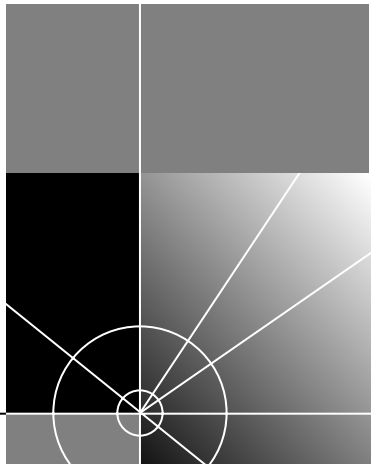
Upgrading Enterprise OS Software

Software version 11.4



http://www.3com.com/

Part No. 09-1551-002
Published January 2000

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

© **3Com Corporation, 2000.** All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for Restricted Rights in Technical Data and Computer Software Clause at 48 C.F.R. 52.227-7013. 3Com Corporation, 5400 Bayfront Plaza, Santa Clara, California 95052-8145.

For civilian agencies:
Restricted Rights Legend: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, Boundary Routing, Net Age, NETBuilder, NETBuilder II, OfficeConnect, SuperStack, and Transcend are registered trademarks of 3Com Corporation. 3TECH and PathBuilder are trademarks of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc. Windows is a registered trademark of Microsoft Corporation. Solaris is a registered trademark of Sun Microsystems, Inc. SunOS is a trademark of Sun Microsystems, Inc. UNIX is a registered trademark of Xopen Company Limited. IBM, APPN, and SNA are registered trademarks of International Business Machines Corporation. HP is a registered trademark of Hewlett-Packard Company. Novell is a registered trademark of Novell, Inc. ProComm Plus for Windows is a registered trademark of DataStorm Corporation. Crosstalk for Windows is a registered trademark of Attachmate Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

The software contained in this product may contain encrypted product which may not be exported or transferred from the U.S. or Canada without an approved U.S. Department of Commerce export license.

Printed on recycled paper.

CONTENTS

ABOUT THIS GUIDE

Conventions 10
Year 2000 Compliance 11

1 OVERVIEW

Upgrade Process 13
Upgrade Utilities and Applications 14
How the Utilities Work 14
Primary, Secondary, and Test Boot Sources 15
Automatic or Manual Recovery 15
Rules and Support Limitations 15
Take Time to Plan 15

2 INSTALLING THE UTILITIES ON A NETWORK MANAGEMENT STATION

Installing the Utilities on a Windows System 17
Preparing for the Installation 17
Procedure 17
Installing the Utilities on a UNIX System 18
Preparing for the Installation 18
Procedure 18
Setting up for Auto Startup 20

3 PLANNING AND PREPARING YOUR UPGRADE

Setting Up a File Transfer Method 21
Setting up for FTP File Transfers 21
On a UNIX NMS 21
On a Windows NMS 22
Setting up for HTTP File Transfers 22
On a UNIX NMS 22
On a Windows NMS 22
Setting up for TFTP File Transfers 22
Choosing Automatic Recovery or Manual Recovery 23
Automatic Recovery 23
Manual Recovery 23
Memory Requirements 24
Planning and Record Keeping 25
Checking DRAM 25

Checking Flash Memory 26
Checking the Software Version 26
Planning Tables 26

4 UPGRADING USING THE NETBUILDER UPGRADE LINK APPLICATION

Preparing for the Upgrade 31
Running Upgrade Link 32
Running Upgrade Link Locally 32
Running Upgrade Link Remotely 32
Status and Settings Pages 34
Settings Page 34
Verifying for Upgrading 35
Installing Software on the NMS 35
36
Upgrading the Software 37

5 UPGRADING USING THE COMMAND LINE UTILITIES

Preparing for the Upgrade 41
Prediagnosing System Problems 42
Installing the Software on the NMS 42
Software Directories 43
Using the Bcmsysupgrade Utility to Upgrade 44
Filenames 45
NETBuilder II Bridge/Router 45
SuperStack II NETBuilder and OfficeConnect NETBuilder Bridge/Routers 46
PathBuilder S5xx Series Switch 46
PathBuilder S400 WAN Convergence Switch 46
Upgrading Software Only 46
Upgrading Using Automatic Recovery 46
Upgrading Using Manual Recovery 48
If the Bridge/Router or Switch Does Not Boot 49
Upgrading Hardware and Software 49
Upgrading Using Automatic Recovery 50
Upgrading Using Manual Recovery 52
If the Bridge/Router or Switch Does Not Boot 55

6 UPGRADING THE SOFTWARE IMAGE ONLY

Preparing for the Upgrade 57
Upgrading the Image Using Upgrade Link 58
Verifying the Device for Upgrading 58
Upgrading the Image 59
Installing the NETBuilder Software 61
Prediagnosing System Problems 61
Upgrading Using Automatic Recovery 61
Upgrading Using Manual Recovery 62
Upgrading the Image Using the Enterprise OS User Interface 63

7 BACKING UP AND RESTORING SOFTWARE

Backing Up the Software Using Upgrade Link 65
- Verifying the Device for Backing Up 66
- Backing Up the Software 66

Backing up the Software Using the Command Line Utilities 67
- Prediagnosing System Problems 67
- Backing Up the Software 67
  - Directory Paths 68

Restoring Software from a Backup 68
- Configuring IP Routing 68
- Configuring SNMP 69
  - Mapping Hostnames Using the etc/snmp.cfg File 69
- Restoring the Software Using Upgrade Link 71
  - Verifying the Device for Restoring 71
  - Restoring the Software 71
- Restoring the Software Using the Command Line 72
  - Prediagnosing System Problems 72
  - Restoring the Software 73

8 REFERENCE FOR THE UPGRADE MANAGEMENT UTILITIES

Accessing and Downloading the Utilities 75
- Downloading the Utilities 75
  - Downloading UNIX Files 75
  - Downloading Windows Files 75

Update Log File 76

Utility Descriptions and Syntax 76
- Overview 76
  - Getting Help 77
- bcmbackup 77
- bcmconfig 78
- bcmctrl 79
- bcmdf 80
- bcmdiagnose 81
- bcminstall 82
- bcmloadconfig 83
- bcmnbrus 84
- bcmrestore 84
- bcmsetup 85
- bcmsysupgrade 85
- bcmuname 86
- bcmupdate 87
- UpgradeLink 88

A TROUBLESHOOTING

Getting Help 89
- Man Pages 89

HTML Help 89
General Troubleshooting Error Messages 89
Return Codes from bcmdiagnose 90
Hardware-Related Messages 91
Installation Troubleshooting Messages 91
Installing the Enterprise OS Upgrade Management Utilities 91
Determining Connectivity 92
Validating the SNMP Service Configuration 92
Testing the NMS/ TFTP Configuration 93
Creating an Upgrade File 93
Uploading an Upgrade File 94
Downloading an Upgrade File 95

B MOUNTING THE CD-ROM ON A UNIX PLATFORM

Mounting the CD-ROM on Solaris 2.6 97
Mounting a Local CD-ROM Drive 97
Mounting from a Remote CD-ROM Drive 97
Mounting the CD-ROM on HP-UX 10.20 99
Mounting from a Local CD-ROM Drive 99
Mounting from a Remote CD-ROM Drive 99
Mounting the CD-ROM on IBM AIX 4.3.2 100
Mounting from a Local CD-ROM Drive 100
Mounting from a Remote CD-ROM Drive 100
Unmounting the CD-ROM 101

C CHOOSING A SOFTWARE PACKAGE

NETBuilder II Upgrade Migration Path 103
SuperStack II NETBuilder Upgrade Migration Path 104
SuperStack II NETBuilder SI Upgrade Migration Path 105
OfficeConnect NETBuilder Upgrade Migration Path 106
PathBuilder Upgrade Migration Path 106

D TECHNICAL SUPPORT

Online Technical Services 109
World Wide Web Site 109
3Com Knowledgebase Web Services 109
3Com FTP Site 109
3Com Bulletin Board Service 110
Access by Analog Modem 110
Access by Digital Modem 110
3Com Facts Automated Fax Service 110
Support from Your Network Supplier 110
Support from 3Com 111
Returning Products for Repair 112

GLOSSARY

INDEX

3COM CORPORATION LIMITED WARRANTY

ABOUT THIS GUIDE

This guide describes how to upgrade your NETBuilder® bridge/router to Enterprise OS software version 11.4. This guide also describes how to upgrade your PathBuilder™ S5xx series switch or PathBuilder S400 WAN Convergence Switch to Enterprise OS software version 11.4.

In addition, this guide describes how to upgrade your NETBuilder bridge/router to previous software versions (8.0 through 11.3) by specifying the correct options.

This guide also describes how to complete an image-only upgrade for patches, new packages, or software recovery. It also describes how to backup and restore software on a network management station.

Chapter 1 provides an overview of the upgrade process, tools (utilities and applications) required to perform the upgrades, and upgrade rules and support limitations.

Chapter 2 describes installing the utilities on a network management station (NMS).

Chapter 3 describes the steps required to prepare your system for the upgrade.

Chapter 4 describes performing the upgrade using the Enterprise OS Upgrade Link application.

Chapter 5 describes performing the upgrade using the command line utilities.

Chapter 6 describes the steps for upgrading the software image only.

Chapter 7 provides information necessary for backup and restoring your software.

Chapter 8 provides command descriptions and syntax.

Chapter A provides troubleshooting information.

Appendix B describes how to mount the CD-ROM on a Unix platform.

Appendix C provides recommended software version upgrade information.

Appendix D provides information on getting technical support.

See the Enterprise OS Software Version 11.4 Release Notes for any changes or additions to the information in this guide.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Important features or instructions
	Caution	Information to alert you to potential damage to a program, system, or device
	Warning	Information to alert you to potential personal injury

Table 2 Text Conventions

Convention	Description
`Syntax`	The word "syntax" means you must evaluate the syntax provided and supply the appropriate values. Placeholders for values you must supply appear in angle brackets. Example: Enable RIPIP using: `SETDefault !<port> -RIPIP CONTrol = Listen` In this example, you must supply a port number for <port>.
`Commands`	The word "command" means you must enter the command exactly as shown in text and press the Return or Enter key. Example: To remove the IP address, enter: **`SETDefault !0 -IP NETaddr = 0.0.0.0`** *This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case-sensitive.*
`Screen displays`	This typeface represents information as it appears on the screen.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names appear in text in one of two ways: ■ Referred to by their labels, such as "the Return key" or "the Escape key" ■ Written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Menu commands and *buttons*	Menu commands or button names appear in italics. Example: From the *Help* menu, select *Contents*.
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

Year 2000 Compliance

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

`http://www.3com.com/products/yr2000.html`

1 OVERVIEW

This chapter provides an overview of the upgrade process, tools (utilities and applications), and support limitations.

You can upgrade your bridge/router from software version 8.0 through 11.3 to any software version after 8.0 through 11.4 on the following platforms:

- NETBuilder II® bridge/router with DPE
- NETBuilder II bridge/router with CEC—The CEC module is not supported after software version 10.1, but you can use the 11.2 utilities to upgrade a CEC module to a DPE module, or to upgrade the CEC module to software version 10.1 or earlier.
- SuperStack® II NETBuilder SI bridge/router
- SuperStack II NETBuilder Token Ring bridge/router
- OfficeConnect® NETBuilder bridge/router

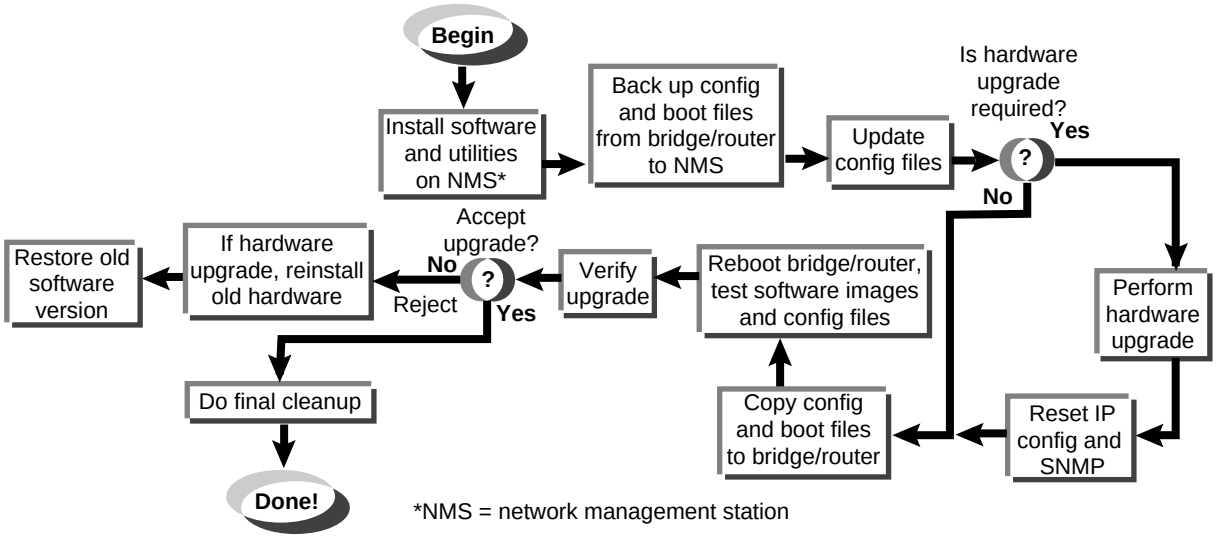
You can upgrade your PathBuilder S5xx series switch to Enterprise OS software version 11.4 from version 11.1.1, version 11.2.x, and version 11.3.

You can upgrade your PathBuilder S400 WAN Convergence switch to Enterprise OS software version 11.4 from version 11.2.2.

Upgrade Process

Figure 1 shows the typical upgrade process.

Figure 1 Upgrade Process



Upgrade Utilities and Applications

The upgrade procedures in this guide use the Enterprise OS Upgrade Management Utilities on a UNIX or Windows network management station (NMS).

Definition of network management station

An NMS is a UNIX or Windows system that has a TFTP/FTP server running in addition to software, such as the Enterprise OS Upgrade Management Utilities, to manage your network. For Windows, the utilities include the 3Com® TFTP/FTP server.

You can use the Enterprise OS Upgrade Link application that is shipped with the utilities. Upgrade link is an easy to use graphical user interface (GUI) for upgrading one or more Enterprise OS devices. Or you can access the utilities directly using the command line.

When upgrading multiple Enterprise OS devices simultaneously using command line utilities, the topology of the network should be considered and the devices should be upgraded in a sequence that will not disrupt the network.

If you are upgrading multiple Enterprise OS devices, you can install and use the Upgrade Manager application in the Transcend® Enterprise Manager or Transcend Network Control Services, available separately. See the Transcend user guide for more information.

If you are performing an image-only upgrade, you can use the utilities or applications, or you can copy the software manually using the Enterprise OS user interface using TFTP or FTP.

The Enterprise OS Upgrade Management Utilities and the Enterprise OS Upgrade Link application are shipped with your software package on a CD-ROM and must be installed on an NMS that resides on the same network as the Enterprise OS device to be upgraded. You can also download the utilities and Upgrade link from the 3Com web, FTP, or BBS sites.

The utilities run on the following operating systems:

- Solaris 2.6 (SunOS 5.6)
- HP-UX 10.20
- IBM AIX 4.3.2 or later
- Windows NT 4.0 with Service Pack 5
- Windows 95/98
- Windows/2000

Supported browsers for use with Upgrade Link include the following:

- Netscape Navigator 4.08, Communicator 4.5
- Netscape Communicator 5.0
- Microsoft Internet Explorer 5.0

How the Utilities Work

The software on your Enterprise OS device consists of a bootable image file and configuration files that store all your settings. The Enterprise OS Upgrade Management Utilities update all your software files after copying them to a UNIX or Windows NMS. Because the upgrade occurs on a copy of the files on the NMS,

the device remains operational during the upgrade. The utilities then copy the new image and updated files back to the device.

Primary, Secondary, and Test Boot Sources

The Enterprise OS device boots from a default directory, called the primary boot source, which can be set using the SysconF command in the Enterprise OS user interface. If you have more than one set of boot images, you can specify a backup directory, called the secondary boot source. There is also a test boot source, which the utilities use to test a new upgrade before making it the primary boot source. Because the boot sources are only pointers to particular directories, the utilities can dynamically change the boot sources without having to move any files.

Automatic or Manual Recovery

If your Enterprise OS device has enough flash memory, you can have both sets of software: the old version and the new version. After a successful test boot with the new software, the primary boot source is changed to the new version. If the test boot is not successful, the device automatically reboots with the old version. Dual-image support is described in the procedures for *automatic recovery*.

If you have only enough flash memory for the new version, you can still recover the old version from the NMS using the utilities. Single-image support is described in the procedures for *manual recovery*.

For memory requirements for automatic or manual recovery, see Chapter 3.

Rules and Support Limitations

Before planning your upgrade, refer to the following rules and support limitations:

- The utilities do not support Remote Boot and Configuration Services (RBCS) or network booting.
- Upgrades from NETBuilder bridge/routers running version 7.x, or earlier, are not supported.
- You cannot upgrade to a different platform. For example, you can only upgrade an OfficeConnect® bridge/router to an OfficeConnect bridge/router. You cannot upgrade a SuperStack® II NETBuilder bridge/router to a SuperStack II NETBuilder SI bridge/router. The only exception is an upgrade from a NETBuilder II® CEC module to a DPE module.

Take Time to Plan

Because networks today have become increasingly complex, upgrading your network requires a systematic approach. 3Com recommends that you plan your upgrade carefully before implementing it. See Chapter 3 to plan your upgrade.

2 INSTALLING THE UTILITIES ON A NETWORK MANAGEMENT STATION

To begin the upgrade process, you must install the Enterprise OS Upgrade Management Utilities on a network management station (NMS). If you are using Transcend Enterprise Manager or Transcend Network Control Services, which has the utilities bundled, you should install the latest utilities to take advantage of new features and version support.

This chapter describes how to install the Enterprise OS Upgrade Management Utilities in the following sections:

- Installing the Utilities on a Windows System
- Installing the Utilities on a UNIX System

Installing the Utilities on a Windows System

You can install the utilities from a CD-ROM or from utilities that you have downloaded to your hard disk. To install the utilities on a Windows system, follow these steps:

Preparing for the Installation

Before installing the utilities, verify the following:

- If you have installed utilities before or have Transcend, check the version by entering:

  `bcmdiagnose`

  If the version is earlier than 11.4, you must reinstall the utilities. If you already have 11.4, you do not need to reinstall the utilities.

Procedure

To install the utilities on a Windows system, follow these steps:

1 Change to the utilities directory.

- If you are using the CD-ROM:

a Insert the CD-ROM into the CD-ROM drive.

b Open a command window.

c Change to the CD-ROM directory.

For example, if E is the drive letter for the CD-ROM, enter:

`E:`

- If you download the utilities to your hard disk (see Chapter 8 for information about downloading the utilities):

a Decompress the utilities.

b Open a command window.

c Change to the utilities directory using:

```
<drive>:\<path>\
```

2 Run the setup program for Windows:

- To install all packages, including the utilities and package definitions for use with Transcend if required, use:

  ```
  bcmsetup <drive>: all
  ```

  Where <drive> is the drive you want to install the utilities on.

The packages install in the default directory \usr\3Com\bcm\, and the following paths are added to the autoexec.bat file:

<drive>:\usr\3com\bcm\bin\

<drive>:\usr\3com\common\bin\

3 Reboot your system to use the path, which is required for all utility commands. Or, if you do not want to reboot, you can enter the path manually at the command prompt:

```
<drive>:\usr\3com\common\data\profile
```

4 Use the bcmdiagnose utility to ensure that your installation is correct by entering:

```
bcmdiagnose
```

Installing the Utilities on a UNIX System

You can install the utilities from a CD-ROM or from utilities that you have downloaded to your hard disk.

Preparing for the Installation

Before installing the utilities, verify the following items:

- Your NMS is running one of the supported operating systems. See "Upgrade Utilities and Applications" on page 14.

  Check the operating system you are running by entering:

  ```
  uname -a
  ```

The version message may refer to Solaris 2.6 as SunOS 5.6.

- You need to upgrade utilities you have already installed. The utilities come bundled with Transcend. To check the version, enter:

  ```
  bcmdiagnose
  ```

- Your root password on the NMS (UNIX only).
- Your NMS is running a TFTP/FTP server.

Procedure

To install the utilities on a UNIX system, follow these steps:

1 Log on as root.

2 Change to the utilities directory.

- If you are using the CD-ROM:

a Mount the CD-ROM.

For more information on mounting instructions for each supported UNIX operating system, see Appendix B.

b Change to the appropriate directory on the CD-ROM for your operating system using:

```
cd /<cd-rom path>/<os>
```

Where <os> is the directory for your operating system. See Table 1 for operating system directory names.

Table 1 UNIX Directories

Operating System	Directory Name
Solaris 2.6	sunos6
HP-UX 10.20	HP_UX
IBM AIX 4.3.2	aix

- If you download the utilities to your hard disk (see Chapter 8 for information about downloading the utilities):

a Decompress the utilities.

b Change to the utilities directory on your hard disk using:

```
cd /<path>/
```

3 Run the setup program.

- To install all packages from the CD-ROM, including the utilities and package definitions for use with Transcend, enter:

```
./bcmsetup all
```

- To install only the upgrade utilities, enter:

```
./bcmsetup bcm
```

If you are working in an HP-UX operating system, the bcmsetup command must be uppercase, that is, BCMSETUP. The options that follow remain lowercase.

