Using Windows online diagnostic tools 23

Overview. 24
Viewing event logs 25
Using TCP/IP diagnostic tools 29
Using the chkdsk utility 38

4 Using serial port diagnostic tools 41

Overview. 42
Shutting down services 43
Conducting TSTSERIO tests 45
Conducting TSTSERIO tests with the loopback plug 49
Restarting services 50

5 Using CallPilot Manager to monitor hardware 53

Understanding fault management 54
Alarm Monitor 56
Event Browser. 58
Channel and Multimedia Monitors 60
The Maintenance screen 61
Viewing component states 65
Starting and stopping components 68
Running integrated diagnostics. 72
Viewing the last diagnostic results 75
Working with the Multimedia Monitor 77
Working with the Channel Monitor 79

6 Using CallPilot system utilities 81

Overview. 82
Diagnostics Tool 83
PEP Maintenance utility 84
Session Trace 85
System Monitor. 87

7 Replacing basic chassis components 93

Removing the front bezel and server cover 94
Replacing air filters. 98
Replacing the power supply 99
Replacing the cooling fan 102
Replacing the fuse (AC system only) 105
Replacing the alarm board 107
Setting jumpers on the alarm board 109
Replacing the status display panel 111

8 Replacing media drives 113

Replacing a faulty hard drive 114
About the media drive bay 118
Removing the media drive carrier from the chassis 119
Replacing a tape, CD-ROM or floppy drive. 123
Installing a tape drive 126

9 RAID operations 129
RAID overview 130
Verifying the RAID firmware 131
Configuring RAID using the LSI Elite1600 controller and Ctrl+M 133
Verifying consistency on the drives 136
RAID splitting 137
Task summary for configuring RAID 141
Task summary for RAID splitting 142

10 Replacing or adding voice processing boards 143
DSP numbering and location 144
Replacing an MPB96 board 145

11 Maintaining the Pentium III SBC card 147
Overview 148
Replacing the Pentium III SBC card 149
Configuring the 1002rp Pentium III BIOS 153
Replacing or adding dual inline memory modules 156
Maintaining the onboard video and network cards 158

Index 159

Chapter 1

About this guide

In this chapter

Maintenance and diagnostics overview 12

Maintenance and diagnostics overview

Introduction

The maintenance and diagnostic activities discussed in this guide are divided into two groups of activities:

- troubleshooting and diagnostics (identifying the cause and resolving system problems)
- performing hardware maintenance

This guide is for administrators, technicians, and engineers responsible for maintaining a CallPilot server. This guide assumes that you have basic computing skills, and are familiar with necessary safety procedures.

If you are not able to resolve your problem with the resources described in this guide, you can also refer to the following document:

- *Troubleshooting Guide* (555-7101-501)

  Note: Nortel Networks continually updates the *Troubleshooting Guide*, which is available from the Partner Information Center (PIC) at http://my.nortelnetworks.com.

The "Starting up and shutting down the CallPilot server" chapter in the *Installation and Configuration Task List* (555-7101-210) explains how to restart, shut down, and power up the CallPilot server. You may be asked to perform one or more of these tasks while maintaining your server.

When you purchased your CallPilot server, it came preinstalled with the Windows operating system and CallPilot server software. If your CallPilot server no longer functions because of a software problem, you may need to reinstall the CallPilot software or rebuild the system.

Reference documents

CallPilot Customer Documentation Map

NTP Number 555-7101-(nnn)

- **Fundamentals**
  - CallPilot Fundamentals (-010)
- **Planning and Engineering**
  - Planning and Engineering Guide (-101)
  - Network Planning Guide (-102)
  - Data Networking for Voice over IP (553-3001-160)
- **Installation and Configuration**
  - Installation and Configuration Task List (-210)
  - **Server Installation Guides**
    - 201i Server Hardware Installation (-220)
    - 703t Server Hardware Installation (-226)
    - 1002rp Server Hardware Installation (-205)
  - **Configuration and Testing Guides**
    - Meridian 1 and CallPilot Server Configuration (-222)
    - Succession 1000 System and CallPilot Server Configuration (-510)
  - **Unified Messaging Software Installation**
    - Desktop Messaging and MyCallPilot Installation Guide (-505)
- **Administration**
  - Administrator's Guide (-301)
  - Software Administration and Maintenance Guide (-202)
  - Desktop Messaging and MyCallPilot Administration Guide (-503)
  - Meridian Mail to CallPilot Migration Guide (-801)
  - Application Builder Guide (-325)
  - Reporter Guide (-310)
- **Maintenance**
  - Troubleshooting Guide (-501)
  - **Server Maintenance and Diagnostics**
    - 201i Server Maintenance and Diagnostics (-119)
    - 703t Server Maintenance and Diagnostics (-227)
    - 1002rp Server Maintenance and Diagnostics (-206)
- **End User Information**

End User Cards	End User Guides
Unified Messaging Quick Reference Card	Multimedia Messaging User Guide
Unified Messaging Wallet Card	Speech Activated Messaging User Guide
Command Comparison Card A-Style	Desktop Messaging User Guide for Microsoft Outlook
Command Comparison S-Style	Desktop Messaging User Guide for Lotus Notes
Menu Interface Quick Reference Card	Desktop Messaging User Guide for Novell Groupwise
Alternate Command Interface Quick Reference Card	Desktop Messaging User Guide for Internet Clients
	MyCallPilot User Guide

Replacement parts

Before replacing any parts on your server, refer to the Nortel Networks product catalog for the part codes.



CAUTION

Risk of system damage

The use of parts that are not supplied by Nortel Networks can cause serious system problems or void your Nortel Networks warranty.

Preparing for maintenance activities

Before you proceed with hardware maintenance activities, review the *1002rp Server Hardware Installation* (555-7101-205) guide for the following information:

- required tools and equipment
- recommended safety precautions for electrostatic discharge, handling cards, and handling your server
- instructions for shutting down your 1002rp server or for taking it out of service

Chapter 2

Troubleshooting your CallPilot system

In this chapter

Startup diagnostics overview 16

Basic hardware check 17

Power-On Self-Test diagnostics 18

Interpreting POST diagnostics 19

Interpreting startup diagnostics from SCSI BIOS 21

What to do when the server fails to boot into service 22

Startup diagnostics overview

Introduction

This section contains procedures for interpreting the startup diagnostics on the 1002rp server.

Types of startup diagnostic

The following types of startup diagnostics are available on the server:

- Basic hardware check (for example LEDs)
- Power-On Self-Test (POST) diagnostics
- SCSI controller diagnostics or RAID controller diagnostics

These diagnostics are available at initial system startup, or after any 1002rp server reset.

Basic hardware check

Introduction

This section describes some basic checks that you can do when you start up the server.

To run the startup test

1. Power on the server and observe the front panel display.

   Result: All LEDs on the panel illuminate for a few seconds. The green power LED remains illuminated.

2. Observe the following server actions:

   - Cooling fans on the front panel start up, and the red fault LED next to each fan extinguishes.
   - Drives spin up, and the amber hard drive activity LEDs over the front panel display extinguish, and then flash with activity.
   - LEDs illuminate temporarily as the system checks the floppy drive, tape drive, and CD-ROM drive.
   - The LED on each power supply lights up red as supply fans spin up and components charge. LEDs turn green when the attached power supply is fully operational.

3. Check the monitor for any error messages as the server counts RAM and completes a POST.

   See “Power-On Self-Test diagnostics” on page 18 for more details on POST.

Power-On Self-Test diagnostics

Introduction

The Power-On Self-Test (POST) is a system diagnostic program (stored in the BIOS) that runs each time the 1002rp server is started. The function of the POST is to test system components and then display status messages.

To run the POST

1 Power up the CallPilot server and monitor.

Result: After a few seconds, POST begins to run.

After the memory test, various screen prompts and messages appear. The screen prompts may be accompanied by a single beep.

2 Observe the screen for any error messages and listen for POST beep codes. When POST completes, the server beeps once.

If the server halts before POST is finished, the server emits a beep code indicating that a fatal system error requires immediate attention. See “Interpreting POST diagnostics” on page 19 for details.

If POST can display a message on the monitor, the server emits two beeps as the message appears.

Record the message that appears on the monitor, and the beep code that you hear. This information is useful if you need assistance from your technical support representative.

Interpreting POST diagnostics

Introduction

This section provides an explanation of the POST diagnostic codes.

POST beep codes

If an error occurs before video initialization, POST emits beep codes that indicate errors in hardware, software, or firmware.

A beep code is a series of separate tones, each equal in length. Record the beep code sequence before calling Nortel Networks technical support.

ATTENTION

Some POST beep codes are fatal and may require that you replace the SBC. See the table below for more information about beep codes.

Beep count	Error message	Description
1	Refresh Failure	The processor board memory refresh circuitry is faulty.
2	Parity Error	A parity error was detected in the base memory (the first block of 64 kbytes) of the system.
3	Base 64KB Memory Failure	A memory failure occurred within the first 64 kbytes of memory.
4	Timer Not Operational	A memory failure occurred within the first 64 kbytes of memory, or Timer #1 on the processor board failed to function properly.

Beep count	Error message	Description
5	Processor Error	The Central Processing Unit (CPU) on the processor board failed to function properly.
6	8042 - Gate A20 Failure	The keyboard controller (8042) contains the Gate A20 switch which allows the CPU to operate in protected mode. This error message means that the BIOS is not able to switch the CPU into protected mode.
7	Processor Exception Interrupt Error	The CPU on the processor board generated an exception interrupt.
8	Display Memory Read/Write Error	The system video adapter is either missing or its memory is faulty. **Note:** This is not a fatal error.
9	ROM Checksum Error	The ROM checksum value does not match the value encoded in the BIOS.
10	CMOS Shutdown Register Read/ Write Error	The shutdown register for the CMOS RAM failed.
11	Cache Memory Bad: Do Note Enable Cache	The cache memory test failed. Cache memory is disabled. **Note:** Do not press <Ctrl><Alt>Shift><+> to enable cache memory.

Interpreting startup diagnostics from SCSI BIOS

Introduction

The results from the SCSI controller diagnostics appear after the POST results.

Applicable cards

Results of the startup diagnostics appear only if you have the following cards installed on your system:

- Adaptec SCSI controller

  The adapter is integrated in the SBC and can be disabled.
- LSI Elite 1600 controller

What to do when the server fails to boot into service

Introduction

This section suggests tasks you can perform to determine why the server fails the bootup cycle.

To determine why the server failed to boot to Windows

1. Make a note of any diagnostic codes.
2. Try restarting the server by pressing the power button on the server.
3. During the boot sequence, view the diagnostic codes on the monitor for failures.
4. Refer to the *Troubleshooting Guide* (555-7101-501) for other suggestions. If you still cannot determine the cause of the startup failure, call your Nortel Networks technical support representative.

To determine why the server failed to boot into CallPilot

If the system ready indicator indicates that the system is not booting into CallPilot, follow these steps:

1. Make a note of any diagnostic codes.
2. Try restarting the server by pressing the power button on the server.
3. During the boot sequence, view the diagnostic codes on the monitor for failures.
4. View the event logs. For instructions, see “Viewing event logs” on page 25.
5. Refer to the *Troubleshooting Guide* (555-7101-501) for other suggestions. If you still cannot determine the cause of the startup failure, call your Nortel Networks technical support representative.

Chapter 3

Using Windows online diagnostic tools

In this chapter

Overview 24

Viewing event logs 25

Using TCP/IP diagnostic tools 29

Using the chkdsk utility 38

Overview

Introduction

This section describes how to access the run-time online diagnostic tools provided by the Windows server software. Use these tools when a serious problem prevents the use of the CallPilot diagnostic tools that are available in CallPilot Manager.

- Windows Event Viewer
- Windows Diagnostics
- TCP/IP diagnostics
- chkdsk utility.



CAUTION

Risk of software corruption

Do not run any utilities that are not documented in this guide.

Viewing event logs

Introduction

When the server startup cycle is complete, and if the CallPilot server has been configured, messages in dialog boxes on the monitor indicate that CallPilot is ready to accept calls.

If one or more messages appear on the monitor, the message may contain information about an event, or a fault may have occurred. To determine what happened, you can use the following:

- Windows Event Viewer on the 1002rp server
- CallPilot Event Browser or Alarm Monitor in CallPilot Manager

Note: The Event Browser and Alarm Monitor include online help for events, which may help you to resolve the problem. If you cannot log on to the CallPilot system using a web browser due to server problems, then use the Windows Event Viewer.

Types of event logs

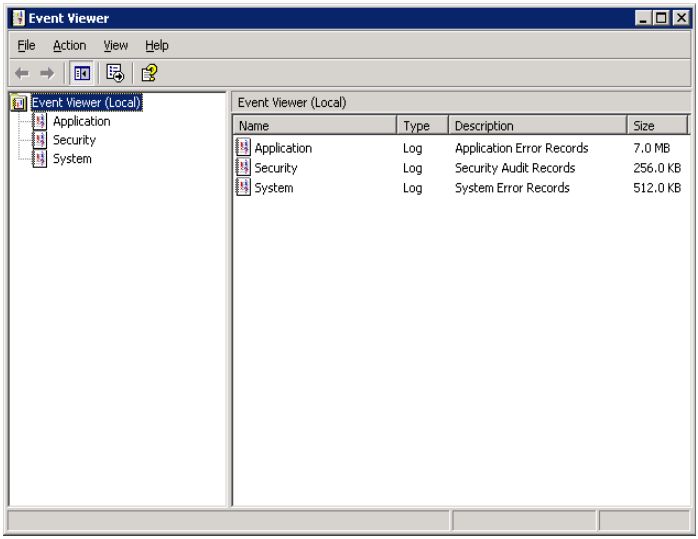
Three types of event logs are available from the Windows Event Viewer, as follows:

Log type	Description
System	Logs events by Windows components, including RAS or other Windows services.
Security	Logs security events, such as logons, logoffs, illegal access. This option is available only to users with Administrative access.
Applications	Logs events by application, such as database file errors.

To use the operating system Event Viewer

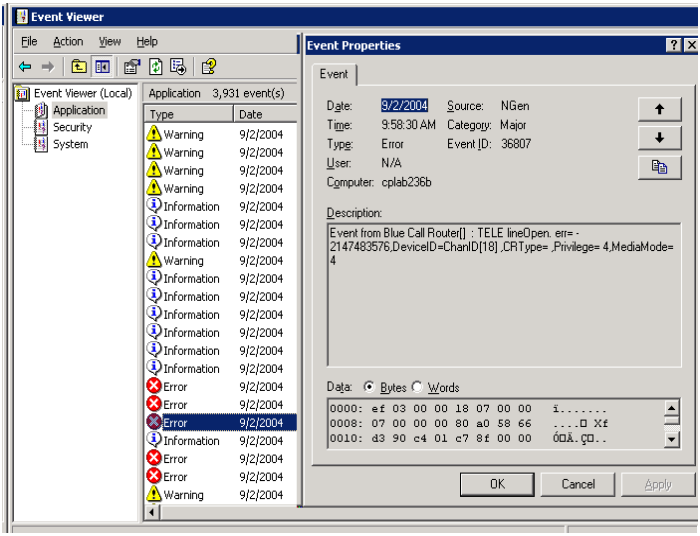
1 Click Start → Programs → Administrative Tools → Event Viewer.

Result: The Event Viewer window appears.

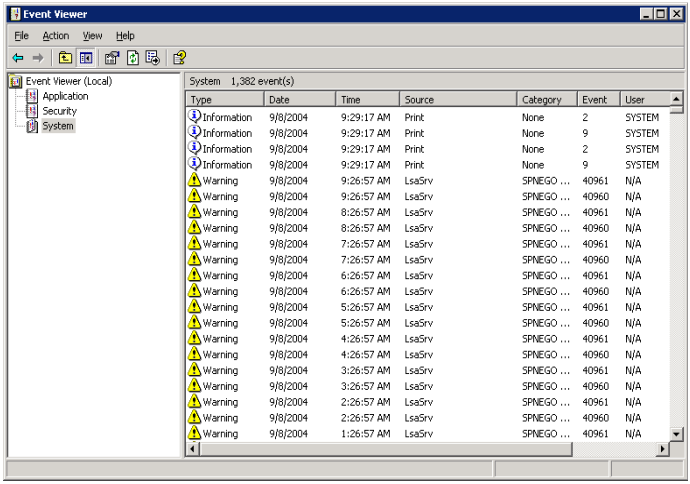


2 To view a log, click the name of the log in the left frame of the window.

The following illustration shows an example of the Application Log.



The following illustration shows an example of a System log.



Note: The Security log available only to administrators is not shown.

3 Look for error codes flagged with  or  that have occurred since the last startup.

Note: Each error is date and time stamped.  indicates major or critical errors.  indicates minor errors, and  indicates information.

4 To determine the cause of the error, select and then double-click the error.

Result: A description of the error appears in an Event detail dialog box. Use the description to help determine how to resolve errors.

Note: If the error persists or does not suggest a solution, contact your Nortel Networks support representative.

5 Click Close.

Result: The event log reappears.

6 Click Log → Exit.

Result: The Event Viewer closes.

Using TCP/IP diagnostic tools

Introduction

This section describes the following TCP/IP diagnostic tools available for the network adapter:

- ipconfig
- ping
- tracert
- arp
- nbtstat
- netstat

These utilities help you to verify network connectivity, test the network interface, and isolate any configuration problems.

The ipconfig command

The ipconfig command displays IP configuration information.

Ipconfig default

If you run the command without flags, it displays the IP address, subnet mask, and default gateway for each adapter bound to TCP/IP.

Ipconfig command syntax

```
ipconfig /[ ]
```

The following flags are available for the ipconfig command:

Flag	Description
/?	Displays Help information.
/all	Displays full configuration information.
/release	Releases the IP address for the specified adapter.
/renew	Renews the IP address for the specified adapter.

To run the ipconfig command from Windows

1 Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

Result: The Command Prompt window appears.

2 At the Command prompt, type **ipconfig** *<with appropriate parameters>*.

Example: ipconfig /all

3 Press Enter.

Result: The system runs the ipconfig utility.

4 Type **Exit** to exit the Command Prompt window and return to Windows.

The ping command

The ping command sends an echo request to a specified host. Use this command to verify network connectivity to the remote device.

