Network Connectivity Monitor IP Management Suite Installation Guide

Cisco Network Connectivity Center

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6291-01

Third-Party Software. The Software may include software of third parties from whom SMARTS has received marketing rights and is subject to some or all of the following additional terms and conditions:

Bundled Software
Sun Microsystems, Inc., Java(TM) Interface Classes, Java API for XML Parsing, Version 1.1. "Java" and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. SMARTS is independent of Sun Microsystems, Inc.

W3C IPR Software
Copyright © 2001-2003 World Wide Web Consortium (http://www.w3.org), (Massachusetts Institute of Technology (http://www.lcs.mit.edu), Institut National de Recherche en Informatique et en Automatique (http://www.inria.fr), Keio University (http://www.keio.ac.jp)). All rights reserved (http://www.w3.org/Consortium/Legal/). Note: The original version of the W3C Software Copyright Notice and License can be found at http://www.w3.org/Consortium/Legal/copyright-software-19980720.

The Apache Software License, Version 1.1
Copyright ©1999-2003 The Apache Software Foundation. All rights reserved. Redistribution and use of Apache source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of Apache source code must retain the above copyright notice, this list of conditions and the Apache disclaimer as written below.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the Apache disclaimer as written below in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:
   "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names “The Jakarta Project”, “Tomcat”, "Xalan", "Xerces", and "Apache Software Foundation" must not be used to endorse or promote products derived from Apache software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this Apache software may not be called "Apache," nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

APACHE DISCLAIMER: THIS APACHE SOFTWARE FOUNDATION SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Apache software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright © 1999, Lotus Development Corporation., http://www.lotus.com. For information on the Apache Software Foundation, please see http://www.apache.org.

FLEXlm Software
© 1994 - 2003, Macrovision Corporation. All rights reserved. "FLEXlm" is a registered trademark of Macrovision Corporation. For product and legal information, see http://www.macrovision.com/solutions/esd/flexlm/flexlm.shtml.

JfreeChart – Java library for GIF generation
The Software is a “work that uses the library” as defined in GNU Lesser General Public License Version 2.1, February 1999 Copyright © 1991, 1999 Free Software Foundation, Inc., and is provided “AS IS” WITHOUT WARRANTY OF ANY KIND EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED IN THE ABOVE-REFERENCED LICENSE BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARITES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. JfreeChart library (included herein as .jar files) is provided in accordance with, and its use is covered by the GNU Lesser General Public License Version 2.1, which is set forth at http://www.object-refinery.com/lgpl.html/.

BMC – product library
The Software contains technology (product library or libraries) owned by BMC Software, Inc. (“BMC Technology”). BMC Software, Inc., its affiliates and licensors (including SMARTS) hereby disclaim all representations, warranties and liability for the BMC Technology.

Crystal Decisions Products
The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 (“Crystal Decisions”). All such software products are the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS’ SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS’ SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS’ TECHNOLOGY, TO SMARTS FOR A FULL REFUND; OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU eTeks PJA Toolkit
Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.
The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEks’ web site: http://www.eteks.com. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at http://www.gnu.org/copyleft/gpl.txt. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY;

without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX
The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform
The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: http://www.hp.com. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies
Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

NetBSD
Copyright © 2001 Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   This product includes software developed for the NetBSD Project. See http://www.netbsd.org/ for information about NetBSD.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

RSA Data Security, Inc.
Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

AES
Copyright © 2003, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

License Terms:

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

Disclaimer: This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose. Issue Date: 26/08/2003

Contents

Preface

This document provides instructions for installing Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM) IP Management Suite products on Solaris, HP-UX, Linux, and Windows platforms.

Intended Audience

This guide is intended for administrators and integrators who are responsible for installing the CNCC NCM IP Management Suite.

Prerequisites

You must have root or administrative privileges on the local host to perform the installation. Also, be sure to read the *Network Connectivity Monitor Read Me First* document.

Document Organization

This guide consists of the following sections:

CHAPTER/APPENDIX	DESCRIPTION
1. OVERVIEW	Describes the contents of the IP Management Suite CD-ROM, product compatibility, and installation tasks.
2. SUPPORTED PLATFORMS FOR THE IP MANAGEMENT SUITE	Lists the products of the suite by platform.
3. PATCH REQUIREMENTS	Lists patches required by platform, including Java patches.
4. REQUIREMENTS FOR THE IP MANAGEMENT SUITE	Summarizes hardware and third-party product requirements for the IP Management Suite.
5. UPGRADING AN EXISTING IP INSTALLATION	Explains how to upgrade an existing IP Management installation to IP Management version 6.2.
6. INSTALLING THE IP MANAGEMENT SUITE	Explains how to install the IP Management Suite as well as individual products.
7. PERFORMING MIGRATION TASKS	Explains how to migrate from: • 6.0 IP Availability Manager, IP Performance Manager, and Discovery Manager • 4.1 (4.1.1, or 4.1.2) IP Availability Manager and IP Performance Manager
8. PERFORMING POST-INSTALLATION TASKS	Explains post-installation tasks.
9. UNINSTALLING THE IP MANAGEMENT SUITE	Describes how to remove the IP Management Suite from your system.
A. INSTALLING THE IP MANAGEMENT SUITE USING CLI MODE	Describes how to install the IP Management Suite using the Command Line Interface (CLI) mode.
B. UNATTENDED INSTALLATION FOR THE IP MANAGEMENT SUITE	Describes how to install the IP Management Suite using command line options from a user-modifiable file.

Table 1: **Document Organization**

Documentation Conventions

Several conventions may be used in this document as shown in Table 2.

CONVENTION	EXPLANATION
`sample code`	Indicates code fragments and examples in Courier font
keyword	Indicates commands, keywords, literals, and operators in bold
`%`	Indicates C shell prompt
`#`	Indicates C shell superuser prompt
<parameter>	Indicates a user-supplied value or a list of non-terminal items in angle brackets
[option]	Indicates optional terms in brackets
/InCharge	Indicates directory path names in italics
yourDomain	Indicates a user-specific or user-supplied value in bold, italics
File > Open	Indicates a menu path in italics

Table 2: **Documentation Conventions**

Directory path names are shown with forward slashes (/). Users of the Windows operating systems should substitute back slashes (\) for forward slashes.

Also, if there are figures illustrating consoles in this document, they represent the consoles as they appear in Windows. Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, a plus sign displays for Windows and an open circle displays for UNIX.

Finally, unless otherwise specified, the term CNCC Manager is used to refer to NCM programs such as Domain Managers, Global Managers, and adapters.

NCM Installation Directory

In this document, the term ***BASEDIR*** represents the location where NCM software is installed.

- For UNIX, this location is: */opt/InCharge<n>/<productsuite>*.
- For Windows, this location is: *C:\InCharge<n>\<productsuite>*.

The *<n>* represents the software platform version number. The *<productsuite>* represents the product suite that the product is part of.

Table 3 defines the <*productsuite*> directory for each product.