The utilities are installed in the default directory /usr/3Com/bcm/.

If you are using the Transcend Network Control Services, you can specify a different directory.

4 Complete the following step for your UNIX shell:

- For a C-shell installation, add the contents of the following file to the .cshrc file for each user you want to have access to the utilities, including root:

  /usr/3Com/common/data/.login-bcm

  Or you can enter the path after every logon:

```
source /usr/3Com/common/data/.login-bcm
```

- For a Bourne shell installation, add the contents of the following file to the .profile file for each user you want to have access to the utilities, including root:

  /usr/3Com/common/data/.profile-bcm

  Or you can enter the path after every logon:

```
. /usr/3Com/common/data/.profile-bcm
```

5 Return to normal privilege by entering:

```
exit
```

6 Use the bcmdiagnose utility to ensure that your installation is correct by entering:

```
bcmdiagnose
```

Setting up for Auto Startup

On a UNIX NMS, after you have completed the previous setup procedures you need to set up the BootP server.

To set up the BootP server, enter:

```
bcmsteup -bootp
```

This command does not need to be used when you are operating on a Windows 95/98/NT-based NMS.

3 PLANNING AND PREPARING YOUR UPGRADE

After installing the Enterprise OS Upgrade Management Utilities, you should spend a few minutes to prepare for and plan your upgrade. This chapter describes the following steps you should take to prepare for the upgrade:

- Setting Up a File Transfer Method
- Choosing Automatic Recovery or Manual Recovery
- Memory Requirements
- Planning and Record Keeping

If you are upgrading multiple devices using Transcend Enterprise Manager or Transcend Network Control Services, or are using the command line utilities, you should make sure each device has enough flash memory and DRAM for the software package you have chosen. The Upgrade Link application automatically checks the memory of the device.

For a list of all software packages and the recommended upgrade path for your version, see Appendix C.

Setting Up a File Transfer Method

You can choose to transfer files using FTP, HTTP, or TFTP.

Setting up for FTP File Transfers

To use FTP, you need to set up your NMS in preparation for FTP file transfers.

For Upgrade Link, the user name and password is specified in the Settings Page, as shown on page 34.

On a UNIX NMS

1. Create a user on your system with /tftpboot as the home directory.
2. When using the upgrade utilities via the command line or the Transcend Upgrade Manager, specify this user name and password in the BCMFTPUSER and BCMFTPPASS environment variables.

   Specify the -ftp flag in all command line utilities that use file transfers (bcmsysupgrade, bcmbackup, bcmrestore) if you want to use FTP file transfer. For example, to specify FTP file transfer use:

   ```
   bcmsysupgrade -s:from_nb -ftp <device>
   ```

If no flag is used, TFTP is used by default for software release 11.0 and lower, but FTP is used by default for software release 11.1 and higher. If the -ftp flag is specified on a bridge/router running software version 11.0 or lower, the FTP password is overwritten with the following text string:

****

On a Windows NMS

1. Create a user in 3Com's 3CServer FTP settings.
2. When using the upgrade utilities via command line or the Transcend Upgrade Manager, specify the ftp user name and password in the BCMFTPUSER and BCMFTPPASS environment variables.

   You can specify the -ftp flag in the utilities (bcmsysupgrade, bcmbackup, bcmrestore) if you want to use FTP file transfer.

If no flag is used, TFTP is used by default for software release 11.0 and lower, but FTP is used by default for software release 11.1 and higher. If the -ftp flag is specified on a bridge/router running software version 11.0 or lower, the FTP password is overwritten with the following text string:

****

Setting up for HTTP File Transfers

To use HTTP, you need to set up your NMS in preparation for HTTP file transfers.

HTTP file transfer is only available with devices running EOS 11.4 or later.

On a UNIX NMS

When using the upgrade utilities via the command line or the Transcend Upgrade Manager, specify the user name and password in the BCMNBUSER and BCMNBPASS environment variables.

Specify the -http flag in all command line utilities that use file transfers (bcmsysupgrade, bcmbackup, bcmrestore) if you want to use HTTP file transfer. For example, to specify HTTP file transfer use:

```
bcmsysupgrade -s:from_nb -http <device>
```

On a Windows NMS

When using the upgrade utilities via command line or the Transcend Upgrade Manager, specify the administrator access user name and password in the BCMNBUSER and BCMNBPASS environment variables.

You can specify the -http flag in the utilities (bcmsysupgrade, bcmbackup, bcmrestore) if you want to use HTTP file transfer.

Setting up for TFTP File Transfers

To use TFTP, you need to set up your NMS in preparation for TFTP file transfers.

Make sure your TFTP server is running. On a Windows workstation, 3Com's 3CServer is shipped along with the utilities. Upgrade Link launches 3CServer during start up.

Specify the -tftp flag in all command line utilities that use file transfers (bcmsysupgrade, bcmbackup, bcmrestore) if you want to use TFTP file transfer. For example, to specify TFTP file transfer use:

```
bcmsysupgrade -s:from_nb -tftp <device>
```

If neither flag is used, TFTP is used by default for software release 11.0 and lower, but FTP is used by default for software release 11.1 and higher. If the -ftp flag is specified on a bridge/router running software version 11.0 or lower, the FTP password is overwritten with the following text string:

```
****
```

Choosing Automatic Recovery or Manual Recovery

If you have enough flash memory for dual-image support, complete your upgrade using automatic recovery. If you have only enough memory for single-image support, complete the upgrade using manual recovery. The following sections describe the difference between automatic and manual recovery and the memory requirements for each platform.

Automatic Recovery

The default upgrade procedure uses automatic recovery. After backing up the current software to the network management station (NMS), the new software is copied into a test directory while the current software remains in the primary directory. If you accept the upgrade after booting from the test directory, the new software becomes the primary boot source, and the old software becomes the secondary boot source.

If you are upgrading your hardware as well as the software, the procedure for automatic recovery saves the software package that was originally on the new hardware as the secondary boot source.

Manual Recovery

An upgrade with manual recovery (using the -m option with the bcmsysupgrade utility) formats the flash memory after backing up the current software, then copies the upgraded files to the bridge/router. If the upgrade is not successful, you must restore the software from the NMS.

If you are upgrading your hardware as well as the software, you can easily recover your old hardware if the upgrade is not successful. However, because you erased the flash memory on the new hardware, you will need to restore the original software from the NMS if you want to return the new hardware to its original state.

Memory Requirements

Table 2 lists the memory requirements for each software package on the platform you are upgrading. If you are upgrading to an earlier version of software, see the guides that came with that version for the memory requirements.

Table 2 Version 11.4 Software Packages

			Flash Memory Required for:	
Software Package	**Model**	**DRAM Required**	**Automatic Recovery**	**Manual Recovery**
NETBuilder II with DPE:			(The standard flash memory card from 3Com is 20 MB)	
(AC) - APPN/Connection Services	DPE	All DPE modules ship with enough DRAM for all software packages.	20 MB	20 MB
(DW) - Multiprotocol Router	DPE		20 MB	20 MB
(DE) - Multiprotocol Router with 56-bit Encryption	DPE	All DPE modules ship with enough DRAM.	20 MB	20 MB
(DL) - Multiprotocol Router with 40-bit Encryption	DPE		20 MB	
(DS) - Multiprotocol Router with 128-bit Encryption	DPE		20 MB	20 MB
SuperStack II NETBuilder Token Ring:				
(CF) Multiprotocol Router	327, 527	12 MB	8 MB	4 MB
(TE) - Multiprotocol Router with 56-bit Encryption	327, 527	12 MB	8 MB	4 MB
SuperStack II NETBuilder SI:				
(NW) - IP/IPX/AT Router	432, 442, 452, 462 532, 542, 552, 562	All SuperStack II NETBuilder SI bridge/routers ship with enough DRAM (16 MB) and flash memory (8 MB) for automatic recovery.		
(BF) - Boundary Router	433, 443, 453, 463 533, 543, 553, 563			
(CF) - Multiprotocol Router	437, 447, 457, 467 537, 547, 557, 567			
(AX) - APPN/Connection Services	438, 448, 458, 468 538, 548, 558, 568			
(NE) - IP/IPX/AT Router with 56-bit Encryption	432, 442, 452, 462 532, 542, 552, 562			
(NS) - IP/IPX/AT Router with 128-bit Encryption	432, 442, 452, 462 532, 542, 552, 562			
(CL) - Multiprotocol Router with 40-bit Encryption	437, 447, 457, 467 537, 547, 557, 567			
(CE) - Multiprotocol Router with 56-bit Encryption	437, 447, 457, 467 537, 547, 557, 567			
(CS) Multiprotocol Router with 128-bit Encryption	437, 447, 457, 467 537, 547, 557, 567			
OfficeConnect NETBuilder:				
(RW) - Low-end IP/IPX Router	10	8 MB	8 MB	4 MB
(JW) - IP/IPX Router	1x4	8 MB	8 MB	4 MB
(NW) - IP/IPX/AT Router	112, 122, 132, 142	8 MB	8 MB	4 MB

Table 2 Version 11.4 Software Packages (continued)

Software Package	Model	DRAM Required	Flash Memory Required for: Automatic Recovery	Flash Memory Required for: Manual Recovery
(BF) - Boundary Router	113, 123, 143	8 MB	8 MB	4 MB
(OF) - Multiprotocol Router	117, 127, 137, 147	12 MB	8 MB	4 MB
(AF) - APPN Router	116, 126, 146	12 MB	8 MB	4 MB
(NE) - IP/IPX/AT Router with 40- or 56-bit Encryption	112, 122, 132, 142	8 MB	8 MB	4 MB
(NS) - IP/IPX/AT Router with 128-bit Encryption	112, 122, 132, 142	8 MB	8 MB	4 MB
(OL) - Multiprotocol Router with 40-bit Encryption	117, 127, 137, 147	12 MB	8 MB	4 MB
(OE) - Multiprotocol Router with 56-bit Encryption	117, 127, 137, 147	12 MB	8 MB	4 MB
(OS) - Multiprotocol Router with 128-bit Encryption	117, 127, 137, 147	12 MB	8 MB	4 MB
PathBuilder S5xx Switch				
(PW) - Multiprotocol Router	S500, S580, S590, S593, S594, S598, S599	All PathBuilder models ship with enough DRAM for all software packages.	16 MB	16 MB
(PL) - Multiprotocol Router with 40-bit Encryption	S500, S580, S590, S593, S594, S598, S599		16 MB	16 MB
(PE) - Multiprotocol Router with 56-bit Encryption	S500, S580, S590, S593, S594, S598, S599		16 MB	16 MB
(PS) - Multiprotocol Router with 128-bit Encryption	S500, S580, S590, S593, S594, S598, S599		16 MB	16 MB
PathBuilder S400 Switch				
(PW) - Multiprotocol Router		All PathBuilder models ship with enough DRAM for all software packages.	16 MB	16 MB
(PL) - Multiprotocol Router with 40-bit Encryption			16 MB	16 MB
(PE) - Multiprotocol Router with 56-bit Encryption			16 MB	16 MB
(PS) - Multiprotocol Router with 128-bit Encryption			16 MB	16 MB

Planning and Record Keeping

You can use the planning tables at the end of this chapter to record your current device specifications.

Checking DRAM

To check how much DRAM you have installed on the switch or bridge/router, on the NMS use:

```
bcmuname -M <device>
```

Where <device> is the IP address or hostname of the switch or bridge/router.

Checking Flash Memory

To check how much flash memory you have installed on the switch or bridge/router, on the NMS use:

```
bcmdf <device>[:<drive:>]
```

Where <device> is the hostname or the IP address of the switch or bridge/router.

Specify drive A for NETBuilder II bridge/routers or PathBuilder switches.

Do not specify a drive for SuperStack II or OfficeConnect bridge/routers.

Checking the Software Version

To display the current software version and package you are running, use the bcmuname utility on the NMS:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the bridge/router.

To display the current software version and package using the Enterprise OS user interface, enter:

```
SHow -SYS VERSion
```

Planning Tables

Photocopy the following planning tables, and fill out background information about your devices before starting the upgrade process. The NETBuilder II table is on page 27. The SuperStack II NETBuilder, SuperStack II NETBuilder SI, OfficeConnect NETBuilder, and PathBuilder Switch table is on page 28.

If you are upgrading both software and hardware, write down the information for the new hardware. For example, if you are replacing a CEC 20 with a DPE module, write down the information for the DPE module.

NETBuilder II Planning Table

IP Address or Name	Flash Memory	Enough Flash Memory for Automatic Recovery?	Enough Flash Memory for Manual Recovery?	DRAM	Current Software Version and Two-Letter Code	New Software Version and Two-Letter Code	Check each appropriate option to use with the command-line utilities:			
							Manual Recovery?	Hardware Upgrade?	Upgrading to Software Version?	Upgrading Unlike Packages?
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>

SuperStack II NETBuilder, SuperStack II NETBuilder SI, OfficeConnect NETBuilder, and PathBuilder Switch Planning Table

IP Address or Name	Flash Memory	Enough Flash Memory for Automatic Recovery?	Enough Flash Memory for Manual Recovery?	DRAM	Current Software Version and Two-Letter Code	New Software Version and Two-Letter Code	Check each appropriate option to use with the command-line utilities:			
							Manual Recovery?	Hardware Upgrade?	Upgrading to Software Version?	Upgrading Unlike Packages?
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>
							❑ -m	❑ -new_hw	❑ -V:<version you are upgrading to>	❑ -k:<package you are upgrading to>

See Chapter 4 to upgrade your device using the Enterprise OS Upgrade Link Applications.

See Chapter 5 to upgrade your device using the command line utilities.

4 UPGRADING USING THE NETBUILDER UPGRADE LINK APPLICATION

This chapter describes how to upgrade the software on an Enterprise OS device using the Upgrade Link application. Upgrade Link is an easy to use GUI for the upgrade utilities that runs in a web server. Access to the server is available via a web browser.

If you are upgrading multiple bridge/routers, you should use Transcend Enterprise Manager or Transcend Network Control Services instead. Contact your network supplier for more information about Transcend. Or if you want to write scripts, you can use the command line utilities as described in Chapter 5.

An NMS is a UNIX or Windows system that has a FTP/TFTP server running in addition to software, such as the Upgrade Management Utilities, to manage your network. For Windows, the utilities include the 3Com FTP/TFTP server called 3CServer.

Preparing for the Upgrade

Before upgrading your system, confirm the following items:

- You have installed the utilities according to Chapter 2.
- You have set the path for the utilities (UNIX only) according to Chapter 2. If you have not set the path, see "Installing the Utilities on a UNIX System" on page 18.
- All configuration files are in the same directory as the boot image.
- You have booted your device from the primary boot source.
- You have a web browser installed with Java support, such as Netscape Navigator 4.08, Netscape Communicator 5.0, or Internet Explorer 5.0, and you have it in your path (UNIX).

CAUTION: *Only one client at a time should access the Upgrade Link Server.*

- There is sufficient disk space on the NMS for the amount of software you are installing.

  Minimal disk storage requirements depend on the number of different software versions that are stored on the disk drive. Calculate:

  - 6 MB for each version of the NETBuilder II bridge/router or PathBuilder switch image
  - 4 MB for each version of the SuperStack II, SuperStack II SI, or OfficeConnect NETBuilder bridge/router image

  While you must purchase one copy of software for each device, you only need to install one copy of a version of software on the NMS.

Running Upgrade Link

The Upgrade Link application contains its own web server called Enterprise OS Upgrade Server. Client access to the web server is available locally or remotely via a web browser.

Running Upgrade Link Locally

Running the Upgrade Link application locally means that the web browser and the web server are running on the same NMS.

To run Upgrade Link locally on a UNIX NMS, use:

```
UpgradeLink [-NoAuthentication] [-NoSecurity]
```

This command starts the Enterprise OS Upgrade Server and the default browser. Two command options are available:

- -NoAuthentication — When NoAuthentication is specified, Upgrade Link will allow a remote client to access the server without user authentication, see "Settings Page" on page 34 for a description of the available settings.
- -NoSecurity — When you specify NoSecurity, Upgrade Link starts and will accept connections from all IP addresses. Otherwise, only those client IP addresses listed in the /usr/3Com/common/data/allow file will be accepted by Upgrade Link.

For security, an administrator can enter the IP addresses of only those clients who will be allowed to upgrade devices. An allow file is an ASCII text file containing the IP addresses of clients to upgrade devices. The allow file looks like the following:

```
129.213.100.151
129.213.100.152
139.87.172.100
```

To run Upgrade Link locally on a Windows NMS, click the *Start* menu, then choose *Programs⇒ Remote Upgrade Utilities⇒Upgrade Link*.

Your default browser is launched. On Windows, the 3Com FTP/TFTP server is also launched.

When you exit Upgrade Link, you will also exit the browser and, for Windows, the FTP/TFTP server.

Running Upgrade Link Remotely

You can access the Enterprise OS Upgrade Server remotely using a browser.

1. Start the Enterprise OS Upgrade Server on the NMS using:

   ```
   bcmnbrus <port> [-NoSecurity | -NoAuthentication]
   ```

   Choose a port and then use that port in your browser URL. For example:

   bcmnbrus 12345

Upgrade Link chooses a port based on the ports that are not in use and shares this information automatically between the "back end" (bcmnbrus) and the "front end" (bcmbrowser).

The port should not be a "well-known" port; that is, one assigned by the Internet Assigned Numbers Authority (IANA). Generally, these are ports whose value is less than 1024.

Two command options are available:

- -NoSecurity — When NoSecurity is specified, the bcmnbrus command allows connections from all IP addresses. Otherwise, only those client IP addresses listed in the /usr/3Com/common/data/allow file will be accepted by Upgrade Link.

  For security, an administrator can enter the IP addresses of only those clients who will be allowed to upgrade devices. An allow file is an ASCII text file containing the IP addresses of clients to upgrade devices. The allowed file looks like the following:

  ```
  129.213.100.151
  129.213.100.152
  139.87.172.100
  ```

- -NoAuthentication — When NoAuthentication is specified, the bcmnbrus command allows the remote client to access the server without user authentication, see "Settings Page" on page 34 for a description of the available settings.

2 Then, to access Upgrade Link from a web browser, enter the following URL:

```
http://<server_nam>:<port>/
```

For example use the Browser URL:

```
http://129.222.224.53:12345/
```

Do not resize the browser window while the Upgrade Link application is running.

CAUTION: *Only one client at a time should access the Upgrade Link Server.*

Status and Settings Pages

After each procedure described in this section, the Status or Settings page appears. Table 3 describes each button on the Status page.

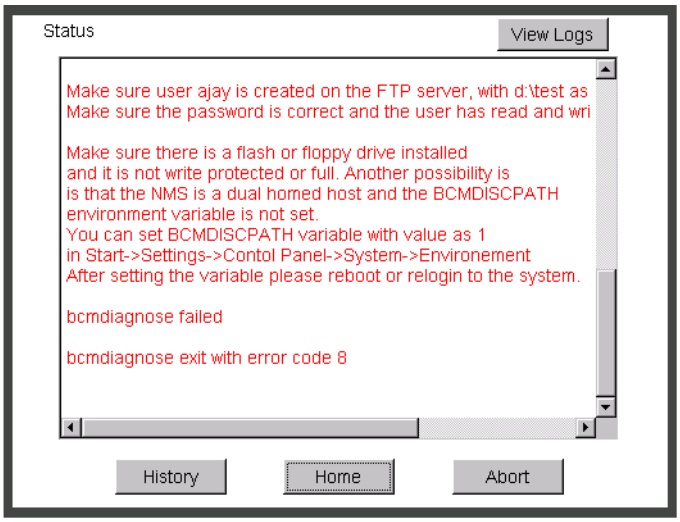
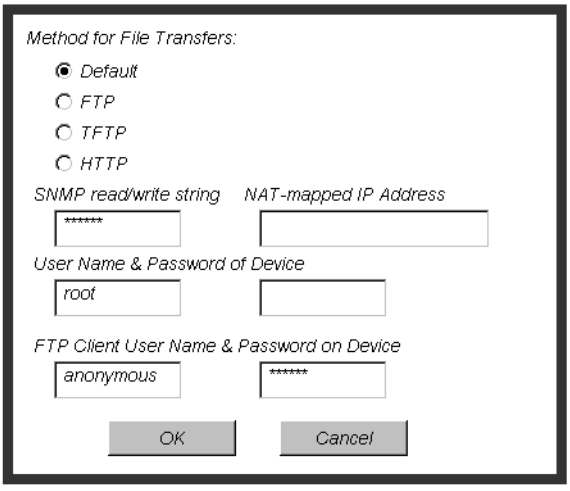


Table 3 Status page buttons

Button	Description
History	Shows the last 20 successful operations performed on the bridge/router or switch.
Home	Returns to the Console page.
Abort	Exits Upgrade Link and aborts the process. Some processes may need to be completed even after clicking *Abort*. Upgrade Link displays a message about any ongoing processes.
View Logs	Opens a page listing the logs available for viewing.

Settings Page

The Setting Page lets you establish basic settings.