Ping command syntax

The ping command uses the following syntax:

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL]
     [-v TOS] [-r count] [-s count]
     [[-j host-list] | [-k host-list]]
     [-w timeout] destination-list
```

Parameter	Description
-t	Pings the specified host until interrupted.
-a	Resolves addresses to host names.
-n count	Specifies the number of echo requests to send.
-l size	Sends buffer size.
-f	Set Don't Fragment flag in packet.
-i TTL	Time To Live
-v TOS	Type Of Service
-r count	Record route for count hops
-s count	Time stamp for count hops
-j host-list	Loose source route along host list
-k host-list	Strict source route along host list
-w timeout	Time-out in milliseconds to wait for each reply

To run the ping command from Windows

1 Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

Result: The Command Prompt window appears.

2 At the Command prompt, type **ping *<destination IP address>*** (for example, ping 200.286.32.0), or **ping *<computer name>***.

3 Press Enter.

Result: The system displays the ping results.

4 Type **Exit** to exit the Command Prompt window and return to Windows.

The tracert command

This utility determines the route taken to a destination.

How tracert works

The tracert utility follows several steps to complete its task:

- Tracert sends Internet Control Message Protocol (ICMP) echo packets with varying Time-To-Live (TTL) values to the destination.
- Each router along the path must decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count.
- When the TTL on a packet reaches 0, the router sends back an ICMP Time Exceeded message to the source system.
- Tracert determines the route by sending the first echo packet with a TTL of 1, and incrementing the TTL by 1 on each subsequent transmission until the target responds, or the maximum TTL is reached.
- Tracert then examines the ICMP Time Exceeded messages sent back by intermediate routers.

Tracert syntax

```
tracert [-d] [-h maximum_hops] [-j host_list]
        [-w timeout] [target_name]
```

Tracert parameters

The tracert command uses the following parameters:

Parameter	Description
-d	Specifies not to resolve addresses to hostnames.
-h maximum_hops	Specifies the maximum number of hops to search for the target.
-j host-list	Specifies a loose source route along the host list.
-w timeout	Waits the number of milliseconds specified by the time-out for each reply.
target_name	The name of the target host.

To run the tracert command from Windows

1 Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

Result: The Command Prompt window appears.

2 At the Command prompt, type the following command:

tracert *[-d] [-h maximum_hops] [-j host_list] [-w timeout] [target_name]*

Example: tracert 200.286.0.32

3 Press Enter.

Result: The system runs the tracert utility.

4 Type **Exit** to exit the Command Prompt window and return to Windows.

The arp command

The arp command displays and modifies the IP-to-physical address translation tables used by Address Resolution Protocol (arp).

Arp command syntax

The arp command uses the following syntax:

```
arp -s inet_addr eth_addr [if_addr]

arp -d inet_addr [if_addr]

arp -a [inet_addr] [-N if_addr]
```

Parameter	Description
-a	Displays current arp entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for only the specified computer appear. If more than one network interface uses arp, entries for each arp table appear.
-g	Same as -a.
inet_addr	Specifies an Internet address.
if_addr	Specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface is used.
eth_addr	Specifies a physical address.
-N if_addr	Displays the arp entries for the network interface specified by if_addr.
-d	Deletes the host specified by inet_addr.
-s	Adds the host and associates the Internet address inet_addr with the physical address eth_addr. The physical address is given as six hexadecimal bytes separated by hyphens. The entry is permanent.

To run the arp command from Windows

1. Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **arp** with the required parameters (for example, arp -g 200.286.0.32).

3. Press Enter.

   Result: The system runs the arp command.

4. Type **Exit** to exit the Command Prompt window and return to Windows.

The nbtstat command

The nbtstat command displays protocol statistics and current TCP/IP connections using NBT.

Nbtstat command syntax

The nbtstat command uses the following syntax:

```
nbtstat [-a remotename] [-A IP address] [-c] [-n]
        [-R] [-r] [-S] [-s] [interval]
```

Parameter	Description
-a remotename	Lists the remote computer name table using its name.
-A IP address	Lists the remote computer name table using its IP address.
-c	Lists the contents of the NetBIOS name cache giving the IP address of each name.
-n	Lists local NetBIOS names. Registered indicates that the name is registered by broadcast (Bnode) or WINS (other node types).
-R	Reloads the LMHOSTS file after purging all names from the NetBIOS name cache.

Parameter	Description
-r	Lists name resolution statistics for Windows networking name resolution. On a Windows computer configured to use WINS, this option returns the number of names resolved and registered through broadcast or through WINS.
-S	Displays both client and server sessions, listing the remote hosts by IP address only.
-s	Displays both client and server sessions, and attempts to convert the remote host IP address to a name using the HOSTS file.
interval	Displays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop displaying statistics. Without this parameter, nbtstat prints the current configuration information once.

To run the nbtstat command from Windows

1 Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

Result: The Command Prompt window appears.

2 At the Command prompt, type **nbtstat** with the required parameters.

3 Press Enter.

Result: The system runs the nbtstat utility.

4 Type **Exit** to exit the Command Prompt window and return to Windows.

The netstat command

The netstat command displays current TCP/IP network connections and protocol statistics.

Netstat command syntax

The netstat command uses the following syntax:

```
netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

Parameter	Description
-a	Displays all connections and listening ports.
-e	Displays Ethernet statistics. This can be combined with the -s option.
-n	Displays addresses and port numbers in numerical form.
-s	Displays statistics for each protocol.
-p proto	Shows connections for the protocol specified by proto. Proto can be tcp or udp. If used with the -s option, proto can be tcp, udp, or ip.
-r	Displays the contents of the routing table.
interval	Redisplays selected statistics, pausing between each display. Press Ctrl+C to stop redisplaying.

To run the netstat command from Windows

1 Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

Result: The Command Prompt window appears.

2 At the Command prompt, type **netstat** with the required parameters.

3 Press Enter.

Result: The system runs the netstat utility.

4 Type **Exit** to exit the Command Prompt window and return to Windows.

Using the chkdsk utility

Introduction

The chkdsk utility checks a specified disk on the server and displays a status report. It can be run on drives C, D, E, or F. It is an online utility, but it reduces system performance while it is running.

The chkdsk utility checks for problems at the Windows file system level. Any problems existing at this level can cause problems for CallPilot. Even if there are no problems at the Windows file system level, CallPilot can still be affected by problems at the CallPilot file system level.

Note: A version of this utility, called autocheck, automatically runs during Windows startup. Output from this utility appears on the blue startup screen.

Chkdsk utility syntax

The chkdsk utility uses the following syntax:

```
chkdsk [drive:][path]filename] [/F] [/V] [/R]
```

Parameter	Description
drive:	The drive letter of the drive that you want to check.
filename	The names of files to check for fragmentation.
/F	Add this parameter to fix errors on the disk.
/V	Add this parameter to display the full pathname of every file on the disk.
/R	Add this parameter to locate bad sectors and to recover readable information.

To run the chkdsk utility from Windows

1. Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **chkdsk *<drive letter:>*** (for example, chkdsk c:).

3. Press Enter.

   Result: The system runs the chkdsk utility.

4. Type **Exit** to exit the Command Prompt window and return to Windows.

Chapter 4

Using serial port diagnostic tools

In this chapter

Overview 42

Shutting down services 43

Conducting TSTSERIO tests 45

Conducting TSTSERIO tests with the loopback plug 49

Restarting services 50

Overview

Introduction

You may want to test the serial ports when remote access does not work.

This chapter describes how to run serial port diagnostics on the CallPilot server using the TSTSERIO command. Direct the TSTSERIO command to serial ports on the server after services on these ports have been shut down manually, as described in this chapter.

Shutting down services

This section describes how to shut down a service using a specific serial port. Use the procedures below before invoking the TSTSERIO local loopback tests.



CAUTION

Risk of communications loss

By stopping the services on COM1 or COM2, you lose the support access feature.



CAUTION

Risk of stopping call processing

By stopping the services on COM2, you stop call processing on CallPilot.

Services to stop for COM1 testing

- Routing and Remote Access Service

Services to stop for COM2 testing

- CallPilot SLEE Service
- CallPilot MWI Service
- CallPilot Access Protocol Emulator
- CallPilot Blue Call Router
- CallPilot Call Channel Router
- CallPilot Time Service
- Routing and Remote Access Service

Net Stop command

Use the Net Stop command to stop a specified service on a serial port.

Net stop command syntax

The Net Stop command uses the following syntax:

net stop "*service_name*"

ATTENTION

You must restart the services that you shut down through the Net Start command after running the diagnostic. For details, see "Restarting services" on page 50.

To invoke the Net Stop command from Windows

1. Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **net stop "*service_name*"**, and then press Enter.

   For example, type **net stop "Remote Access Server"**, and then press Enter.

   Note: The quotation marks are required, as in the example above.

   Result: The system runs the Net Stop command utility.

3. Type **Exit**, and then press Enter to exit the Command Prompt window.

Conducting TSTSERIO tests

Introduction

The TSTSERIO command performs local loopback tests of the serial communication ports from the server run-time environment.

Note: Before conducting these tests, shut down the appropriate services. See "Shutting down services" on page 43.



CAUTION

Risk of communications loss

By stopping the services on COM1 or COM2, you lose the support access feature.



CAUTION

Risk of stopping call processing

By stopping the services on COM2, you stop call processing on CallPilot.

TSTSERIO command syntax

The syntax for the TSTSERIO command is as follows:

TSTSERIO [/?] /P:comport [/S:subtstname] [/L:loops]

Flag	Requirement	Description
?	n/a	Displays Help.
/P:comport	Required	Specifies the symbolic port name assigned to the port you want to test.

Flag	Requirement	Description
/S:subtstname	Optional	Specifies a TSTSERIO subtest. See the following table for a description of the available subtests.
/L:loops	Optional	Specifies the number of times (up to a maximum of 65 535) to execute the requested test. The default number of tests is 1. A value of 0 infinitely loops until you enter CTRL+C.

TSTSERIO internal loopback diagnostic subtests

The following internal loopback subtests are available for the TSTSERIO command. For each of these tests, the communications resource must be available:

Subtest name	Description
idata	Internal data bus loopback
imsr	Internal modem status register
baud	Internal data bus loopback at various baud rates
word	Test 5-, 6-, 7-, and 8-bit data lengths
stop	Test 1, 1.5, and 2 stop bits
pari	Test odd/even parity
fifo	Test that device can operate in fifo mode

To invoke the TSTSERIO /P command from Windows

1. Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **tstserio** with the required parameters, and then press Enter.

   For example, type **TSTSERIO /P com1** or **TSTSERIO /P com 2**, and then press Enter.

3. Type **Exit**, and then press Enter to exit the Command Prompt window.

TSTSERIO external loopback plug subtests

The following external loopback subtests are available for the TSTSERIO command. For each of these tests, an external loopback connector must be used. For more information, see "Conducting TSTSERIO tests with the loopback plug" on page 49.

Subtest name	Description
edata	External data bus loopback. This test requires an external loopback connector.
emsr	External modem status register. This test requires an external loopback connector.
eint	Test ability of device to generate interrupts. This test requires an external loopback connector.

To invoke the TSTSERIO /S command from Windows

1. Click Start → Programs → Accessories → Command Prompt to display the command prompt window.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **tstserio** with the required parameters, and then press Enter.

   For example, type **TSTSERIO /P com1 /S extr**, and then press Enter.

3. Type **Exit**, and then press Enter to exit the Command Prompt window.

Conducting TSTSERIO tests with the loopback plug

Introduction

The TSTSERIO command requires an external loopback connector plug for its edata, emsr, and eint subtests.

9-pin connector plug

The standard serial loopback connector is a female 9-pin D-sub connector. This connector has the following pins wired together:

- CTS (pin 8) wired to (pin 7) RTS
- SIN (pin 2) wired to (pin 3) SOUT
- DTR (pin 4) wired to (pin 6) DSR

Once the plug is installed on the serial port, TSTSERIO can be invoked according to the procedure outlined in the previous section.

Restarting services

Introduction

This section describes how to restart the services for COM1 or COM2 after invoking the TSTSERIO local loopback tests.

Services to restart after COM1 testing

- Routing and Remote Access Service

Services to restart after COM2 testing

- CallPilot SLEE Service
- CallPilot MWI Service
- CallPilot Access Protocol Emulator
- CallPilot Blue Call Router
- CallPilot Call Channel Router
- CallPilot Time Service
- Routing and Remote Access Service

Net Start command

Use the Net Start command to restart a specified service on a serial port. The syntax for the Net Start command is as follows:

```
net start "[service-name]"
```

To invoke the Net Start command from Windows

1. Click Start → Programs → Accessories → Command Prompt.

   Result: The Command Prompt window appears.

2. At the Command prompt, type **net start "*service_name*"**, and then press Enter.

   For example, type **net start "Remote Access Server"**, and then press Enter.

   Note: The quotation marks are required, as in the example above.

3. Type **Exit**, and then press Enter to exit the Command Prompt window.

Chapter 5

Using CallPilot Manager to monitor hardware

In this chapter

Understanding fault management 54
Alarm Monitor 56
Event Browser 58
Channel and Multimedia Monitors 60
The Maintenance screen 61
Viewing component states 65
Starting and stopping components 68
Running integrated diagnostics 72
Viewing the last diagnostic results 75
Working with the Multimedia Monitor 77
Working with the Channel Monitor 79

Understanding fault management

Introduction

Fault management is a term that describes how the CallPilot server detects and notifies you of potential or real hardware problems (faults). The server processes events to detect hardware problems and raises alarms to notify you when these problems occur.

Event processing

An event is any change in system configuration or operational state. An event is also any action taken by the system that requires user notification. Events can be as insignificant as a user logon attempt or as serious as a faulty MPB96 card switching to disabled status.

All events are reported to the fault management server, a subsystem within the CallPilot server. The fault management server enables the server to listen and respond to its clients. The interaction is called event processing and is the means by which the server detects hardware faults.

Alarm notification

Alarms are warnings generated by events. Alarms communicate the same information as events. However, alarms are reported in the Alarm Monitor instead of the Event Browser, and are managed differently than events.

When an alarm appears in the Alarm Monitor, you must investigate the problem, isolate it, and then fix the cause of the problem. When you fix the problem, the alarm is cleared from the Alarm Monitor.

Component dependencies

The status of some components are dependent on the operational status of other components. If a component fails or is stopped, the dependent components go out of service.

Note: Based on the CallPilot server type, and the type of switch connected to CallPilot, some of these components may not appear on your system.

Component	Dependent components
Media Bus	All MPBs, and all multimedia and call channels.
MPB board	All multimedia and call channels associated with the MPB board.
Time Switch	All multimedia and call channels associated with the same MPB as the timeswitch.
MPB96	All multimedia channels on the MPB96 card.
DS30X	All DS30X channels associated with the DS30X link.

Detecting hardware problems

Typically, you first become aware of a hardware problem when an alarm is raised. All hardware faults produce an alarm (or series of alarms, depending on the problem) in the Alarm Monitor.

Other indications of a hardware problem include the following:

- user complaints
- call processing difficulties, such as busy signals, static, dropped calls, connection problems, and cross talk (hearing other conversations)
- system administrator logon difficulties
- alert icons on the Maintenance screen

Alarm Monitor

Introduction

Use the Alarm Monitor to investigate one or more raised alarms.

About alarms

Alarms are warnings generated by events. Alarms communicate the same information as events. However, alarms are reported in the Alarm Monitor instead of the Event Browser, and are managed differently than events:

- Alarms appear in the Alarm Monitor only for Minor, Major, and Critical events (not Information events). All events can be reported in the Event Browser (depending on filtering criteria defined in the Event Browser).
- The first time an event occurs, it generates an alarm that appears in the Alarm Monitor. If the same event continues to occur, a new alarm is not generated. Instead, the time and date assigned to the original generated alarm is updated.
- Alarms can be cleared from the Alarm Monitor, but the event that generated the alarm is not cleared from the event log or the Event Browser.

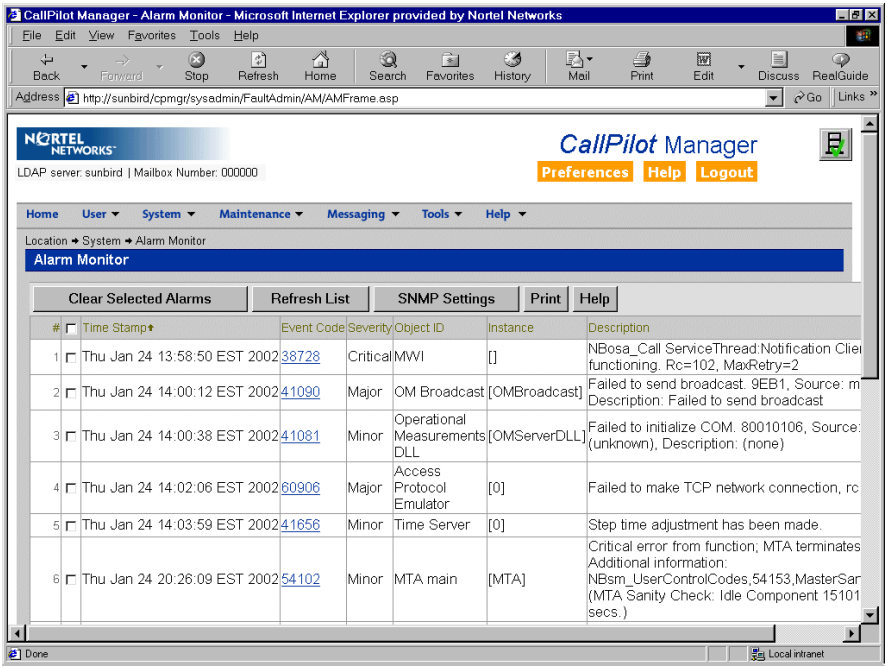
Each alarm in the Alarm Monitor has Help text that often provides a solution to the problem. If the solution is not apparent, use the Event Browser or the Maintenance screen to further investigate the problem.

To investigate using the Alarm Monitor

1 Run CallPilot Manager and login.

2 In CallPilot Manager, click System → Alarm Monitor.

Result: The Alarm Monitor screen appears.



3 Click the Event Code for the first critical or major alarm.

Result: A description of the event appears in a new web browser window.

4 Review the description and recovery action.

5 Repeat steps 3 and 4 for a few more alarms, if necessary.

6 If the solution to the problem is not apparent, obtain the return code of the first event and continue the investigation by using the Event Browser (see “Event Browser” on page 58).

Event Browser

Introduction

Use the Event Browser to investigate a series of events that occurred around the time an alarm was raised. The event listing can help you determine the root cause of a problem.

About events

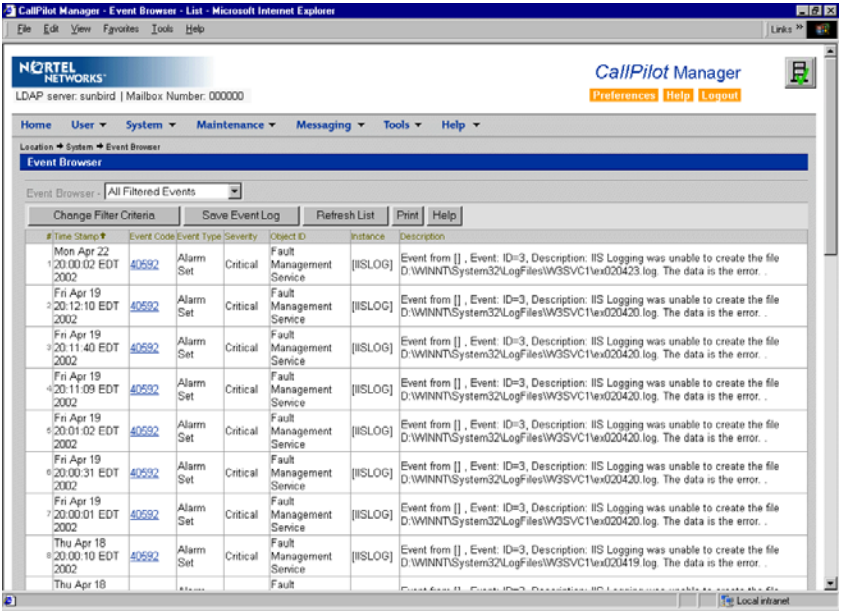
The Event Browser displays events that have been recorded in the server log. Each event identifies the time the event occurred, the object that generated the event, and the cause of the event.

Events are classified as Information, Minor, Major, or Critical. By default, the Event Browser displays only the latest 100 critical events.

To investigate using the Event Browser

1. Run CallPilot Manager and login.
2. In CallPilot Manager, click System → Event Browser.

   Result: The Event Browser screen appears.



3. Click an event that appears to be related to the problem, or an event that occurred near the time the alarm was raised.

   Result: A description of the event appears in a new web browser window.
4. View the description and recovery action.
5. Repeat steps 3 and 4 for a few more events, if necessary.
6. If the solution to the problem is not apparent, contact your Nortel Networks technical support representative.

Note: For information on how to use the Event Browser refer to the CallPilot Manager online Help.

Channel and Multimedia Monitors

Introduction

The Channel Monitor shows the status of call channels. The call channels are the connections between the server and the switch that carry the call signals to CallPilot.

The Multimedia Monitor shows the status of multimedia channels. The multimedia channels are the DSP ports that process the calls. They are the voice, fax, and speech recognition channels.