PRODUCT SUITE	INCLUDES THESE PRODUCTS	DIRECTORY
CNCC NCM IP Management Suite	• IP Availability Manager • IP Performance Manager • IP Discovery Manager • CNCC NCM Adapter for HP OpenView NNM • CNCC NCM Adapter for IBM/Tivoli NetView • CNCC NCM Adapter for CiscoWorks LMS and ITEM	/IP
CNCC NCM Service Assurance Management Suite	• Service Assurance Manager • Global Console • Business Dashboard • Business Impact Manager • Report Manager • SAM Failover System • Notification Adapters • Adapter Platform • SQL Data Interface Adapter • SNMP Trap Adapter • Syslog Adapter • XML Adapter • Adapter for Remedy • Adapter for TIBCO Rendezvous • Adapter for Concord eHealth • Adapter for InfoVista • Adapter for NetIQ AppManager	/SAM
InCharge Application Management Suite	• Application Services Manager • Beacon for WebSphere • Application Connectivity Monitor	/APP
InCharge Security Infrastructure Management Suite	• Security Infrastructure Manager • Firewall Performance Manager • InCharge Adapter for Check Point/Nokia • Incharge Adapter for Cisco Security	/SIM
InCharge Software Development Kit	• Software Development Kit	/SDK

Table 3: **Product Suite Directory for NCM Products**

For example, on UNIX operating systems, CNCC NCM IP Availability Manager is, by default, installed to */opt/InCharge6/IP/smarts*. This location is referred to as ***BASEDIR****/smarts*.

Optionally, you can specify the root of ***BASEDIR*** to be something other than */opt/InCharge6* (on UNIX) or *C:\InCharge6* (on Windows), but you cannot change the <*productsuite*> location under the root directory.

For more information about the directory structure of NCM software, refer to the *Network Connectivity Monitor System Administration Guide*.

Additional Resources

In addition to this manual, Cisco provides the following resources.

Commands

Descriptions of commands are available as HTML pages. The *index.html* file, which provides an index to the various commands, is located in the ***BASEDIR/****smarts/doc/html/usage* directory.

Documentation

Readers of this manual may find other documentation (also available in the ***BASEDIR/****smarts/doc/pdf* directory) helpful.

Network Connectivity Monitor Documentation

The following documents are product independent and thus relevant to users of all Network Connectivity Monitor products:

- *Release Notes for Network Connectivity Monitor 1.1*
- *Network Connectivity Monitor Documentation Roadmap*
- *Network Connectivity Monitor System Administration Guide*
- *ICIM Reference*
- *InCharge ASL Reference Guide*
- *Cisco Network Connectivity Center Perl Reference Guide*

Network Connectivity Monitor IP Management Documentation

The following documents are relevant to users of CNCC NCM IP Management Suite products:

- *Network Connectivity Monitor IP Management Suite Installation Guide*
- *Network Connectivity Monitor IP Deployment Guide*
- *Network Connectivity Monitor IP Discovery Guide*
- *Network Connectivity Monitor IP Availability Manager User's Guide*
- *InCharge IP Performance Manager User's Guide*
- *InCharge IP Adapters User's Guide*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

1

Overview

This chapter describes the Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM) IP Management Suite products, compatibility with other NCM products, and installation tasks.

The product suite is distributed on a CD-ROM and is installed in the */IP* subdirectory under the InCharge root directory.

Suite Contents

This section describes the suite contents.

IP Management Suite

The suite contains the following:

- *CNCC NCM IP Availability Manager:* The IP Availability Manager product diagnoses connectivity failures, including analysis of root causes, in IP networks.
- *InCharge IP Performance Manager:* The IP Performance Manager product diagnoses faults, including device- and performance-centric analysis of root causes, in IP networks. If you wish to use the InCharge IP Server Performance Manager, you need to install the IP Performance Manager.
- *InCharge Discovery Manager:* The Discovery Manager performs layer-3 and layer-2 connectivity and device containment discovery for IP networks. It also discovers information about a system's resources.

- *CNCC NCM Adapter for HP OpenView NNM:* The CNCC Adapter for HP OpenView NNM product imports topology and traps from HP OpenView NNM.
- *CNCC NCM Adapter for IBM/Tivoli NetView:* The CNCC Adapter for IBM/Tivoli NetView product imports topology and traps from IBM/Tivoli NetView.
- *CNCC NCM Adapter for CiscoWorks LMS and ITEM*: The CNCC NCM Adapter for CiscoWorks LAN Management Solution (LMS) and IP Telephony Environment Monitor (ITEM) product imports topology from CiscoWorks LMS and ITEM.
- *CNCC Perl API:* The Perl APIs provide functionality needed for a Perl client application to communicate with NCM. The Perl APIs are compatible with Perl version 5.6.1 or 5.8.0.

Product and Version Compatibility

The following identifies the compatibility of NCM 1.1 products with other NCM products or components.

SAM Global Manager 6.2

Requires Global Console 6.2.

Compatible with InCharge IP Availability Manager 4.1, 4.1.1, or 4.1.2.

Requires Broker 5.0 or later.

Compatible with Application Services Manager 1.0 and Application Connectivity Monitor 1.1.

Compatible with Report Manager 6.2.

SAM 6.2 Global Console

Requires SAM Global Manager 6.2.

6.2 IP Management Products

Requires installation of SAM 6.2.

Note: Customers who migrate from SAM 6.0 to SAM 6.2 should retain an installation of a 6.0 Global Console in order to continue to administer any remaining (non-migrated) 6.0 Global Managers.

Installation Tasks

The successful deployment of NCM products requires knowledge of your operational environment and the management tools already in place. You can integrate NCM with third-party applications and prior installations of InCharge applications without disturbing the existing environment.

The 6.2 installation tasks vary according to one of these scenarios:

- New IP installation, no pre-existing InCharge installations
- 6.0 IP installation already exists
- 4.1, 4.1.1, or 4.1.2 IP installation already exists
- 6.2 IP installation already exists and you wish to add more 6.2 products

To add more 6.2 products to the existing 6.2 directory, perform the tasks that are listed to upgrade an existing 6.0 IP installation.

Figure 1 illustrates the decision process for these scenarios. Tasks are summarized in the sections identified in the illustration.

Select the scenario that best suits your needs. If you need assistance, contact Cisco Technical Assistance Center (TAC).

Note that NCM provides advanced security features. For information about the levels of security and how they might affect your deployment, see the *Network Connectivity Monitor System Administration Guide*.