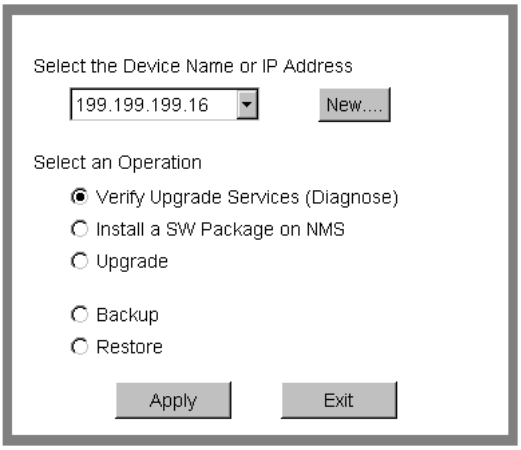
- You can choose the method of file transfers. TFTP is used by default for EOS 11.0 and lower while FTP is used by default for EOS 11.1 and higher and EOS 11.4. You can choose HTTP if your device is running EOS 11.4 or later.

- Enter an SNMP read/write string and the Enterprise OS device user name and password.
- If -NoAuthentication was not specified in Upgrade Link or on the bcmnbrus command line, authentication will be used and you must enter the Enterprise OS device username and password.
- If -NoAuthentication was specified in Upgrade Link or on the bcmnbrus command line, no authentication is required and any user name and password entries are ignored.
- If using FTP, enter the FTP client user name and password.
- If using HTTP, enter the NETBuilder user name and password.

Verifying for Upgrading

Before upgrading, run the diagnostic utility in Upgrade Link to verify connectivity to the device by following these steps:

1 Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.



2 Select *Verify Upgrade Services (Diagnose)* and click *Apply*.

The Settings Page appears. Select the appropriate settings as described in "Settings Page" on page 34 and click *OK* to close that window.

The Status page appears showing the results of the diagnostic tests.

3 If the Status page shows a failure, check the SNMP read/write community string and FTP/HTTP/TFTP server settings.

If the Status page shows a success, click *Home* to continue with the upgrade and return to the Console page.

Installing Software on the NMS

Upgrade Link installs the Enterprise OS software for the device on the NMS in the following directory:

Windows:

\%tftpboot%\image\<platform>\SW|FW\<version>\<pkg>

UNIX:

/tftpboot/image/<platform>/SW|FW/<version>/<pkg>

For UNIX, if there is not enough space on the disk, you can link /tftpboot to another disk. For example, to link /tftpboot to the usr directory, enter:

```
ln -s /usr/tftpboot /tftpboot/
```

The utilities work only with the default directory names and structures.

Values

tftpboot	For UNIX: Directory specified in inetd or tftpd for tftpd files.	
%tftpboot%	For Windows (using the default 3Com TFTP server): Directory specified in the 3Server configuration.	
<platform>	NETBuilder II with CEC Module:	NBII
	NETBuilder II with DPE Module:	NBDPE
	SuperStack II NETBuilder SI bridge/router:	NBSI
	SuperStack II NETBuilder Ethernet bridge/router:	NBRO
	SuperStack II NETBuilder Token Ring bridge/router:	NBR2T
	SuperStack II NETBuilder Ethernet/ISDN bridge/router:	NBRI
	SuperStack II NETBuilder Token Ring/ISDN bridge/router:	NBR2TI
	OfficeConnect NETBuilder bridge/router:	NBOCF
	PathBuilder S5xx switch:	NBPB500
	PathBuilder S400 switch:	PBS400
<package>	Two letter designator shown on the CD-ROM label.	
[SW | FW]	The software or firmware directory.	
<version>	Software version 9.0 through 11.4.	

To install the new software on the NMS, follow these steps:

You must be logged in as root for this procedure (UNIX).

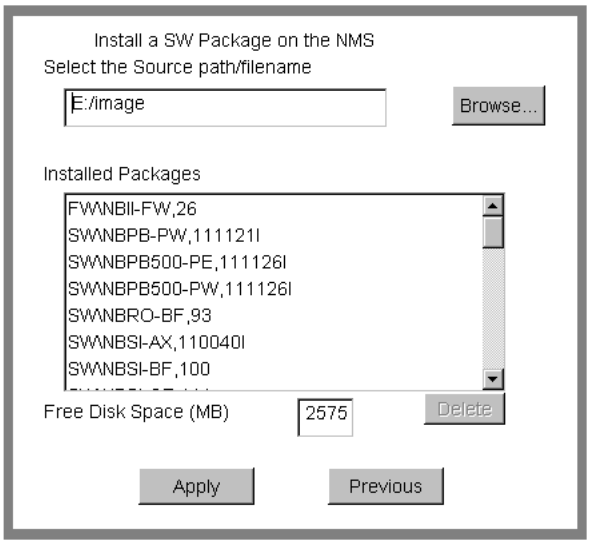
1. You can install the software from a CD-ROM, a tar archive, or a boot image (image-only upgrade). If you are installing from a CD-ROM, mount the CD-ROM on the NMS.

   See Appendix B for information on how to mount the CD-ROM on a UNIX system.

2. For UNIX, log in as root.
3. Run Upgrade Link if you have not already done so.
4. Select *Install a SW Package on NMS* from the Console page.

5 Click *Apply*.

The Install page appears.



6 Enter the path for the software, or click *Browse* to use a file browse page.

- For UNIX CD-ROM, use the following path:

  `cdrom/<mount path>/image/`

- For Windows CD-ROM, use the following path:

  `<CD-ROM drive>:\image\`

- For Archive, enter the entire path including the filename.
- For an FTP or HTTP site, enter the full URL

  For HTTP file transfers, clicking the *Browse...* button causes an error message to appear because you can not browse the HTTP server for files.

7 Click *Apply* to install the software.

If the source begins with either ftp: or http:, a dialog box appears that allows you to specify the FTP or HTTP Site *Username* and *Password*. The values supplied in this dialog box are placed into the environment variables BCMNBCUSER and BCMNBCPASS for HTTP or BCMFTPCUSER/PASS for FTP. These variables are used by bcminstall to connect to the HTTP or FTP server.

The Status page appears while the software is installing.

8 Select a package from the list that you want to uninstall. Click *Delete* to begin uninstalling the package. Confirm you selection when prompted.

9 When the installation is complete, click *Home* to continue with the upgrade.

Upgrading the Software

To upgrade the software, follow these steps:

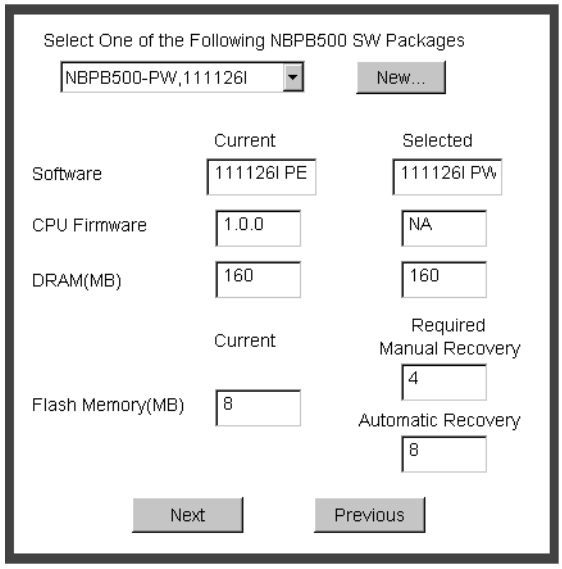
1 Run Upgrade Link if you have not already done so.

2 Choose a device to upgrade from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains bridge/routers and switches that you have upgraded or backed-up previously.

3 Select *Upgrade* and click *Apply*.

The Settings Page appears. Select the appropriate settings as described in "Settings Page" on page 34 and click *OK* to close the window.

The Upgrade page appears.

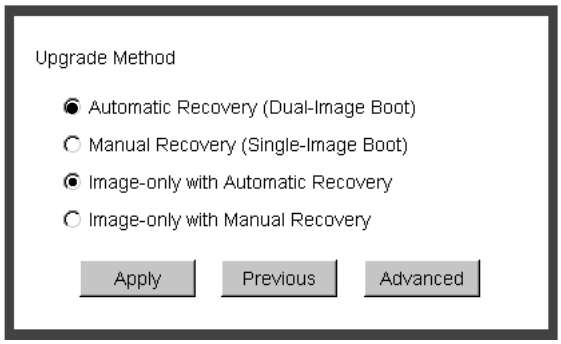


4 Select a software package from the pop-up list. The list includes all packages you have installed on the NMS for your platform. If your package is not listed, install the software by clicking New and see "Installing Software on the NMS" on page 35.

CAUTION: When upgrading to a package containing encryption, you will be presented with an export restriction message. To upgrade to an encrypted package, you must acknowledge this restriction notice, otherwise the upgrade will not continue.

The Upgrade page shows information about your system, including the flash memory requirements for a manual or automatic recovery upgrade.

5 Click *Next*.

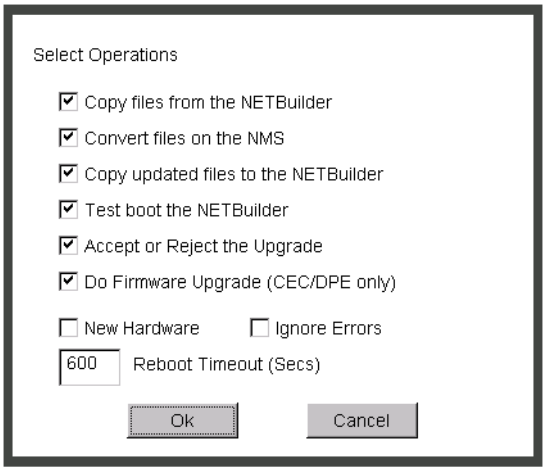


6 The recommended upgrade method is selected based on the amount of memory you have installed. If you do not wish to perform a customized upgrade, go to step 12.

CAUTION: *If you override the Upgrade Link selection, your upgrade may fail.*

7 Click on the Advanced button if you want to customize the upgrade process, that is, you do not want to perform all of the upgrade stages at this time.

The Advanced page appears.



8 Click the check box for each of the stages you want to complete in the current operation.

9 Click *New Hardware* if you are replacing your device with a new system. For example, click *New Hardware* if you are replacing the CEC module with a DPE module.

You cannot upgrade to a different platform. For example, you can only upgrade an OfficeConnect bridge/router to an OfficeConnect bridge/router. You cannot upgrade a SuperStack II NETBuilder bridge/router to a SuperStack II NETBuilder SI bridge/router. The only exception is an upgrade from a NETBuilder II CEC module to a DPE module.

10 If you want to alter the Reboot Timeout, enter a new number in the box. The default setting is appropriate for most networks.

11 Click *OK*.

12 Click *Apply* to begin the upgrade.

The Status page appears.

13 If you are performing a hardware upgrade, replacing a CEC module with a DPE module for example, a message to replace the hardware appears after the software has been backed up to the NMS. Replace the hardware at this time.

14 When the upgrade is complete, the bridge/router reboots from the new software. If the boot is not successful:

- **For automatic recovery**, the bridge/router reboots from the original software after the reboot timeout (default = 10 minutes).
- **For manual recovery**, you must configure the device at the local console to reestablish IP connectivity. Once connectivity is established, you can restore the software to return the device to a preupgrade state. See Chapter 7 for the procedure to restore connectivity and the software.

15 Click *Home* then *Exit* on the Console page to exit Upgrade Link.

5 UPGRADING USING THE COMMAND LINE UTILITIES

This chapter describes how to upgrade the software on an Enterprise OS device using the command line Upgrade Management Utilities. 3Com recommends using the Upgrade Link application described in Chapter 4, but you can use the command line utilities instead if you want to write scripts or if you do not have a web browser on your NMS. Use Transcend Enterprise Manager or Transcend Network Control Services to upgrade multiple bridge/routers.

You can perform the following types of upgrades:

- Upgrading Software Only
  - Upgrading Using Automatic Recovery
  - Upgrading Using Manual Recovery
- Upgrading Hardware and Software
  - Upgrading Using Automatic Recovery
  - Upgrading Using Manual Recovery

Preparing for the Upgrade

Before upgrading your Enterprise OS device, confirm the following items:

- You have installed the utilities according to Chapter 2.
- You have set the path for the utilities (UNIX only) according to Chapter 2. If you have not set the path, see "Installing the Utilities on a UNIX System" on page 18.
- All configuration files are in the same directory as the boot image.
- You have booted your device from the primary boot source.
- There is sufficient disk space on the NMS for the amount of software you are installing.

  Minimal disk storage requirements depend on the number of different software versions that are stored on the disk drive. Calculate:

  - 6 MB for each version of the NETBuilder II bridge/router or PathBuilder switch image
  - 4 MB for each version of the SuperStack II, SuperStack II SI, or OfficeConnect NETBuilder bridge/router image

  While you must purchase one copy of software for each bridge/router or switch, you only need to install one copy of a version of software on the NMS.
- You have set up a file transfer method as described in Chapter 3.

Prediagnosing System Problems

Before you begin your upgrade, 3Com recommends that you run the bcmdiagnose utility specifying the file transfer utility, FTP, HTTP, or TFTP and the IP address or hostname of the device you are upgrading.

Before using the bcmdiagnose utility, you should set the BCMFTPUSER and BCMFTPPASS environment variables. When using FTP, an error message is generated and the file transfer is aborted if these variables are not set.

The bcmdiagnose utility helps detect any problems with SNMP, FTP, HTTP, or TFTP connectivity.

To run the bcmdiagnose utility on your NMS, use:

```
bcmdiagnose [ -ftp | -http | -tftp ] [<device> | -h]
```

Where <device> is the IP address or hostname of the device you are upgrading. The -ftp, -http, and -tftp flags force the specified file transfer types. See Appendix A for more information about any error messages that may appear.

Installing the Software on the NMS

To install the Enterprise OS software for the device, follow these steps:

1. **For UNIX**, login as root.
2. If you are using a CD-ROM, insert the CD-ROM into the CD-ROM drive on the NMS.
   a. Mount the CD-ROM (UNIX only).

      See Appendix B for information on how to mount the CD-ROM.
3. Make sure you are using version 11.4 of the Enterprise OS Upgrade Management Utilities.

   To check which version you have installed, enter:

   `bcmdiagnose -h`

   The version of the installed utilities is displayed in the following message:

   ```
   bcmdiagnose version 11.4. Copyright 3Com Corporation 1999
   ```

   If the version of the utilities you have installed is not version 11.4, you must first install the 11.4 utilities according to Chapter 2.
4. Install the software.
   - **From a CD-ROM:**

     For UNIX, enter:

     `bcminstall`

     The path option may be used to install the utilities on an NMS that has two or more CD-ROM drives or to install from a remote CD-ROM drive. You must explicitly specify the second or remote CD-ROM drive using:

     ```
     bcminstall -cdrom [<path>]
     ```

     For example, to install software from a second CD-ROM drive on a Solaris machine, enter:

     `bcminstall -cdrom /cdrom/cdrom1/image`

After the installation is complete, the screen shows an inventory of all bridge/router packages installed, including previous versions you have installed.

For Windows, open a command window and use:

```
bcminstall -cdrom <CD-ROM drive>:\image
```

- **From a Tarred File**, use:

  ```
  bcminstall -tar <path>/<filename>
  ```

- **From an Image File**, use:

  ```
  bcminstall -image <path>/<filename>
  ```

The image file is the Enterprise OS device's boot file, for example, boot.29K or boot.68k.

Software Directories

The bcminstall utility installs the software on the NMS in the following directory:

Windows:

\%tftpboot%\image\<platform>\SW|FW\<version>\<pkg>

UNIX:

/tftpboot/image/<platform>/SW|FW/<version>/<pkg>

For UNIX, if there is not enough space on the disk, you can link /tftpboot to another disk. For example, to link /tftpboot to the usr directory enter:

```
ln -s /usr/tftpboot /tftpboot
```

The utilities work only with the default directory names and structures.

Values

tftpboot	For UNIX: Directory specified in inetd or tftpd for tftpd files.	
%tftpboot%	For Windows (using the default 3Com TFTP server): Directory specified in the Win.ini file in the "[3Com.nm] TFTPROOT=" section. The Win.ini file is located in the default Windows directory, for example C:\windows or C:\winnt4.	
<platform>	NETBuilder II with CEC Module:	NBII
	NETBuilder II with DPE Module:	NBDPE
	SuperStack II NETBuilder SI bridge/router:	NBSI
	SuperStack II NETBuilder Ethernet bridge/router:	NBRO
	SuperStack II NETBuilder Token Ring bridge/router:	NBR2T
	SuperStack II NETBuilder Ethernet/ISDN bridge/router:	NBRI
	SuperStack II NETBuilder Token Ring/ISDN bridge/router:	NBR2TI
	OfficeConnect NETBuilder bridge/router:	NBOCF
	PathBuilder S5xx Switch:	NBPB500
	PathBuilder WAN Convergence Switch	NBPB400
<package>	Two letter designator shown on the CD-ROM label.	
[SW | FW]	The software or firmware directory.	
<version>	Software version 9.0 through 11.4.	

Use the bcmuname utility to display your current platform, package, and version.

Using the Bcmsysupgrade Utility to Upgrade

This section describes how to use the bcmsysupgrade utility for the most common software upgrades.

The command syntax for the bcmsysupgrade utility is:

```
bcmsysupgrade [options] <stage> <device>
```

See "bcmsysupgrade" on page 85 for more information.

The procedures described in the following sections assume you are performing a *like-package* upgrade to version 11.4 with automatic recovery (see "Choosing Automatic Recovery or Manual Recovery" on page 23 for more information).

An example of a like-package upgrade is from the CF package to the CF package. A like-package upgrade is an upgrade where the software package in the version you are upgrading *from* and the version you are upgrading *to* have the same two-letter designator.

If your upgrade is not a like-package upgrade with automatic recovery, or you are upgrading to a version other than the default, you must use the bcmsysupgrade utility with other options. Be sure to use the same options during each stage of the upgrade process. See Table 4 for a description of the options.

For UNIX, after you have upgraded, check the /tftpboot/CLIENTS/<IP address or mac address>/tmp/stages.log file to ensure that the options were used consistently throughout the upgrade process.

For Windows, after you have upgraded, check the \%tftpboot%\CLIENTS\<IP address or mac address>\tmp\stages.log file to ensure that the options were used consistently throughout the upgrade process.

Table 4 lists the most common bcmsysupgrade options.

Table 4 Common Options for Bcmsysupgrade

Task	Option
Image-only upgrade **or** Upgrading to a software version other than 11.4	`-V:<version you are upgrading to>`
Upgrading unlike packages	`-k:<package you are upgrading to>`
Upgrading with Manual Recovery	`-m`
Specifying encryption license agreement.	`-EncryptionLicenseRead`
Using TFTP file transfer.	`-tftp`
Using HTTP file transfer.	`-http`
Using FTP file transfer.	`-ftp`

Whenever you specify an option with bcmsysupgrade, you must repeat that option for all steps in the procedure.

Example To upgrade a device from the SW/NBII-WA,8.3 package to the SW/NBII-FF, 10.1005 package (unlike packages, manual recovery, *and* a different package from 11.0), use:

```
bcmsysupgrade -s:from_nb -k:FF -V:101005 -m <device>
```

The same options must be used to upgrade configuration files:

```
bcmsysupgrade -s:update -k:FF -V:101005 -m <device>
```

See Chapter 8 for more information about how to use bcmsysupgrade for specialized cases.

Filenames

The following sections list the files that may be used when you upgrade a NETBuilder system.

NETBuilder II Bridge/Router

- **boot.29k** — image file that boots the main processor module.
- **mp6e.29k** — image file that boots the MP 6-port Ethernet module.
- **mpatm.29k** — image file that boots the MP ATMLink module.
- **mbri.68k** — image file that boots the HSS 8-Port BRI module.
- **4portwan.860** — image file that boots the HSS 4-Port WAN module.
- **iofw_upd.29k** — file that updates the firmware for HSS 3-port, HSS 4-port, HSS 8-port, and MP modules.
- **sys** — file that is used during the upgrade process to determine the source OT target software version.

- **ccsmacro** — file that contains predefined user macros.
- **fpupdate.29k** *(CEC Only)* — file that updates the CEC module firmware.

You may also have several configuration files that will be upgraded by the utilities.

SuperStack II NETBuilder and OfficeConnect NETBuilder Bridge/Routers

- **boot.68k** — image file that boots the system.
- **sys** — file that may be used during the upgrade process to determine the source or target software version.

You may also have several configuration files that will be upgraded by the utilities.

PathBuilder S5xx Series Switch

- **boot.ppc** — image file that boots the system.
- **sys** — file that may be used during the upgrade process to determine the source or target software version.

PathBuilder S400 WAN Convergence Switch

- **boot.ppc** — image file that boots the system.
- **sys** — file that may be used during the upgrade process to determine the source or target software version.

Upgrading Software Only

This section describes how to upgrade the software on your existing hardware using either automatic or manual recovery. If you are upgrading or replacing your bridge/router, switch or main processor module (NETBuilder II), follow the procedure in "Upgrading Hardware and Software" on page 49.

Upgrading Using Automatic Recovery

This section describes how to perform an upgrade of the Enterprise OS software that does not include a hardware upgrade. See Chapter 3 for the memory requirements for automatic recovery.