Disabling call channels

If you must take the CallPilot system out of service to perform software or hardware maintenance, Nortel Networks recommends that you disable all call channels first. There are two ways to disable the call channels:

- Courtesy stop the channels (preferred method).

  When you courtesy stop call channels, CallPilot waits until the channels are no longer active before disabling them, instead of suddenly terminating active calls.

- Stop the channels.

  When you stop channels, you suddenly disable them and terminate all active calls.

The Maintenance screen

Introduction

Use the Maintenance screen in CallPilot Manager to do the following:

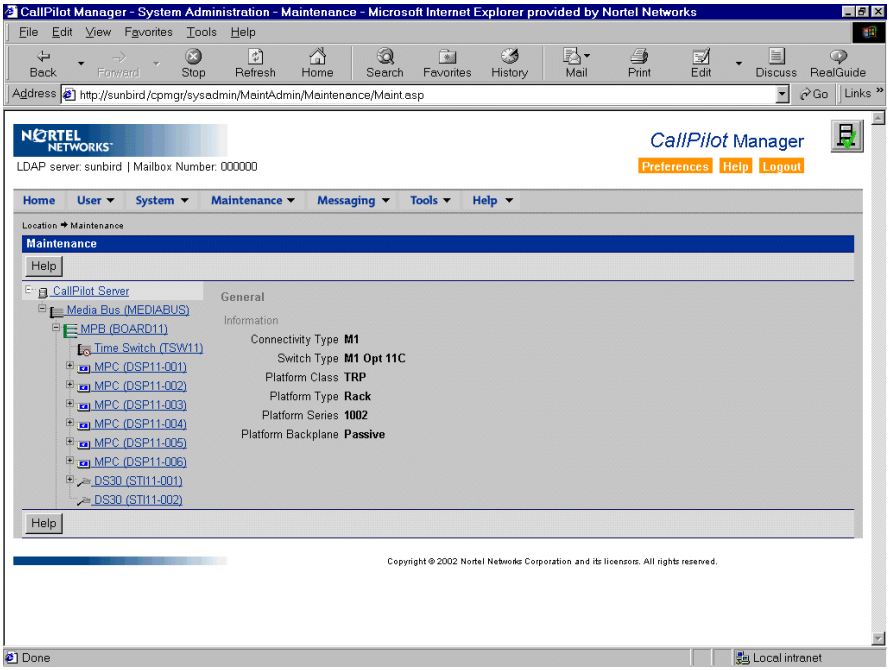
- Obtain general information about components.
- View component states.
- Start and stop components.
- Run integrated diagnostic tests.
- View the results of the last diagnostic test run against a component.

What the Maintenance screen provides

The Maintenance screen identifies the server platform and switch connectivity type. It also provides a tree that, when expanded, lists the physical and logical hardware components down the left side of the screen. To list the server hardware components, click the plus sign (+) at the top of the tree. To list the subcomponents for each component, click the plus sign (+) beside the component.

Note: The components that are listed on the Maintenance screen are based on the CallPilot server type and the switch that is connected to CallPilot. The examples in this chapter are for illustration purposes and may not appear exactly the same on your system.

The following is an example of a partially expanded tree for the 1002rp server:



When you click a component, the screen refreshes to show the details about that component. Details are divided into the sections described in the following table:

Section	Description
General	This section shows general technical information about the selected component. This typically includes the following details: ■ the name, class, type, series, or version of a component ■ various capabilities of a component (for example, whether a component is removable) **Note:** This section does not appear for all components.

Section	Description
Maintenance	This section shows the state of the selected component. Use this section to start and stop a component before running a diagnostic test. This section appears only for components on which you are allowed to perform maintenance administration. For more information about working with component states, see the following sections: ■ "Viewing component states" on page 65 ■ "Starting and stopping components" on page 68
Diagnostics	Use the Diagnostics section to run one or more diagnostic tests, or to view the results of the last diagnostic tests that were run on the selected component. This section appears only for components on which you are allowed to run diagnostics. For more information about running diagnostics, see the following sections: ■ "Running integrated diagnostics" on page 72 ■ "Viewing the last diagnostic results" on page 75

Maintenance activities for each component

The following table identifies the maintenance activities you can perform for each component that is listed in the component tree:

Component	Start, stop?	Courtesy stop?	Diagnostics available?	Replaceable?
Media Bus	Yes	No	Yes	No
MPB96 board	Yes	No	Yes	Yes
Time Switch	No	No	No	No
MPCs (embedded on MPB boards)	Yes	No	Yes	embedded: No
Multimedia channels	Yes	Yes	Yes	No
Call channels	Yes	Yes	No	No
DS30X link	Yes	No	No	No

Note: The MGate card and DS30X cable are replaceable. If you are having problems with the DS30X link, determine if either one or both of those items are causing the problem and need to be replaced.

Viewing component states

Introduction

View a component state to determine the general condition of the component, including whether the component is disabled or off duty. The component state is shown in the Maintenance section of the Maintenance screen.

Component states

You can determine the state of a component by looking at the State box in the Maintenance section.

State	Description
Active	The component is working and currently involved in processing a call.
Disabled	The diagnostic failed.
Idle	The component is working but not currently involved in processing a call.
InTest	A diagnostic is running on the resource or device.
Loading	The component has been started, which takes it out of the Off Duty state. This state occurs quickly and is immediately followed by Idle.
Local (Red) Alarm	A Receive Loss of Synchronization error occurred on incoming data over a T1 link and lasted more than 2.5 seconds. This condition will exist until synchronization is recovered and remains recovered for 12 seconds.

State	Description
No resources	The hardware required for the component to operate is not installed or is not operating properly.
Not Configured	The device is not configured in CallPilot. For example, a DSP is not being used because it was not allocated in the Configuration Wizard.
Off Duty	The component has been stopped.
Remote Off Duty	The component has been taken out of service at the switch.
Remote (Yellow) Alarm	This alarm is sent by the receiving T1 device to CallPilot. It indicates that a red alarm exists at the receiving device, and remains in effect until the red alarm is cleared at the receiving device.
Shutting Down	The component is in the process of stopping. This state occurs quickly and is immediately followed by Off Duty.
Uninitiated	The call processing component has not initialized the resource.

Alert icons

If one of the following icons appears next to a component in the tree, then the component or one of its subcomponents is experiencing a problem:

Icon	Description
	A problem exists with a subcomponent of the selected component. Expand the tree to locate the subcomponent with the problem.
	A problem exists with the selected component.

To view the state of a hardware component

1. Run CallPilot Manager and login.
2. In CallPilot Manager, click Maintenance → Maintenance Admin.

   Result: The Maintenance screen appears.
3. Click the plus sign (+) beside the CallPilot server to expand the component tree.
4. Continue clicking the plus sign (+) until the component with which you want to work is visible.
5. Click the hardware component with which you want to work.

   Result: The Maintenance screen refreshes to show details about the component.
6. Scroll down to the Maintenance section.
7. View the state of the selected component in the State box.

Starting and stopping components

Introduction

When you stop a component, you take it out of service and prevent it from operating. You must stop a component before you can replace it (if the component is replaceable) or run a diagnostic test on it.

To bring an out-of-service component back into service, you must start it.

Start and stop components from the Maintenance section on the Maintenance screen.

ATTENTION

Nortel Networks recommends that, if possible, you courtesy stop a component. Courtesy stop is available only at the individual channel level.

To courtesy stop CallPilot, use the following:

- Multimedia Monitor: to courtesy stop a range of multimedia channels
- Channel Monitor: to courtesy stop a range of call (DS30X, also known as DS0) channels

Stop versus Courtesy stop

The following two methods of taking a component out of service allow you to choose how active calls are affected:

Courtesy stop

A courtesy stop takes the component out of service only after the component has finished processing the active call.

- If the component is currently processing a call, the call is not dropped; the component remains active until the call is finished.
- If the component is not currently in use, it is taken out of service immediately.

Courtesy stop is preferred over a regular stop.

Stop

A stop takes the component out of service immediately, regardless of whether the component is currently processing calls. All active calls are dropped. Typically, you perform a stop only when severe problems that are affecting a large number of incoming calls occur or if your organization determines a special need for it.

Components that can be started and stopped

Only the following components can be started and stopped:

Note: If you want to start or stop more than one or two multimedia (DSP) or call (DS30X) channels, use the Multimedia Monitor or Channel Monitor.

Component	Effect of stopping
Media Bus	Takes all call processing resources out of service.
MPB board	Takes all call processing resources on the selected board out of service.

Component	Effect of stopping
Time Switch	You cannot perform maintenance administration on the timeswitch.
Multimedia Channel	Takes the selected Multimedia Channel out of service.
Channels	Takes the selected DS30X channel out of service.
DS30X link	Takes the selected DS30X link out of service.

To start or stop a component

1. Run CallPilot Manager and login.
2. In CallPilot Manager, click Maintenance → Maintenance Admin.

   Result: The Maintenance screen appears.
3. Click the plus sign (+) beside the CallPilot server to expand the component tree.
4. Continue clicking the plus sign (+) until the component with which you want to work is visible.
5. Click the hardware component that you want to start or stop.

   Result: The Maintenance screen refreshes to show details about the component.
6. Scroll down to the Maintenance section.
7. Click Courtesy Stop, Stop, or Start, as required.

Button	Description
Start	If the selected component is out of service, click this button to put it into service.

Button	Description
Courtesy Stop	Click this button to take the selected component out of service. CallPilot waits for the call to be completed before disabling the component. **ATTENTION** If you are courtesy stopping all components (that is, you are taking the entire system down), ensure that you inform all administrators, desktop messaging users, and web messaging users so that they can log off their sessions before you proceed. The system asks you to confirm the courtesy stop. If you click OK, the component is put out of service after all calls are finished.
Stop	Click this button to take the selected component out of service immediately. All calls that are in progress are disconnected immediately. **ATTENTION** If you are stopping all components (that is, you are taking the entire system down), ensure that you inform all administrators, desktop messaging users, and web messaging users so that they can log off their sessions before you proceed.

Running integrated diagnostics

Introduction

You should run diagnostic tests from the Diagnostics section on the Maintenance screen in the following circumstances:

- You want to ensure that a component is operating properly after installing or reinstalling it.
- The CallPilot server is having trouble processing incoming calls and you are hoping that diagnostic results can tell you why.

  Problems include static, dropped calls, and cross talk (hearing another conversation).

Before you begin

ATTENTION

Take the component out of service before you run the diagnostic test. See "Starting and stopping components" on page 68.

Components that have diagnostic tests available

The following table identifies the components on which you can run diagnostics:

Component	Diagnostics available?	Replaceable?
Media Bus	No	No
MPB96 board	Yes	Yes
Time Switch	No	No

Component	Diagnostics available?	Replaceable?
Multimedia Channels	Yes	No
Channels	No	No
DS30X link (cable)	Yes	Yes

Diagnostic tests available for each component

The diagnostic tests that are available for each component are listed in the Diagnostic section of the Maintenance screen. To view the list of diagnostic tests for a particular component, click the component in the component tree.

If a diagnostic test fails or cannot be run

If a warning message appears, the diagnostic test cannot be run because a prerequisite condition has not been met. If a diagnostic test fails, a message appears in a new browser window (see the example on screen 74).

In both cases, check the Alarm Monitor to determine the reason and the appropriate action to take.

If the Alarm Monitor and Event Browser do not provide a solution to a hardware problem, you may need to replace or service a component. If the problem is with a component that is not replaceable because it is not a physical entity (such as the Time Switch), you must either replace its parent component or contact your Nortel Networks technical support representative, depending on the component.

To run a diagnostic test

ATTENTION

Nortel Networks recommends that you courtesy stop rather than stop a component if possible. For instructions, see "Starting and stopping components" on page 68.

1. Run CallPilot Manager and login.
2. In CallPilot Manager, click Maintenance → Maintenance Admin.

   Result: The Maintenance screen appears.
3. Click the plus sign (+) beside the CallPilot server to expand the component tree.
4. Continue clicking the plus sign (+) until the component with which you want to work is visible.
5. Click the hardware component for which you want to run diagnostics.

   Result: The Maintenance screen refreshes to show details about the component.
6. Scroll down to the Maintenance section, and ensure that the component is out of service.
7. Scroll down to the Diagnostics section.
8. Check the check box for each diagnostic that you want to run.

   Note: If you want to run all of the diagnostics, check the Diagnostic Description check box at the top of the list.
9. Click Run.

   Result: A new web browser window opens to display the progress and results of the diagnostics.

   Note: The Diagnostic Results box in the Diagnostics section displays diagnostic results when you click Get Last Result.

Viewing the last diagnostic results

Introduction

You can review the results of diagnostics by clicking the Get Last Results button for a component.

To view the last diagnostics result

ATTENTION

Nortel Networks recommends that you courtesy stop rather than stop a component if possible. For instructions, see "Starting and stopping components" on page 68.

1. Run CallPilot Manager and login.
2. In CallPilot Manager, click Maintenance → Maintenance Admin.

   Result: The Maintenance screen appears.
3. Click the plus sign (+) beside the CallPilot server to expand the component tree.
4. Continue clicking the plus sign (+) until the component with which you want to work is visible.
5. Click the hardware component for which you want to run diagnostics.

   Result: The Maintenance screen refreshes to show details about the component.
6. Scroll down to the Diagnostics section.
7. Check the check box for each diagnostic for which you want to review results.

8 Click Get Last Result.

Result: The results appear in the Diagnostic Results box with the following information:
- diagnostic title
- diagnostic result: pass or fail
- the date and time the test was completed

Working with the Multimedia Monitor

Introduction

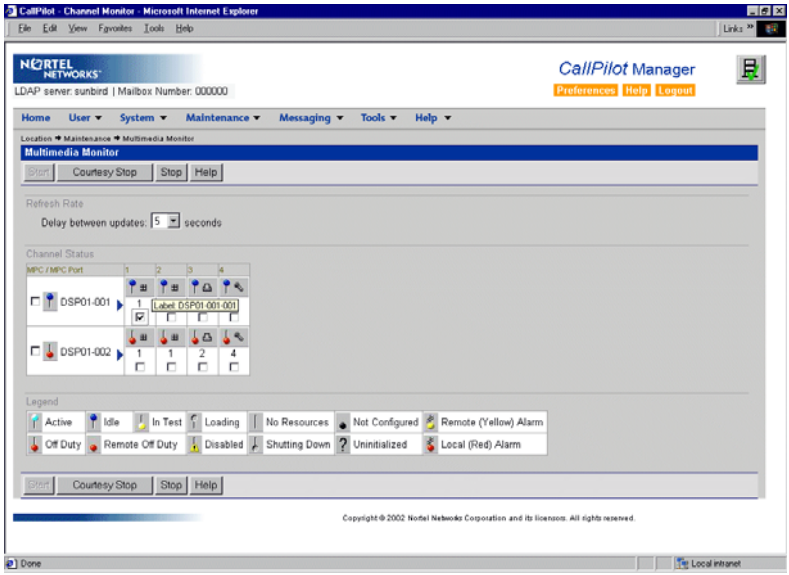
The Multimedia Monitor shows the status of multimedia channels. The multimedia channels are the DSP ports that process the calls. They are the voice, fax, and speech recognition channels.

To view or work with multimedia channel states

1 Run CallPilot Manager and login.

2 In CallPilot Manager, click Maintenance → Multimedia Monitor.

Result: The Multimedia Monitor screen appears, showing the channels associated with each DSP.



Note: For an explanation of the channel states, refer to the CallPilot Manager online Help.

3 Do one of the following:

IF you want to stop or start	THEN
all of the channels associated with a DSP	check the check box to the left of the DSP that you want to stop or start. Repeat this step for each DSP.
only one or several channels that are associated with a DSP	check the check box for each channel that you want to stop or start.

4 Click Courtesy Stop, Stop, or Start as required.

Result: If you clicked Courtesy Stop or Stop, you are asked to confirm the Courtesy Stop or Stop. Click OK.

The selected channels change to off-duty or on-duty status, according to the action you chose.

Note: If the buttons are not available, wait a few seconds for the screen to refresh.

Working with the Channel Monitor

Introduction

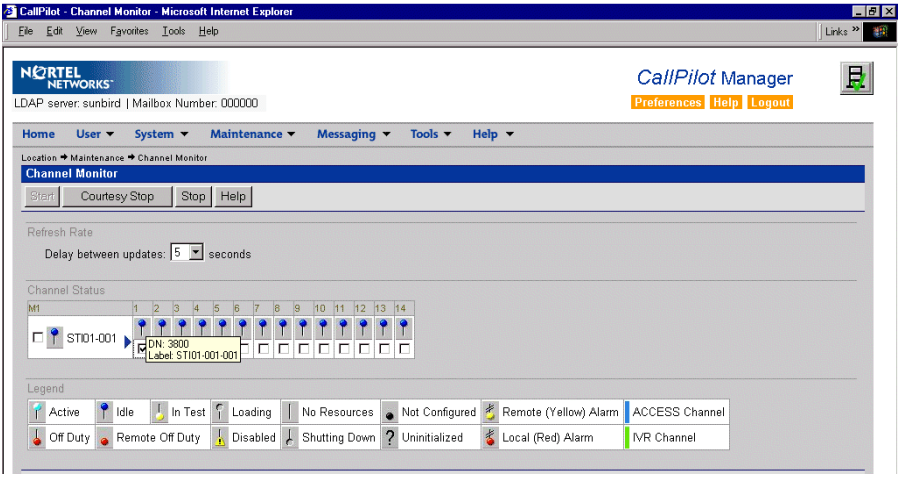
The Channel Monitor shows the status of call channels. The call channels are the connections between the server and the switch that carry the call signals to CallPilot.

To view or work with call channel states

1 Run CallPilot Manager and login.

2 In CallPilot Manager, click Maintenance → Channel Monitor.

Result: The Channel Monitor screen appears, showing the DS30X (also known as DS0) channels associated with each DS30X link.



Note: For an explanation of the channel states, refer to the CallPilot Manager online Help.

3 Do one of the following:

IF you want to stop or start	THEN
all of the channels associated with a DS30X link	check the check box to the left of the DS30X link that you want to stop or start. Repeat this step for each DS30X link.
only one or several channels that are associated with a DS30X link	check the check box for each channel that you want to stop or start.

4 Click Courtesy Stop, Stop, or Start, as required.

Result: If you clicked Courtesy Stop or Stop, you are asked to confirm the Courtesy Stop or Stop. Click OK.

The selected channels change to off-duty or on-duty status, according to the action you chose.

Note: If the buttons are not available, wait a few seconds for the screen to refresh.

Chapter 6

Using CallPilot system utilities

In this chapter

Overview 82

Diagnostics Tool 83

PEP Maintenance utility 84

Session Trace 85

System Monitor 87

Overview

Introduction

The following table lists the CallPilot system utilities:

Utility	Description
Diagnostics Tool	Allows CallPilot startup diagnostics to be enabled or disabled (turned on or off).
PEP Maintenance	Displays a list of installed PEPs and enables PEP uninstall.
Session Trace	The Session Trace tool displays detailed information about the activity in a user's mailbox and the state of the message waiting indicator (MWI).
System Monitor	Displays the following information: ■ the status of all CallPilot channels ■ the status of all CallPilot services **Note:** This status is more accurate than the status that Windows provides in the Services control panel. ■ particulars about the CallPilot System, such as names, keycodes, serial numbers, IP addresses, and system numbers

Accessing the system utilities

All CallPilot utilities are accessible from the CallPilot server in the Start → Programs → CallPilot → System Utilities menu.