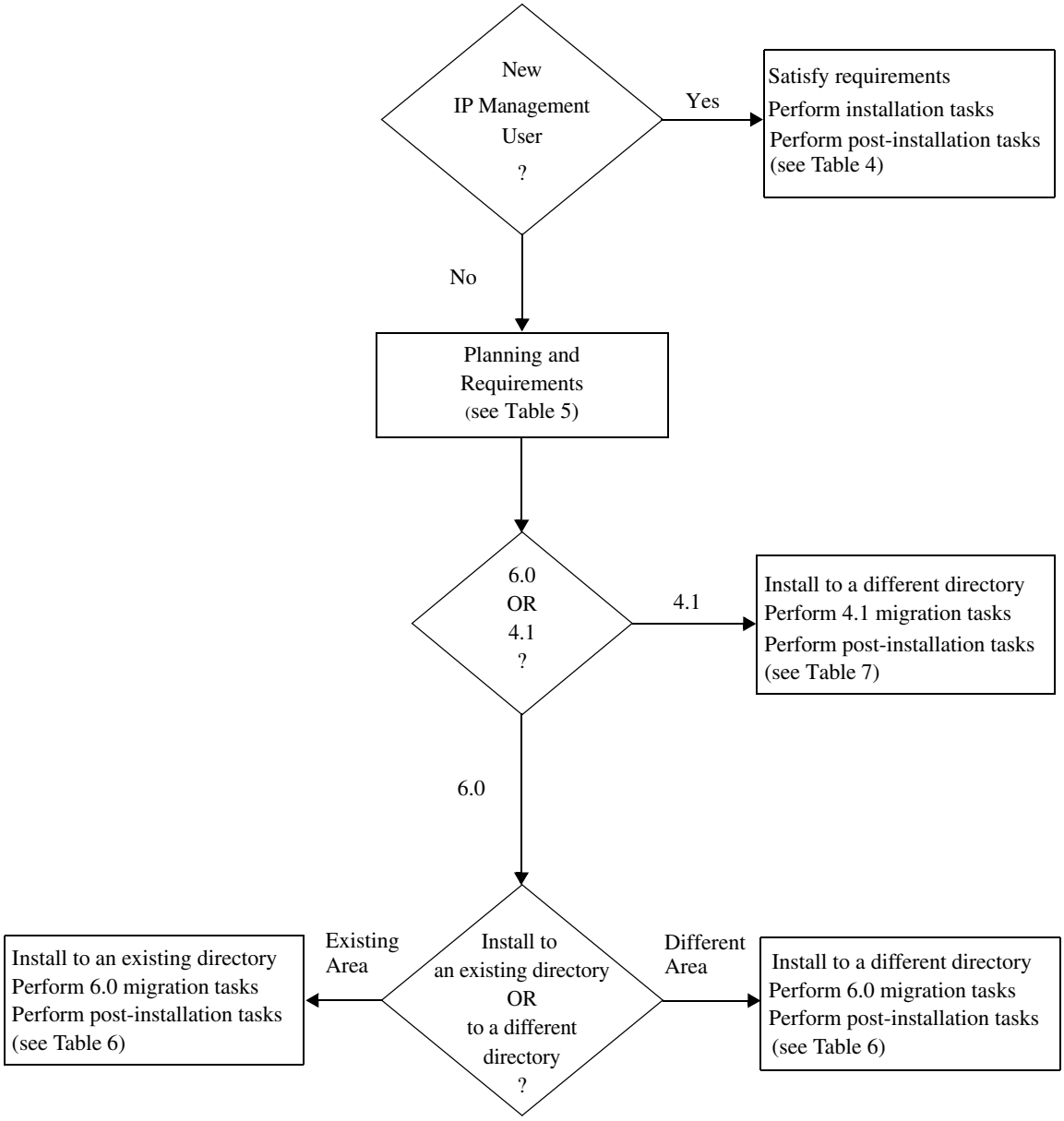

Figure 1: **Installation Decision Tree**

New IP Installation Scenario

If you are installing the IP Management Suite for the first time and you plan to install the 6.2 IP Management Suite on a system where no other InCharge installations exist, you need to satisfy or perform the following tasks.

TASKS	GO TO:
Before You Install:	
Review the important release issues.	*Network Connectivity Monitor Read Me First*
Obtain an evaluation or permanent license.	*Network Connectivity Monitor System Administration Guide* for license information To request a license, contact Cisco TAC. See the *Supplement and Read Me First for Cisco Network Connectivity Center* for more information.
Determine if the products you are installing are supported for your platform.	*Supported Platforms for the IP Management Suite* on page 13
Determine if your system meets the hardware requirements for the products you are installing.	*Requirements for the IP Management Suite* on page 21
Apply operating system-specific patches to your system.	*Patch Requirements* on page 15
To run the installation program, ensure Java Runtime Environment (JRE) version 1.4 (or later) is installed on your system.	*JRE Requirement for the Installation Program* on page 21 for information and instructions for a user-defined location.
Check other requirements for administrative privileges and third-party requirements for adapters.	• *Privileges Requirement* on page 22 • *Adapter Requirements* on page 25
Installation Method:	
Install the IP Management Suite.	Choose one of the following installation methods: • *Installing the IP Management Suite* on page 33 • UNIX only, *Installing the IP Management Suite Using CLI Mode* on page 55 • *Unattended Installation for the IP Management Suite* on page 59
After You Install:	
Save your license in the proper location: • Evaluation license—Save *trial.dat* to the ***BASEDIR****/smarts/local/conf* directory. Edit the SM_LICENSE variable in the *runcmd_env.sh* file so that the variable specifies the full path name to the *trial.dat* file. • Permanent license—Save *smarts.lic* to the ***BASEDIR*** directory. By default, ***BASEDIR*** is */opt/InCharge<n>/IP* for UNIX and C:\InCharge<n>\IP for Windows.	*Network Connectivity Monitor System Administration Guide*

Default encryption is enabled during the 6.2 installation process. You can configure NCM installations with a variety of levels of security. Cisco highly recommends that you increase your level of security.	*Network Connectivity Monitor System Administration Guide*
If you installed the products as services, you need to start them for the first time.	*Starting NCM Products* on page 47
Verify the current state of the products and NCM Broker	*Verifying the NCM Product Status* on page 49
Start and restart OpenView or NetView and start the adapters	*HP OpenView and IBM/Tivoli NetView* on page 50
Start the Global Console	*Starting the Global Console* on page 50
If applicable, for the specialized version of IP Performance Manager, IP Server Performance Manager, enable monitoring of server disk and file systems through the Domain Manager Administration Console.	*InCharge IP Performance Manager User's Guide*

Table 4: **Tasks for a New IP Installation**

Existing 6.0 IP Installation Scenario

If you plan to upgrade an existing 6.0 IP Management Suite to 6.2 IP Management Suite, you need to satisfy or perform the following tasks.

These tasks also apply if you plan to add more 6.2 products to an existing 6.2 IP directory.