Whenever you specify an option with bcmsysupgrade, you must repeat that option for all steps in the procedure. See Table 4 on page 45 or "bcmsysupgrade" on page 85 for a list of the options available to use with the bcmsysupgrade utility.

To upgrade the bridge/router software to the default version, follow these steps:

1 Back up your current software to the NMS using:

```
bcmsysupgrade [options] -s:from_nb <device>
```

where [-options] lets you specify the -EncryptionLicenseRead flag that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the bridge/router you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

The bcmsysupgrade utility only backs up the files in the primary boot source. To archive both the primary and secondary boot sources, use bcmbackup instead of bcmsysupgrade. See "bcmbackup" on page 77 for more information.

2 *NETBuilder II with CEC only* — (The CEC module is *not* supported in software version 11.4. However, you can use the utilities to upgrade your CEC module to software version 10.1 or earlier.) If you are running CEC firmware versions 2.0 or 2.1, which are standard with NETBuilder II software versions 8.0, 8.1, and 8.2, you must upgrade your CEC firmware before proceeding to the next step.

CAUTION: *If you are running any other firmware version besides 2.0 or 2.1, you should upgrade the firmware* after *upgrading the software.*

To upgrade the CEC firmware, follow these steps:

a Make sure there is a floppy diskette with write access in the floppy drive on the bridge/router. The diskette is formatted during the upgrade, so make sure that the contents of the diskette you intend to use can be overwritten. Perform a manually recoverable firmware upgrade using the option -m if you do not want the floppy diskette formatted.

b Upgrade your firmware to version 2.6 using:

```
bcmsysupgrade -s:upgrade_cec_fw -V:<version you are upgrading to>
  <device>
```

After the firmware has been upgraded, the bridge/router reboots.

3 Update your configuration files using:

```
bcmsysupgrade -s:update <device>
```

4 Copy the upgraded software to the bridge/router using:

```
bcmsysupgrade -s:to_nb <device>
```

5 Test your new software using:

```
bcmsysupgrade -s:test_boot <device>
```

The bridge/router is rebooted, and the utilities confirm IP connectivity and that the expected version of software is running.

6 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded device. These may include:

- Some standard checks based on services active.

  A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific bridge/routers.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

7 Accept or reject the upgrade.

- If your upgrade completed successfully, accept your upgrade using:

  ```
  bcmsysupgrade -s:accept <device>
  ```

- If the upgrade process failed to meet your verification criteria, reject your upgrade using:

  ```
  bcmsysupgrade -s:reject <device>
  ```

  The bridge/router is rebooted using the previous version of software.

8 *NETBuilder II with CEC only* — (The CEC module is *not* supported in software version 11.4. However, you can use the utilities to upgrade your CEC module to software version 10.1 or earlier.) If the upgrade is successful, and if you have not already done so in step 2, upgrade the CEC firmware by following these steps:

   a Make sure there is a floppy diskette with write access in the floppy drive on the bridge/router. Make sure that the contents of the diskette you intend to use can be overwritten. Perform a manually recoverable firmware upgrade using the option -m if you do not want the floppy diskette formatted.

   b Upgrade your firmware to version 2.6 using:

   ```
   bcmsysupgrade -s:upgrade_cec_fw -V:<version you are upgrading to>
    <device>
   ```

   After the firmware has been upgraded, the bridge/router reboots.

9 *NETBuilder II only* — If the upgrade is successful, and the NETBuilder II bridge/router has a multiport HSS module or an MP module, upgrade the firmware for all these modules using:

   ```
   bcmsysupgrade -s:upgrade_io_fw -m <device>
   ```

   The bridge/router reboots after the firmware is upgraded.

Upgrading Using Manual Recovery

This section describes how to perform a software upgrade with manual recovery of a bridge/router that does not include a hardware upgrade. See Chapter 3 for the memory requirements for manual recovery.

Whenever you specify an option with bcmsysupgrade (such as -m), you must repeat that option for all steps in the procedure. See Table 4 on page 45 or "bcmsysupgrade" on page 85 for a list of the options available to use with the bcmsysupgrade utility.

To upgrade the bridge/router, follow these steps:

1 Back up your current software to the NMS using:

   ```
   bcmsysupgrade [-options] -s:from_nb -m <device>
   ```

   where [-options] lets you specify the -EncryptionLicenseRead flag that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the bridge/router you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

The bcmsysupgrade utility only backs up the files in the primary boot source. To archive both the primary and secondary boot sources, use bcmbackup instead of bcmsysupgrade. See "bcmbackup" on page 77 for more information.

2 Update your configuration files using:

   ```
   bcmsysupgrade -s:update -m <device>
   ```

3 Copy the upgraded software to the bridge/router using:

```
bcmsysupgrade -s:to_nb -m <device>
```

4 Accept your upgrade using:

```
bcmsysupgrade -s:accept -m <device>
```

The device reboots.

5 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded device. These may include:

- Some standard checks based on services active.

  A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific NETBuilder bridge/router.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

6 If you determine that the new software does not meet your requirements, you can reject the upgrade and revert to the software version you were running before the upgrade by using the bcmrestore utility.

To reject your upgrade, use:

```
bcmrestore <device>
```

7 *NETBuilder II only* — If the upgrade is successful, and the NETBuilder II bridge/router has a multiport HSS module or an MP module, upgrade the firmware for all these modules using:

```
bcmsysupgrade -s:upgrade_io_fw -m <device>
```

The bridge/router reboots after the firmware is upgraded.

If the Bridge/Router or Switch Does Not Boot

If a failure causes the bridge/router or switch not to boot, or if the bridge/router or switch is inaccessible using Telnet, you must configure the bridge/router at the local console to reestablish IP connectivity. After connectivity is reestablished, you can use the bcmrestore utility to return the bridge/router or switch to a preupgrade state. See Chapter 7 for connectivity and recovery procedures.

Upgrading Hardware and Software

This section describes how to upgrade the software on a bridge/router on which you are upgrading or replacing your bridge/router or switch or main processor module (NETBuilder II) using either automatic or manual recovery. If you are upgrading only the software, follow the procedure in "Upgrading Software Only" on page 46.

Upgrading Using Automatic Recovery

This section describes how to perform a software and hardware upgrade with automatic recovery. See Chapter 3 for the memory requirements for automatic recovery.

Whenever you specify an option with bcmsysupgrade (such as -new_hw), you must repeat that option for all steps in the procedure. See Table 4 on page 45 or "bcmsysupgrade" on page 85 for a list of the options available to use with the bcmsysupgrade utility.

To upgrade the bridge/router software and hardware, follow these steps:

1. Back up your current software to the NMS using:

   ```
   bcmsysupgrade [options] -s:from_nb -new_hw <device>
   ```

   where [-options] lets you specify the -EncryptionLicenseRead flag that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the bridge/router you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

The bcmsysupgrade utility only backs up the files in the primary boot source. To archive both the primary and secondary boot sources, use bcmbackup instead of bcmsysupgrade. See "bcmbackup" on page 77 for more information.

2. *NETBuilder II with CEC only* — (The CEC module is *not* supported in software version 11.1. However, you can use the utilities to upgrade your CEC module to software version 10.1 or earlier.) If you are running CEC firmware versions 2.0 or 2.1, which are standard with NETBuilder II software versions 8.0, 8.1, and 8.2, you must upgrade your CEC firmware before proceeding to the next step.

CAUTION: *If you are running any other firmware version besides 2.0 or 2.1, you should upgrade the firmware* after *upgrading the software.*

   To upgrade the CEC firmware, follow these steps:

   a. Make sure there is a floppy diskette with write access in the floppy drive on the bridge/router. Make sure that the contents of the diskette you intend to use can be overwritten. Perform a manually recoverable firmware upgrade using the option -m if you do not want the floppy diskette formatted.

   b. Upgrade your firmware to version 2.6 using:

      ```
      bcmsysupgrade -s:upgrade_cec_fw -V:<version you are upgrading to>
        <device>
      ```

   After the firmware has been upgraded, the bridge/router reboots.

3. Update your configuration files using:

   ```
   bcmsysupgrade -s:update -new_hw <device>
   ```

4. Swap your hardware.

5. Attach a console to the Console port on the bridge/router.

6. Set up IP routing by following these steps:

   a. Log on to the bridge/router as root and press the Return key.

      The password prompt is displayed.

b At the password prompt, press the Return key.

The network manager prompt (Enterprise OS #) is displayed.

c Set up an IP address and subnet mask using:

```
SETDefault !<port> -IP NETaddr = <IP address> [<subnet mask>]
```

Where <port> is the port through which the bridge/router can be accessed by the NMS.

d Enable IP routing by entering:

```
SETDefault -IP CONTrol = ROute
```

e Enable a route discovery protocol. For example, enable OSPF by using:

```
SETDefault !<port> -OSPF CONTrol = Enable
```

f Check your configuration by pinging the bridge/router from the NMS:

```
ping <IP address>
```

Where <IP address> is the IP address of the bridge/router.

7 Set up SNMP.

This guide does not describe in detail how to set up the SNMP Service. See *Using Enterprise OS Software* and *Reference for Enterprise OS Software* for more information.

To enable SNMP read/write access, you need to modify two parameters in the SNMP Service: COMmunity and MANager.

a The COMmunity parameter modifies the list of communities. For information on how to use the COMmunity parameter, See *Using Enterprise OS Software* and *Reference for Enterprise OS Software.*

By default all bridge/router configuration files are accessible to an SNMP-based manager with read privileges. To change SNMP access to configuration files to read/write for a network management station for a community named public, enter:

```
ADD -SNMP COMmunity "public" RW
```

b With the MANager parameter, create a new manager with read/write access to the bridge/router. For security reasons, limit the number of network management stations by entering the IP address of the network management station that will have access. For example, enter:

```
ADD -SNMP MANager “sysadm” 129.213.224.1
```

8 Copy the upgraded software to the bridge/router using:

```
bcmsysupgrade -s:to_nb -new_hw <device>
```

9 Test your new software using:

```
bcmsysupgrade -s:test_boot -new_hw <device>
```

The bridge/router is rebooted, and the utilities confirm IP connectivity and that the expected version of software is running.

10 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded device. These may include:

- Some standard checks based on services active.

A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific bridge/routers.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

11 Accept or reject the upgrade.

- If your software upgrade completed successfully, accept your upgrade using:

  ```
  bcmsysupgrade -s:accept -new_hw <device>
  ```

- If the upgrade process failed to meet your verification criteria, reject your upgrade using:

  ```
  bcmsysupgrade -s:reject -new_hw <device>
  ```

  The bridge/router is rebooted using the previous version of software.

12 *NETBuilder II with CEC only* — (The CEC module is *not* supported in software version 11.1. However, you can use the utilities to upgrade your CEC module to software version 10.1 or earlier.) If the upgrade is successful, and if you have not already done so in step 2, upgrade the CEC firmware by following these steps:

a Make sure there is a floppy diskette with write access in the floppy drive on the bridge/router. Make sure that the contents of the diskette you intend to use can be overwritten. Perform a manually recoverable firmware upgrade using the option -m if you do not want the floppy diskette formatted.

b Upgrade your firmware to version 2.6 using:

```
bcmsysupgrade -s:upgrade_cec_fw -V:<version you are upgrading to>
 <device>
```

After the firmware has been upgraded, the bridge/router reboots.

13 *NETBuilder II only* — If the upgrade is successful, and the NETBuilder II bridge/router has a multiport HSS module or an MP module, upgrade the firmware for all these modules using:

```
bcmsysupgrade -s:upgrade_io_fw -m <device>
```

The bridge/router reboots after the firmware is upgraded.

Upgrading Using Manual Recovery

This section describes how to perform a software and hardware upgrade with manual recovery. See Chapter 3 for the memory requirements for manual recovery.

Whenever you specify an option with bcmsysupgrade (such as -m and -new_hw), you must repeat that option for all steps in the procedure. See Table 4 on page 45 or "bcmsysupgrade" on page 85 for a list of the options available to use with the bcmsysupgrade utility.

To upgrade the bridge/router, follow these steps:

1. Back up your current software to the NMS using:

   ```
   bcmsysupgrade [options] -s:from_nb -m -new_hw <device>
   ```

   where [-options] lets you specify -EncryptionLicenseRead that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the bridge/router you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

The bcmsysupgrade utility only backs up the files in the primary boot source. To archive both the primary and secondary boot sources, use bcmbackup instead of bcmsysupgrade. See "bcmbackup" on page 77 for more information.

2. Update your configuration files using:

   ```
   bcmsysupgrade -s:update -m -new_hw <device>
   ```

3. Upgrade your hardware.
4. Attach a console to the Console port on the bridge/router.
5. Set up IP routing by following these steps:
   a. Log on to the bridge/router as root and press the Return key.

      The password prompt is displayed.

   b. At the password prompt, press the Return key.

      The network manager prompt (Enterprise OS #) is displayed.

   c. Set up an IP address and subnet mask using:

      ```
      SETDefault !<port> -IP NETaddr = <IP address> [<subnet mask>]
      ```

      Where <port> is the port through which the bridge/router can be accessed by the NMS.

   d. Enable IP routing by entering:

      SETDefault -IP CONTrol = ROute

   e. Enable a routing protocol. For example, enable RIP by using:

      ```
      SETDefault !<port> -RIPIP CONTrol = (TAlk, LIsten)
      ```

   f. Check your configuration by verifying that the bridge/router is accessible by using the following at the network management station:

      ```
      PING <IP address>
      ```

      <IP address> is the IP address of the bridge/router.

6. Set up SNMP.

   This guide does not describe in detail how to set up the SNMP Service. See *Using Enterprise OS Software* and *Reference for Enterprise OS Software* for more information.

   To enable SNMP read/write access, you need to modify two parameters in the SNMP Service: COMmunity and MANager.

a The COMmunity parameter modifies the list of communities. For information on how to use the COMmunity parameter, see *Using Enterprise OS Software* and *Reference for Enterprise OS Software.*

By default all configuration files are accessible to an SNMP-based manager with read privileges. To change SNMP access to configuration files to read/write for a network management station for a community named public, enter:

```
ADD -SNMP COMmunity "public" RW
```

b With the MANager parameter, create a new manager with read/write access to the bridge/router. For security reasons, limit the number of network management stations by entering the IP address of the network management station that will have access.

For example, enter:

```
ADD -SNMP MANager “sysadm” 129.213.224.1
```

7 Copy the upgraded software to the bridge/router using:

```
bcmsysupgrade -s:to_nb -m -new_hw <device>
```

8 Accept your upgrade using:

```
bcmsysupgrade -s:accept -m -new_hw <device>
```

The bridge/router reboots.

9 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded bridge/router. These may include:

- Some standard checks based on services active.

  A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific NETBuilder bridge/routers.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

10 If you determine that the new software does not meet your requirements, you can reject the upgrade, and revert to the software version you were running before the upgrade, by using the bcmrestore utility.

To reject your upgrade, use:

```
bcmrestore -new_hw <device>
```

11 *NETBuilder II only* — If the upgrade is successful, and the NETBuilder II bridge/router has a multiport HSS module or an MP module, upgrade the firmware for all these modules using:

```
bcmsysupgrade -s:upgrade_io_fw -m <device>
```

The bridge/router reboots after the firmware is upgraded.

If the Bridge/Router or Switch Does Not Boot

If a failure causes the bridge/router not to boot, or if the bridge/router or switch is inaccessible using Telnet, you must configure the bridge/router or switch at the local console to reestablish IP connectivity. After connectivity is reestablished, you can use the bcmrestore utility to return the bridge/router or switch to a preupgrade state. See Chapter 7 for connectivity and recovery procedures.

6 UPGRADING THE SOFTWARE IMAGE ONLY

An image-only upgrade is an upgrade that replaces the NETBuilder bridge/router, PathBuilder S5xx series switch, or PathBuilder S400 WAN Convergence switch boot image file but does not upgrade any configuration files. You can perform an image-only upgrade in the following cases:

- You are installing a patch release for your current version of software.
- You are upgrading to a different package of the same version.
- Your new version does not require updated configuration files (for example, 10.1 to 10.3).
- You are upgrading a PathBuilder S5xx series switch or PathBuilder S400 WAN Convergence switch.

You can upgrade:

- Using the Upgrade Link application
- Using the command line utilities
- Using the Enterprise OS user interface

You can also use Transcend Enterprise Manager or Transcend Network Control Services to perform an image-only upgrade. See the guide that came with Transcend for more information.

3Com recommends using the utilities instead of the Enterprise OS user interface. The utilities automatically back up the software and perform all the necessary copying and boot source settings automatically.

Preparing for the Upgrade

If you are using Upgrade Link or the command line, confirm the following items:

- You have installed the utilities according to Chapter 2.
- You have set the path for the utilities (UNIX only) according to Chapter 2. If you have not set the path, see "Installing the Utilities on a UNIX System" on page 18.
- All configuration files are in the same directory as the boot image.
- You have booted your Enterprise OS device from the primary boot source.
- *For Upgrade Link* — You have a web browser installed with Java support, such as Netscape Navigator 4.08, Netscape Communicator 5.0, or Internet Explorer 5.0, and it is in your path (UNIX).
- There is sufficient disk space on the NMS for the amount of software you are installing.

Minimal disk storage requirements depend on the number of different software versions that are stored on the disk drive. Calculate:

- 6 MB for each version of the NETBuilder II bridge/router or PathBuilder switch image
- 4 MB for each version of the SuperStack II, SuperStack II SI, or OfficeConnect NETBuilder bridge/router image

While you must purchase one copy of software for each device, you only need to install one copy of a version of software on the NMS.

- You have set up a file transfer method as described in Chapter 3.

Upgrading the Image Using Upgrade Link

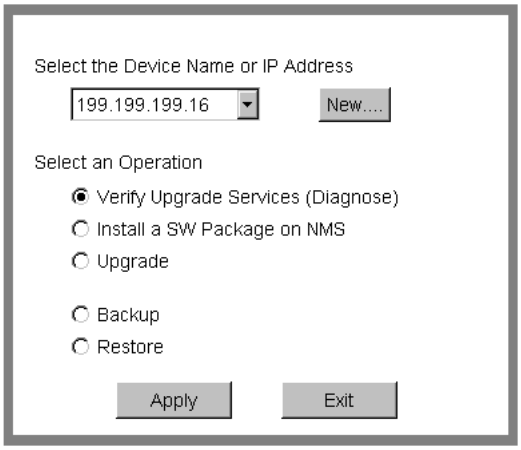
Upgrade Link contains its own web server. Client access to the web server is available locally or remotely via a web browser. Running the Upgrade Link application locally means that the web browser and the web server are running on the same NMS.

See Chapter 4 for information on starting and using the Upgrade Link application.

Verifying the Device for Upgrading

Before upgrading, run the diagnostic utility in Upgrade Link to verify connectivity to the Enterprise OS device by following these steps:

1 Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.



2 Select *Verify Upgrade Services (Diagnose)* and click *Apply*.

The Settings Page appears. Select the appropriate settings as described in "Settings Page" on page 34 and click *OK* to close that window.

The Status page appears showing the results of the diagnostic tests.

3 If the Status page shows a failure, check the SNMP read/write community string and FTP/TFTP server settings.

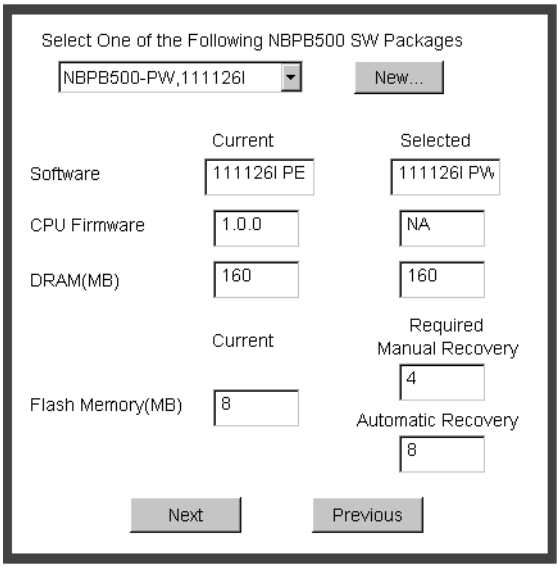
If the Status page shows a success, click *Home* to continue with the upgrade and return to the console page.

Upgrading the Image

To upgrade the image, follow these steps:

1. Run Upgrade Link if you have not already done so.
2. Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.
3. Select *Upgrade* and click *Apply*.

   The Upgrade page appears.

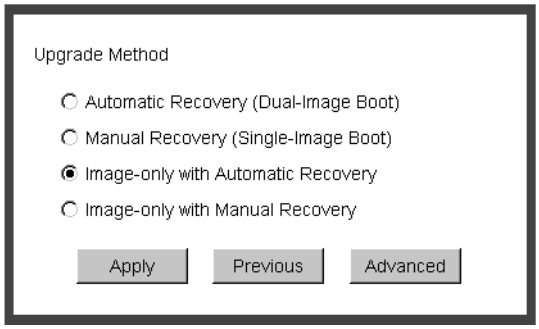


4. Select a software package from the pop-up list. The list includes all packages you have installed on the NMS for your platform. If your package is not listed, install the software using the procedure in "Installing the Utilities on a Network Management Station" on page 17.