Diagnostics Tool

Introduction

The Diagnostics Tool allows you to enable or disable CallPilot startup diagnostics. CallPilot startup diagnostics automatically identify hardware problems that may exist when the system and its services are started. When you disable startup diagnostics, you can save time during system maintenance operations where restarts or call processing services restarts are required. There are three recommended steps:

- Use the Diagnostics Tool to turn off CallPilot startup diagnostics.
- Perform system maintenance.
- Use the Diagnostics Tool to turn on CallPilot startup diagnostics.

To access the Diagnostics Tool

On the Windows desktop, click Start → Programs → CallPilot → System Utilities → Diagnostic Tool.

Result: The Diagnostics Tool window appears.

To enable startup diagnostics

From the Diagnostics Tool window, select Configuration → Maintenance Startup Diag → Enable.

To disable startup diagnostics

ATTENTION

Nortel Networks recommends that you leave the startup diagnostics turned on. When you disable CallPilot startup diagnostics, you prevent CallPilot from automatically identifying hardware problems that may exist when the system and its services are started (DSP, TimeSwitch, MediaBus).

On the Diagnostics Tool window, select Configuration → Maintenance Startup Diag → Disable.

PEP Maintenance utility

Introduction

The PEP Maintenance utility displays a list of all installed PEPs on the server and enables you to uninstall PEPS. For information on installing or uninstalling PEPs, refer to the *Installation and Configuration Task List* (555-7101-210).

To access the PEP Maintenance utility

From the Windows desktop, click Start → Programs → CallPilot → System Utilities → PEP Maintenance Utility.

Result: The DMI Viewer window appears.

To view a list of all installed PEPs

1. Click the component for which you want to display the PEP list.
2. Click Show PEPs.

   Result: A list of all installed PEPs appears in the left pane.
3. If you want to review the readme file associated with a PEP, click the PEP, and then click Read.

   Result: The readme file opens in Notepad.

Session Trace

Introduction

The Session Trace tool displays detailed information about the activity in a user's mailbox and the state of the message waiting indicator (MWI). The session information includes

- voice messaging
- call answering
- express messaging activity (messages composed and sent, or left in a mailbox)
- the number of messages played or unplayed at the beginning, middle, and end of a session
- messages and personal distribution lists restored into a mailbox
- the last change to the MWI (turned on or off, or untouched)

This session information allows an administrator or technician to study the state of a user's mailbox and the MWI, and to use that information to follow up on any user complaints. For example, a user may complain that the MWI was on, but no voice messages were in the mailbox when the user logged on. The session information can tell the administrator why the MWI was turned on.

To access the session trace tool

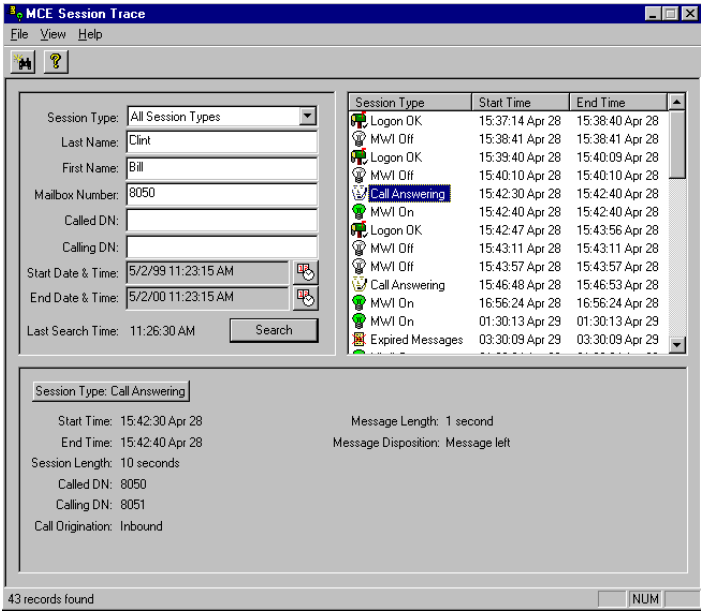
From the Windows desktop, click Start → Programs → CallPilot → System Utilities → Session Trace Tool.

Result: The MCE Session Trace window appears.

To find a session

1. From the Session Type drop-down menu, choose the type of session. To display a list of all session types, select All Session Types.
2. Enter as much information in the search criteria boxes to identify the session you want to view. To display a list of all users for the selected Session Type, leave the search criteria boxes blank.
3. Click Search to initiate the search.
   a. If you did not enter any user information, a list of users matching the Session Type appears at the bottom of the window. To select a user from the list, double-click the user name to display session type information.
   b. If you selected All Session Types for a user, the session type information appears to the right of the window.
4. Double-click the session type to display the session information.

   Result: The Session Type information appears at the bottom of the window. The following example shows Call Answering session type information.



System Monitor

Introduction

The System Monitor consists of three tabs, as described in the following table:

Tab	Description
Channel Monitor	Shows the status of all CallPilot services, multimedia channels, and call channels (DS30X channels).
System Info	Displays particulars about the CallPilot System, such as features purchased, keycode, serial number, and CallPilot server IP addresses.
Legend/Help	Provides a description of icons and terminology displayed in the System Monitor window.

System Monitor is a nondestructive tool that does not alter the behavior of any CallPilot components.

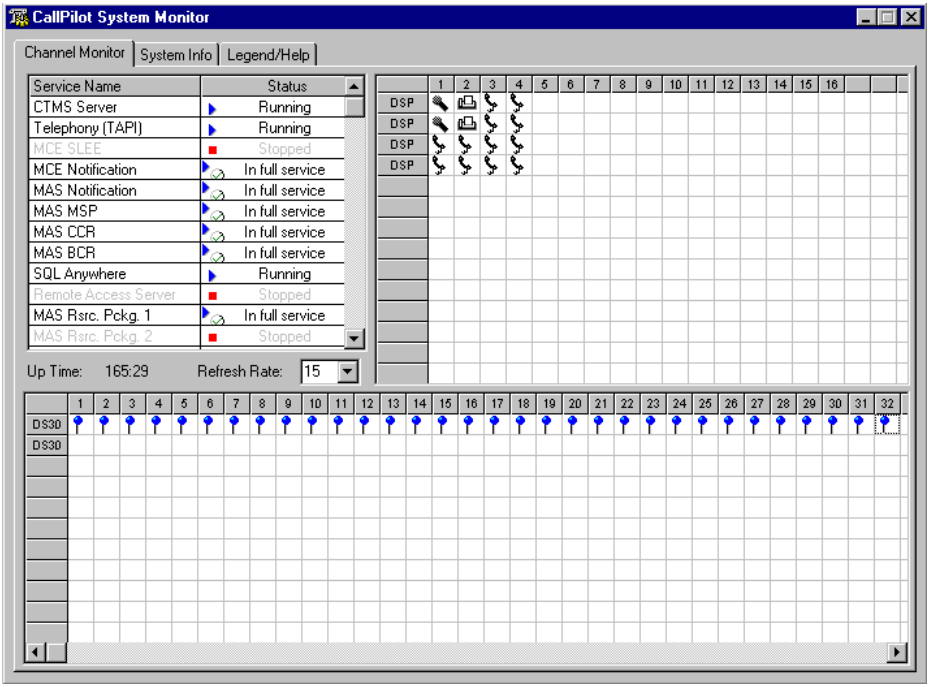
To access the System Monitor

On the Windows desktop, click Start → Programs → CallPilot → System Utilities → System Monitor.

Result: The CallPilot System Monitor window appears. By default, the Channel Monitor tab appears on top. Click the other tabs to view the information on those tabs.

About the Channel Monitor tab

The following is an example of the Channel Monitor tab, followed by a description of its contents:



CallPilot services

The Service Name pane shows the status of services from a CallPilot perspective. The status shown in the Windows Services control panel may state that a service is running, but it may not actually be fully running or in service from a CallPilot perspective. Refer to the System Monitor tool Channel Monitor tab for the true status.

The services listed under Service Name should be either running or in full service when CallPilot is functioning optimally. If any CallPilot services are stopped, investigate the cause of this. Call Nortel Networks technical support for assistance.

Note: While any stopped services should be investigated, some services are not critical. CallPilot may continue to handle call processing even with some services stopped.

The critical services that are needed for basic CallPilot call answering are listed in the following table. For your reference, the equivalent names as they appear in the Windows Control Panel are also listed.

CallPilot System Monitor	Windows Control Panel equivalent
CTMS Service	CTMS Server
Telephony (TAPI)	Telephony Service
MCE SLEE	CallPilot SLEE Service
MCE Notification	CallPilot MWI Service
MAS Notification	CallPilot Notification Service
MAS CCR	CallPilot Call Channel Router
MAS BCR	CallPilot Blue Call Router
SQL Anywhere	Adaptive Server Anywhere - %ComputerName%_SQLANY
MAS MltmediaCache	CallPilot Multimedia Cache
MAS MltmediaVol1	CallPilot Multimedia Volume 1
MAS MltmediaVol102 (TRP only)	CallPilot Multimedia Volume 102 (TRP only)
MAS MltmediaVol103 (TRP only)	CallPilot Multimedia Volume 103 (TRP only)
MAS Rsrc. Pckg. 1	CallPilot Resource Package1

DSPs

In the DSP pane, each DSP is represented in a separate row. Each box in the row is one DSP channel or multimedia channel. Click the Legend/Help tab to view descriptions of the multimedia channel icons.

For tower and rackmount CallPilot servers, DSPs reside in MPB96 and MPB16-4 boards and MPC-8 cards. For 1002rp servers, DSPs are distributed as follows:

- MPB96 board has 12 DSP sections embedded on board
- One MPB16-4 board consists of two embedded DSPs and up to four MPC-8 cards.
- Each MPC-8 card contains a single DSP.

DS30X links

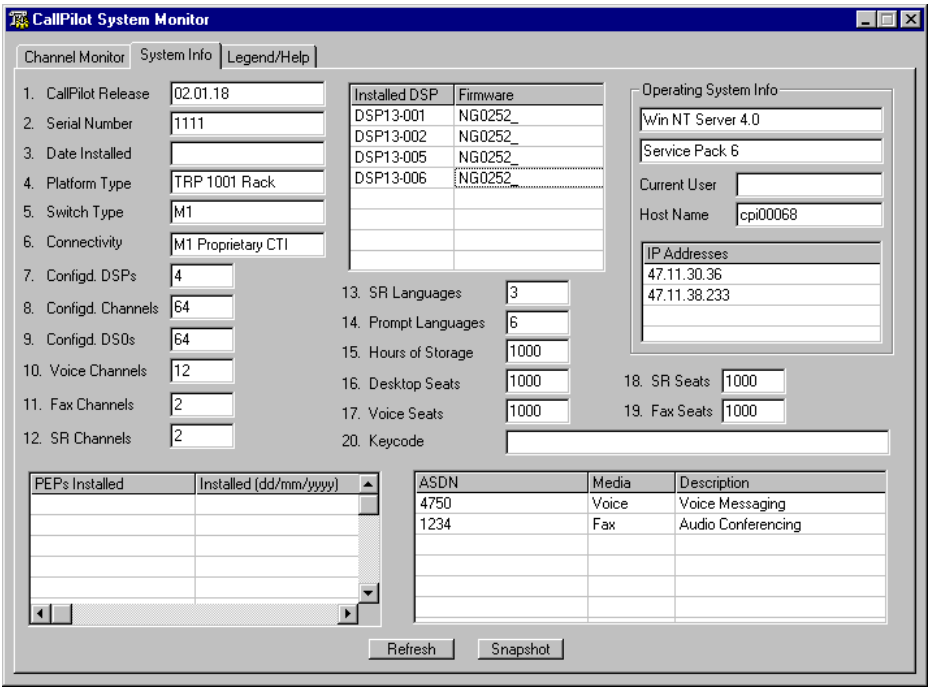
In the DS30X link pane, each DS30 row represents a separate DS30X link (also referred to as a DS30 link). Each box in the row represents one DS30X channel.

The DS30X links connect the CallPilot server to the MGate card (NTRB18CA) in the Meridian 1 switch or Succession 1000 system.

For the 1002rp server, the DS30X link to the switch is supported by the connection of the server to the switch backplane.

About the System Info tab

The following is an example of the System Info tab, followed by a description of its contents:

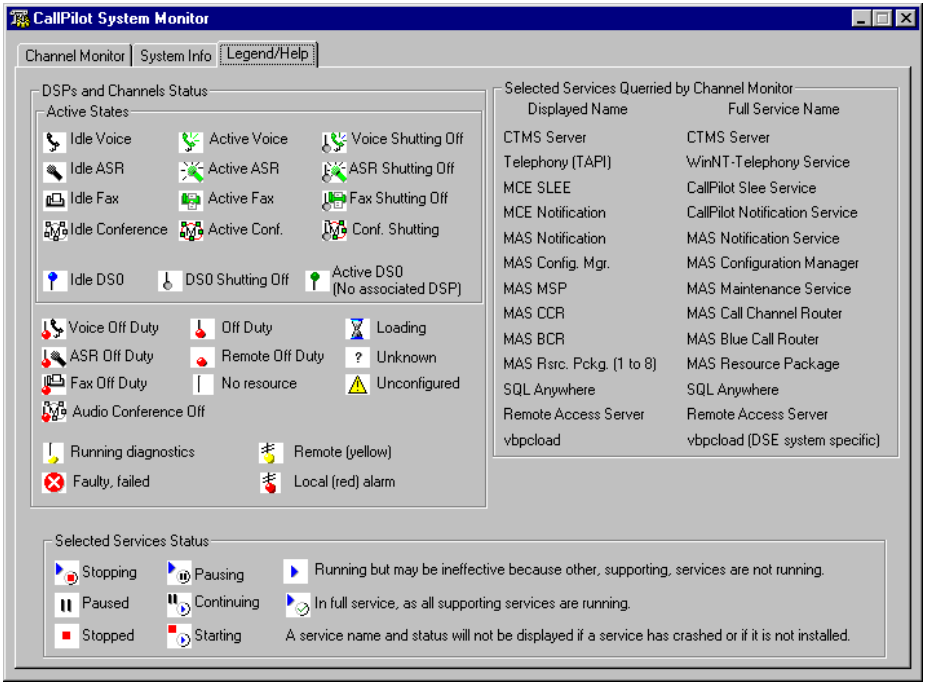


The numbered items provide information about the features purchased. Information about the underlying operating system is provided in the top right corner, including the server IP addresses.

PEP information and configured Service DNs are listed in the bottom part of the window.

About the Legend/Help tab

The following is an example of the Legend/Help tab. Consult this window for descriptions of the icons found in the Channel Monitor tab:



Chapter 7

Replacing basic chassis components

In this chapter

Removing the front bezel and server cover 94
Replacing air filters 98
Replacing the power supply 99
Replacing the cooling fan 102
Replacing the fuse (AC system only) 105
Replacing the alarm board 107
Setting jumpers on the alarm board 109
Replacing the status display panel 111

Removing the front bezel and server cover

Introduction

If the maintenance task requires replacing front panel components, you must remove the front bezel. The exception is the hard drives, which can be accessed by simply unlocking and opening the front bezel doors.

If you require access to the server interior, remove both the front bezel and the server cover.

Requirements

Before removing the front bezel and server cover, gather the following tools:

- the customer's chassis keys for the front bezel doors
- flat-blade screwdriver
- antistatic wrist strap

About the front bezel doors

Two locked doors on the front of the server cover the front panel, including the CD-ROM drive and tape drive.

These doors are part of the front bezel. You must unlock the front panel doors before you can remove the front bezel.

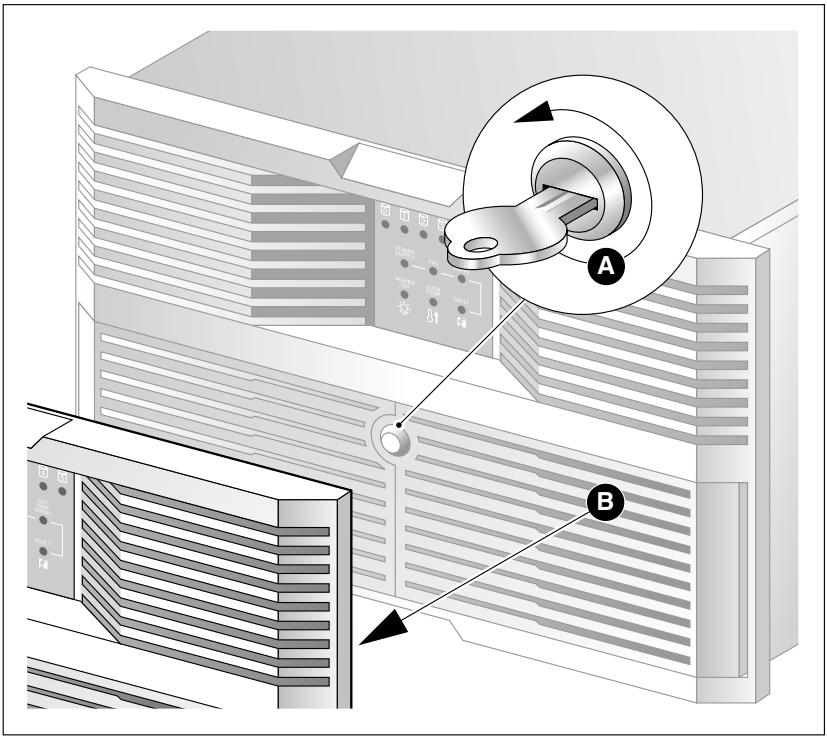
To remove the front bezel

CAUTION

Risk of equipment damage

Do not attempt to move or lift the server before you have removed the front bezel. If the front bezel is attached, the server can disengage from the front bezel and fall.

1. Unlock and open the double doors of the front bezel. See A in the following diagram.
2. Firmly grasp the front bezel by the hand-holds on either side of the chassis, and pull the front bezel from the chassis.



G101733

To remove the server cover



DANGER

Risk of electric shock

High current inside the chassis can cause severe injury.



CAUTION

Risk of equipment damage

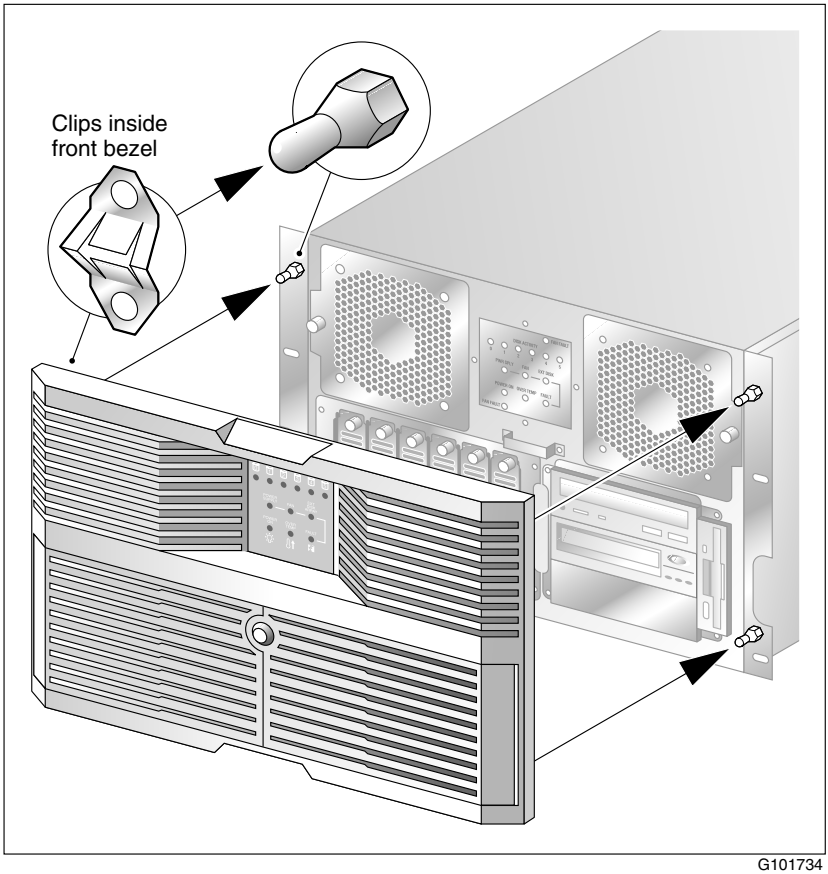
Take precautions to protect internal components. Electrostatic discharge (ESD) can damage boards and make them unusable. Wear an ESD wrist strap.