TASKS	GO TO:
Planning Considerations:	
Review the important release issues.	*Network Connectivity Monitor Read Me First*
The 6.2 IP Management Suite can be installed into an existing 6.0 directory or to a different directory. Your choice affects the installation process and which steps you need to perform afterwards.	
Identify the system (host) and the location of the existing Broker and FLEXlm license server. This determines your installation order: • If the FLEXlm license server and the Broker were installed together for 6.0 IP, update the 6.0 IP Management Suite first. • If the broker was not installed with the license server, update the suite where the license server is running, followed by the suite for the broker and other Managers for that suite. • Finally, install Managers and adapters for other suites, including a hierarchical SAM if necessary. For each installation, you need to perform post-installation tasks.	• *Network Connectivity Monitor Service Assurance Management Suite Installation Guide* • *Network Connectivity Monitor IP Management Suite Installation Guide*
Before You Install:	

Obtain an evaluation or permanent license. If you have a permanent license for 6.0 IP Management, request a new one that supports the FLEXlm license software version 9.2. If you are installing the 6.2 IP Management Suite into an existing 6.0 directory, ensure that your license is in the proper location. If you are installing to a different directory, perform this task after installation. The proper location for a license is: • Evaluation license—Save *trial.dat* to the ***BASEDIR****/smarts/local/conf* directory. Edit the SM_LICENSE variable in the *runcmd_env.sh* file so that the variable specifies the full path name to the *trial.dat* file. • Permanent license—Save *smarts.lic* to the ***BASEDIR*** directory. By default, ***BASEDIR*** is */opt/InCharge<n>/IP* for UNIX and *C:\InCharge<n>\IP* for Windows. *Do not* save *smarts.lic* to the ***BASEDIR****/smarts/local/conf*, ***BASEDIR****/smarts/script,* or ***BASEDIR****/smarts/conf* directory.	*Network Connectivity Monitor System Administration Guide* for license information To request a license, contact Cisco TAC. See the *Supplement and Read Me First for Cisco Network Connectivity Center* for more information.
Determine if the products you are installing are supported for your platform.	*Supported Platforms for the IP Management Suite* on page 13
Determine if your system meets the hardware requirements for the products you are installing.	*Requirements for the IP Management Suite* on page 21
Apply operating system-specific patches to your system.	*Patch Requirements* on page 15
To run the installation program, ensure Java Runtime Environment (JRE) version 1.4 (or later) is installed on your system.	*JRE Requirement for the Installation Program* on page 21 for information and instructions for a user-defined location.
Check other requirements for administrative privileges and third-party requirements for adapters.	• *Privileges Requirement* on page 22 • *Adapter Requirements* on page 25

Table 5: **Planning and Requirements If IP Management Suite Is Already Installed**

After you examine the planning considerations and requirements, you need to install the 6.2 IP Management Suite into either the existing 6.0 directory or a different directory (see Table 6).

TASKS	GO TO:
Stop the services for the suite.	*Upgrading an Existing IP Installation* on page 29 or the *Network Connectivity Monitor System Administration Guide*
Are you installing into the existing 6.0 directory or to a different directory?	
Install into the existing 6.0 directory.	*Upgrading an Existing IP Installation* on page 29
Install into a different directory. Remember to change the root portion of ***BASEDIR***.	Choose one of the following installation methods: • *Installing the IP Management Suite* on page 33 • UNIX only, *Installing the IP Management Suite Using CLI Mode* on page 55 • *Unattended Installation for the IP Management Suite* on page 59
After You Install:	
If you installed the 6.2 IP Management Suite to a different directory, you must ensure that your license is in the proper location. The proper location for a license is: • Evaluation license—Save *trial.dat* to the ***BASEDIR****/smarts/local/conf* directory. Edit the SM_LICENSE variable in the *runcmd_env.sh* file so that the variable specifies the full path name to the *trial.dat* file. • Permanent license—Save *smarts.lic* to the ***BASEDIR*** directory. By default, ***BASEDIR*** is */opt/InCharge<n>/IP* for UNIX and *C:\InCharge<n>\IP* for Windows. *Do not* save *smarts.lic* to the ***BASEDIR****/smarts/local/conf*, ***BASEDIR****/smarts/script,* or ***BASEDIR****/smarts/conf* directory.	*Network Connectivity Monitor System Administration Guide*
Set up new and old license servers.	*Network Connectivity Monitor System Administration Guide*
Perform migration tasks: • Reconcile previously installed 6.0 patches before starting any services. • Examine existing files in the */local* directory for customizations you wish to retain.	*Migrating From IP Management Suite 6.0* on page 39
Set SM_INCOMING_PROTOCOL and SM_OUTGOING_PROTOCOL in the *runcmd_env.sh* file for encrypted connections.	*Network Connectivity Monitor System Administration Guide*

Encrypt the existing security configuration files to obtain a level of encryption equivalent to the level of default encryption. Use the sm_edit utility to either add the required first line of code for encryption or merge entries from existing security configuration files into the new files located in the */local* directory. You can configure NCM installations with a variety of levels of security. Cisco highly recommends that you increase your level of security.	*Network Connectivity Monitor System Administration Guide* for security information.
Encrypt the existing seed files. Use the sm_edit utility to add the required first line of code for encryption.	*Network Connectivity Monitor IP Discovery Guide*
If you installed the products as services, you need to start them for the first time.	*Starting NCM Products* on page 47
Verify the current state of the products and the Broker	*Verifying the NCM Product Status* on page 49
Start and restart OpenView or NetView and start the adapters	*HP OpenView and IBM/Tivoli NetView* on page 50
Start the Global Console	*Starting the Global Console* on page 50
If applicable, for the specialized version of IP Performance Manager, IP Server Performance Manager, enable monitoring of server disk and file systems through the Domain Manager Administration Console.	*InCharge IP Performance Manager User's Guide*
Perform validation tests	*Network Connectivity Monitor IP Deployment Guide*

Table 6: **Tasks for an Existing 6.0 IP Management Suite Installation**

Existing 4.1, 4.1.1, or 4.1.2 IP Installation Scenario

If you plan to upgrade an existing 4.1, 4.1.1, or 4.1.2 IP installation to 6.2 IP Management Suite, see Table 5 for planning considerations and requirements. You also need to perform the following tasks.

Note: For this scenario, the 6.2 IP Management Suite can only be installed into a different directory. The 6.2 IP Management Suite should not be installed into an existing directory that has pre-6.0 InCharge software.

TASKS	GO TO:
Installation Method:	
Install into a different directory. Remember to change the root portion of ***BASEDIR***.	Choose one of the following installation methods: • *Installing the IP Management Suite* on page 33 • UNIX only, *Installing the IP Management Suite Using CLI Mode* on page 55 • *Unattended Installation for the IP Management Suite* on page 59
After You Install:	
Ensure that your license is in the proper location. The proper location for a license is: • Evaluation license—Save *trial.dat* to the ***BASEDIR****/smarts/local/conf* directory. Edit the SM_LICENSE variable in the *runcmd_env.sh* file so that the variable specifies the full path name to the *trial.dat* file. • Permanent license—Save *smarts.lic* to the ***BASEDIR*** directory. By default, ***BASEDIR*** is */opt/InCharge<n>/IP* for UNIX and *C:\InCharge<n>\IP* for Windows. *Do not* save *smarts.lic* to the ***BASEDIR****/smarts/local/conf*, ***BASEDIR****/smarts/script,* or ***BASEDIR****/smarts/conf* directory.	*Network Connectivity Monitor System Administration Guide*
Set up new and old license servers.	*Network Connectivity Monitor System Administration Guide*
Perform migration tasks: • Reconcile previously installed 4.1 patches before starting any services. • Examine existing files for customizations you wish to retain • Migrate 4.1, 4.1.1, or 4.1.2 topology and create ISDN threshold groups if necessary	*Migrating From IP Applications 4.1, 4.1.1, or 4.1.2* on page 43
Set SM_INCOMING_PROTOCOL and SM_OUTGOING_PROTOCOL in the *runcmd_env.sh* file for encrypted connections.	*Network Connectivity Monitor System Administration Guide*
Encrypt the existing security configuration files to obtain a level of encryption equivalent to the level of default encryption. Use the sm_edit utility to either add the required first line of code for encryption or merge entries from existing security configuration files into the new files located in the */local* directory. You can configure NCM installations with a variety of levels of security. Cisco highly recommends that you increase your level of security.	*Network Connectivity Monitor System Administration Guide* for security information.
Encrypt the existing seed files. Use the sm_edit utility to add the required first line of code for encryption.	*Network Connectivity Monitor IP Discovery Guide*