CAUTION: *If you select an Enterprise OS software package that includes encryption, a message regarding the license agreement appears. To proceed with the installation you must accept this agreement.*

The Upgrade window shows information about your system, including the flash memory requirements for a manual or automatic recovery upgrade.

5. Click *Next*.

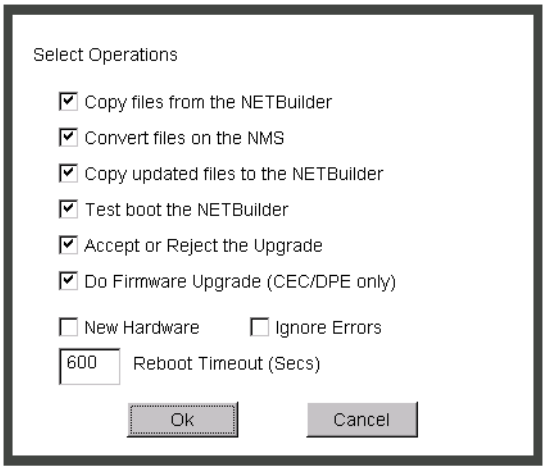


6 The recommended upgrade method is selected based on the amount of memory you have installed. If you do not wish to perform a customized upgrade, go to step 12.

CAUTION: *If you override the Upgrade Link selection, your upgrade may fail.*

7 Click on the Advanced button if you want to customize the upgrade process, that is you do not want to perform all of the upgrade at this time.

The Advanced Dialog box appears.



8 Click *New Hardware* if you are replacing your device with a new system. For example, click *New Hardware* if you are replacing the CEC module with a DPE module.

You cannot upgrade to a different platform. For example, you can only upgrade an OfficeConnect bridge/router to an OfficeConnect bridge/router. You cannot upgrade a SuperStack II NETBuilder bridge/router to a SuperStack II NETBuilder SI bridge/router. The only exception is an upgrade from a NETBuilder II CEC module to a DPE module.

9 If you want to alter the Reboot Timeout, enter a new number in the box. The default setting is appropriate for most networks.

10 Click the check box for each of the stages you want to complete in the current operation.

11 Click *OK*.

12 Click *Apply* to begin the upgrade.

The Status page appears.

13 If you are performing a hardware upgrade, replacing a CEC module with a DPE module for example, a message to replace the hardware appears after the software has been backed up to the NMS. Replace the hardware at this time.

14 When the upgrade is complete, the device reboots from the new software. If the boot is not successful:

- **For automatic recovery**, the bridge/router reboots from the old software.
- **For manual recovery**, you must configure the device at the local console to reestablish IP connectivity. Once connectivity is established, you can restore the software to return the device to a preupgrade state. See Chapter 7 for the procedure to restore connectivity and the software.

15 Click *Home* then *Exit* to exit Upgrade Link.

Upgrading the Image Using the Command Line Utilities

Use the command line utilities within a script or execute the commands manually. Otherwise, use Upgrade Link as described on page 58.

Installing the NETBuilder Software

You can upgrade from a CD-ROM, a tar file, or an image you have downloaded from 3Com. If you are installing the software from a CD-ROM, complete the procedure in "Installing the Software on the NMS" on page 42.

You can choose to transfer files using FTP, HTTP, or TFTP. Complete the procedure in "Setting Up a File Transfer Method" on page 21.

Prediagnosing System Problems

Detect any problems with SNMP or FTP/HTTP/TFTP connectivity using:

```
bcmdiagnose [ -ftp | -http | -tftp ] [<device> | -h]
```

Where <device> is the IP address or hostname of the device you are upgrading. The -ftp, -http, and -tftp flags force the specified file transfer types. See Appendix A for more information about any error messages that may appear.

Upgrading Using Automatic Recovery

To perform an image-only upgrade using automatic recovery, follow these steps. See Chapter 3 for the memory requirements for automatic recovery.

Whenever you specify an option with bcmsysupgrade, you must repeat that option for all steps in the procedure.

1 Back up your current software to the NMS using:

```
bcmsysupgrade [-options] -s:from_nb -I -V:<software version> <device>
```

where [-options] lets you specify the EncryptionLicenseRead option that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the Enterprise OS device you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

2 Copy the configuration files into the new software directory on the NMS using:

```
bcmsysupgrade -s:update -I -V:<software version> <device>
```

3 Copy the upgraded software to the device using:

```
bcmsysupgrade -s:to_nb -I -V:<software version> <device>
```

4 Test your new software using:

```
bcmsysupgrade -s:test_boot -I -V:<software version> <device>
```

The bridge/router is rebooted, and the utilities confirm IP connectivity and that the expected version of software is running.

5 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded network. These may include:

- Some standard checks based on services active.

A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific bridge/routers or switches.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

6 Accept or reject the upgrade.

- If your software upgrade completed successfully, accept your upgrade using:

  ```
  bcmsysupgrade -s:accept -I -V:<software version> <device>
  ```

- If the upgrade process failed to meet your verification criteria, reject your upgrade using:

  ```
  bcmsysupgrade -s:reject -I -V:<software version> <device>
  ```

  The Enterprise OS device is rebooted using the previous version of software.

Upgrading Using Manual Recovery

To perform an image-only upgrade using manual recovery, follow these steps. See Chapter 3 for the memory requirements for manual recovery.

Whenever you specify an option with bcmsysupgrade, you must repeat that option for all steps in the procedure.

1 Back up your current software to the NMS using:

```
bcmsysupgrade [-options] -s:from_nb -m -I -V:<software version> <device>
```

where [-options] lets you specify the EncryptionLicenseRead option that indicates you have read and understand the encryption license agreement notice and <device> is the IP address or hostname of the bridge/router you are upgrading.

CAUTION: *When upgrading to a package containing encryption, you must specify the -EncyrptionLicenseRead option flag. If you attempt to upgrade to an encrypted package and you have not specified the -EncryptionLicenseRead option, the upgrade will fail.*

2 Copy the configuration files into the new software directory on the NMS using:

```
bcmsysupgrade -s:update -m -I -V:<software version> <device>
```

3 Copy the new software to the bridge/router using:

```
bcmsysupgrade -s:to_nb -m -I -V:<software version> <device>
```

4 Accept the upgrade using:

```
bcmsysupgrade -s:accept -I -m -V:<software version> <device>
```

The bridge/router reboots.

5 Verify that your upgrade completed successfully.

To verify that the software is working properly, you can perform a set of operational integrity checks on the newly upgraded network. These may include:

- Some standard checks based on services active.

  A basic service verification test can Ping to specific IP addresses.

- Connectivity checks based on network topology.

  Examples of a connectivity verification include:

  - Checking the connectivity between devices on different networks, through designated bridge/routers or switches.
  - Testing typical device connections on terminals, printers, or hosts.
  - Testing the connectivity with specific bridge/routers or switches.

- Custom checks based on applications and typical network use.

  For instance, you can check normal operation over the network and perform file transfers, as well as run traces on specific routes or check routing tables.

6 If you determine that the new software does not meet your requirements, you can reject the upgrade, and revert to the software version you were running before the upgrade, by using the bcmrestore utility.

To reject your upgrade, use:

```
bcmrestore <device>
```

Upgrading the Image Using the Enterprise OS User Interface

If you have not installed the utilities, you can copy the boot image to the Enterprise OS device using the Enterprise OS user interface. To copy the boot image to the device, follow these steps:

1 Install the software on a FTP/HTTP/TFTP server on the LAN.

2 Attach a console or Telnet to the Enterprise OS device.

3 Log in with Network Manager privilege.

4 Change to the primary boot source directory using:

```
ChangeDir [<device>:]<path>
```

The default device is drive A.

5 Complete one of the following procedures:

- If you have enough room on the bridge/router for both the current and new image files, change the name of the current boot image using:

  ```
  ReName <image name> <new name>
  ```

  For example:

  `ReName boot.68k oldboot`

- If you do not have enough room on the bridge/router for both images, copy the current image to the FTP/HTTP/TFTP server for backup using:

  ```
  COpy <image name> <IP address of server>:<path/>
  ```

  Then delete the image on the Enterprise OS device using:

  ```
  RemoveFile <image name>
  ```

6 Copy the new boot file from the FTP/HTTP/TFTP server to the current (primary boot) directory using:

```
COpy <IP address of server>:<path/><image name>
```

For example:

COpy 129.142.10.10:image/NBSI/SW/114/CF/boot.68k boot.68k

7 Reboot the system by entering:

ReBoot

If the reboot is unsuccessful, the device enters the monitor utility. Boot from the old boot file using:

BT /<path>/<old name>

For example:

BT /primary/oldboot

7 BACKING UP AND RESTORING SOFTWARE

You should always back up your software and configuration files to a network management station (NMS) in case your hardware or software fails. This chapter describes how to back up and restore the software using Upgrade Link or the command line utilities.

Preparing for the Backup

Confirm the following items:

- You have installed the utilities according to Chapter 2.
- You have set the path for the utilities (UNIX only) according to Chapter 2. If you have not set the path, see "Installing the Utilities on a UNIX System" on page 18.
- *For NETBuilder II with DPE* — All boot sources (primary, secondary, and test) are on drive A. Since the DPE module has flash memory drives A and B, the Enterprise OS Upgrade Management Utilities support both drives; however, the configuration and image files must be located on the same drive. Use the bcmconfig utility or the SysconF command on the NETBuilder II user interface to set up the boot sources if they are not on drive A.
- All configuration files are in the same directory as the boot image.
- You have booted your device from the primary boot source.
- *For Upgrade Link* — You have a web browser installed with Java support, such as Netscape Navigator 4.08, Communicator 4.5, Netscape Communicator 5.0, or Microsoft Internet Explorer 5.0, and it is in your path (UNIX).
- You have set up a file transfer method as described in Chapter 3.

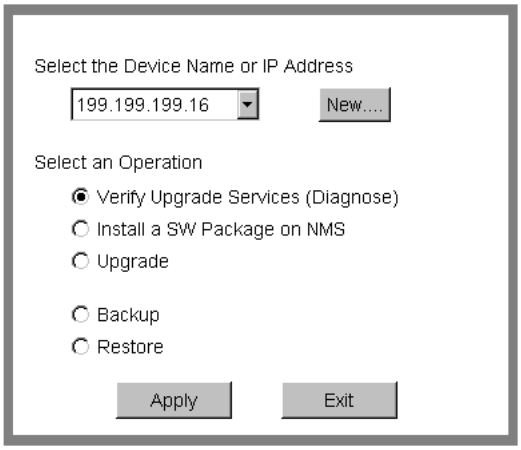
Backing Up the Software Using Upgrade Link

Upgrade Link is an easy to use GUI for the utilities that runs in a web browser. See Chapter 4 for information on running Upgrade Link locally or remotely. Make sure you select and set up your file transfer method.

Verifying the Device for Backing Up

Before backing up, run the diagnostic utility in Upgrade Link to verify connectivity to the device by following these steps:

1. Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.



2. Select *Verify Upgrade Services (Diagnose)* and click *Apply*.

   The Settings Page appears. Select the appropriate settings as described in "Settings Page" on page 34 and click *OK* to close that window.

   The Status page appears showing the results of the diagnostic tests.

3. If the Status window shows a failure, check the SNMP read/write community string for FTP/HTTP/TFTP file transfer permissions.

   If the Status window shows a success, click *Home* to continue with the backup.

Backing Up the Software

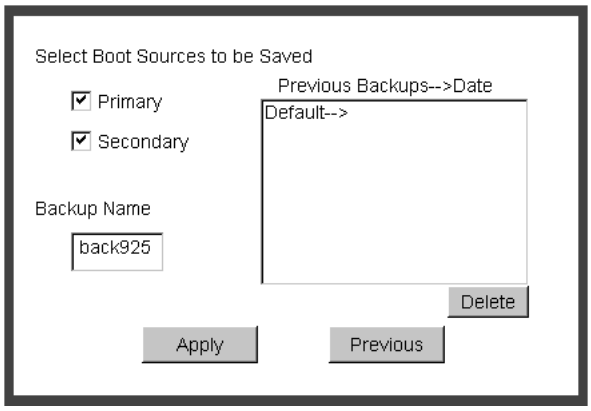
To back up the software, follow these steps:

1. Run Upgrade Link if you have not already done so.
2. Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devicess that you have upgraded or backed-up before.
3. Select *Backup* and click *Apply*.

   The Settings page appears.

4. Select the appropriate settings and click *OK*.

   The Backup page appears.



5 Select the boot source you want to back up.

The box on the right shows information about the previous backups.

Assign a name to the current backup by entering a name in the edit box. Names can be only eight characters long and may only contain alphanumeric characters.

6 Click *Apply* to begin the backup.

The Status window shows when the backup is complete.

7 Click *Home* then *Exit* to exit Upgrade Link.

Backing up the Software Using the Command Line Utilities

You can use the command line utilities if you want to write scripts or if you do not have a web browser on your NMS. See Chapter 5 for information on using the command line utilities. Make sure you select and set up your file transfer method.

Use the command line utilities if you have a script or if you do not have a web browser. Otherwise, use Upgrade Link as described on page 65.

Prediagnosing System Problems

Detect any problems with SNMP or FTP/HTTP/TFTP connectivity using:

```
bcmdiagnose [ -ftp | -http | -tftp ] [<device> | -h] [-NoAuthentication]
```

Where <device> is the IP address or hostname of the device you are upgrading. The -ftp, -http, and -tftp flags force the specified file transfer types. See Appendix A for more information about any error messages that may appear.

If diagnosing a device running Enterprise OS 8.3 or earlier, use the -NoAuthentication command.

Backing Up the Software

To back up your software to an NMS, use:

```
bcmbackup [both | primary | secondary] [-name:<backname>]<device>]
```

Values

both	Backs up both the primary and secondary boot source. This value is the default.
primary	Backs up the primary boot source.
secondary	Backs up the secondary boot source.
<backname>	Specifies the name of the backup for the boot blocks.

<device> The IP address or hostname of the device.

Directory Paths

All backups and upgrades use the following directory paths.

For UNIX:

```
/tftpboot/CLIENTS/<mac_address>/bcm/<backname><directory name on
   bridge/router>/
```

For example:

/tftpboot/CLIENTS/0800020A399E/bcm/name/primary/

For Windows:

```
\%tftpboot%\CLIENTS\<mac_address>\bcm\<backname>\<directory name on
   bridge/router>\
```

For example:

\tftpboot\CLIENTS\0800020A399E\bcm\name\primary

Values

tftpboot	For UNIX: Directory specified in inetd or tftpd for tftpd files.
%tftpboot%	For Windows (using the default 3Com TFTP server): Directory specified in the Win.ini file in the "[3Com.nm] TFTPROOT=" section. The Win.ini file is located in the default Windows directory, for example C:\windows or C:\winnt4.
CLIENTS	Name of the directory.
<mac_ address>	The MAC address of the device.
<directory name on bridge/router>	The name of the boot directory on the device. If the primary boot source is set to "/," the name of the current version of software is used instead. If the secondary boot source is set to "/," then the directory is called "secondar".

Restoring Software from a Backup

If your Enterprise OS device fails, you can restore software from a backup on the NMS. If your hardware fails or you lose IP and SNMP configuration, you must first reconfigure IP and SNMP on the device. If you still have connectivity, go to "Restoring the Software Using Upgrade Link" on page 71 or "Restoring the Software Using the Command Line" on page 72.

Configuring IP Routing

If the device failure interrupted IP connectivity, you must set up IP routing before restoring software.

To set up IP routing, follow these steps:

1. Attach a console to the Console port on the device.
2. Log on as root and press the Return key.

   The password prompt is displayed.
3. At the password prompt, press the Return key.

   The network manager prompt (Enterprise OS #) is displayed.

4 Set up an IP address and subnet mask using:

```
SETDefault !<port> -IP NETaddr = <IP address> [<subnet mask>]
```

For more information on IP configuration, see *Using Enterprise OS Software.*

5 Enable IP routing by entering:

```
SETDefault -IP CONTrol = ROute
```

6 Enable a routing protocol. For example, enable OSPF using:

```
SETDefault !<port> -OSPF CONTrol = Enable
```

7 Ensure your configuration by verifying that the device is accessible from the NMS using:

```
PING <IP address>
```

Where <IP address> is the IP address of the device.

Configuring SNMP

This chapter does not describe in detail how to set up the SNMP Service. See *Using Enterprise OS Software* and *Reference for Enterprise OS Software* for more information.

To enable SNMP read/write access, you need to modify two parameters in the SNMP service: Community Manager and Manager.

1 The Community Manager parameter modifies the list of communities. For information on how to use the COMmunity parameter, see *Using Enterprise OS Software* and *Reference for Enterprise OS Software.*

By default all device configuration files are accessible to an SNMP-based manager with read privileges. To change SNMP access to configuration files to read/write for a network management station with a community named "public," enter:

```
ADD -SNMP COMmunity "public" RW
```

2 With the Manager parameter, create a new manager with read/write access to the device. For security reasons, limit the number of network management stations by entering the IP address of the network management station that will have access. For example, enter:

```
ADD -SNMP Manager "sysadm" 129.213.224.1
```

Mapping Hostnames Using the etc/snmp.cfg File

/etc/snmp.cfg is used to configure a mapping between hostnames and/or IP addresses and SNMP community strings. If the device is configured to accept a community string other than "public", you need to update this file with the new community string. Follow the examples in the file when adding your own entries.

You need to use this file when you have several devices with different SNMP COMmunity strings. For example, most devices in your network have the SNMP COMmunity string "secure," but one device, with IP address 100.100.1.5, has an SNMP COMmunity string of "extrasecure." The entry in /etc/snmp.cfg for that bridge/router would be:

```
#Name       read       write      Timeout
100.100.1.5 extrasecure extrasecure 10
```

You do not need entries in /etc/snmp.cfg for the other bridge/routers with a common SNMP COMmunity string.

Another reason to use the /etc/snmp.cfg file is when you want the "write COMmunity string to be different from the "read" COMmunity string. For example, you want to use "secure as the "read" COMmunity string and "extrasecure" as the "write" COMmunity string. The entry in /etc/snmp.,cfg for that bridge/router would be:

```
#Name        read        write       Timeout
100.100.1.1 secure      extrasecure 10
100.100.1.2  secure     extrasecure 10
```

You will need an entry in /etc/snmp.cfg for every bridge/router for which this situation applies. Also, the SNMP COMmunity string "extrasecure" can be used for reading, as the bridge/router cannot be configured with a "write-only" SNMP COMmunity string.

The following is an example file.

```
#
# This file indicates which community strings are to be used
# with a particular device.  Follow the examples below
# Timeout values are given in seconds.
#
# Name     read   write   Timeout [Platform]
# foo      public private 10      netbuilder
#
# [platform] is optional, and must be one of:
# netbuilder
# netbuilder2
# netbuilderro
# netbuilder+
# lanplex5004
# lanplex5012
# lanplex6004
# lanplex6004R4
# lanplex6012
# lanplex6012R4
# lanplex2500
# lanplex2016
# fms
# fmsII
# fmsbridge
# fmstp8i
# linkswitch
# linkswitch1000
# linkswitch2200
# linkswitch3000
# msh
# msh4bridge
# mshfddi
# mshlinkswitch
# mshtrbridge
# linkconverter
#
# Example:
# 192.0.10.4 private private 10
100.100.1.5 extrasecure extrasecure 10
100.100.1.1 secure      extrasecure 10
100.100.1.2  secure     extrasecure 10
```

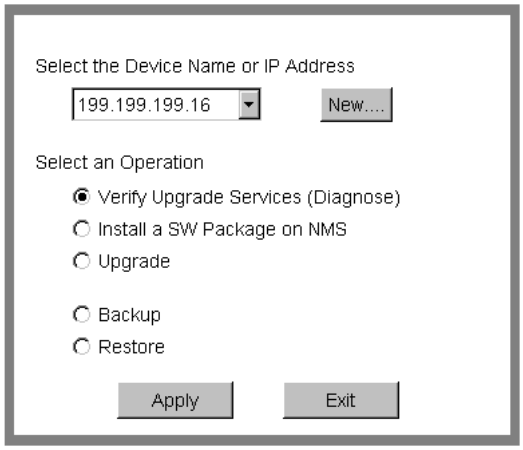
Restoring the Software Using Upgrade Link

Upgrade Link is an easy to use GUI for the utilities that runs in a web browser. See Chapter 4 for information on running Upgrade Link locally or remotely. Make sure you select and set up your file transfer method.

Verifying the Device for Restoring

Before restoring, you should run the diagnostic utility in Upgrade Link to verify connectivity to the device by following these steps:

1. Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.



2. Select *Verify Upgrade Services (Diagnose)* and click *Apply*.

   The Settings Page appears. Select the appropriate settings as described in "Settings Page" on page 34 and click *OK* to close that window.

   The Status page appears showing the results of the diagnostic tests.

3. If the Status window shows a failure, check the SNMP read/write community string for FTP/HTTP/TFTP file transfer permissions.

   If the Status window shows a success, click *Home* to continue with the restoration.