1. Remove the front bezel.
2. Power down the server and disconnect all power cords.
3. Loosen the three thumbscrews at the rear of the top cover.
4. Remove the server cover by pulling the cover toward the rear of the chassis, and then lifting it up and off.
5. Clip the lead from your ESD wrist strap to an unpainted metal section of the chassis.

To replace the front bezel after maintenance is complete

When the CallPilot server maintenance is complete, replace the front bezel.

1 Align the front bezel with the ball studs located at each faceplate corner. See the following diagram:



2 Apply pressure evenly until the bezel snaps onto each ball stud.

3 Close and lock the double doors of the front bezel.

Replacing air filters

Introduction

To ensure your server cools and functions properly, remove and clean air filters every six months in clean environments and every three months in industrial or dirty environments. If they appear to be damaged or become inefficient, replace the filters. There are four air filters on the 1002rp server—one inside each of the two doors of the front bezel, and two on the top half of the front bezel. They are made of polyester foam material and are flame retardant.

Requirements

You require the customer's chassis keys for the front bezel.

To replace the front bezel air filter

1. Remove the front bezel from the chassis. See "To remove the front bezel" on page 95.
2. Pull the filters away from the Velcro strips that secure them to the bezel.
3. Replace the filter by seating the new filter pads evenly over the Velcro strips and securing them.
4. Install and lock the front bezel on the chassis.

To replace the door air filter

1. Unlock and open the front doors.
2. The air filter is trapped between the inside of the door and the wire. The wire pivots near the key lock. Pull the wire away from the key lock to free the air filter.
3. Remove and replace the air filter.
4. Pivot the wire to trap the filter, ensuring that the ends of the wires are pinched inside the door.
5. Close and lock the doors.

Replacing the power supply

Introduction

The power supply is hot-swappable. This means that you can replace the power supply without powering down the server.

Requirements

Before hot-swapping a power supply, gather the following tools:

- one flat-blade screwdriver
- one Phillips screwdriver
- one antistatic wrist strap
- the replacement power supply

When to hot-swap the power supply

A green LED indicates that the power supply is working properly. If the green LED on the power supply module is unlit or red, the module is failing or has failed. Other indicators of failure are the alarm that sounds and the power supply module LED on status display that turns red.

To hot-swap a power supply

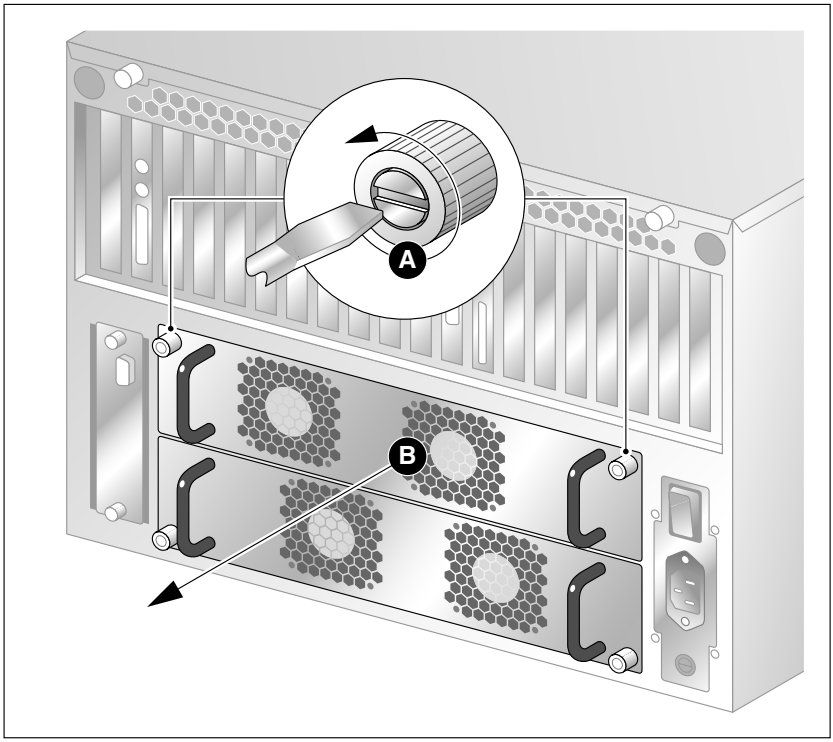
DANGER

Risk of electric shock

High current inside the chassis can cause severe injury.

1 Loosen the thumbscrews at the top right and left of the failed power supply module (see A in the following diagram).

If needed, use a flat-blade screwdriver. The thumbscrew must rotate freely and not contact the chassis threads.



2 Grasp the molded horizontal handles on the power supply module and pull the power supply module free from the chassis (see B in the preceding diagram).

3 Align the replacement module with the empty chassis bay.

4 Slide the replacement power supply module into the bay until the module is secured by its connector. Use some force, if necessary.

5 Secure the power supply module to the chassis with two thumbscrews at the corners of the power supply faceplate.

Result: The power supply LED illuminates green.

Note: If the LED does not illuminate, remove and reinstall the power supply with more force. If this does not work, contact your Nortel Networks customer support representative.

Replacing the cooling fan

Introduction

The cooling fan is hot-swappable, so you can replace the cooling fan without powering down the server.

When to hot-swap the cooling fan

When the LED associated with a cooling fan turns red, the fan requires replacement.



CAUTION

Risk of equipment damage

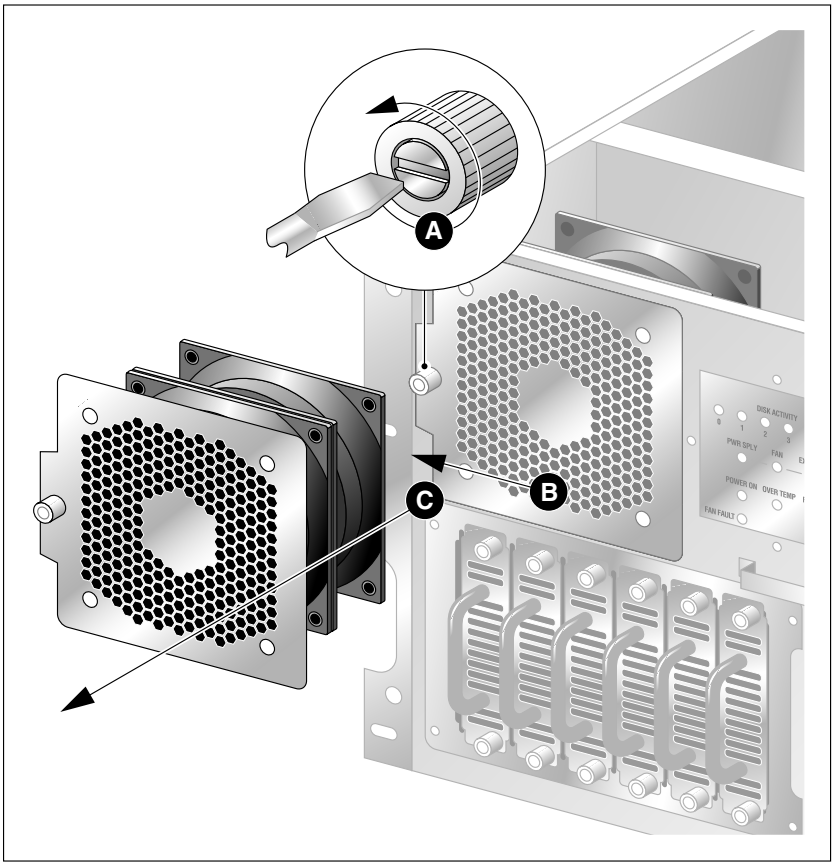
Use an ESD wrist strap to protect static-sensitive components.

To hot-swap a cooling fan

1. Remove the front bezel.
2. Use the front panel display LED to locate the defective fan.

3 Loosen the thumbscrew located on the outside of the failed cooling fan module (see A in the following diagram).

If needed, use a flat-blade screwdriver. The thumbscrew must rotate freely and not contact the chassis threads.



G101728

4 Unseat the cooling fan module by sliding the module horizontally away from the display and toward the rack rail (see B in the preceding diagram).

Result: The module power connector unseats from the power connector located behind the display and LEDs.

5 Slide the failed cooling fan module out of the chassis (see C in the preceding diagram).

6 Align the replacement cooling fan module tabs with the four support slots on the chassis.

Ensure that the module is oriented with the thumbscrew, and insert the tabs into the supporting slots of the chassis.

7 Slide the cooling fan module toward the front panel display and into position.

Result: The fan module connects with slight resistance. The fans rotate and pull air into the chassis. The cooling fan LED goes out.

8 Tighten the module thumbscrew and replace the front bezel.

Replacing the fuse (AC system only)

Introduction

The fuse is located below the power input socket on the rear panel. When the server fuse blows, the server stops operating.



CAUTION

Risk of equipment damage and personal injury

Disconnect power from the server before replacing a fuse.

Requirements

You require the following:

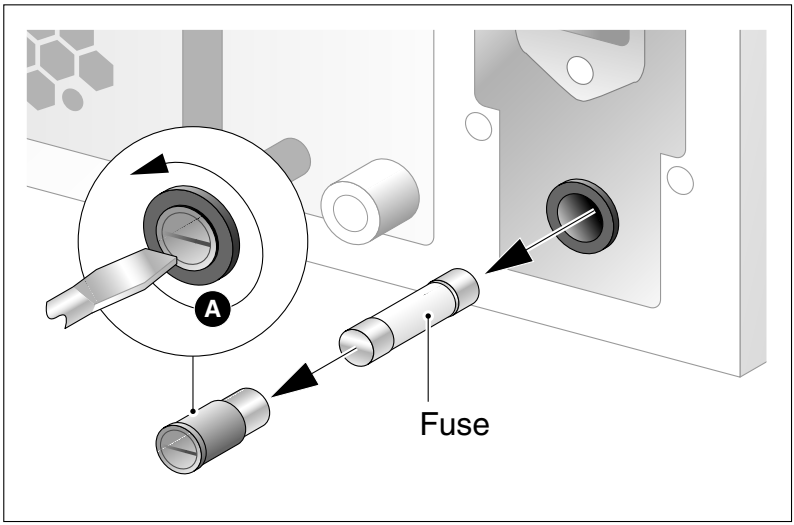
- an approved fuse for replacement

  Two different types of fuses exist: one for North America, and one for international use. Ensure that the fuse you are replacing has been approved by Nortel Networks for your region.
- flat-blade screwdriver

To replace the fuse

1. Power off the server.
2. Unplug the power cable from the wall outlet.
3. Unplug the power cable from the power input socket on the server.

4 Unscrew the fuse receptacle (see A in the following diagram).



5 Slide the fuse receptacle out of the fuse chamber.

Note: Observe how the blown fuse is positioned in the receptacle.

6 Remove the blown fuse from the fuse receptacle.

7 Install the approved replacement fuse. Use a flat-blade screwdriver to screw in the fuse receptacle with a push and 1/4 clockwise turn.

8 Slide the fuse receptacle back into its chamber.

9 Fasten the fuse receptacle with a flat-blade screwdriver.

10 Plug the power cable back into the power input socket on the server.

11 Plug the power cable into the wall outlet.

12 Power on the server.

ATTENTION

If the fuse blows after replacement, swap one power supply module with the other. If this does not work, call your Nortel Networks customer support representative.

Replacing the alarm board

Introduction

The 1002rp server alarm board and status panel are used to monitor and indicate the server status. The basic hardware check on page 17 fails if the board is defective or damaged. When these units are damaged, replace them immediately.



CAUTION

Risk of equipment damage

Take precautions to protect computer boards. ESD can damage boards and make them unusable. Wear an ESD wrist strap.

Requirements

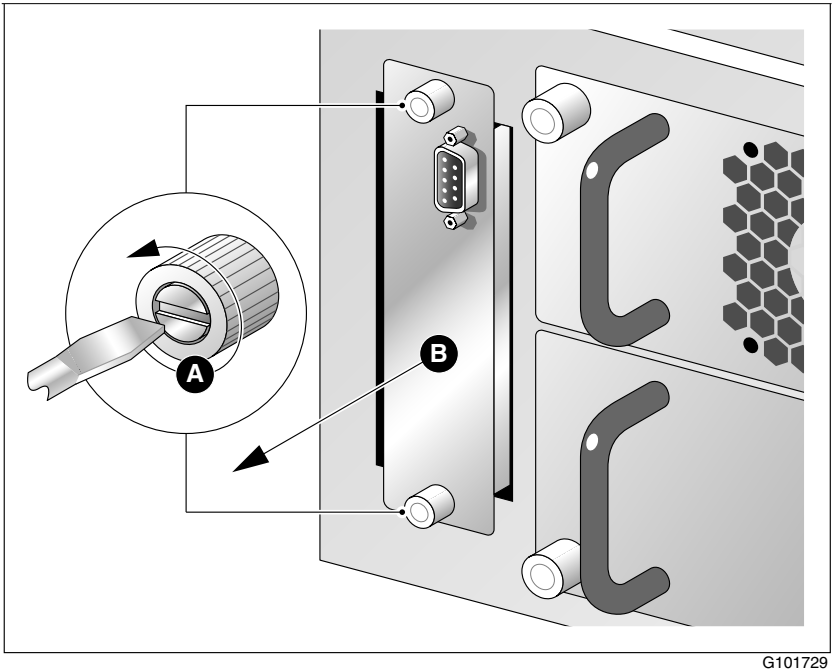
Before replacing the alarm board or panel display, gather the following tools:

- a Phillips screwdriver
- an antistatic wrist strap
- the replacement component(s)

To replace the alarm board

1. Power off the server.
2. Loosen the two thumbscrews securing the faceplate to the left of the 1002rp server power supply modules (see A in the following diagram).

   If needed, use a flat-blade screwdriver. The thumbscrew must rotate freely and not contact the chassis threads.



G101729

3. Pull the carrier free from the chassis (see B in the preceding diagram).
4. The alarm board is secured to the carrier by two Phillips-head screws. Remove the defective alarm board from the carrier.
5. Secure the replacement alarm board to the carrier using two Phillips-head screws.
6. Align the carrier with the chassis and slide the board into the chassis.

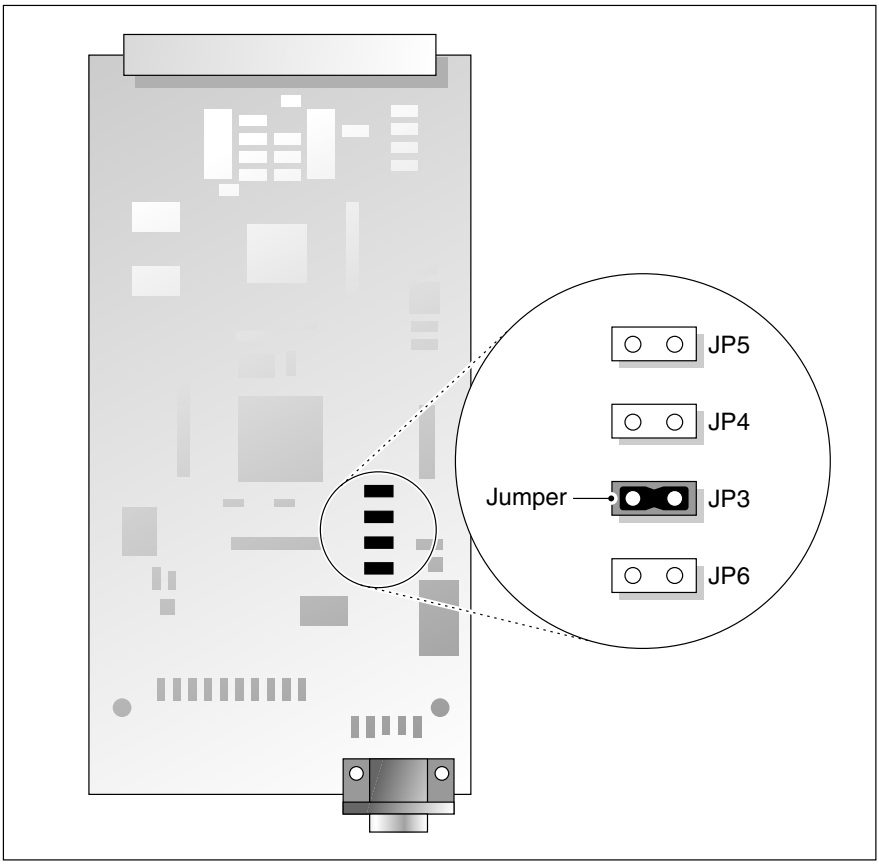
   Note: The card encounters some resistance as it meets the connector.
7. Tighten the thumbscrews to secure the faceplate to the chassis.

Setting jumpers on the alarm board

Introduction

The jumpers on the alarm board enable or disable sensing and display functions. This section describes the features that are enabled or disabled by setting jumpers on the alarm board.

The default and recommended setting is to have only JP3 jumpered (see the following). This setting enables normal sensing and LED display.



Jumper descriptions

JP6—do not change

Leave the jumper installed on JP6.

JP5—Disarming No Power in the bottom bay

If you are operating with one power supply, you can disable sensing of no power from the bottom power supply. To do this, install a jumper on jumper block 1, JP5.

Ensure that the functioning power supply is installed in the upper power bay.

JP4

Not used.

JP3—LED display

Install a jumper on jumper block 1, JP3, to configure the alarm board to send alarm signals to the full array of LEDs. This is the default setting and the required setting for normal server operation.

If this jumper is not installed over both pins, the alarm board does not send the correct format of signals to the front panel display.

Replacing the status display panel

Locating the display

The display is located at the front of the chassis and is cabled to the rear of the chassis and the alarm board.

To replace the status display panel



CAUTION

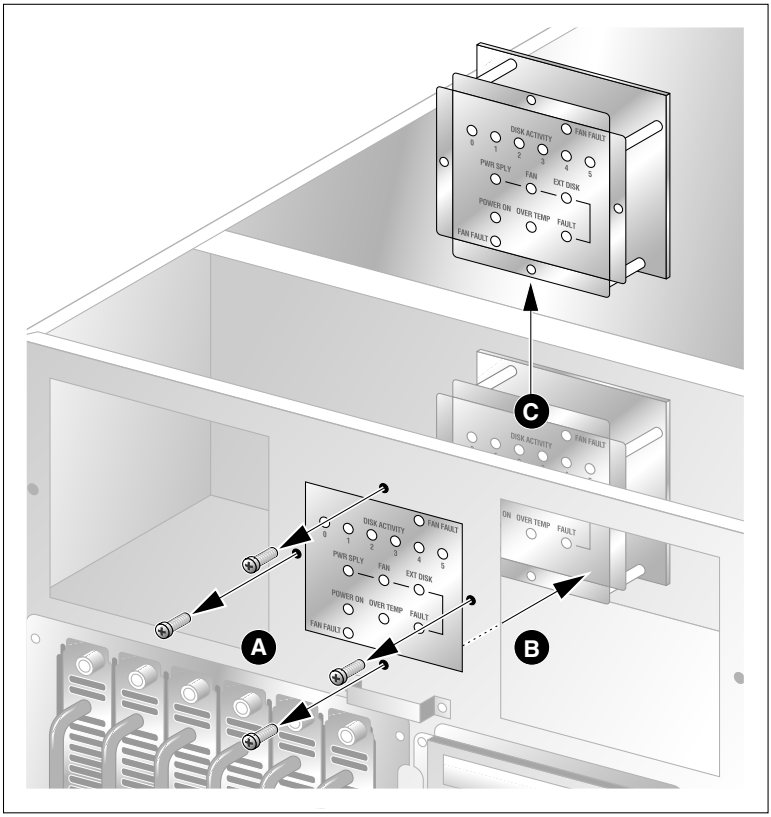
Risk of equipment damage

Use an ESD wrist strap to protect static-sensitive components.