If you installed the products as services, you need to start them for the first time.	*Starting NCM Products* on page 47
Verify the current state of the products and the Broker	*Verifying the NCM Product Status* on page 49
Start and restart OpenView or NetView and start the adapters	*HP OpenView and IBM/Tivoli NetView* on page 50
Start the Global Console	*Starting the Global Console* on page 50
If applicable, for the specialized version of IP Performance Manager, IP Server Performance Manager, enable monitoring of server disk and file systems through the Domain Manager Administration Console.	*InCharge IP Performance Manager User's Guide*
Perform validation tests	*Network Connectivity Monitor IP Deployment Guide*

Table 7: **Tasks for an Existing 4.1, 4.1.1, or 4.1.2 IP Installation**

2

Supported Platforms for the IP Management Suite

Table 8 summarizes the supported platforms for each product in the IP Management Suite.

PRODUCT	PLATFORM				
	SOLARIS	HP-UX	AIX	LINUX	WINDOWS
IP Availability Manager	8 and 9	11.00 and 11.11	N/A	Red Hat Linux Advanced Server ES, AS, or WS 2.1.	Windows 2000 Server, Advanced Server. Windows 2003.
IP Performance Manager	8 and 9	11.00 and 11.11	N/A	Red Hat Linux Advanced Server ES, AS, or WS 2.1.	Windows 2000 Server, Advanced Server. Windows 2003.
Discovery Manager	8 and 9	11.00 and 11.11	N/A	Red Hat Linux Advanced Server ES, AS, or WS 2.1.	Windows 2000 Server, Advanced Server. Windows 2003.
CNCC NCM Adapter for HP OpenView NNM	8 and 9	11.00 and 11.11	N/A	N/A	Windows 2000 Server, Advanced Server.
CNC Adapter for IBM/Tivoli NetView	8 and 9	N/A	N/A	N/A	Windows 2000 Server, Advanced Server.
CNCC NCM Adapter for CiscoWorks LMS/ITEM	8 and 9	N/A	N/A	N/A	Windows 2000 Server, Advanced Server. Windows 2003.
Perl API	8 and 9	11.00 and 11.11	N/A	Red Hat Linux Advanced Server ES, AS, or WS 2.1.	Windows 2000 Server, Advanced Server. Windows 2003.

Table 8: **Supported Platforms for IP Management Suite**

3

Patch Requirements

This chapter describes operating system patch requirements for all suites, including:

- General patches for the proper operation of code produced by Cisco.
- System patches for the NCM installation program.
- Java patches for the proper operation of NCM products.

The patches *must be* applied before starting the installation process. If these required patches are not at the correct level, a system failure and installation failure may occur.

During installation, the setup program performs a requirements check for patches. If your system fails the requirements check, the installation process stops and you must apply the necessary patches.

Required Patches for Solaris

This section lists the minimum patch requirements for all suites running on Solaris.

Table 9 summarizes general patches and Java patches, such as patch cluster and font packages.

SOLARIS VERSION	PATCH
Solaris 8	C++ Runtime 108434-12
	Linker 109147-21
	J2SE Solaris 8 (patch cluster)
	SUNWxwfnt (X Window System platform fonts)
	SUNWi1of (ISO-8859-1 (Latin-1) fonts)
Solaris 9	C++ Runtime 111711-05
	Linker 112963-05
	J2SE Solaris 9 (patch cluster)
	SUNWxwfnt (X Window System platform fonts)
	SUNWi1of (ISO-8859-1 (Latin-1) fonts)

Table 9: **Patches Required for Solaris**

How to Obtain Java Cluster Patches

Cisco installs JRE 1.4.2 for the proper operation of NCM products and assumes that prerequisite patches are applied to your system.

If the J2SE Solaris 8 patch cluster or J2SE Solaris 9 patch cluster does not exist on your system, you can obtain it from Sun Microsystems. Sun produces a patch cluster that contains the required Java patches.

1. Go to the web page, *http://java.sun.com/j2se/1.4.2/download.html*.
2. In the Solaris OS Patches section, select **Download** in the Solaris SPARC column to display the J2SE Cluster Patches.
3. Download the patch and the Readme file for J2SE Cluster Patches for Solaris 8 or Solaris 9 (do *not* download x86 versions). Follow the instructions in the Readme file.

How To Verify Font Patches

It may be necessary to install one or more font packages on your system.

To check whether the required font support for the basic locales is present, issue the following command and check the result which should match the following:

```
$ /bin/pkginfo SUNWi1of SUNWxwfnt
system SUNWi1of ISO-8859-1 (Latin-1) Optional Fonts
system SUNWxwfnt X Window System platform required fonts
```

If you receive a message such as:

```
ERROR: information for "SUNWxwfnt" was not found
```

the corresponding package does not exist on your system and must be installed from your Solaris 8 or 9 Software CD-ROM.

If you need any fonts beyond the basic set, information is available from Sun at *http://java.sun.com/j2se/1.4.2/font-requirements.html*.

Required Patches for HP-UX

This section lists the minimum patch requirements for all suites running on HP-UX.

WARNING: For HP-UX 11.00 only, patch PHKL_28060 must be installed prior to attempting to read the InCharge CD-ROM. Without this patch, random errors will occur while reading the CD-ROM. According to HP, it is possible for the system to crash.

Table 10 summarizes general patches. Java patches are described in the subsequent section.

PLATFORM	PATCH ID	DESCRIPTION
HP-UX 11.00	PHKL_28060	Y2k; Rock Ridge extension for ISO-9660
	PHSS_26945	aCC run-time
	PHSS_28302	libcl patch
	PHSS_28434	dld and cumulative linker tools patch
	PHCO_28425	libc cumulative patch
	PHCO_26960	libpthread

PLATFORM	PATCH ID	DESCRIPTION
HP-UX 11.11	PHSS_26946	aCC run time
	PHCO_28427	libc cumulative patch
	PHSS_28303	libcl patch
	PHSS_30049	dld and cumulative linker tools patch
	PHCO_27632	libpthread

Table 10: **Patches Required for HP-UX**

Required Java Patches

Cisco installs JRE 1.4.2 for the proper operation of NCM products and assumes that prerequisite patches are applied to your system.

For HP-UX, there are many required Java patches. Cisco recommends you use the HPjconfig tool to analyze your system and to download and apply any required patches. This tool is available from HP at http://www.hp.com/go/java. Select the link HPjconfig configuration tool which includes instructions.