Restoring the Software

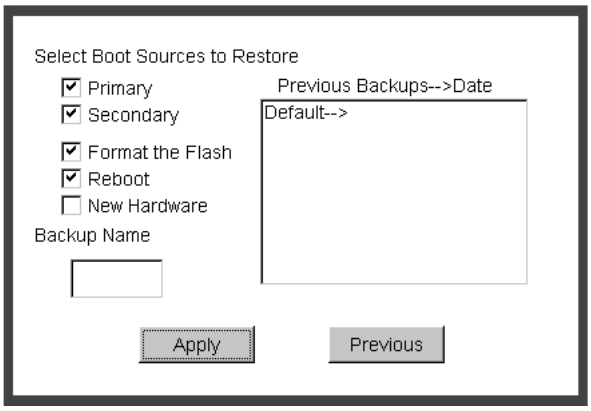
To restore the software, follow these steps:

1. Run Upgrade Link if you have not already done so.
2. Choose a device from the pop-up list in the Console page, or click *New* to enter the IP address or hostname. The pop-up list contains devices that you have upgraded or backed-up before.
3. Select *Restore* and click *Apply*.

   The Setting page appears.

4. Select the appropriate settings and click *OK*.

   The Restore page appears.



5 Select the boot source you want to restore.

The boxes on the right show information about the backups, including the names directories and dates. You can select a backup by double-clicking it, or by entering the name in the edit box.

6 Check the appropriate options:

- Format the Flash — formats the flash memory before restoring the software. If you uncheck this option, Upgrade Link will attempt to restore the software in the available space. If there is not enough space for the image, the restoration will fail.
- Reboot — automatically reboots when the restoration is complete.
- New Hardware — must be checked if you are replacing the hardware.

7 Click *Apply* to begin the restoration.

The Status window shows when the restoration is complete.

8 Click *Home* then *Exit* to exit Upgrade Link.

Restoring the Software Using the Command Line

Use the command line utilities if you have a script or if you do not have a web browser. Otherwise, use the Upgrade Link application as described on page 71.

Prediagnosing System Problems

Detect any problems with SNMP or FTP/HTTP/TFTP connectivity using:

```
bcmdiagnose [ -ftp | -http | -tftp ] [<device> | -h]
```

Where <device> is the IP address or hostname of the device you are upgrading. The -ftp, -http, and -tftp flags force the specified file transfer types. See Appendix A for more information about any error messages that may appear.

If bcmdiagnose shows a failure, check the SNMP read/write community string for FTP/TFTP file transfer permissions.

Restoring the Software

If you are replacing the hardware, restore the software using:

```
bcmrestore -new_hw [ -<backname>] <device>
```

If you are not replacing the hardware, use:

```
bcmrestore [ -<backname>] <device>
```

Where <backname> is the name of the backup for the boot blocks.

8 REFERENCE FOR THE UPGRADE MANAGEMENT UTILITIES

This chapter describes the syntax and options for each utility, as well as how to download the utilities, and where they are installed on your system.

Accessing and Downloading the Utilities

The Upgrade Management Utilities are provided on CD-ROM with every Enterprise OS software package. See Chapter 2 to install the utilities from CD-ROM.

The upgrade utilities are installed into the directory /usr/3Com/bcm/.

Downloading the Utilities

You can download the latest utilities from the following locations:

- FTP — ftp.3Com.com
- World Wide Web — http://www.infodeli.3Com.com/
- 3Com Bulletin Board Service (3ComBBS) — See Appendix D for local BBS numbers.

See the ruu114.txt file accompanying the utilities for instructions on decompression and installation of the utilities.

Downloading UNIX Files

The UNIX files compressed with the UNIX compress utility. To use the downloaded files, you must first expand the files using the UNIX decompress utility. For instructions on how to download and decompress the utilities, see the ruu111.txt file.

The following are the UNIX files:

ruusol114.Z	Contains the utilities for Solaris 2.x.
ruuhp114.Z	Contains the utilities for HP-UX 9.0.5, 10.10, and 10.20.
ruuaix114.Z	Contains the utilities for IBM AIX 3.2.5, 4.1.4, and 4.2.
ruu114.txt	Contains the instructions for downloading and decompressing the utilities.

Downloading Windows Files

The Windows files are compressed with a compression utility. To use the downloaded files, you must first expand them using the decompress utility PKUNZip. PKUNZip can be downloaded from the following URLs:

- **http://www.pkware.com/**

  or

- **http://infodeli.3com.com/infodeli/swlib**

For instructions on how to decompress and install the utilities, see the ruu110.txt file.

The following are the Windows files:

ruu114.zip	Contains the utilities for Windows95, Window98, and Windows NT 4.0.
ruu114.txt	Contains the instructions for downloading and decompressing the utilities.

Update Log File

The bcmsysupgrade utility creates log files in the tftpboot/CLIENTS/<mac_address>/tmp directory. These log files include the following:

- **bcmsysupgrade.log.<stage>** — contains a detailed listing of transactions executed for a stage.
- **stages.log** — contains a history of bcmsysupgrade, bcmbackup, and bcmrestore commands for all successfully completed stages and operations. This file acts as an upgrade record of completed stages, and includes the date and time of execution.
- **bcmupdate.log** — contains a list of the configuration files converted during the upgrade process. The file contains all stderr and stdout text, the log and stage files. This file is appended to the bcmsysupgrade.log file when the upgrade procedure is completed.

Utility Descriptions and Syntax

This section describes each of the Upgrade Management Utilities as well as the syntax and options. The error codes for individual Enterprise OS Upgrade Management Utilities are accessible in the man pages for the utilities. Utilities are in alphabetical order.

Overview

Table 5 summarizes the functions of the upgrade utilities.

Table 5 Network Management Utilities Functions

Utility	Function
bcmbackup	Backs up the current device operational state and files to the network management station.
bcmconfig	Manages the device boot source parameters.
bcmctrl	Manipulates the device boot sources. Performs booting-related functions. Queries or waits on file transfer states.
bcmdf	Checks the media and displays the amount of used and free space.
bcmdiagnose	Identifies the most common network management station installation and device configuration problems.
bcmftp	Sets the FTP username and password and initializes the FTP client on the device.
bcminstall	Installs device software and firmware on a network management station.
bcmloadconfig	Allows you to execute commands in a text file.
(continued)	
bcmrestore	Restores a device to a previous operational state by copying files from the network management station to the device and setting the boot sources.

Table 5 Network Management Utilities Functions (continued)

Utility	Function
bcmsetup	Places the latest version of the Enterprise OS Upgrade Management Utilities on the network management station. Integrates the Upgrade Management Utilities with Transcend.
bcmsysupgrade	Performs all upgrade functions on Enterprise OS devices.
bcmuname	Displays general information about the device.
bcmupdate	Converts configuration files on the network management station for use with a newer version of software.
UpgradeLink	Launches Upgrade Link.

Getting Help

Help is available in HTML or (UNIX) man pages.

Man Pages On a UNIX system, access the man pages by entering:

```
man bcm-intro
```

To access the man pages for a specific utility, use:

```
man <NMU_name>
```

where <NMU_name> is the name of the upgrade utility.

HTML Help To access the HTML help, enter the following URL in your browser:

```
/usr/3Com/bcm/gui/hlp/bcm-intro.html
```

Or to access help for a specific utility, use:

```
/usr/3Com/bcm/gui/hlp/<utility>.html
```

bcmbackup

Syntax `bcmbackup [both | primary | secondary] <-ftp | -http | -tftp> [-name: <backname>] <device>`

Description You can use this utility to prepare a network management station as a secondary boot source, to archive the configuration as a backup copy, to obtain a baseline configuration, or to perform an off-line configuration. The bcmbackup utility copies the primary and secondary boot sources from a device to a network management station. The bcmbackup utility can be used instead of the -s:from_nb stage of bcmsysupgrade, which captures only the primary boot source.

You can assign names to the backup directories, which allows you to maintain multiple backups of the primary and secondary boot blocks. This symbolic name is applicable to both the primary and secondary boot blocks. The default boot block names are supported to maintain backward compatibility.

Values

both	Default value, which backs up both the primary and secondary boot sources.
primary	Backs up the primary boot source.
secondary	Backs up the secondary boot source.
<device>	Indicates the IP address or hostname of the device.
<-ftp | -http | -tftp>	Specifies the file transfer protocol to be used in the backup process.
<backname>	Specifies the name to be given to the backup file of the boot blocks.

Options No available options.

Example For example, to backup the primary boot block as MyBackup01 using FTP, enter:

```
bcmbackup primary -ftp -name:MyBackup01 199.199.199.2
```

bcmconfig

Syntax

```
bcmconfig <device>[:<slot>] [<boot_source>] [options]
```

Description The bcmconfig utility performs EEPROM configuration of the device and retrieves or sets the following parameters for each boot source:

- Path and name for load image
- Path and name for configuration files

The bcmconfig utility does not alter the running state of the device. It only determines what happens the next time the device is rebooted. The utility also detects the following error and warning conditions:

- Files/paths not present locally to the box or locally to this server.
- Inconsistency with other configurations in other blocks (such as subnet masks).

Values

<device>	Indicates the name or IP address of the device.
<slot>	Indicates the slot number of an I/O module. (Use options marked with *.)
<boot_source>	Designates type of boot source: master, primary, secondary, test, dump, or all.

Options Where <boot source> is master, the [options] are:

-st[artup	(once	|	Attempts to boot once.
	forever	|	Attempts to boot forever.
	local)		Forces boot from local media.

Where <boot source> is primary, secondary, test, or dump, the [options] are:

-configp[ath]:<file_path>			Path to the configuration files.
-fi[le]:<file_name>*			Name of boot file.
-bo[otdevice]:	(network	|	Boots from network.
	localA	|	Boots from local media A.
	localB)		Boots from local media B.
-configd[evice]:	(bootdevice	|	Depends on -bootdevice.
	local	|	Local media configuration.
	network)		Network configuration.
-fo[rmat]:(canonical | noncanonical)			Address format.
-cl[ock]:(internal | external)			Internal/external clocking.
-conn[ector]:(v35 | rs232)			Connector type.
-ba[udrate]:			<9.6KB | 19.2KB | 38.4KB | 56KB | 64KB | 128KB | 256KB | 448KB | 1536KB | 2048KB | 4MB | 16MB>
-sl[ot]:1..8			Boot slot.
-in[terface]:(a | b)			Interface number.
-pa[ssword]:<wan_password>			A character string from 0–5 characters.
-di[scovery]:(<localaddr> | <bootp>)			Address discovery.
-ga[teway]:<IPADDRESS>			Default gateway IP address.
-lo[calip]:<IPADDRESS>			Device IP address.
-se[rver]:<IPADDRESS>			TFTP boot server IP address.
-cf[gserver]:<IPADDRESS>			Server where configuration files are stored.
-ma[sk]:<IPADDRESS>			Device subnet mask.
-notraps			Disables the sending of SNMP traps useful during upgrading.
-re[tries]:0..255			Number of retries from 0–255.
-traps			Enables the sending of SNMP traps; useful after upgrade completes.

bcmctrl

Syntax `bcmctrl <device>[:<slot>] [-<option>[:<value>]]`

Description The bcmctrl utility does the following tasks:

- Reboots a device. This follows a normal boot sequence, where the load image and configuration files are found in the primary boot source.
- Performs a test reboot.
- Copies all the parameters in the test boot source to the primary boot source.
- Reports reboot and file transfer states.
- Reboots a specified multiprocessor module.

Values

<device> Identifies the device that receives the changes specified by the bcmctrl utility.

<slot> Specifies the slot where the I/O module is located that receives the changes specified by the bcmctrl utility.

Options

-u[pdate]	Copies the complete set of boot parameters from the test boot source to the primary boot source.This operation is typically performed after a successful test reboot to ensure that the next normal reboot uses the same parameters.
-s[wap]	Swaps the parameters in the primary and secondary boot sources.
-c[ommit]	Cancels the test reboot countdown timer. This stops the automatic test reboot begun by the test reboot parameter.
-r[eboot]*	Reboots the device or the I/O module specified by the <slot> parameter.
-t[estreboot]: [<seconds>]*	Reboots the device from the test boot source so that if this command is not used again with the -c option, the device automatically reboots with its primary configuration. The optional seconds parameter indicates the length of time in seconds the device should count down before automatically rebooting. If you do not supply a value for <seconds>, the default value of 120 seconds is used.
-q:r[eboot]	Queries the reboot status of the device or I/O module specified by the <slot> parameter.
-q:t[ransfer]	Queries the transfer status of the device.
-w:r[eboot]	Waits for the device to reboot.
-w:t[ransfer]	Waits for the last requested transfer to complete.

The options marked with an asterisk will reboot the device or individual modules.

bcmdf

Syntax `bcmdf <device>[:<drive:>]`

Description The bcmdf utility displays the amount of total and available disk space.

Values

<device>	The hostname or the IP address of the device.
<drive:>	The device drive that holds the disk for which the amount of total and available disk space will be counted and displayed.

Options No available options

bcmdiagnose

Syntax `bcmdiagnose [ -ftp | -http | -tftp ] [-NoAuthentication] [<device>] [-h]`

Description The bcmdiagnose utility identifies the most common installation and configuration problems. 3Com recommends that this utility be run immediately following bcmsetup and before running any other upgrade management utility. The bcmdiagnose utility validates that the upgrade management installation process went as expected, and tests that the device and network management station are configured correctly. The bcmdiagnose utility validates that:

- The upgrade utilities are installed correctly on the NMS.
- The device is reachable over IP.
- The device SNMP Service is correctly configured.
- The TFTP server and file permissions are correctly configured.
- The boot images and the configuration files are in the same directory on drive A or derive B.
- The software is compatible with the firmware (NETBuilder II bridge/router with CEC only).
- The ;user has administrative access to the device. The user name and password must be configured by settinghte BCMNBUSER and BCMNB PASS environment variables.
- When FTP is specified for file transfer, the FTP user name and password must be correctly configured by setting the BCMFTPUSER and BCMFTPPASS environment variables.

The bcmdiagnose utility displays troubleshooting messages and has two error return codes:

- 0 for success
- 1 for failure

Values

<device> Indicates the hostname or the IP address of the device. If bcmdiagnose is invoked without the device IP address or host name, only the installation tests of the Enterprise OS Upgrade Management Utilities is executed. If the device is specified, the installation test is skipped, but the utility performs the IP, SNMP, and TFTP server configuration tests.

Options

-ftp	Specifies FTP as the file transfer protocol to be used. FTP is the default protocol for Enterprise OS software versions 11.1 and higher.
-http	Specifies HTTP (HyperText Transfer Protocol) as the file transfer protocol to be used and checks the user name and password.
-tftp	Specifies TFTP as the file transfer protocol to be used. TFTP is the default protocol for Enterprise OS software versions 11.0 and lower.

-NoAuthentication	Specifies that the check for administator user access is not performed. This is necessary when the device is running software version 8.3 or earlier.
[-h]	Displays help message.

bcminstall

Syntax

```
bcminstall [-h | -cdrom [<path>] | -tar <path> | -r | -diskette | -image
   <path> | <device>]
```

Description

The bcminstall utility installs device software and firmware onto a network management station from either a CD-ROM, tar files, an image file, a device, or a network management station floppy diskette. You must install all applicable Enterprise OS software packages before beginning the upgrade process. On a UNIX system, you must have superuser privileges to run the bcminstall utility.

The default method of installing a Enterprise OS package is to install it from a CD-ROM drive on the network management station. The bcminstall utility copies the files on the CD-ROM into a directory under /%tftpboot%/image. Using the path option allows installation from a network management station that has two or more CD-ROM drives, or from a remote CD-ROM drive. On a UNIX system, you must specify the path if you are installing from a CD-ROM that is not cdrom0. For example, to install a Enterprise OS software package from a second CD-ROM on Solaris, enter:

```
bcminstall -cdrom /cdrom/cdrom1/image
```

The following example shows how to install a boot image for an image-only upgrade from the directory /tmp/:

```
bcminstall -image /tmp/boot.68k
```

Options

-h	Displays a usage message. Installs using the first CD-ROM on the network management station.
-cdrom [<path>]	Installs using the CD-ROM from a directory path. Required for Windows.
-tar <path>	Installs a tarred package file.
-r	Reports all installed device packages on the network management station.
-diskette	Installs from the network management station floppy drive (version 9.1 and earlier).
-image <path>	Installs an image file (for image-only upgrades only).
<device>	The IP address of the device from which the over-the-network installation occurs.

Default

If no command line options are specified, the bcminstall utility uses the network management station local CD-ROM drive.

bcmloadconfig

Syntax

```
bcmloadconfig [-s "<service1> [<service2>...]" | -l <line number>] [-i] -f
   <config file path>/<filename> <device> [-b] [-t:<reboot timeout>]
```

Description

You can execute multiple commands on the Enterprise OS user interface at once by entering the commands in a text file, then loading the file. The bcmloadconfig utility copies a specified configuration file to the device and executes the commands in the file.

The utility can execute only the SETDefault, SHow, SHowDefault, ADD, DELete, and SAVEbgp commands. Blank lines and comment lines (lines beginning with the # character) are allowed in the file. If the command requires more than one line, the backslash (\) can be used to terminate the current line and to indicate that the command continues on the next line. A line cannot contain more than one command.

If you specify one or more services, only the commands belonging to those services are executed. Up to 10 services can be specified. Instead of specifying a service, you can specify a line number to indicate the starting line number within the file to execute.

By default, the bcmloadconfig utility terminates whenever it detects a bad command, a command that is not supported by the bcmloadconfig utility, or a command that fails to execute successfully on the device. If -i is specified, the utility continues execution when an error is encountered.

All commands and comments and any generated messages are written to the CONFIG.LOG file in the /tftpboot/CLIENTS/<MAC address>/cfg/ directory on the NMS. Any passwords specified in the commands are replaced by a string of asterisks. Skipped commands are not written to the CONFIG.LOG file.

Values

-s "<service1> [<service2>...]"	Only commands found for these services are executed. Up to 10 services may be specified. The default is to execute the configuration commands for all services.
-l <line number>	The Line in the configuration file to be executed. Comments and blank lines are considered lines in the file.
	-s and -l are mutually exclusive.
-i	Continue executing commands even when errors are detected.
-f <config file path>	The directory containing the command file that is to be executed. The default path is the current working directory.
<filename>	The name of the command file that is to be executed. There is no default filename. This parameter is required.
<device>	The IP address or hostname of the device that will execute the commands.

-b	Specifies that after the configuration file is copied to the device a bcmctrl -reboot is executed.
-t:<reboot timeout>	Specifies a reboot time out period. If the device does not boot within the reboot timeout period (default: 600 seconds) bcmloadconfig returns an error.

bcmnbrus

Syntax `bcmnbrus <port> [-NoSecurity] [-NoAuthentication]`

Description The bcmnbrus utility launches the Upgrade Link application backend process.

Values

<port>	Specifies the TCP socket on which the client communicates with the server. On UNIX systems you can add this command to cron and on Windows 95/98/NT systems this command can be running as a service.

Options

-NoSecurity	Indicates that the bcmnbrus utility will allow connections from all IP addresses.
-NoAuthentication	Specifies that bcmnbrus will not prompt for a user name and password.

bcmrestore

Syntax `bcmrestore [both | primary | secondary] [options] <device>`

Description The bcmrestore utility restores the Enterprise OS software from a backup on the network management station to the device. The software, including the image and configuration files, is copied to the device, and the primary boot source is set to the restored directory.

Values

both	Restores both the primary and secondary boot sources. This value is the default.
primary	Restores the primary boot source.
secondary	Restores the secondary boot source.
<device>	Indicates the IP address or hostname of the device.

Options

-ftp | -http | -tftp	Specifies the file transfer protocol to be used in the restore process.
-NoF[ormat]	Does not format the drive before restore.
-NoR[eboot]	Does not reboot when restoration is complete.
-U[naccept]	Rejects a previously accepted automatically recoverable upgrade by swapping the primary and test boot sources.
-new_hw	Used to restore software to a new device. Use this option when a failed device is exchanged for a new one. After IP and SNMP connectivity is established, use this option to copy the original software to the new device.

bcmsetup

Syntax

For UNIX:

```
bcmsetup <packages> [install_directory]
```

For Windows:

```
bcmsetup <drive:> [all | bcm | nat]
```

Description

The bcmsetup utility places the latest version of the Enterprise OS Upgrade Management Utilities on the network managment station. It also sets up the initial package definitions for use by Transcend. You must be root to run the bcmsetup utility.

Values

all	Installs both the utilities and package definitions (bcm and nat).
bcm	Enterprise OS Upgrade Management Utilities.
nat	Package definitions for use by Transcend.

Options

[Install_directory] UNIX only	Defines the directory where the utilities and other files set up with bcmsetup are to be located.

Default

For UNIX, unless an alternate installation directory is specified, the utilities are installed in the /usr/3Com/bcm directory.

For Windows, the utilities are always installed in \usr\3Com\bcm.

<drive:>	Identifies the target drive where the utilities and other files set up with bcmsetup are to be located.

bcmsysupgrade

Syntax

```
bcmsysupgrade [options] <stage> <device>
```

Description

The bcmsysupgrade utility is a master script that assists you in upgrading a device to the latest version of software and/or firmware. The bcmsysupgrade utility uses many of the other Enterprise OS Upgrade Utilities to perform a complete upgrade of a device over the network.

Values

<stage>

-s:from_nb	Downloads configuration files from the device.
-s:update	Upgrades configuration files on the network management station.
-s:to_nb	Uploads configuration and image files to the device.
-s:test_boot *	Test boots the upgraded configuration.
-s:accept*	Accepts the upgrade (cannot be used with -s:reject stage).
-s:reject*	Rejects the upgrade (cannot be used with -s:accept stage).
-s:upgrade_cec_fw*	Upgrades the NETBuilder II CEC firmware.
-s:upgrade_io_fw*	Upgrades the I/O firmware.