1. Power off the server.
2. Remove the top cover and the front bezel from the chassis.
3. Remove the cooling fans (see “Replacing the cooling fan” on page 102).

   The cooling fans block the access to the status panel.

4 Loosen the four Phillips-head screws that secure the status display panel to the front of the chassis (see A in the following diagram).



G101727

5 Label and remove the 40-pin flat cable from the back of the status display panel.

6 Move the defective status display panel towards the back of the chassis, and then lift it out of the chassis (see B and C in the preceding diagram).

7 Set the replacement status display panel into position, and secure it to the chassis by replacing the Phillips-head screws.

8 Reconnect the cable.

9 Replace the top cover and front bezel.

Chapter 8

Replacing media drives

In this chapter

Replacing a faulty hard drive 114

About the media drive bay 118

Removing the media drive carrier from the chassis 119

Replacing a tape, CD-ROM or floppy drive 123

Installing a tape drive 126

Replacing a faulty hard drive

Introduction

The hard drives are hot-swappable. This means that you can replace a faulty hard drive without powering down the server.

When to hot-swap hard drives

With a RAID controller, hot-swap device drivers, and operating system support, faulty SCA SCSI hard drives can be hot-swapped on the 1002rp server.



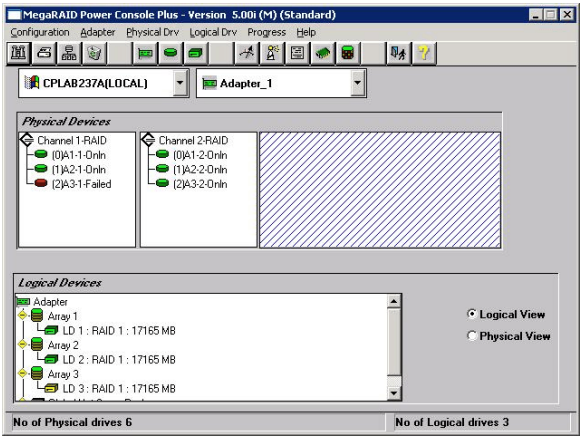
CAUTION

Without the RAID controller, hot-swap device drivers, and operating system support, replacing a drive during server operation can cause a fatal error and force a system restart. If a RAID controller is not installed, shut down the system first and then replace the drives.

Note: Identify which hard drive to remove using the Windows Event Viewer (see “Viewing event logs” on page 25). The appearance of event codes such as 40211(disk access error) or 40218 (error reading or writing multimedia volume) may be an indication of a failing disk drive.

Use the RAID management software to check if any drives are in a failed state.

The following image shows a failed drive highlighted in red with the corresponding logical drive highlighted in yellow (degraded mode).



RAID SCSI hard drive configuration

The following table indicates proper SCSI drive bay, channel, and ID configurations in the hot-swappable drive bay. The SCSI backplane assigns the SCSI IDs as shown in the following table:

Hard drive bay	SCSI channel	SCSI ID	Logical drive label[a]
1 (far left)	0	0	A01-01 (primary hard drive)
2	0	1	A02-01 (primary hard drive)
3	0	2	A03-01 (primary hard drive)
4	1	0	A01-02 (secondary hard drive)
5	1	1	A02-02 (secondary hard drive)
6 (far right)	1	2	A03-02 (secondary hard drive)

a. RAID pairs (logical drives) consist of the following pairs: hard drives 1 and 4, 2 and 5, and 3 and 6. These pairs are represented in the software with the labels A01-01 and A01-02, A02-01 and A02-02, and A03-01 and A03-02, where the first number is the logical drive number (for example, A03) and the second number indicates if it is the primary or secondary hard drive (01 for primary and 02 for secondary).

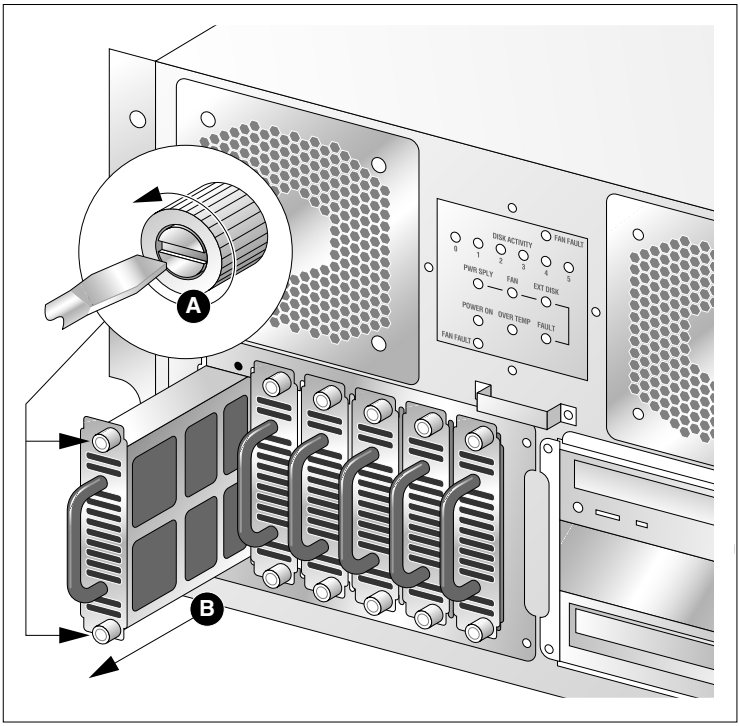
To replace hot-pluggable SCA SCSI hard drives

CAUTION

Risk of equipment damage

Use an ESD wrist strap to protect static-sensitive components.

1. Ensure the new hard drive has the SCSI ID set to 0, termination disabled, and parity checking enabled.
2. Open the front bezel doors.
3. Locate the SCA SCSI drive frame below a cooling fan and beside the media drive.
4. Loosen the two thumbscrews on the carrier of the faulty hard drive, and remove the carrier from the chassis.



G101735

5 Remove the faulty drive by loosening the four Phillips-head screws that secure it to the carrier.

6 Attach the new drive to the carrier by four Phillips-head screws.

7 Align the carrier with the drive frame and slide it into the chassis.

Note: Expect resistance as the carrier and backplane connectors meet.

8 Fasten the two thumbscrews.

9 Close the front bezel and lock it.

About the media drive bay

Overview

Media drive bays contain media devices, including CD-ROM, tape, and floppy drives. If your media drives become damaged or you want to upgrade, you can replace these drives. This section provides procedures for replacing or upgrading any device in the media drive bay.

Procedures

Perform the procedures in the following order to replace media drives:

1. “Removing the media drive carrier from the chassis” on page 119
2. “Replacing a tape, CD-ROM or floppy drive” on page 123

Removing the media drive carrier from the chassis

Introduction

When replacing the media hard drives, the first step is to remove the media drive carrier from the media drive bay.

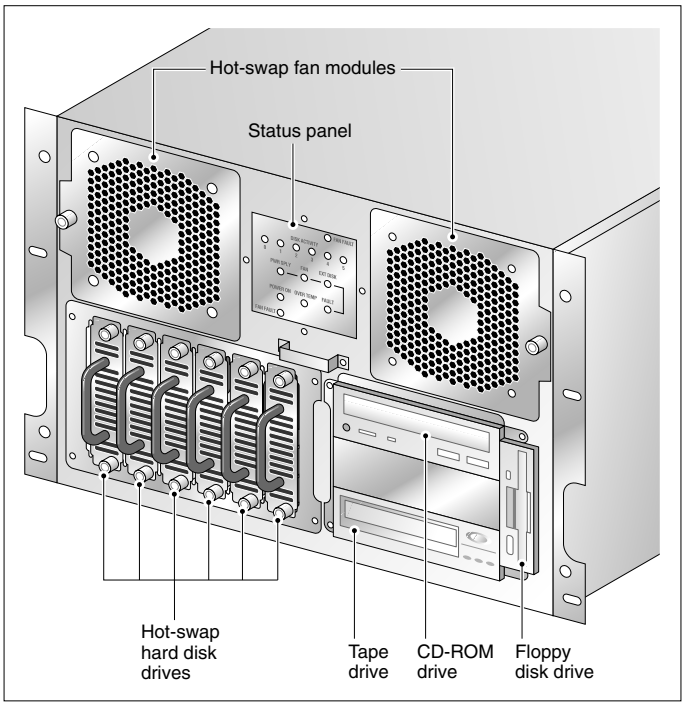
Requirements

To remove the media drive carrier from the media drive bay, you require the following:

- keys for the front bezel doors
- a Phillips screwdriver
- cable identification labels
- a pen or pencil

Locate the media drives

The media drives (CD-ROM drive, tape drive, and floppy drive) are shown in the bottom right corner of the following diagram.



Media drive carrier

The media drives are housed in a media drive carrier that can be removed from the server, as described later in this section. Where no media device is installed, a blank panel is secured to the media drive carrier for protection.

Media drive carrier slot assignment

The carrier is designed to stack three devices horizontally, and to house the floppy drive vertically to the right side of the carrier frame.

To remove the media drive carrier from the chassis



DANGER

Risk of electrocution

High current inside the chassis can cause severe injury.



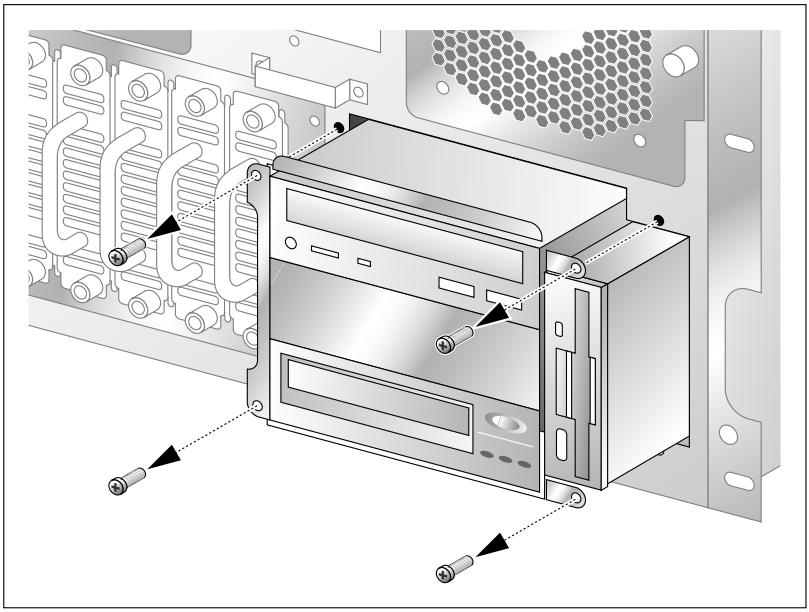
CAUTION

Risk of equipment damage

Electrostatic discharge due to improper handling can cause components to be damaged or rendered unusable.

1 Remove the front bezel from the chassis. See “Removing the front bezel and server cover” on page 94.

2 Locate the media drive carrier, and loosen the four Phillips-head screws and washers securing the carrier to the drive bay, as shown in the following diagram:



G100747

3 Hold cables away from the drive bay as you pull the media drive carrier away from the chassis until the connectors attached behind the components can be reached.



CAUTION

Risk of equipment damage

To avoid damaging cables during this procedure, ensure that no cables are crossed when moving the media drive carrier in and out of the drive bay.

4 Label and disconnect cables from installed media drives, and then free the carrier from the chassis.

Replacing a tape, CD-ROM or floppy drive

Introduction

This section describes how to replace a media drive (tape, CD-ROM, or floppy drive) in the media drive carrier.

To replace a media drive



CAUTION

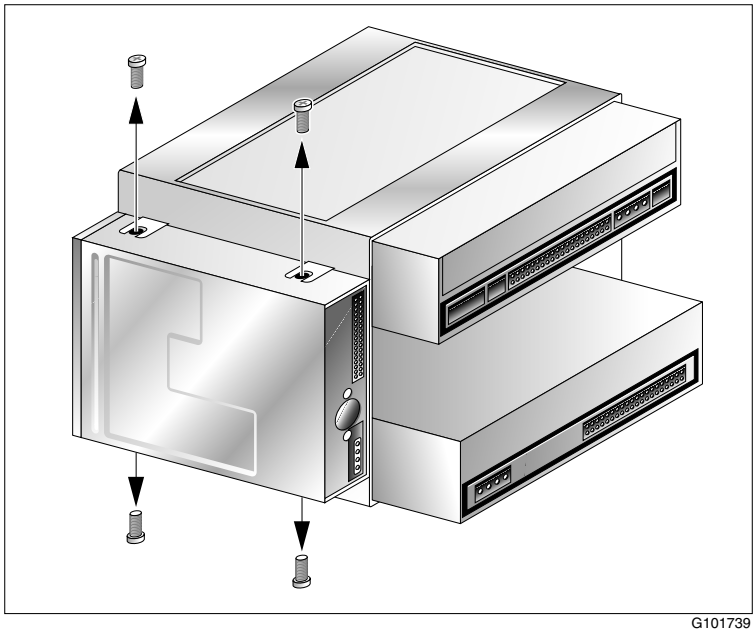
Risk of equipment damage

Use an ESD wrist strap to protect static-sensitive components.

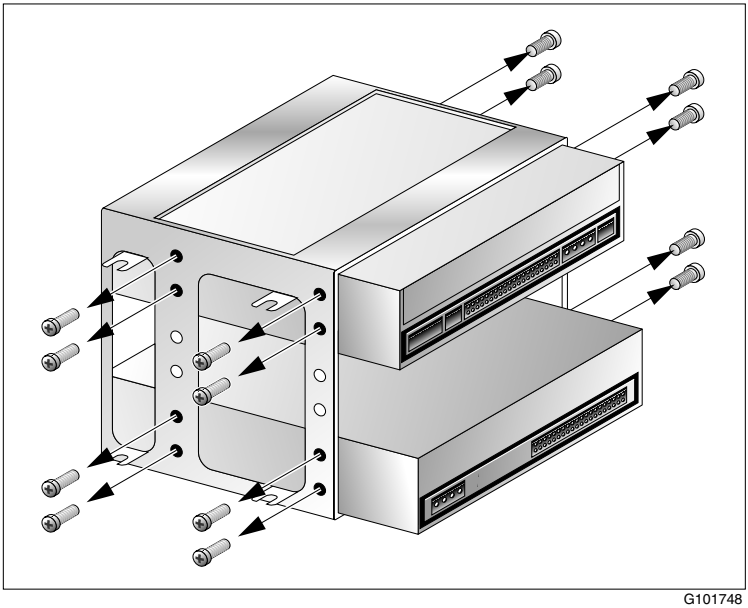
1 Remove the media drive carrier from the chassis (see “Removing the media drive carrier from the chassis” on page 119).

2 Remove the faulty drive from the media drive carrier and save the screws (see the diagrams that follow).

Note: To remove the tape drive or CD-ROM drive, you must first remove the floppy drive.



G101739



G101748

3 If you are installing a tape drive, configure it as described in “To configure the tape drive” on page 127.

4 Slide the new drive into the media drive carrier, and secure it with the screws that were previously removed.

5 Reattach any media drives that you removed to access a specific media drive slot.

6 Position the media drive carrier in the media drive bay, leaving enough room to reach behind the carrier, and attach the connectors.

7 Carefully connect the existing signal and power cables as shown in “Cabling example” on page 126.

Note: If your tape drive is a narrow device, you require a wide-to-narrow adapter to connect to the wide SCSI cable.

8 Slide the carrier into the media drive bay.

Note: Ensure that the cables are free and undamaged.

9 Secure the media drive carrier to the chassis with four Phillips-head screws.

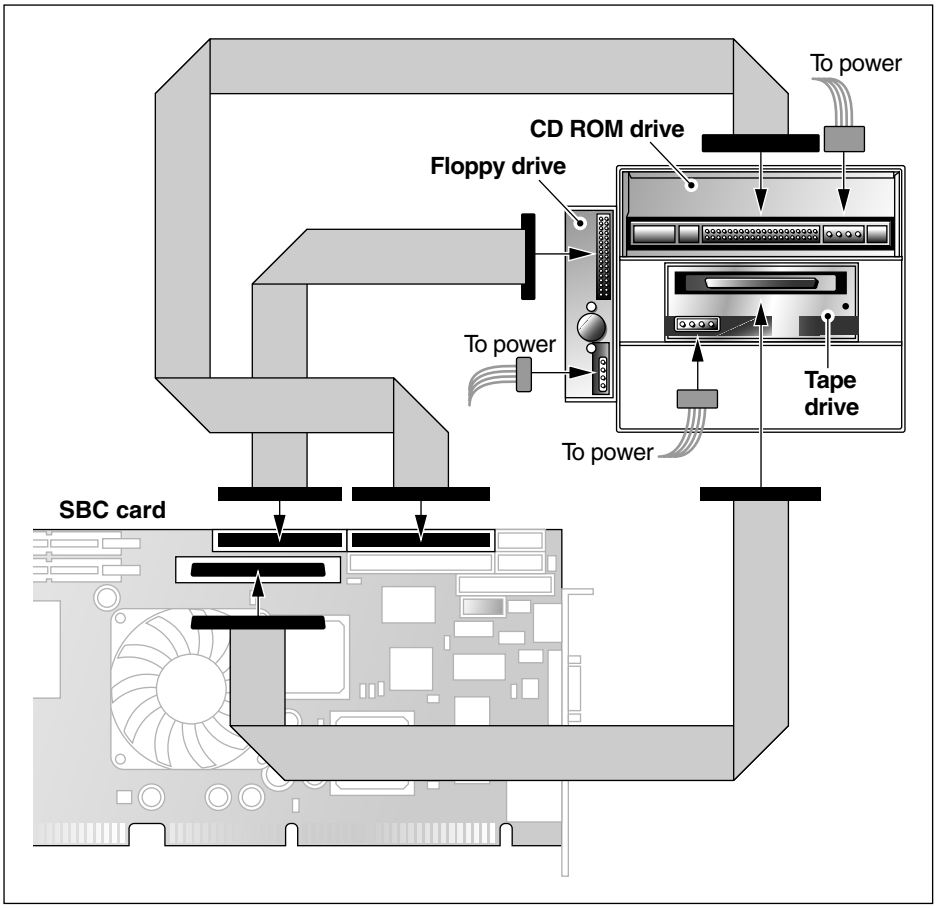
10 Replace and lock the front bezel.

Installing a tape drive

Introduction

This procedure provides instructions for installing a tape drive on a server that currently does not have a tape drive.

Cabling example



G101651

To configure the tape drive

Note: Some settings may already be properly configured. If it is not clear from the drive manufacturer's documentation how to set jumpers, contact your Nortel Networks technical support representative.

1 Set the SCSI ID to 6.

2 Disable the Active Terminators (Term Enable).

Note: Termination is provided by an active SCSI terminator that you connect to the end of the SCSI cable (see "Cabling example" on page 126).

3 Enable Parity Checking.

4 Enable Termination power (TPWR).

5 Leave the remaining settings at the default values.

To install a new tape drive (no tape drive previously installed)



CAUTION

Risk of equipment damage

Use an ESD wrist strap to protect static-sensitive components.