Note: The HPjconfig tool also checks kernel parameter values. The kernel parameter values required for Cisco software usually exceed the minimum values recommended by HPjconfig. You should use the larger of the two values—either the value listed in the requirements chapter for your suite or the value recommended by HPjconfig.

Required Patches for Linux

This section lists the minimum patch requirements for all suites running on Red Hat Linux Advanced Server ES, AS, or WS 2.1.

Table 11 summarizes general patches. Compiler patches are not required for Red Hat Linux.

PLATFORM	PATCH ID	DESCRIPTION
Red Hat Linux Advanced Server ES, AS, or WS 2.1	glibc-2.2.4-32	C library consolidated patches
	glibc-common-2.2.4-32	C library consolidated patches

Table 11: **Patches Required for Linux**

Required Java Patches

Cisco installs JRE 1.4.2 for the proper operation of NCM products and assumes that prerequisite patches are applied to your system.

For Linux, if the prerequisite patches do not exist on your system, you can obtain them from Sun Microsystems. Go to the web page http://java.sun.com/j2se/1.4.2/system-configurations.html for information about supported system configurations. For downloads, go to web page http://java.sun.com/j2se/1.4.2/download.html.

How To Verify Linux Patches

To check for required patches, issue the following command and check the result which should match the following:

```
$ rpm -q glibc glibc-common
glibc-2.2.4-32
glibc-common-2.2.4-32
```

The `-32` is the patch release number. The result should indicate -32 or later.

These patches are available from Red Hat at http://www.redhat.com/apps/download and use the general search facility to search for the specific patches. Or, go to http://rhn.redhat.com/errata/RHSA-2003-089.html, select the link Red Hat Linux 7.2, and select patches in the i386 section.

To check the version of Linux, perform the following steps

1. Issue the `uname` command:

   ```
   $ uname -a
   Linux king 2.4.9-e.3smp #1 SMP Fri May 3 16:48:54 EDT 2002
   i686 unknown
   ```

   The result should indicate 2.4.9 or later.

2 Issue the cat command:

```
$ cat /etc/redhat-release
Red Hat Linux Advanced Server release 2.1AS (Pensacola)
```

The result should read release 2.1 and may be Advanced Server, Enterprise Server, or Workstation Server.

Required Patches for Windows

The required patches are listed in Table 12.

PLATFORM	PATCHES
Windows XP	N/A
Windows 2000 (Professional, Server and Advanced Server)	Service Pack 4 or later
Windows 2003	N/A

Table 12: **Patch Requirements for Windows**

For more information on how to obtain service packs, please access the Microsoft Technical Support Web site at *http://support.microsoft.com.*

Patch maintenance may or may not be necessary for your system. Subsequent installation steps assume that the proper maintenance has been completed.

Required Java Patches

Cisco installs JRE 1.4.2 for the proper operation of NCM products and assumes that prerequisite patches are applied to your system.

For Windows, if the prerequisite patches do not exist on your system, you can obtain them from Sun Microsystems. Go to the web page *http://java.sun.com/j2se/1.4.2/system-configurations.html* for information about supported system configurations. For downloads, go to web page *http://java.sun.com/j2se/1.4.2/download.html*.

4

Requirements for the IP Management Suite

This chapter describes pre-installation requirements for the IP Management Suite. It includes:

- JRE Requirement for the installation program
- Privileges requirement
- Hardware requirements
- Additional HP-UX Requirements
- X Server Settings (UNIX Only)
- Adapter requirements, including supported versions for third-party integration

JRE Requirement for the Installation Program

To run the installation program, you must have Java Runtime Environment (JRE) version 1.4 (or later) installed on your system. The installation program attempts to detect that a compatible JRE version has been installed on your system.

To obtain the required JRE version for HP-UX platform, download it from *http://www.hp.com/products1/unix/java/index.html* and, for all other platforms, download it from *http://java.sun.com*. Also, the required JRE version is available from Cisco TAC.

For UNIX only, if a compatible JRE version is installed and the installation program cannot locate it, you must specify the location when you execute the installation program. The syntax is:

```
# ./setup-solaris.bin -is:javahome <local_java_dir>
```

where ***<local_java_dir>*** is the directory path, including the JRE file name. The Setup command is described in *Mounting the CD-ROM and Executing Installation Setup*.

Privileges Requirement

To install products, you must either:

- Be superuser (User ID 0) on UNIX platforms.
- Have administrative privileges on Windows platforms.

Hardware Requirements

Hardware and software requirements summarized here represent the minimum levels. Table 13 lists disk space requirements for installing all products in the IP Management Suite.

PLATFORM	DISK SPACE
Solaris 8 and 9	350 MB
HP-UX 11.00 and 11.11	550 MB
AIX 5.1	N/A
Red Hat Linux Advanced Server ES, AS, or WS 2.1	200 MB
Windows 2000 and 2003	150 MB

Table 13: **Required Disk Space for the IP Management Suite**

Table 14 lists minimum requirements for CPUs, memory, and data disk space used by the software for writeable files such as logs, repository files, and output files.

If you are installing more than one product, then your system must meet the products' total memory and data disk space requirements.

PRODUCT	CPUS	MEMORY (RAM)	DATA DISK SPACE
IP Availability Manager	2	512 MB	100 MB each
IP Performance Manager	2	512 MB	100 MB each
Discovery Manager	1	512 MB	100 MB each
CNCC NCM Adapter for HP OpenView NNM	1	256 MB	N/A
CNCC NCM Adapter for IBM/Tivoli NetView	1	256 MB	N/A

Table 14: **CPU, Memory, and Data Disk Space Requirements**

Table 15 lists minimum hardware requirements.

PLATFORM	PRODUCT	HARDWARE
Solaris 8 and 9	All products	Sun Fire 280
HP-UX 11.00 and 11.11	IP Availability Manager, IP Performance Manager, Discovery Manager	L2000/rp5400
	Adapters	b2600
AIX 5.1	N/A	N/A
Red Hat Linux Advanced Server ES, AS, or WS 2.1	IP Availability Manager, IP Performance Manager, Discovery Manager	2xPentium 4, 2 GHz
Windows 2000	IP Availability Manager, IP Performance Manager, Discovery Manager	2xPentium 4, 2 GHz
	Adapters	Pentium III, 1.6 GHz
Windows 2003	IP Availability Manager, IP Performance Manager, Discovery Manager	2xPentium 4, 2 GHz

Table 15: **Hardware Requirements for the IP Management Suite**

Additional HP-UX Requirements

This section lists additional requirements for HP-UX 11.00 and HP-UX 11.11.

Use the HP-UX system administration manager tool to verify that the following parameters in Table 16 are set accordingly. Use “Choose Kernel Configuration,” “Choose Configurable Parameter” to get to the definition page. The necessary procedures are described in the HP-UX System Administration Tasks manual.

If necessary, make changes. Then, rebuild the kernel and reboot the system. You may want to contact your system administrator if you need additional help.

Note: You can also use the HPjconfig tool that checks kernel parameter values as well as patches. The kernel parameter values required for Cisco software usually exceed the minimum values recommended by HPjconfig. You should use the larger of the two values—either the value based on the formula below or the value recommended by HPjconfig. See the Patch Requirements chapter for information about the HPjconfig tool.