<device>	Specifies the IP address or hostname of the target device.

Stages with an asterisk may reboot the device. The -s:accept stage only reboots manual and patch upgrades.

Options

-EncryptionLicenseRead	Specifies that the encryption license agreement has been read and accepted. This flag must be used when upgrading to any package with encryption.
-ftp | -http | -tftp	Specifies the file transfer protocol to be used in the backup process. The default is FTP for devices running Enterprise OS software version 11.1 or above. The default is TFTP for devices running Enterprise OS software version 11.0 or lower. HTTP is available on devices running software version 11.4 or later.
-d	Runs bcmdiagnose utlility first.
-f	Forces action, and ignores warnings. Use with extreme caution!
-I	Upgrades boot image only. The default is images and configurations.
-k:<package>	Package type to upgrade to. For <package>, use the two-letter designator printed on the CD-ROM. The default is to use the package being upgraded from.
-m	Specifies a manually recoverable upgrade. The default is automatic recovery.
-t	Timeout value in seconds (defaults to 600, the range is 480 to 720 seconds).
-new_hw	Indicates the replacement with like hardware. (Examples, CEC with DPE, OCNB with OCNB)
-V:<version upgrading to>	When upgrading to a software version other than the default, you must enter the software version you are upgrading to. The default version is the same as the version of the upgrade software. Run "bcmdiagnose" to determine the version.

bcmuname

Syntax `bcmuname [options] <device>[:<slot> | <drive>]`

Description The bcmuname utility displays system information about the specified device or switch or Intelligent I/O module (IIO). If no options are specified, all the device-level options are printed.

Values

<device>	Specifies either the hostname or the IP address of the device.
<slot>	Specifies slot of an I/O module within the device. This parameter is optional and is used only with the options marked with (IIO).

<drive>	Specifies the storage device (usually a flash drive) attached to a device. This parameter is optional. When you specify letters A: or B: they are assumed to be drive letters, any numeric character is assumed to be a slot designator.

Options

-2	Prints the @m mac address (used in bcmcp) (llO).
-@	Prints the @M mac address (used in bcmcp) (llO).
-a	Prints all the above information (llO).
-c	Prints the contact information.
-d	Prints the tftp directory that will be used by bcmcp.
-f:<sys_filename>	Displays system information based on the contents of the specified <path>/sys file.
-l	Prints the machine location.
-M	Prints the memory type.
-m	Prints the machine platform name (llO).
-n	Prints the node name.
-r	Prints the software release (llO).
-R	Prints the major software release.
-s	Prints the software system name.
-t	Prints the software or firmware type.
-w	Prints the firmware release.

If an option is required, it must be specified in very stage of the upgrade process.

bcmupdate

Syntax `bcmupdate -f:<from_path> -t:<to_path> [options]`

Description The bcmupdate utility converts the device configuration files that work with an older version of software to files that work with the newer version of software. 3Com recommends that this utility only be invoked with the bcmsysupgrade utility script.

Values

-f:<path>	Path to upgrade from.
-t:<path>	Path to upgrade to.

Options

-v:<version>	Version to upgrade from.
-V:<version>	Version to upgrade to.
-p:<platform>	Device platform type.
-m	Saves user macros.
-n	Prints trace messages.

When using the bcmupdate option on a Windows95, Windows98, or Windows NT version 4.0 system, the following files are copied but not converted or changed:

bgp	bgpnet	bgpol	smt
bgpas	dir	bgppeer	
ds	egp	dua	
iineighb	ipns	area	
iistuff	systemna	iicurcui	
user	name	NatMap	

The filenames are numbers in the es directory, and the text files are located in the filter directory.

UpgradeLink

Syntax `UpgradeLink [-NoSecurity | -NoAuthentication]`

Description The Upgrade Link utility runs the Upgrade Link application and launches your default web browser. On Windows, it launches the 3Com TFTP server that is installed with the utilities.

Upgrade Link is an easy to use GUI for upgrading, backing up, or restoring software on a single device.

Options

-NoSecurity	Indicates that the bcmnbrus utility will allow connections from all IP addresses.
-NoAuthentication	Specifies that bcmnbrus will not prompt for a user name and password.

A TROUBLESHOOTING

This appendix describes error codes and messages that may be displayed during the upgrade process as a result of running the bcmdiagnose utility or when network dependencies have not been met.

Getting Help

For UNIX, to obtain help information about a utility, use:

```
<utility> -h
```

Help is available in HTML or (UNIX) man pages.

Man Pages

On a UNIX system, access the man pages by entering:

```
man bcm-intro
```

To access the man pages for a specific utility, use:

```
man <NMU_name>
```

where <NMU_name> is the name of the upgrade utility.

HTML Help

To access the HTML help, enter the following URL in your browser:

```
/usr/3Com/bcm/gui/hlp/bcm-intro.html
```

Or to access help for a specific utility, use:

```
/usr/3Com/bcm/gui/hlp/<NMU_name>.html
```

For more information about using the Enterprise OS Upgrade Management Utilities, see Chapter 8.

General Troubleshooting Error Messages

The master boot block startup value is set to monitor. This is not a supported value.

Meaning: The master boot block startup value is set to monitor.
Action: Make sure that your bcmconfig <ipaddr> master -startup value is set to try boot once or try forever.

The primary boot block must access the boot file locally. That is, all files must physically reside on the NETBuilder.

Meaning: The primary boot source is set to boot from the network.
Action: Set the primary boot source to local. Make sure the bcmconfig <ipaddr> primary -bootdevice value is set to either localA or localB.

The required file(s) <ipaddress>:<drive>:/<config file path> could not be located.

Meaning: The bcmtest utility was unable to verify the presence of a file or directory.

Action: Make sure that the required files and directories are available to the bcmtest utility.

Return Codes from bcmdiagnose

The bcmdiagnose utility can display the following exit return codes:

Table 6 bcmdiagnose Return Codes

Code	Meaning
0	The operation was successful.
1	A command line parsing error occurred.
2	A command line argument is invalid.
3	A installation error occurred.
4	A Enterprise OS Upgrade Management utility failed.
5	The device is not responding.
6	Internal parsing error.
7	A UNIX command failed.
8	The device configuration is incompatible with the operation.
9	The attempted operation is unsafe.
10	No arguments in a function call.
11	No sys file was found.
12	The boot image was not found.
13	The boot image is bad.
14	The module upgrade failed.
15	The module failed to reboot.
16	The boot image is not set.
17	Missing device address (DNS name or IP address).
18	The Enterprise OS software is not installed.
19	Error installing a Enterprise OS SW or FW package.
20	An error occurred during a UNIX file copy.
21	Enterprise OS software installation not performed.
22	Failed to perform a software upgrade.
22	Failed to perform firmware upgrade.
23	Test-Boot and/or reboot timed-out.
24	The Upgrade of the device and image is not supported.
25	A critical file was missing or corrupted in a file transfer.

Hardware-Related Messages

The XX package must have 20 MB of memory installed on the CEC or DPE module. There is only 12 MB available.

Meaning: The bcmsysupgrade utility cannot continue because it does not detect a CEC 20 or DPE in the system. The software package requires a CEC 20 or DPE module.

Action: If you have a CEC 20 module, run the Memory Expansion Board utility supplied with the memory upgrade by putting the diskette in the floppy drive and entering bt memupgrd.29k. The program updates the EPROM.

The hardware configuration of this NETBuilder could not be confirmed.

Meaning: Your hardware may not support the software package you are upgrading to. The bcmsysupgrade script allows the upgrade to proceed even if the hardware configuration is not recommended.

Action: Ensure that the bridge/router meets the hardware requirements for the package you are upgrading to, and that it is on the recommended upgrade migration path.

The NETBuilder hardware will not safely support the upgrade.

Meaning: The hardware is not sufficient to safely support the software upgrade, and the bridge/router configuration is not on the upgrade migration path.

Action: Contact your 3Com supplier for information about a hardware upgrade.

Installation Troubleshooting Messages

The troubleshooting messages in this section are displayed during installation.

Installing the Enterprise OS Upgrade Management Utilities

Testing the Enterprise OS Upgrade Utilities installation.

Meaning: This is an introductory message displayed when the bcmdiagnose utility is initiated.

Action: None.

There is a problem with the installation of the Enterprise OS Upgrade Utilities. The path /usr/3Com/bcm/bin and usr/3Com/common/bin should be in the PATH environment variable.

Meaning: The installation process has searched for certain utilities in /usr/3Com/bcm/bin and /usr/3Com/common/bin directories but cannot find them unless the path /usr/3Com/bcm/bin is first.

Action: Check that /usr/3Com/bcm/bin and /usr/3Com/common/bin have been added in the path environment variable.

There is a problem with the installation of the Enterprise OS Upgrade Utilities. The path /usr/3Com/bcm/bin should be first in the PATH environment variable.

Meaning: The installation process cannot find the necessary directories unless the path /usr/3Com/bcm/bin is first.

Action: Check that /usr/3Com/bcm/bin is first in the path environment variable.

There is a problem with the installation of the Enterprise OS Upgrade Utilities. The location of the Enterprise OS Upgrade Utilities was not added to the path environment variable or the directory does not contain all the required programs.

Meaning: The installation process cannot find the utilities because it does not know where to look for them.

Action: Check that a location for the utilities was specified in the path environment variable.

There is a problem with the installation of the Enterprise OS Upgrade Utilities. The version numbers of the Enterprise OS Upgrade Utilities are not consistent.

Meaning: The bcmdiagnose utility has assumed that the version of the Enterprise OS Upgrade Management Utilities in bcmcommon.sh is correct and has checked that each executable utility has the same version number. At least one utility is different.

Action: Check that you have specified version number for the utilities you are installing correctly.

Determining Connectivity

Pinging <IP address>

Meaning: This is an introductory message that appears when the utilities are attempting to reach a bridge/router with an IP address specified on the command line.

Action: None.

The NETBuilder did not respond to a ping. Make sure the IP address or host name is correct and that the NETBuilder is reachable via IP.

Meaning: The device that the utilities were trying to reach did not respond.

Action: Ensure the device can be reached using IP.

The NETBuilder responded to ping.

Meaning: The device which was specified in the IP address is reachable.

Action: None.

Validating the SNMP Service Configuration

Testing SNMP read access

Meaning: This is an introductory message. Check to see if the SNMP Service is active on the bridge/router.

Action: None.

The NETBuilder is not responding to SNMP get requests. Ensure that the SNMP Service is configured on the NETBuilder and that you have read and write access via SNMP. Also check the values of the community strings in the /etc/snmp.cfg file. They should match the NETBuilder's SNMP community strings.

Meaning: The bcmdiagnose utility has attempted to verify whether the bridge/router specified by the <IP address> value has been configured.

Action: Configure the SNMP server on your bridge/router to allow read access to your network management station. See the Network Management chapter in *Using NETBuilder Family Software*.

The bridge/router is not responding to SNMP set requests. Ensure that the SNMP service is configured on the bridge/router and that you have read and write access via SNMP. Also check the values of the community strings in the /etc/snmp.cfg file. They should match the bridge/router's SNMP community strings.

Meaning: The bcmdiagnose utility has attempted to verify whether the bridge/router specified by the <IP address> value has been configured.

Action: Configure the SNMP server on your bridge/router to allow write access to your network management station. See the Network Management chapter in *Using NETBuilder Family Software*.

SNMP read access OK

Meaning: There is no problem with SNMP configuration on the bridge/router.

Action: None.

Testing SNMP write access

Meaning: This is an introductory message. Check to see if SNMP Service is active on the bridge router.

Action: None.

SNMP write access OK

Meaning: There is no problem with SNMP configuration on the bridge/router.

Action: None.

Testing the NMS/ TFTP Configuration

Creating an Upgrade File

Testing file transfers using TFTP

Meaning: This is an introductory message displayed as the bcmdiagnose utility begins its test.

Action: None.

The TFTP safe directory is <tftpboot_dir>. Make sure that the TFTP safe dir exists.

Meaning: The TFTP safe directory is the root directory under which the utilities will store your bridge/router files.

Action: Check that your TFTP safe directory exists.

The directory <tftpboot_dir> does not exist. Create <tftpboot_dir> with full read/write/create file permissions. Make sure that this directory has the proper file access permissions and is being used by the TFTP server.

Meaning: The bcmdiagnose utility has attempted to create a test file using the TFTP safe directory and has failed.

Action: Assign full read/write/create file access permissions to the TFTP directory.

Creating "test3.com"

Meaning: This information message is displayed while the UNIX copy command tries to create the test file.

Action: None.

Could not remove "test3.com". Check that <tftpboot_dir> and subdirectories have full read/write/create file permissions

Meaning: The UNIX remove command could not delete the test file.

Action: Assign full read/write/create file access permissions to the directories.

Could not create "test3.com". Check that <tftpboot_dir> and subdirectories have full read/write/create file permissions.
Meaning: The UNIX copy command could not create the test file.
Action: Assign full read/write/create file access permissions to the directories.

The file "test3.com" was not created with read access. Make sure <tftpboot_dir> has full read/write/create file permissions.
Meaning: When the UNIX copy command created the file, read access was not assigned.
Action: Assign full read/write/create file access permissions to the directories.

The file "test3.com" was not created with write access. Make sure <tftpboot_dir> has full read/write/create file permissions.
Meaning: When the UNIX copy command created the file, write access was not assigned.
Action: Assign full read/write/create file access permissions to the directories.

Uploading an Upgrade File

Could not remove "<ipaddress> | DNSname>:a:/test3.com". Check that the NETBuilder media is not write protected and that "<ipaddress> | DNSname>:a:/test3.com" is not the name of a directory on the NETBuilder.
Meaning: The bcmrm utility could not delete the file on the bridge/router.
Action: Make sure that your floppy disk write protect tab allows writing to the diskette.

Copying TestFile from the NMS to "<ipaddress> | DNSname>:a:/test3.com".
Meaning: This is a status message.
Action: None.

The bcmcp command could not write the file "testfile" on NBAddress or DNS name. Make sure there is a flash or floppy drive installed and that it is not write protected.
Meaning: The bcmcp utility has been denied write access to the bridge/router.
Action: Make sure there is a flash or floppy diskette installed and that it is not write-protected.

The file "<ipaddress> | DNSname>:a:/test3.com" is not present on the brouter even though bcmcp did not report an error.
Meaning: The bcmtest utility could not locate the file on the bridge/router.
Action: Check with your systems administrator.

The checksums of "test3.com" and "<ipaddress> | DNSname>:a:/test3.com" are different even though bcmcp did not report an error.
Meaning: The bcmsum utility reported differing checksums on the local and remote test files.
Action: Check your network connection for possible corruption on the line.

The bcmcp command could not reliably copy the "test3.com" file to the bridge/router.
Meaning: This is an information message.
Action: None.

Downloading an Upgrade File

$local TestFile could not be removed. Make sure <tftpboot_dir> and "test3.com" have full read/write/create file permissions.
Meaning: The UNIX remove command could not delete the test file.
Action: Assign full read/write/create file access permissions to the directories.

The bcmcp command could not write the file "testfile" on the NMS. Check that the file access permissions are read/write/create in the TFTP server safe directory. Make sure there is enough space available.
Meaning: The bcmcopy utility could not write the test file.
Action: Assign full read/write/create file access permissions to the directories.The file “test3Com” is not present on the NMS even though bcmcp did not report an error.

The file “test3Com” is not present on the NMS even though bcmcp did not report an error.
Meaning: The UNIX test command could not validate that the test file exists on the TFTP safe directory.
Action: Check with your systems administrator.

The checksums of "test3.com" and "<ipaddress> | DNSname>:a:/test3.com" are different even though bcmcp did not report an error.
Meaning: The bcmsum utility reported differing checksums on the local and remote test files.
Action: Check with your systems administrator.

The bcmcp command could not reliably copy the file "testfile" to the NMS.
Meaning: This is an information message.
Action: None.

Could not remove file "<ipaddress> | DNSname>:a:/test3.com". Check that the NETBuilder media is not write protected and that "<ipaddress> | DNSname>:a:/test3.com" is not the name of a directory on the NETBuilder.
Meaning: The bcmrm utility could not delete the test file.
Action: Check with your systems administrator.

"test3.com" could not be removed. Make sure <tftpboot_dir> and "test3.com" have full read/write/create permissions.
Meaning: The UNIX remove command could not delete the test file.
Action: Assign full read/write/create file access permissions to the directories.

File transfers using TFTP are OK.
Meaning: No problem was found with TFTP file transfers between the network management station and bridge/router.
Action: None.

B

MOUNTING THE CD-ROM ON A UNIX PLATFORM

This appendix describes how to mount the CD-ROM for UNIX Solaris 2.6, HP-UX 10.20, and IBM AIX 4.3.2 operating systems.

Mounting the CD-ROM on Solaris 2.6

If you are mounting the CD-ROM from a drive that is directly connected to the network management station where you have installed the Enterprise OS Upgrade Management Utilities, enter the commands in this section. If you are mounting the CD-ROM remotely, proceed to "Mounting from a Remote CD-ROM Drive."

Mounting a Local CD-ROM Drive

To mount the CD-ROM from a local drive, follow these steps:

1. Insert the CD-ROM containing the bridge/router software into the CD-ROM drive.
2. Mount the CD-ROM in a directory in your file system. You must have Superuser (root) access throughout the installation process.
   a. At the command prompt, enter:

      /usr/bin/su

   b. At the Password prompt, enter your root password.

   Solaris 2.6 uses a Volume Management Utility that by default mounts the CD-ROM under the /cdrom directory.
3. Verify that the mount occurred by entering:

   ls /cdrom

   The display shows the cdrom0 directory.
4. If Solaris Volume Management is not installed, or has been deactivated, mount the CD-ROM drive by entering:

   ```
   mkdir /cdrom/cdrom0 (if you have not already done so)
   mount -r -F hsfs /dev/sr0 /cdrom/cdrom0
   ```

   After your CD-ROM has been mounted, you are ready to begin installing the software.

Mounting from a Remote CD-ROM Drive

On the remote system, make sure that the CD-ROM is properly connected and powered up. To allow other systems to access the remote system, follow these steps:

1. Insert the CD-ROM containing the bridge/router software into the CD-ROM drive.
2. Mount the CD-ROM in a directory in your file system. You must have Superuser (root) access to complete the installation process.

a At the command prompt on the remote system, enter:

```
/usr/bin/su
```

b At the Password prompt, enter your root password.

Solaris 2.6 uses a Volume Management Utility that by default mounts the CD-ROM under the /cdrom directory.

3 Verify that the mount occurred by entering:

```
ls /cdrom
```

The display shows the cdrom0 directory.

4 Verify that Solaris Volume Management is installed by entering:

```
ps -aux | grep vold
```

or

```
ps -ef | grep vold
```

If /usr/sbin/vold is displayed, then Volume Management is installed. Proceed to step 5.

If Solaris Volume Management is not installed, or has been deactivated, mount the CD-ROM drive by entering:

```
mkdir /cdrom (if you have not already done so)
mount -r -F hsfs /dev/sr0 /cdrom/cdrom0
```

5 Make the CD-ROM directory (/cdrom/cdrom0) available for Network File System (NFS) clients.

Edit the /etc/dfs/dfstab file by adding the following line:

```
share -F nfs -o ro /cdrom/cdrom0
```

a Change directories to /etc/init.d and enter:

```
./nfs.server start
```

b Enter:

```
shareall
```

or

```
exportfs -a
```

You may need to start the NFS daemons.

6 On the local network management station (the one where you are installing the software), at the command prompt, enter:

```
mkdir /cdrom/remote (if you have not already done so)
mount -r <remote_system>:/cdrom/cdrom0 /cdrom/remote
```

For <remote_system>, enter the IP address or host name of the remote system that does not have a CD-ROM drive.

7 You can verify that the mount occurred by entering:

```
cd /cdrom
```

8 To display a directory of the CD-ROM, enter:

```
ls
```

After your CD-ROM has been mounted, you are ready to begin installing the software.

Mounting the CD-ROM on HP-UX 10.20

If you are mounting the CD-ROM from a drive that is directly connected to the network management station where you have installed the Enterprise OS Upgrade Management Utilities, enter the commands in this section. If you will mount the CD-ROM remotely, proceed to "Mounting from a Remote CD-ROM Drive."