1 Courtesy down CallPilot, and then power down the server.

2 Ensure that the tape drive settings are as described in "To configure the tape drive".

3 Remove the chassis cover.

4 Remove the media drive carrier (see "Removing the media drive carrier from the chassis" on page 119).

5 Slide the new tape drive into the media drive carrier, and secure it with four undercut Phillips-head screws.

Note: You may need to first remove other media drives from the carrier to access the tape drive slot.

6 Reattach any media drives that you removed to access the tape drive slot.

7 Position the media drive carrier in the media drive bay, leaving enough room to reach behind the carrier, and attach the connectors.

8 Carefully connect the existing signal and power cables as shown in “Cabling example” on page 126.

9 Slide the carrier into the media drive bay.

Note: Ensure that the cables are free and undamaged.

10 Secure the media drive carrier to the chassis with four Phillips-head screws.

Result: The tape drive is installed.

11 Replace the chassis cover and front bezel.

12 Power on the server.

Result: The tape drive should be detected by Windows, and the tape drive should be ready to use.

Chapter 9

RAID operations

In this chapter

RAID overview 130

Verifying the RAID firmware 131

Configuring RAID using the LSI Elite1600 controller and Ctrl+M 133

Verifying consistency on the drives 136

RAID splitting 137

Task summary for configuring RAID 141

Task summary for RAID splitting 142

RAID overview

Redundant Array of Independent Disks (RAID) is a technology that can combine two or more drives for fault tolerance and continued system performance. The CallPilot RAID controller is a PCI RAID SCSI card that provides high-performance disk mirroring. CallPilot uses RAID Level 1.

With Level 1 mirroring, two equal-capacity disk drives mirror one another. One disk drive serves as the backup copy of the other disk drive. If one disk drive fails, the other continues to run.

RAID configuring and splitting

Working with RAID involves the following:

- Verifying the RAID LSI Elite 1600 firmware version
- Upgrading or downgrading the RAID firmware
- Configuring RAID using the LSI Elite 1600 controller and the Ctrl+M menu at server bootup
- Ensuring that your system is fully working and the RAID hardware is properly configured
- Performing full data backup
- Performing RAID splitting
- Performing a CallPilot software upgrade
- Performing RAID synching if upgrade successful
- Performing RAID synching if upgrade NOT successful

Verifying the RAID firmware

The minimum requirement for RAID firmware:

- firmware: 111U

To verify the RAID firmware version

To determine what the current RAID firmware version is on the RAID LSI Elite 1600 card do the following:

1. Turn on the server and press Ctrl+M when prompted during system bootup.

   Note: The Ctrl+M utility can take up to 1 minute to launch with 111U firmware. The system may appear frozen. Do not reset.

2. Select Objects menu→ Adapter → Adapter Information.
   Or

   a. Launch the MegaRAID client using: Start > Programs > MegaRAID Client.

   b. From the MegaRAID Power Console Plus - Server Selection window, select Access Mode→Full Access to view or change configuration information and click OK.

   c. From the MegaRAID console, choose Adapter→ Properties.

3. Review the information on the screen. Ensure that Power Console Plus is version 5.00i or later. The LSI Elite 1600 controller firmware should be 111U.

4. If the firmware is not correct, perform a firmware update. For instructions, see “To upgrade or downgrade the RAID firmware” on page 132.

To upgrade or downgrade the RAID firmware

The RAID card's firmware is upgraded through a flash process. The flash process is initiated by running the RAID card firmware update utility on the CallPilot CD-ROM.

ATTENTION

Perform this procedure only if the firmware version is not the version identified in this section.

1. Insert the CallPilot 3.0 rackmount 1002rp Image CD-ROM 1 of 2, into the server CD-ROM drive.
2. Restart the server and observe the startup diagnostics.
3. When the processor diagnostics screen appears, press Esc.

   Result: The following message appears at the bottom of the screen:

   ```
   Entering the boot menu ....
   ```

   The system continues with the SCSI and RAID startup diagnostics, and when done, a menu appears.
4. Choose ATAPI CD-ROM, and press Enter.

   Result: The Startup menu appears.
5. Choose Other Utilities (Firmware, etc.), and then press Enter.

   Result: A menu appears.
6. Choose LSI Elite 1600 RAID card Firmware update, and press Enter.
7. Press Y for yes and then Enter to confirm that the 471gen.rom file is detected.
8. Respond to the remaining prompts to proceed with the update.

   Result: The update proceeds. When it is finished, you are informed that the update completed successfully and you are asked to restart the server.
9. Remove the CD-ROM from the CD-ROM drive.
10. Press Ctrl+Alt+Delete to restart the server.

Configuring RAID using the LSI Elite1600 controller and Ctrl+M

The RAID card's configuration is stored on both the card and on the hard drive, so typically you are not required to reconfigure RAID unless you are making a change to the RAID system (for example, if you replace the hard drives with higher-capacity hard drives).



CAUTION

Risk of data loss

This procedure requires that the logical drive be initialized. When you initialize the logical drive, all data on the hard drives is erased.

Do not perform this procedure unless you are replacing the hard drives, or you are rebuilding the CallPilot system (that is, reinstalling the Windows operating system and CallPilot software).

To configure an LSI Elite 1600 RAID system

To configure RAID, do the following:

1. Turn on the server and press Ctrl+M when prompted during system bootup.

   Note: The Ctrl+M utility can take up to 1 minute to launch with 111U firmware. The system may appear frozen. Do not reset.
2. From the Management menu, select the Objects menu and press Enter.
3. Select the Objects → Adapter and press Enter.
4. Select Adapter → Factory Default.
5. Select Yes to confirm the selection and press Enter.

6 Press Ctrl+Alt+Delete when prompted to restart system.

7 During bootup, press Ctrl+M to re-enter the RAID setup utility.

8 From the Management menu select Objects → Adapter, then ensure the values are set as follows:

Flex RAID Power Fail: **Enabled**
Fast Initialization: **On**
Disk Spinup Timings: **One every 6 seconds**
Cache Flush Timings: **Every 4 seconds**
Rebuild Rate: **30%**
Alarm: **Enabled**
Other Adapter Settings:
— Emulation: **Mass Storage**
— Auto Rebuild: **Disabled**
— Initiator ID: **7**
— Cluster Mode: **Disabled**
— Multiple PCI Delayed Transactions: **Disabled**
— Force Boot: **Off**
— Coercion Algorithm: **GigaByte Way**
— Cc Restoration: **Enabled**

Note: The Coercion Algorithm must be set properly. Once changed, it cannot be changed again. The only way to reset it is to reconfigure RAID from scratch and load the default configuration, then reboot.

9 Select Objects → Channel and press Enter. Ensure that the values are set as follows:

Termination State: **Enabled**
SCSI Transfer Rate: **160M**

10 In the Configure menu, select New Configuration. Press Yes to proceed.

Result: The system should display both SCSI channels, each having three drives. SCSI ID's should be listed in order from 0 to 2 for each channel, starting from the top. All disk drives should be in READY state.

Note: Do not use the Load command on the Configure menu. This command is not for RAID operations.

11 Create the first logical drive by selecting A01-01 (first drive from channel 0), to A01-02 (first drive from channel 1) and pressing the space bar.

Result: After selection, the drives will blink.

12 Press Enter to create the first logical drive.

13 Repeat the process for the second and third logical drives to create packs as follows:

A02-01 and A02-02 as second pack
A03-01 and A03-02 as third pack

14 Press Enter or F10 to configure the logical drives.

15 Press the space bar to Select Configuration Array. *Span-1* appears in the box opened for A01 logical drive. DO NOT select and press the space bar for the other logical drives at this point.

16 Configure logical drive A01, by pressing F10.
RAID 1;
Size: accept the size displayed;
Accept
SPAN = NO

17 Press Enter to accept these new values. Repeat for the two remaining logical drives.

Result: After the last logical drive, the system will prompt you to save the configuration.

18 Highlight YES and press Enter.

19 Press ESC to exit the submenu.

20 In the Management menu choose the Initialize submenu.

21 Press F2 to select all three logical drives.

22 Press F10 and consecutively select YES to initialize the drive packs.

23 When the initialization is complete, press any key to return to the Management menu.

24 Press ESC to exit the utility. Save the configuration when prompted.

25 Press Ctrl+Alt+Delete as indicated by the menu to reboot.

Verifying consistency on the drives

This optional consistency check on the RAID system's logical drive ensures that the data on the drives is identical. If any errors are found, they are corrected automatically. Perform a consistency check *before* you split the RAID system pack. A good data backup on an offline drive will be important if you need to revert to the CallPilot system from an unsuccessful upgrade or update. The consistency check can take up to 2 hours to complete.

To perform a consistency check

1. In Windows, click Start → Programs → MegaRAID Client.

   The MegaRAID Power Console Plus Server Selection window appears.

2. Ensure that Access Mode → Full Access is selected, and click OK.

   Result: The MegaRAID Power Console Plus window appears displaying the Logical View of the Physical Devices and the Logical Devices. The status bar at the bottom of the window indicates that RAID channels are being scanned. When scanning is done, the screen refreshes and displays the Physical and Logical Devices.

3. In the Logical Drives section, right-click the logical drive, and then choose Check Consistency from the pop-up menu that appears.

   Result: The Check Consistency status dialog appears.

   Note: The check can take up to 2 hours to complete. You are informed when it is finished. If any errors are found, a window with an error message is displayed.

4. Select Configuration → Exit to close the MegaRAID console.

   Result: An end of session message appears.

5. Click OK.

RAID splitting

Ensure that your system is in full working order and the RAID hardware configuration is set up properly as described on page 133.

ATTENTION

The most important thing to verify is that the RAID channel 1 is connected to the first three hard drives on the left as facing the machine, and channel 2 is connected to the last three to the right. Do that by either opening the lid and following the cables or by taking offline one hard drive and observing which drive is marked FAIL by the system. If the drive matches the graphic location on the Windows MegaRAID console, proceed with the next step.

ATTENTION

The drives must not be un-seated, re-seated or disconnected during the RAID splitting process unless you are planning to replace the drives.

Full data backup

ATTENTION

As an extra precaution, it is recommended that a full system backup be performed PRIOR to performing a RAID-split. For more information on system backups refer to the CallPilot Manager online help.

RAID splitting

ATTENTION

Because the 1002rp has three physical drives, the RAID splitting must be done at the Ctrl+M utility level. Do not perform this procedure using the Windows MegaRAID console. There is a risk of database corruption.

1 Restart the CallPilot system and press Ctrl+M when prompted, to enter the RAID setup utility during bootup.

2 From the Management menu select Objects → Physical Drive.

Result: A list of all drives organized per channel appears.

3 Select the A01- 2 drive using the cursor and press Enter.

4 Select Fail Drive.

Result: A warning message will appear. Ignore it and select Yes. The drive status will change to FAILED. The alarm should start beeping

5 Repeat this process for the remaining two drives present on Channel 2.

6 Press Esc three times to exit the Ctrl+M utility.

7 Reboot.

Result: The system reports that three drives are in critical mode and it will start beeping but it will still boot. This is OK.

ATTENTION

The alarm can be silenced, but under no circumstances should it be disabled. Select Objects → Adapter → Alarm Console → Silence Alarm from the toolbar.

At this point, the RAID is split, and the drives marked FAILED are the backup drives and will no longer be written to. A release upgrade or PEP installation can now be completed without impact to the ‘backup’ drives.

Perform a CallPilot software upgrade

Let the system boot. The system will still run after all of the drives on Channel 2 of the RAID card are taken out of service, and will boot to Windows. Perform the software upgrade.

RAID synching after a successful upgrade

1 **WITHOUT** shutting down the server, right click the Channel 2 first drive (i.e. (0) A1-2-Failed).

2 From the right mouse pop-up menu select Rebuild. When the Rebuild is done repeat the process for the remaining two drives on Channel 2.

Result: When all three drives are done the drives status will change to ONLINE and the color of the icons should change to green. The alarm should stop beeping unless it was temporarily silenced. The process can take up to one hour. **DO NOT** shut down the machine before the rebuild has completed. You can monitor the rebuild by opening the Windows MegaRAID console.

RAID synching after an unsuccessful upgrade

If the software upgrade or update has failed, the system needs to be returned to the original configuration.

1 Restart the server and enter the Ctrl+M utility when prompted during system bootup.

2 Select Objects → Physical Drive → FAIL Drive for each of the three drives on Channel 1.

Result: At this point all 6 drives will be marked FAIL.

3 Select each of the 3 drives on Channel 2 (previously taken offline) and make them ONLINE. Ignore the warning message.

Result: At this point all three drives on the Channel 2 are ONLINE and all three on the Channel 1 are marked FAILED.

4 Exit the utility and press Ctrl+Alt+Delete to reboot the server.

Result: The system will boot up to the original configuration before the software upgrade and an audible alarm will indicate the state CRITICAL for all three drives. At this time, you can silence the alarm but DO NOT disable it.

5 Once the system is fully booted, rebuild the FAIL drives on Channel 1 using the same process indicated in “RAID synching after a successful upgrade,” on page 139. Reverting from a failed software upgrade is now complete. The audible alarm, if left on, should automatically stop.

Task summary for configuring RAID

Note: This summary should be used only after reviewing the more detailed procedures and warnings in this chapter.

What to do	How to do
Verify the firmware revision	Firmware: 111U. Use the Windows MegaRAID console under Adapter › Properties. Or turn on the server and press Ctrl+M. Select Objects menu› Adapter › Adapter Information.
Upgrade or downgrade firmware	Use the CallPilot 3.0 rackmount 1002rp Image CD-ROM 1 of 2, and select Utilities, 1002rp RAID F/W upgrade.
Configure RAID using LSI 1600 controller using the Ctrl+M menu at server boot-up Note: **The Ctrl+M utility can take up to 1 minute to launch with 111U firmware. The system may appear frozen. Do not reset.**	1 Start the server and press Ctrl+M. Select Objects menu › Adapter › Factory Default, and select Yes to confirm the selection. Press Ctrl+Alt+Delete when prompted to restart system and re-enter Ctrl+M utility. 2 Select Objects › Adapter, then ensure the following values are set as following: Flex RAID Power Fail: **Enabled** Fast Initialization: **On** Disk Spinup Timings: **One every 6 seconds** Cache Flush Timings: **Every 4 seconds** Rebuild Rate: **30%** Alarm: **Enabled** Other Adapter Settings: — Emulation: **Mass Storage** — Auto Rebuild: **Disabled** — Initiator ID: **7** — Cluster Mode: **Disabled** — Multiple PCI Delayed Transactions: **Disabled** — Force Boot: **Off** — Coercion Algorithm: **GigaByte Way** — Cc Restoration: **Enabled** 3 Select Objects › Channel, then ensure that the following values are set as follows: Termination State: **Enabled** SCSI Transfer Rate: **160M** 4 In the Configure menu, select New Configuration. Press Yes to proceed. The system should display both SCSI channels, each having three drives. SCSI ID's should be listed in order from 0 to 2 for each channel, starting from the top. All disk drives should be in READY state. **Note:** Do not use the Load command on the Configure menu. This command is not for RAID operations. 5 Create the first logical drive by selecting A01-01 (first drive from channel 0), to A01-02 (first drive from channel 1) by using the space bar. After selecting, the drives will blink, press Enter to create first logical drive. 6 Repeat procedure for the second and third logical drives to create packs as follows: A02-01 and A02-02 as second pack A03-01 and A03-02 as third pack 7 Configure the logical drives by pressing Enter or F10. 8 Press Space to Select Configuration Array. Span-1 will appear in the box opened for A01 logical drive. DO NOT select and press Space on the other logical drives at this point. 9 Configure logical drive A01, by pressing F10. RAID 1; Size: accept the size displayed; Accept SPAN = NO Repeat procedures described in step 8and 9 for the second and third logical drives(A02 and A03) to configure the logical drives A02 and A03. After the last logical drive, the system will prompt to save the configuration. Save and exit the submenu by pressing Esc. 10 In the main menu enter the Initialize submenu. Select all three logical drives by pressing F2. Press F10 and consecutively select **YES** to initialize the drive packs. When done, press any key to return to the main menu. 11 Exit the utility by pressing Esc. Save the configuration when prompted. Press Ctrl+Alt+Delete as indicated by the menu to reboot.

Task summary for RAID splitting

This summary should be used only after reviewing the more detailed procedures and warnings in this chapter. **Note**: The drives must not be un-seated, re-seated or disconnected during the RAID splitting process unless you are planning to replace the drives.

What to do	How to do
Ensure that your system is fully working and the RAID hardware is properly configured.	The most important thing to verify is that the RAID channel 1 is connected to the first three hard drives on the left as facing the machine, and channel 2 is connected to the last three to the right. Open the lid and follow the cables or take offline one hard drive and observe which drive is marked FAIL by the system. If the drive matches the graphic location on the Windows MegaRAID console, proceed with the next step.
Full data backup	Do a full data backup before RAID splitting is performed as an extra safety precaution.
RAID splitting **Note:** Because the 1002rp has three physical drives, the RAID splitting must be done at the Ctrl+M utility level. Do not perform this procedure using the Windows MegaRAID console. There is a risk of database corruption.	1 Restart the CallPilot system and go to Ctrl+M utility as the machine boots. 2 Select Objects › Physical Drive. A list of all drives organized per channel will be displayed. Using the cursor, select the A01- 2 drive and press Enter. Select Fail Drive. A warning message will pop-up. Ignore it and select Yes. The drive status will change to FAILED. The alarm should start beeping. 3 Repeat the process for the two remaining drives present on Channel 2. Press Esc three times to exit the Ctrl+M utility. Reboot. The system should report that three drives are in critical mode and will start beeping but will still boot. This is OK. **Note**: The alarm can be silenced, but under no circumstances should it be disabled. Select Objects › Adapter › Alarm Console › Silence Alarm from the toolbar.
Perform CallPilot software upgrade	Let the system boot. The system will still run after Channel 2 of the RAID card was taken out of service and will boot to Windows. Perform the software upgrade.
RAID synching for upgrade successful	**WITHOUT** shutting down the server, right click the Channel 2 first drive (i.e. (0) A1-2-Failed). From the right mouse pop-up menu select Rebuild. When the Rebuild is done repeat the process for the remaining two drives on Channel 2. When all three drives are done the drives status will change to ONLINE and the color of the icon should change to green. The alarm should stop beeping unless it was temporarily silenced. The process can take up to one hour. **DO NOT** shut down the machine before the rebuild has completed. You can monitor the rebuild by opening the Windows MegaRAID console.
RAID synching for upgrade NOT successful	If the software upgrade has failed, the system needs to be returned to the original configuration. 1 Restart the server and enter the Ctrl+M utility. 2 Select Objects › Physical Drive › FAIL Drive for each of the three drives on Channel 1. At this point all 6 drives will be marked FAIL. 3 Select each of the 3 drives on Channel 2 (previously taken offline) and make them ONLINE. Ignore the warning message. At this point all three drives on the Channel 2 are ONLINE and all three on the Channel 1 are marked FAIL. 4 Exit the utility and reboot. The system will boot up to the original configuration before the software upgrade and an audible alarm will indicate the state CRITICAL for all three drives. At this time, you can silence the alarm but DO NOT disable it. 5 Once the system is fully booted, rebuild the FAIL drives on Channel 1 using the same process indicated in “RAID synching for upgrade successful”. The software upgrade or reverting from a failed software upgrade is now complete. The audible alarm, if left on, should automatically stop.