Table 16 summarizes HP-UX parameter requirements and their values.

PARAMETER	VALUE
maxdsiz	at least 512 MB (536870912 bytes)
max_thread_proc	at least 256
ncallout	nproc + 10*nCisco
nkthread	2*nproc + max_thread_proc*nCisco

Table 16: HP-UX Parameters and Values

Formulas are provided as follows.

- The process data size limit kernel parameter (maxdsiz) must be set to at least 512 MB (536870912 bytes).

  The value of this parameter is in decimal bytes. If it is below 512 MB (536870912 bytes), increase it, rebuild the kernel, and restart the system.

- The max_thread_proc parameter must be set to at least 256, and the ncallout and nkthread parameters are calculated as follows.

  In the formulas, “nCisco” is the total number of CNCC Managers and consoles running simultaneously on the machine and “nproc” is a varying system parameter displayed by HP-UX system administration manager. It represents the maximum number of processes on the machine.

- The ncallout value must be equal to at least the calculated result, although the HP-UX system administration manager default is almost always sufficient.

  ncallout = nproc + 10*nCisco

- The nkthread value must be equal to at least the calculated result:

  nkthread = 2*nproc + max_thread_proc*nCisco

  (The max_thread_proc parameter must be at least 256.)

X Server Settings (UNIX Only)

One of the installation methods, the InstallShield Wizard method, uses a graphical wizard. In this case, for UNIX, the installation program is an X11 application. The host on which you install the NCM software and the host on which you log on must be configured to run X11.

Adapter Requirements

This section describes the platforms that are supported for adapters, supported versions of OpenView NNM and IBM/Tivoli NetView, and other requirements depending upon the adapter, such as the location where an adapter must reside.

Adapters That Have Third-Party Requirements

Table 17 identifies the supported versions of the third-party applications.

PLATFORM	CNCC NCM ADAPTER FOR HP OPENVIEW NNM	CNCC NCM ADAPTER FOR IBM/TIVOLI NETVIEW	CNCC NCM ADAPTER FOR CISCOWORKS LMS AND ITEM
	OPENVIEW NNM	IBM/TIVOLI NETVIEW	CISCOWORKS
Solaris 8, Solaris 9	6.4	7.1	One of the following: • LMS 2.1 or later. • ITEM 2.0 with latest IDU • ITEM1.4 with DFM 1.2.7.
HP-UX 11.00, HP-UX 11.11	6.4	N/A	N/A
AIX 5.1	N/A	N/A	N/A
Red Hat Linux Advanced Server ES, AS, or WS 2.1	N/A	N/A	N/A
Windows 2000 SP 4 or later	6.4	7.1	One of the following: • LMS 2.1 or later. • ITEM 2.0 with latest IDU • ITEM1.4 with DFM 1.2.7.
Windows 2003	N/A	N/A	CiscoWorks CD One, 5th Edition orCommon Services 2.2 running one of the following: • LMS 2.1 or 2.2 with or without LMS Update 1. • ITEM 2.0 or ITEM 1.4 with DFM 1.2.7.

Table 17: **Third-Party Product Requirements for NCM Adapters**

The CNCC NCM Adapter for HP OpenView NNM and the CNCC NCM Adapter for IBM/Tivoli NetView must run on the same host as OpenView NNM and IBM/Tivoli NetView, respectively.

The CNCC NCM Adapter for CiscoWorks LMS and ITEM must run on the same host as CNCC NCM IP Availability Manager.

OpenView Account and Service Requirements

For the CNCC NCM Adapter for HP OpenView NNM on Windows, if OpenView is installed on an NTFS partition, the adapter may not start. Before you install the adapter, use the Control Panel Services to configure the HP OpenView Process Manager service to start under an account that has full NTFS privileges (for example, Administrator). For instructions to create a user account and configure a service, see the *InCharge IP Adapters User's Guide*.

5

Upgrading an Existing IP Installation

This chapter describes the additional screens which display during the InstallShield Wizard installation method if you are:

- Installing the 6.2 IP Management Suite into an existing 6.0 IP directory
- Adding products to an existing 6.2 IP directory

The InstallShield Wizard installation method is described in *Installing the IP Management Suite* on page 33. If you are installing the IP Management Suite into a different directory, follow those instructions.

The installation process is the same except for these steps:

1. Make backup copies of following subdirectories under the *InCharge6/IP/smarts* directory: */local* and */setup*.

   If you previously applied SmartPack 1, you can use the smgetinfo utility to back up these directories. The smgetinfo utility is briefly described in *Using the smgetinfo Utility* on page 31. More complete information is provided in the *Network Connectivity Monitor System Administration Guide*.

2. During the installation process, the following steps might display:

   - The Installation Type screen. Select Upgrade for the installation type if you already have products from this suite installed and you want to install more into the same directory.

     Only select Install, if you wish to retain an existing installation and you wish to install the suite in a different directory on the same host. Later, you will be prompted to specify a different directory.

- If an existing license is detected, the Installed License Manager screen indicates whether the installation program will continue. Click **Next** to continue.

  Next is disabled if the license, *smarts.lic*, is not located in the directory ***BASEDIR*** or the license file name is not exact. (By default, ***BASEDIR*** is */opt/InCharge<n>/<productsuite>* for UNIX and *C:\InCharge<n>\<productsuite>* for Windows.)

- If they exist, previously installed 6.0 patches are displayed in the screen. Make a note of those patches for later evaluation (see *Reconciling Previously Installed Patches* on page 41). Also, a list of the installed patches is saved in a file named *SmartsPatchReport.<x.y.z>.SP0.txt* in the ***BASEDIR/****smarts/setup/info* directory. Click **Next** to continue.

- If there is an NCM service running for the suite, the Services screen appears and **Next** is disabled. Stop the service(s) with the method appropriate for your platform. Then in the Services screen, click **Refresh** and make sure that all NCM services are stopped. Then click **Next** to continue.

  UNIX:

  Stop the sm_serviced, a component of the sm_service utility that manages programs. Stopping the sm_serviced will stop all of the services that were automatically and manually started. The script is stored in a system-specific location: */etc/init.d* on Solaris and Linux; and /sbin/init.d on HP-UX. Issue the command:

  ```
  # <system-dependent path>/ic-serviced stop
  ```

  Windows:

  To stop all services, use the Control Panel Administrative Tools dialog box to start and stop services. You can also issue the command (entered on one line):

  ```
  BASEDIR\smarts\bin\sm_service stop <service_name>
  <service_name> ...]
  ```

  where ***<service_name>*** is the name of the service.

  For information about sm_serviced and general information about the sm_service utility, see the *Network Connectivity Monitor System Administration Guide*.

Using the smgetinfo Utility

The smgetinfo utility stores subdirectories and collects version information in a .tar file or a .zip file. The saved subdirectories are: */conf*, */local*, */rules*, and */setup*.

For all platforms, to collect information about installed products and components, the Perl interpreter (version 5.0 or later) must be installed.