Mounting from a Local CD-ROM Drive

To mount the CD-ROM from a local drive, follow these steps:

1. Open a command window.
2. Insert the CD-ROM.
3. Confirm that the CD-ROM is mounted by entering:

   ```
   mount | grep cdrom
   ```

   If you receive no output command, you must mount the CD-ROM by entering:

   ```
   su
   mkdir /cdrom (if you have not already done so)
   ```

   If you are running HP-UX 10.10, enter:

   ```
   mount -r -t cdfs /dev/dsk/c0t2d0 /cdrom
   ```

   If you are running HP-UX 10.20, enter:

   ```
   mount -r /dev/dsk/c0t2d0 /cdrom
   ```

Mounting from a Remote CD-ROM Drive

To mount the CD-ROM from a remote drive, follow these steps:

1. Open a command window.
2. Insert the CD-ROM.
3. Mount the CD-ROM by entering:

   ```
   su
   mkdir /cdrom (if you have not already done so)
   ```

   If you are running HP-UX 10.20, enter:

   ```
   mount -r /dev/dsk/c0t2d0 /cdrom
   ```

4. Create the /etc/exports file if it does not already exist.
5. Add the following line to the /etc/exports file, if you have not already done so:

   ```
   /cdrom -ro
   ```

6. If the /etc/exports file existed previously, enter:

   ```
   /usr/etc/exportfs -a
   ```

7. If the /etc/exports file did not exist previously, reboot to become an NFS server.
8. On the local machine (the machine on which you are installing the bridge/router software), enter:

   ```
   su
   mkdir /cdrom (if you have not already done so)
   mount -r <remote machine>:/cdrom /cdrom
   ```

   For <remote_system>, enter the IP address or host name of the remote system that does not have a CD-ROM drive.

Mounting the CD-ROM on IBM AIX 4.3.2

If you are mounting the CD-ROM from a drive that is directly connected to the network management station, enter the commands in this section. If you will mount the CD-ROM remotely, proceed to "Mounting from a Remote CD-ROM Drive."

Mounting from a Local CD-ROM Drive

To mount the CD-ROM from a local drive, follow these steps:

1. Open a command window.
2. Insert the CD-ROM.
3. Confirm that the CD-ROM is mounted by entering:

   ```
   mount | grep cdrom
   ```

   If you receive no output command, you must mount the CD-ROM by entering:

   ```
   su
   mkdir /cdrom (if you have not already done so)
   mount -v cdrfs -r /dev/cd0 /cdrom
   ```

Mounting from a Remote CD-ROM Drive

To mount the CD-ROM from a remote drive, follow these steps:

1. Open a command window.
2. Insert the CD-ROM.
3. Enter:

   ```
   su
   mkdir /cdrom (if you have not already done so)
   mount -v cdrfs -r /dev/cd0 /cdrom
   ```

4. Create the /etc/exports file if it does not already exist.
5. Add the following line to the /etc/exports file, if you have not already done so:

   ```
   /cdrom -ro
   ```

6. If the /etc/exports file existed previously, enter:

   ```
   /usr/sbin/exportfs -a
   ```

7. If the /etc/exports file did not exist previously, reboot to become an NFS server.
8. On the local machine (the machine on which you are installing the bridge/router utilities), enter:

   ```
   su
   mkdir /cdrom/remote (if you have not already done so)
   mount -n <remote machine>:/cdrom /cdrom/remote
   ```

   For <remote_system>, enter the IP address or host name of the remote system that does not have a CD-ROM drive.

Unmounting the CD-ROM

To unmount the CD-ROM, follow these steps:

1. Make sure that no processes (shelltool, commandtool or any other application) have /cdrom as the current working directory.
2. Make sure that you have Superuser (root) access. If you do not have this access, at the command prompt enter:

   ```
   /usr/bin/su
   ```

3. Unmount the CD-ROM as root.

   On Solaris 2.6 with or without "vold" running, at the # prompt enter:

   ```
   umount /cdrom/cdrom0
   eject /cdrom
   ```

C

CHOOSING A SOFTWARE PACKAGE

This chapter lists Enterprise OS version software packages and provides recommended equivalent packages in Enterprise OS version 11.4.

NETBuilder II Upgrade Migration Path

Table 7 outlines the recommended migration path from previous versions of Enterprise OS software packages to the latest packages supported in version 11.4. Use this table to identify the new software package that is most similar to the package you are currently using. Packages are identified by the two-letter designator of the version string, which is found on your product CD-ROM disk label.

You can also identify the software package using:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the system you are planning to upgrade. Or enter the Enterprise OS user interface command:

```
SHow -SYS VERsion
```

Table 7 NETBuilder II Software Package Migration to 11.4

Recommended Upgrade		Notes
From	**To Version 11.4**	
AC	AC	
AP	AP	
CP	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
CX	AC	
DE	DE	You can optionally upgrade to the DS package.
DS	DS	
DW	DW	You can optionally upgrade to the DL, DE, or DS packages.
FF	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
FP	DW	You can optionally upgrade to the DE or DS package. A hardware upgrade may be needed prior to installing version 11.4.
IA	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.

Table 7 NETBuilder II Software Package Migration to 11.4

Recommended Upgrade		Notes
LM	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
LT	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
WA	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
WM	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.
WT	DW	You can optionally upgrade to the DL, DE, or DS packages. A hardware upgrade may be needed prior to installing version 11.4.

SuperStack II NETBuilder Upgrade Migration Path

Table 8 outlines the recommended migration path from prior version software packages to the latest packages supported in version 11.4. Use this table to identify the new software package that is most similar to the package you are currently using.

Packages are identified by the two-letter designator of the version string, which is found on your product diskette label.

You can also identify the package using:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the system you are planning to upgrade. Or enter the Enterprise OS user interface command:

```
SHow -SYS VERsion
```

Table 8 SuperStack II NETBuilder Bridge/Router Software Package Migration to 11.4

Model	Recommended Upgrade		Notes
22x Series	**From**	**To Version 11.4**	
	BA, RB, BX, AR, CF or CX	n/a	There is no equivalent package in version 11.4.
32x Series	**From**	**To Version 11.4**	
	FD, BF, CF	n/a	There is no equivalent package in version 11.4.
	CF	TE	
	TE	TE	
42x Series	**From**	**To Version 11.4**	
	BX, BF, AR, CF, EE	n/a	There is no equivalent package in version 11.4.
52x Series	**From**	**To Version 11.4**	
	AF, BF, CF	n/a	There is no equivalent package in version 11.4.
	From	**To Version 11.4**	
	TE	TE	

SuperStack II NETBuilder SI Upgrade Migration Path

Table 9 outlines the recommended migration path from prior version software packages to the latest packages supported in version 11.4. Use this table to identify the new software package that is most similar to the package you are currently using.

Packages are identified by the two-letter designator of the version string, which is found on your product diskette label. You can also identify the package using:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the system you are planning to upgrade. Or enter the Enterprise OS user interface command:

```
SHow -SYS VERsion
```

Table 9 SuperStack II NETBuilder SI Bridge/Router Software Package Migration to 11.4

Recommended Upgrade		Notes
From	**To Version 11.4**	
AB	NW	You can optionally upgrade to the NE or NS package.
AF	AX	
AX	AX	
BF	BF	
BX	BF	
CE	CE	You can optionally upgrade to the CS package.
CF	CF	You can optionally upgrade to the CE, CL, or CS packages.
CS	CS	
CX	AX	
NE	NE	You can optionally upgrade to the NS package.
NS	NS	
NW	NW	You can optionally upgarde to the NE or NS packages.

OfficeConnect NETBuilder Upgrade Migration Path

Table 10 outlines the recommended migration path from previous software package versions to the latest packages supported in version 11.4. Use this table to identify the new software package that is most similar to the package you are currently using.

Packages are identified by the two-letter designator of the version string, which is found on your product diskette label.

You can also identify the package using:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the system you are planning to upgrade. Or enter the Enterprise OS user interface command:

```
SHow -SYS VERsion
```

Table 10 OfficeConnect Software Package Migration to 11.4

Recommended Upgrade		Notes
From Version 11.3	**To Version 11.4**	
AB	NW	You can optionally upgrade to the NE or NS packages. A hardware upgrade may be required prior to installing version 11.4.
AF	AF	
BF	BF	
FD		There is no equivalent package in version 11.4.
JW	JW	You can optionally upgrade to the JE or JS packages.
OE	OE	You can optionally upgrade to the OS package.
OF	OF	You can optionally upgrade to the OE, OL or OS packages.
OS	OS	
NE	NE	You can optionally upgrade to the NS package.
NS	NS	
NW	NW	You can optionally upgrade to the NE or NS packages.
RW	RW	You can optionally upgrade to the RE or RS packages.
VE		There is no equivalent package in version 11.4. The last version of the VE package (Quick Step VPN for the OfficeConnect bridge/router is version 11.3.

PathBuilder Upgrade Migration Path

Table 11 outlines the recommended migration path from previous software packages to the latest packages supported in version 11.4. Use this table to identify the new software package that is most similar to the package you are currently using. Packages are identified by the two-letter designator of the version string, which is found on your product CD-ROM disk label.

You can also identify the software package using:

```
bcmuname -R <device>
```

Where <device> is the IP address or hostname of the system you are planning to upgrade. Or enter the Enterprise OS user interface command:

```
SHow -SYS VERsion
```

Table 11 PathBuilder Software Package Migration to 11.4

Recommended Upgrade		**Notes**
From	**To Version 11.4**	
PE	PE	You can optionally upgarde to the PS package.
PS	PS	
PW	PW	You can optionally upgarde to the PL, PE, or PS packages.

D

TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3Com Facts℠ Automated Fax Service

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site enter this URL into your Internet browser:

http://www.3com.com/

This service provides access to online support information such as technical documentation and software library, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **http://knowledgebase.3com.com**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**

You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

3Com Bulletin Board Service

The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 28,800 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680

Country	Data Rate	Telephone Number
Japan	Up to 14,400 bps	81 3 5977 7977
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 53,333 bps	1 847 262 6000

Access by Digital Modem

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 64 Kbps. To access the 3Com BBS using ISDN, call the following number:

1 847 262 6000

3Com Facts Automated Fax Service

The 3Com Facts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3Com Facts using your Touch-Tone telephone:

1 408 727 7021

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
Asia Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590
India	+61 2 9937 5085	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	
Japan	0031 61 6439	From anywhere in S. Korea:	00798 611 2230
Malaysia	1800 801 777	From Seoul:	(0)2 3455 6455
New Zealand	0800 446 398	Taiwan, R.O.C.	0080 611 261
Pakistan	+61 2 9937 5085	Thailand	001 800 611 2000
Philippines	1235 61 266 2602		
Europe			
From anywhere in Europe, call:	+31 (0)30 6029900 phone +31 (0)30 6029999 fax		
Europe, South Africa, and Middle East			
From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	00800 3111206
Finland	0800 113153	Portugal	0800 831416
France	0800 917959	South Africa	0800 995014
Germany	0800 1821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1800 553117	Switzerland	0800 55 3072
Israel	1800 9453794	U.K.	0800 966197
Italy	1678 79489		
Latin America			
Argentina	AT&T +800 666 5065	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266	Peru	AT&T +800 666 5065
Chile	1230 020 0645	Puerto Rico	800 666 5065
Colombia	98012 2127	Venezuela	AT&T +800 666 5065
North America	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876-3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+65 543 6500	+65 543 6348
Europe, South Africa, and Middle East	+31 30 6029900	+31 30 6029999
Latin America	1 408 326 2927	1 408 326 3355
From the following countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800 553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876 3266	1 408 326 7120 (not toll-free)

23 MAR 99

GLOSSARY

automatic recovery An upgrade method that copies the primary boot source to the NMS, then copies the upgraded software back to the bridge/router as the test boot source. After a successful test boot, the upgraded software is designated as the primary boot source while the original software still present on the flash memory, is designated the secondary boot source. If the upgrade fails, the bridge/router automatically reboots from the original software. Automatic recovery requires enough flash memory to hold two software sets.

backup Copying the software, including the images and configuration files, from the bridge/router to the NMS using Upgrade Link or the bcmbackup utility.

backup location *See* default directory structure.

baseline A copy of the bridge/router configuration files stored in a directory on the network management station. Baselining establishes a known good configuration set by checking for consistency between similar configuration files on the network management station and the NETBuilder bridge/router. Baselining assumes that the versions of software and firmware running on the NETBuilder system have not changed since the baseline was established.

BCM Boot Change Management. Individual command-line utilities and scripts that use SNMP to perform EEPROM boot block and file manipulation operations on the NETBuilder bridge/router and between the NETBuilder bridge/router and Network Management Stations. This includes file transfer using TFTP.

bcm utilities *See* NETBuilder Upgrade Management Utilities.

bcmupdate An upgrade management utility that is used to upgrade configuration files on a network management station.

boot image A software file that is loaded into DRAM and executed by a bridge/router. The main boot image files are named boot.29k and boot.68k.

BOOTP Bootstrap Protocol. Allows a bridge/router to obtain its IP address dynamically from a network management station instead of from local EEPROM.

boot source A reference to a directory on the bridge/router where the boot and configuration files are stored. You can set and view boot source information using the bcmconfig utility or the Sysconf command.

CCS Compact Configuration Storage. An ASN.1-based file format used to store bridge/router configuration information.

configuration files Files on the bridge/router that store parameter values and settings you have set in the software.

default directory structure The default directory structure specifies where to find new installations of your bridge/router software and backups of your bridge/router software on the NMS.

dual-image The ability of a bridge/router to store two sets of image and configuration files.

EOS Enterprise OS. Software that executes on NETBuilder bridge/routers and PathBuilder series switches.

FTP File Transfer Protocol. Allows the transfer of files between a host and a client.

HTTP Hypertext Transfer Protocol. A protocol for transfering hypertext documents.

image file *See* boot image.

manual recovery An upgrade method that copies the primary boot source to the NMS, formats the flash memory on the bridge/router, then copies the upgraded software back to the bridge/router. If the upgrade fails, you must restore the software from the backup on the NMS. Manual recovery requires enough flash memory to hold one software set, compared to automatic recovery which must have enough memory for two sets.

network management station A UNIX or Windows system that has a TFTP server running in addition to software, such as the NETBuilder Upgrade Management Utilities, to manage your network.

NMS *See* network management station.

offline upgrade A method of copying configuration files to a network management station, updating those files to the latest release, and then copying them back to the bridge/router with the new images while the bridge/router remains operational.

primary boot source The default boot source used to boot the bridge/router.

primary image The boot image specified in the primary boot directory.

restore A method of copying a software backup from the network management station to a bridge/router using Upgrade Link or the bcmrestore utility and returning a bridge/router to its previous operational state. Restoring can be used when different versions of software have been installed on the bridge/router.

Remote Upgrade Utilities BCM utilities expressly used for remote upgrading. These utilities allow you to manipulate NETBuilder bridge/router boot blocks and the NETBuilder bridge/router file system via the SNMP protocol. These utilities also allow you to reboot the NETBuilder bridge/router and to obtain accurate status information.

secondary boot source The boot source used in the event of primary boot source failure.

secondary image The software image designated for use by the bridge/router if the primary image is inaccessible or cannot be booted. The secondary image is specified as the local boot file in the secondary boot directory.

single-image The capability of a bridge/router to store only one set of software images and configuration files.

SNMP Simple Network Management Protocol. An Internet protocol that defines a way to monitor and set configuration and runtime parameters.

software set A combination of bootable images for a particular version of bridge/router software along with the configuration files that have been created for the operation of the bridge/router. For version 11.0 and later, the software includes web application files like Quick Step VPN.

software package A defined subset of bridge/router services and protocols that are appropriate for a particular model of the NETBuilder bridge/router family of products.

split image files A boot image that spans multiple diskettes. Split images occur on a few SuperStack II NETBuilder bridge/router packages (for example, the CF package prior to 9.1). If you are upgrading to one of these older packages, bcminstall will automatically recombine the split image before performing your upgrade.

Telnet Terminal Emulation Link Protocol.

TEM/TNCS 3Com's Transcend Enterprise Manager/Transcend Network Control Service, which runs on Windows NT, Windows 95, Solaris, HP, and IBM platforms.

test boot source The boot source used during the test boot process.

test boot image The software image specified as the local boot file in the test source.

TFTP Trivial File Transfer Protocol. Allows file transfer between an IP host and an IP client.

upgrade A method to bring a bridge/router up-to-date with later versions of software and firmware without the need for reconfiguring individual bridge/router parameters and settings. The upgrade is performed using the NETBuilder Upgrade Management Utilities or Transcend.

Upgrade Management Utilities A set of utilities to upgrade bridge/routers or switches. Some functions performed by the utilities include copying software, firmware, and configuration files from the bridge/router, and upgrading configuration files. In addition, the utilities can configure the boot sources on the bridge/router, execute the test boot, and configure the bridge/router boot sources to use the software in standard boot situations.

Upgrade Link Backend The server application that fetches HTML and Java class files, runs the PERI scripts, and accesses the file system.

Upgrade Link Front end The JAVA applet that runs in a browser. All the GUI components are part of the front end.

Upgrade Migration Path The 3Com supported package for upgrading a bridge/router.

WINTEL All windows on INTEL platforms including Windows 95, Windows 98 and Windows NT.

INDEX

Numbers

3Com bulletin board service (3Com BBS) 110
3Com Knowledgebase Web Services 109
3Com URL 109
3ComFacts 110

B

Back up verification 66
bcmbackup 76
  syntax 77
bcmconfig 76
  syntax 78
bcmctrl 76
  syntax 79
bcmdf 76, 80
  syntax 80, 81
bcmdiagnose 42, 76
  return codes 90
  syntax 81
bcminstall 76
  syntax 82
bcmloadconfig 76, 83
bcmrestore 49, 55, 76
  rejecting upgrade 49, 54, 63
  syntax 84
bcmsetup 77
  syntax 85
bcmsum
  syntax 85
bcmsysupgrade 45
  repeating options 44
  syntax 85
bcmuname 77
  syntax 86
bcmupdate 77
  syntax 87
bulletin board service 110

C

configuration,updating files 15
conventions
  notice icons, About This Guide 10
  text, About This Guide 11

D

disk storage requirements
  network management station 31, 41, 58

F

fax service (3ComFacts) 110
files
  backing up 76
  locations 43
  log files 76
firmware
  I/O module upgrade 48, 49, 52, 54
  installing on network management station 76
  monitoring bcm status 76
  parameters, managing 76
  rebooting 76
  test booting 76
  test media storage 76
  testing media storage 76
  upgrade 47, 50

H

hardware
  replacing
    setting up SNMP 69
  setting up IP address 69
  troubleshooting messages 91
HTTP file transfer setup 22

I

identifying upgrade problems 76
images
  updating files 15
IP address
  setting up 69

L

log file 76
logging function 76

M

manual recovery
  NETBuilder II upgrade 52
manual recovery,NETBuilder II upgrade 48
MIBs 109
migration paths
  NETBuilder II 103
  OfficeConnect 106
  PathBuilder 106
  SuperStack II 104, 105

N

NETBuilder II
  migration paths 103
  remote upgrade 48, 52
  upgrading 77
  using bcmdiagnose 42
NETBuilder Upgrade Management Utilities
  files location 43
network management station
  disk storage requirements 31, 41, 58
network supplier support 110

O

online technical services 109

P

patch upgrade
  installation with auto recovery 62
patch upgrade,installation with auto recovery 61
PathBuilder
  image-only upgrade 57
  migration paths 106
  upgrading 77
PathBuilder upgrade
  disk storage requirements 31
privilege level
  changing SNMP access 51, 54
  changing SNMP access to files 69

R

restoring bridge/router to previous operational state 76
returning products for repair 112

S

Simple Network Management Protocol. *See* SNMP
SNMP
  changing file access 69
  changing manager access 51, 54
  setting up 69
    for NETBuilder II upgrade
software
  converting files on network management station 77
  displaying information 77
  installing on network management station 76
  patch installation with auto recovery 61, 62
  rules and support limitations 15
  upgrading 37
SuperStack II,upgrading 77

T

technical support
  3Com Knowledgebase Web Services 109
  3Com URL 109
  bulletin board service 110
  fax service 110

network suppliers 110
product repair 112
Transcend Enterprise Manager 31
Transcend Network Control Services 31
troubleshooting messages
connectivity 92
creating an upgrade file 93
downloading an upgrade file 95
hardware-related 91
SNMP configuration 92
TFTP connection 93
uploading an upgrade file 94
utilities installation 91
validating safety 89

U

update script function 76
upgrade
bcmsysupgrade options 44, 45
identifying problems 76
migration paths
NETBuilder II 103
PathBuilder 106
patch installation
with auto recovery 61, 62
upgrading with bcmsysupgrade utility 77
Upgrade Link
running locally 32
running remotely 32
Settings page 34
Status page 34
Upgrade Link application 31
Upgrade Management Utilities
accessing and downloading 75
accessing MAN pages 77, 89
commands 76
installation
troubleshooting messages 91
with bcmsetup 77
syntax 76
Upgrade verification 35
URL 109

W

World Wide Web (WWW) 109

3Com Corporation LIMITED WARRANTY

HARDWARE

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its authorized reseller:

Network Interface Cards	Lifetime
Other hardware products *unless otherwise specified above	1 year*
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation with respect to this express warranty shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product.

YEAR 2000 WARRANTY

In addition to the Hardware Products Warranty and Software Products Warranty identified above, 3Com warrants that all Heritage 3Com products sold or licensed to Customer on and after January 1, 1998 that are date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com products, including hardware, software, and firmware, accurately exchange date data with the 3Com products, with the exception of those products identified at 3Com's Web site, http://www.3com.com/products/yr2000.html, as not meeting this standard. A product is considered a "Heritage 3Com product" if it is a member of a product family which was manufactured by 3Com prior to its merger with US Robotics Corporation. This Year 2000 limited warranty does not apply to Heritage US Robotics Corporation products. If it appears that any such product does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days or until April 1, 2000, whichever is later.

OBTAINING WARRANTY SERVICE

Customer must contact 3Com's Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

Dead- or Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the defective product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE,

USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (408) 764-5000