Chapter 10

Replacing or adding voice processing boards

In this chapter

DSP numbering and location 144

Replacing an MPB96 board 145

DSP numbering and location

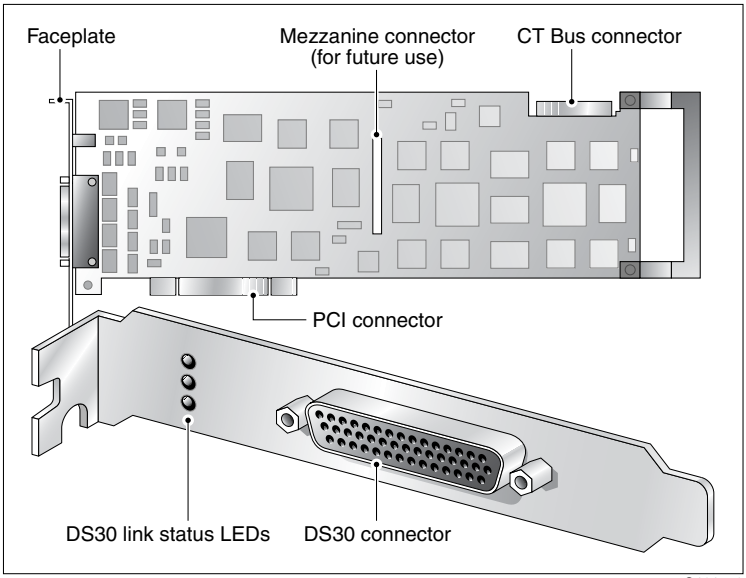
Introduction

DSPs are the built-in voice processing components on MPB boards. DSPs are numbered to distinguish them in CallPilot maintenance programs, such as the Maintenance page in CallPilot Manager. Each DSP supports up to eight multimedia channels.

DSP numbering on MPB96 boards

The MPB96 board has 12 embedded DSPs. MPC-8 cards are not required. If an embedded DSP is faulty, you must replace the entire MPB96 board.

The following diagram shows the MPB96 board:



Replacing an MPB96 board

Introduction

This section describes how to replace an MPB96 board.

You will need to replace an MPB96 board:

- if the board becomes faulty
- when the PCI firmware needs to be updated, and the board must be sent back to the factory



CAUTION

Risk of electrical damage

- Wear an antistatic ESD wrist strap when handling cards or boards, or when working inside the server.
- Do not touch the components or gold-edge connectors of cards or boards.
- Place the board on an antistatic surface until you are ready to install it.

To replace or add an MPB96 board

1. Courtesy stop all CallPilot channels.
2. Power down the server and all peripheral devices.
3. Disconnect the following cables:
   — power cable
   — peripheral device cables
   — DS30X cable(s) (Meridian 1 and Succession 1000 only)
4. Remove the server cover.

   For instructions on removing the server cover, see “Removing the front bezel and server cover” on page 94.

5 Unpack the replacement MPB96 board.

6 Hold the MPB96 board by its top edge or upper corners and then align it with the following:

- end-plate opening in the chassis
  Ensure that the tapered foot of the board's retaining bracket fits into the slot in the expansion slot frame.
- PCI connector

7 Press the new MPB96 board firmly into its slot.

8 Secure the board using the retaining screw.

9 Replace the server cover.

10 Replace the front bezel and lock it.

11 Reconnect the peripheral device and power cables.

12 Reconnect the DS30X cable to the faceplate of the MPB96 board.

Note: Ensure that a single-point ground reference is available for all the power outlets serving the CallPilot server and its peripherals. Before the CallPilot server installation, a qualified electrician must implement the single-point ground reference requirement between the power outlets of the CallPilot server and the power outlets of the switch.

13 Power up the server and log on to Windows.

14 Run the Configuration Wizard to detect the new hardware.

For instructions, refer to "Running the Configuration Wizard" in the *Installation and Configuration Task List* (555-7101-210*)*.

Result: The MPB96 board replacement is complete.

15 Test the multimedia channels to ensure the new MPB96 board is functioning properly.

Refer to "Testing the CallPilot installation" in the *Installation and Configuration Task List* (555-7101-210).

Chapter 11

Maintaining the Pentium III SBC card

In this chapter

Overview 148

Replacing the Pentium III SBC card 149

Configuring the 1002rp Pentium III BIOS 153

Replacing or adding dual inline memory modules 156

Maintaining the onboard video and network cards 158

Overview

Introduction

This section describes the Pentium III SBC card (single board card). It covers procedures for replacing and configuring the SBC card. The SBC card is always installed in the SBC slot located between the ISA expansion slots and the PCI slots on the backplane.

Procedures included

Procedures covered include the following:

- replacing the SBC card (page 149)
- upgrading and configuring the BIOS (page 153)
- adding memory DIMMs to the SBC (page 156)

Intended audience

This section is written primarily for field service technicians. It is intended to act as a guide for installing, repairing, replacing, and upgrading hardware and software components. This section assumes that the reader has basic computing skills, is familiar with necessary safety procedures, and has the hardware documentation provided by the manufacturer available as a reference.

Replacing the Pentium III SBC card

Introduction

Use system diagnostic tools and refer to error codes to determine whether the SBC card should be replaced. This section provides instructions for replacing the SBC card.

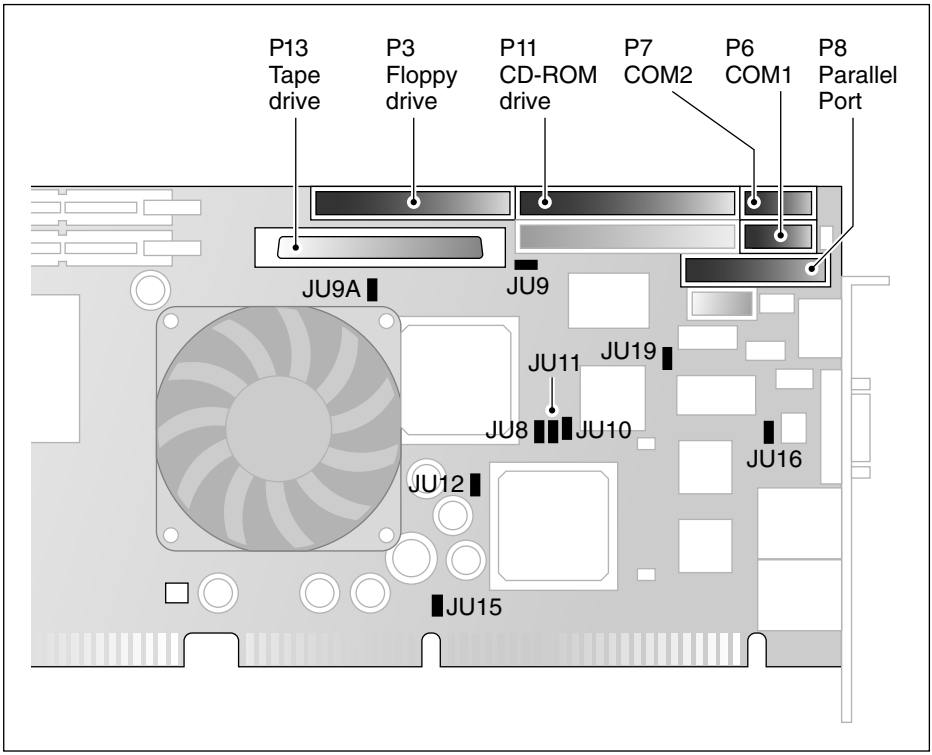
Requirements

Before replacing the SBC card, gather the following tools:

- one Phillips-head screwdriver
- one antistatic wrist strap
- the replacement SBC card
- cable labels

SBC card connectors and jumpers

The following diagram shows the location of connectors where cables must be disconnected or connected as part of the procedure to replace the SBC card. The jumpers shown in this diagram are used in the BIOS configuration procedures.



To replace the SBC card



DANGER

Risk of explosion

The SBC has a lithium battery installed. If you are discarding the SBC, dispose of used batteries according to the manufacturer's instructions. Replacement of the battery with an incorrect type also raises the risk of an explosion.

1. Power down the server.
2. Disconnect the power cord.
3. Remove the top cover.
4. Disconnect and label all cables from the SBC card. See "SBC card connectors and jumpers" on page 150.

   Note: If necessary, refer to the installation guides to locate the SBC card.
5. Disconnect and label cables from the SBC card faceplate.
6. Loosen and remove the screw that is securing the SBC card.
7. Loosen and remove the screw located at the top of the card faceplate.
8. Loosen the SBC and pull it up from the backplane.

   Note: You can now do the following:

   - Replace the SBC with a new card. To replace it, continue with step 9.
   - Increase RAM by adding DIMM(s) to the card. See "To add SDRAM DIMMs to the SBC card" on page 157.
9. Remove the new card from its protective wrapping.
10. Align the card with its slot on the backplane and press it into place.

    Result: The board seats properly in both the ISA-style and PCI-style connectors.
11. Fasten the card down with the screw provided.
12. Install the new I/O bracket.

13 Fasten the I/O bracket using the screw provided.

14 Remove the labels attached to all connectors and reconnect them to the card. See “SBC card connectors and jumpers” on page 150.

15 Replace the top cover.

Configuring the 1002rp Pentium III BIOS

Introduction

BIOS is the Basic Input/Output System of the computer. It is Flash ROM-based code. The system is equipped with Flash BIOS, which enables you to upgrade by running a single program that writes updated code to the Flash ROM chips.

When to upgrade the BIOS

Do not upgrade the BIOS unless specifically instructed to do so by your Nortel Networks representative. The CallPilot server is shipped to the customer with the required minimum BIOS vintage, so an upgrade is only necessary if Nortel Networks deems this necessary to solve a system problem. The minimum release BIOS for CallPilot 3.0 is NNCXUA07 or later.

When to configure the BIOS

BIOS configuration is performed at the factory before the CallPilot server is shipped to the customer. It may be necessary to reconfigure the BIOS at a customer site after a BIOS or CMOS failure and recovery.

Requirements for upgrading or reconfiguring the BIOS

- CallPilot Operating System Installation CD
- You must perform both of the following procedures to upgrade the BIOS:
  - Upgrade the BIOS (page 154).
  - Configure the SBC (page 154).

To upgrade the BIOS



CAUTION

Risk of data loss

Perform this procedure only if specifically instructed to do so by your Nortel Networks representative.

1. Shut down the CallPilot server and power off the server.
2. Start up the CallPilot server and follow the prompts on the screen to launch the BIOS Flash utility.
3. Select N when asked if you want to save the old BIOS.
4. Select NNCXUA07.ROM for the filename of the new BIOS.
5. Select Y to confirm the Program Boot Block.
6. Select Y to confirm that you want to program the BIOS.
7. Allow the Flash process to complete.
8. Shut down the system.
9. Configure the BIOS, as indicated in the procedure below.

To configure the Pentium III SBC



CAUTION

Risk of data loss

Perform this procedure only if specifically instructed to do so by your Nortel Networks representative.

1. Restart the server, and then press Delete to enter Setup when prompted.
2. Set the MPS 1.4 Support value to **Disabled** the Chipset menu.
3. Press F9 to accept the other default values.
4. Press Enter when prompted to confirm this change.

5 Press F10 to save and exit the BIOS setup.

6 Restart the server.

Result: BIOS reconfiguration is completed.

Replacing or adding dual inline memory modules

Introduction

The DIMMs are located on the SBC. The gold-plated edge connectors on DIMMs are designed to plug into matching edge-connector slots. The design allows you to add or remove these modules repeatedly without tools or damage. Install DIMMs on the SBC only.

Capacity

The base CallPilot has one 512-Mbyte DIMM installed in Bank 1. Another 512-Mbyte DIMM can be installed in Bank 2 for total memory of 1 Gbyte. No other memory configurations are supported on this server.

Requirements

To add DIMMs to the card, you require the following:

- an antistatic wrist strap
- DIMMs with gold-plated edge connectors

To add SDRAM DIMMs to the SBC card



CAUTION

Risk of electrical damage

- Wear an antistatic ESD wrist strap when handling cards or boards, or when working inside the server.

1. Remove the SBC card from the server and lay it down on a flat surface.

   Note: To remove old DIMMs, perform steps 2 to 4. To add new DIMMs, go to step 5.

2. Push the DIMM release tab outwards at both sides of the DIMM to be removed.
3. Hold the DIMM by its edges, being careful not to touch its components. Remove the DIMM by lifting it away from its slot. Store it in an antistatic package.
4. Remove other DIMMs as necessary.
5. Orient the DIMM so that the two notches in the bottom edge of the DIMM align with the keyed slot.
6. Insert the bottom edge of the DIMM into the slot, and press down firmly on the DIMM until it seats correctly.

   When the DIMM seats correctly, release the tabs lock back to an upright position. If the DIMM does not seat correctly, remove it and reinstall. Do not force the locking tabs to close.

   Note: The optional DIMMs can be installed when the SBC is in the server. If you do this, you must ensure that the server is **powered off**, and you must support the back of the SBC when you press the DIMM into the slot.
7. Repeat the above two steps to install each additional DIMM.
8. Replace the SBC card in the server.

Maintaining the onboard video and network cards

Network card failure

The network cards are integrated into the SBC card. If the network cards fail, they cannot be replaced by add-in network cards in the expansion slots.

Video card failure

The video cards are integrated into the SBC card. If the video cards fail, they cannot be replaced by add-in video cards in the expansion slots.

Indicators for video card failure

If the monitor appears to be functioning but no display is visible, look for the following indicators of video card malfunction.

- Brightness and contrast are set at normal level.
- The server is powered on, and one long beep is followed by two short beeps.
- The floppy drive light goes on when the server is powered, but no display is visible on the monitor.
- The floppy drive light comes on when the user types dir a: and presses Enter, but no display is visible on the monitor.

Numerics

9-pin connector 49

A

add DIMMs to the SBC 157
air filter, door
  replacement of 98
air filter, front bezel
  replacement of 98
alarm board
  jumpers 109
  replacement of 107
Alarm Monitor 56
alarms
  about 54, 56
  investigating 57
alert icons, component states 66
application event log
  definition 26
arp command 34
  parameters and descriptions 34
  running from Windows 35
  syntax 34

B

backplane, SCSI 115
bezel, front 94
  removal of 95
  replacement of 97
BIOS
  requirements for upgrading 153
boot failure
  CallPilot
    what to do 22
  Windows
    what to do 22

C

call channels
  disabling 60
  working with 79–80
CallPilot
  utilities
    Diagnostics Tool 82
    PEP Maintenance 82, 84
    Session Trace 85
    System Monitor 82
CallPilot Manager
  alarms
    about 54, 56
    investigating 57
  alert icons, component states 66
  Channel Monitor, using 60, 79–80
  Event Browser, using 58–59
  events
    about 54, 58
    investigating 59
  fault management
    alarm notification 54
    event processing 54
  Maintenance screen
    Diagnostics section 63
    General section 62
    Maintenance section 63
    purpose 61
  Multimedia Monitor, using 60, 77–78
CallPilot services
  Channel Monitor tab 88
CD-ROM drive
  replacement of 123
Channel Monitor tab 88

CallPilot services 88
critical 89
DS30X links pane in 90
DSP pane in 90
Channel Monitor, using 60, 79–80
channels
call, working with 79–80
disabling 60
multimedia, working with 77–78
chassis keys 94
chkdsk utility 38
parameters and descriptions 38
running from Windows 39
syntax 38
commands
Net Start 50
Net Stop 44
TSTSERIO 45, 46, 47, 49
commands, TCP/IP
arp 34
ipconfig 29
nbtstat 35
netstat 37
ping 31
tracert 32
components
CallPilot Manager maintenance activities 64
dependencies 55
diagnostics that can be run 73
diagnostics-eligible 72
list 62
replacing 14
states
Alert icons 66
description 65–66
viewing 67
configure the Pentium III SBC 154
configuring
RAID system 133
Courtesy stop, description 69
critical services, CallPilot 89

D

diagnostic tools
TSTSERIO tests 45, 46, 47, 49
diagnostics
integrated
running 72, 74
troubleshooting failures 73
when to run 72
last results
viewing 75–76
serial port
overview 42
TCP/IP 29
arp 34
ipconfig 29
nbtstat 35
netstat 37
ping 31
tracert 32
Diagnostics section, Maintenance screen 63
Diagnostics Tool 82
system utility 83
diagnostics tool
TCP/IP 29
display panel, status
replacement of 111
doors on the front bezel 94
D-sub connector
9-pin 49
Dual Inline Memory Modules (DIMMs) 156

E

Event Browser, using 58–59
event log
application 26
security 26
system 26
event logs
types, description 26
viewing 26
events

about 54, 58
investigating 59

F

fan, hot-swap 102
fault management
alarm notification 54
event processing 54
firmware revision
verifying 131
firmware, flashing the 132
floppy drive
replacement of 123
front bezel 94
fuse
replacement of 105

G

General section, Maintenance screen 62

H

hard drive bay 115
hard drive, RAID SCSI
configuration of 115
hard drive, SCSI hot-pluggable
replacement of 116
hard drives
when to hot-swap 114
hardware problems, detecting 55

I

indicators 158
integrated diagnostics
running 74
troubleshooting failures 73
when to run 72
ipconfig command 29
flags and descriptions 30
running from Windows 30
syntax 29
ipconfig default 29

L

LED, non-illumination of 101
Legend/Help tab 92
location
MPB96 DSP 144
logs
event types
viewing 26
event, viewing 26

M

maintenance
activities by component 64
preparing for 14
Maintenance screen, CallPilot Manager
Diagnostics section 63
General section 62
Maintenance section 63
purpose 61
media drive bay
order of replacement procedures 118
media drive carrier
removal from chassis 121
media drives
location 120
MPB96 board 144
replacing or adding 145
multimedia channels, working with 77–78
Multimedia Monitor, using 60, 77–78

N

nbtstat command 35
  parameters and descriptions 35
  running from Windows 36
  syntax 35
Net Start command 50
Net Stop
  Windows 44
Net Stop command 44
netstat command 37
  parameters and descriptions 37
  running from Windows 37
  syntax 37
network card
  failure 158

P

parts, obtaining replacement 14
Pentium III SBC 149
PEP Maintenance utility 82, 84
ping command 31
  parameters and descriptions 31
  running from Windows 32
  syntax 31
POST error codes and messages 21
POST message formats 18
power supply, hot-swap 100
Power-On Self-Test
  See POST

Q

quitting
  system 43

R

RAID 130
RAID configuring summary 141
RAID firmware
  upgrading 132
RAID splitting summary 142
RAID system
  configuration 133
  configuring 133
Redundant Array of Independent Disks (RAID) 130
replacement parts, obtaining 14
restarting system after TSTSERIO tests 50

S

SBC card, Pentium III
  replacing 151
SCSI controller
  error messages 21
SCSI ID 115
SCSI unit 115
security event log
  definition 26
serial port
  diagnostics 42
server cover 94
  removal of 96
Session Trace utility 85
shutting down
  system 43
startup problems
  what to do 22
Stop, description 69
system
  restarting after TSTSERIO tests 50
  shutting down 43
system event log
  definition 26
System Info tab 91
System Monitor 82
  Channel Monitor tab 88
  Legend/Help tab 92
  System Info tab 91
System Monitor utility 87
system utilities

Diagnostics Tool 83
System Monitor 87

T

tape drive
cabling example 126
configuration of 127
installation of new 127
replacement of 123
TCP/IP diagnostics 29
arp 34
ipconfig 29
nbtstat 35
netstat 37
ping 31
tracert 32
tracert command 32
parameters and descriptions 33
running from Windows 33
syntax 33
TSTSERIO
Windows 47
TSTSERIO command 45

U

utilities
chkdsk 38
Diagnostics Tool 82, 83
PEP Maintenance 82, 84
Session Trace 85
System Monitor 82, 87

V

video card, failure 158
viewing 26

W

Windows
Net Stop utility 44
TSTSERIO 47
viewing 26

CallPilot

1002rp Server Maintenance and Diagnostics

Copyright © 2004 Nortel Networks, All Rights Reserved

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the CallPilot server and the switch or system is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	555-7101-206
Product release:	3.0
Document release:	Standard 1.0
Date:	November 2004

Printed in Canada