For Windows, to save information, WinZip is required. WinZip is commonly shipped with Windows systems. If WinZip is not installed in its default directory, set the variable ZIPPER to point to WinZip directory.

To run the smgetinfo utility, change to the ***BASEDIR****/smarts/script* directory and execute the following command.

UNIX:

```
./smgetinfo
```

or

```
sh smgetinfo
```

Windows:

```
smgetinfo.cmd
```

6

Installing the IP Management Suite

This chapter describes instructions if you:

- Are installing this product suite or individual products for the first time
- Have an existing 4.1 (4.1.1 or 4.1.2) IP Management installation and are installing the 6.2 IP Management Suite into a different directory
- Have an existing 6.0 IP Management installation and are installing the 6.2 IP Management Suite into a different directory

The basic installation steps are the same for all supported UNIX and Windows platforms.

Installation Steps

This section describes how to install the NCM products.

Note: For Windows, if you have autorun enabled, the installation setup program starts automatically. If autorun is disabled, you need to locate the */suite* directory on the CD-ROM and execute the Setup command as described in Step 4.

Mounting the CD-ROM and Executing Installation Setup

1. Insert the CD-ROM into the CD-ROM drive.
2. For UNIX operating systems, mount the CD-ROM. Follow the mounting instructions for your operating system. For device information, ask your system administrator.

   Solaris:

   If the Volume Manager is running, it automatically mounts the CD-ROM to */cdrom/<**incharge**>* where ***<incharge>*** is the format:

   ```
   <suite>_<productversionNumber>_<buildNumber>
   ```

   For example, ***<incharge>*** can be: IP_6_2_0_6219. The build number might vary.

   If the Volume Manager is not running, use the **mount** command:

   ```
   # mount -o ro -F hsfs DEVICE /mnt
   ```

   where ***DEVICE*** is your CD-ROM. For example,

   ```
   # mount -o ro -F hsfs /dev/dsk/c0t6d0s0 /mnt
   ```

   HP-UX:

   Use the **mount** command:

   ```
   # mount -ocdcase -o ro -F cdfs DEVICE /mnt/cdrom
   ```

   where ***DEVICE*** is your CD-ROM. For example,

   ```
   # mount -ocdcase -o ro -F cdfs /dev/cdrom /mnt/cdrom
   ```

   Linux:

   If the CD-ROM does not automatically mount, use the **mount** command:

   ```
   # mount DEVICE
   ```

   where ***DEVICE*** is your CD-ROM. For example,

   ```
   # mount /dev/cdrom
   ```

3. Change directory to the mounted CD-ROM.

   Solaris:

   ```
   # cd /cdrom/<incharge>/suite
   ```

   where ***<incharge>*** might be: IP_6_2_0_6219.

If the Volume Manager is not running, use this command instead:

```
# cd /mnt/suite
```

HP-UX:

```
# cd /mnt/cdrom/suite
```

Linux:

```
# cd /cdrom/incharge/suite
```

If the automount utility is not running, use this command instead:

```
# cd /mnt/cdrom/suite
```

Windows:

Access the CD-ROM drive from Windows Explorer and locate the */suite* directory.

4 Execute the Setup command and then the Cisco Welcome screen displays:

OPERATING SYSTEM	EXECUTE:
Solaris	`# ./setup-solaris.bin`
HP-UX	`# ./setup-hpux.bin`
AIX	`N/A`
Red Hat Linux	`# ./setup-linux.bin`
Windows	`setup-winnt.exe`

Table 18: **The Setup Commands**

Running the Installation Setup

The installation program presents you with a series of screens. At almost any point in the process, you may return to a previous screen, continue, or cancel the process. All of the products are installed to the local host.

Note: Depending upon your selections, certain steps might not be necessary and corresponding screens might not display.

1 On your system, stop all NCM services, NCM daemon processes, NCM cron jobs, and any other process that uses programs or libraries in *any* NCM installation area. Click **OK** in the Warning dialog box if you have stopped all NCM services.

2 Click **Next** in the Welcome screen to continue.

If you wish to view the requirements check results, click **Get System Information**. The installation setup program performs a requirements check for patches and operating system requirements, except for memory.

Next is disabled if:

- You do not have administrative privileges for the products you are attempting to install. A message also displays.
- Your system failed the requirements check. If this occurs, review the check results by clicking **Get System Information**, cancel the installation setup program, and upgrade your system. See the Requirements chapter.

Note: The installation setup program does not check for the memory requirement for a particular product. If you install a product with less the minimum memory requirement on the host, the program will perform slowly.

3 Accept the Cisco end user license agreement and click **Next**.

4 If the installation program detects an existing installation, the Installation Type screen displays. This screen does not display if you are installing the suite for the first time.

- Select Install, if you wish to retain an existing installation and you wish to install the suite in a different directory on the same host. Later, you will be prompted to specify a different directory.
- Select Upgrade for the installation type if you already have products from this suite installed and you want to install more products into the same directory.

5 Click **Next** to accept the default installation directory or type your preferred directory and click **Next**.

The default installation directory is */opt/InCharge6* (on UNIX) or *C:\InCharge6* (on Windows).

If you specify a directory, be sure to use forward slashes ("/") for both UNIX and Windows directories. Directory names cannot contain spaces. If the specified directory does not exist, it will be created. If you do not have write privileges, an error message displays.

6 In the Setup screen, if you select:

- Complete to install the entire suite, go to Step 8.
- Custom to install specific products, go to Step 7.

7 In the Product Selection screen, click **Next** to install the entire suite of products (by default, all products are selected) or deselect products that you do not wish to install.

Note: If you wish to use the InCharge IP Server Performance Manager, you need to install the InCharge IP Performance Manager.

8 Select the products that you wish to install as services and click **Next**. If a product is not selectable (displays as gray text), click **Back** to return to the Product Selection screen and select the product.

Cisco recommends installing products as services. Refer to the *Network Connectivity Monitor System Administration Guide* for information on managing products installed as services.

9 Choose a location to install the NCM Broker or specify the location of an existing broker. Click **Next** to continue. The default values are: localhost for the host name and 426 for the port number.

Note: If you are installing additional products for the same suite, the Broker Location screen does not display.

For a broker being installed as a service (selected in the previous screen), you can specify a different port number if necessary. The host name value is localhost.

For a broker being installed as a manual process (not selected as a service), you can accept the localhost value or specify another host name.

Or, if you wish to use a broker located on a different host, specify that host name and port number. (To determine the host and port currently configured as the broker location in your installation, execute the **brcontrol** command.)

If your system has an existing broker (InCharge 5.0 or later), click **Next** if you wish to use it. The new broker will not supersede it.

If your system has a pre-5.0 version of the broker running, for migration purposes, a new broker with a different port number can be installed on the same system.

10 Accept the Perl API license agreement and click **Next**.

11 Review the list of products that will be installed and the target installation directory. At the bottom, the total amount of disk space required for the selected products is provided so that you can verify that adequate disk space is available. To install the products, click **Next** and the Installation Progress screen displays.

12 Upon completion, the Installation Summary displays informational messages such as successful confirmations, error messages, and warnings. Click **Finish** to exit the installation. It is not necessary to re-boot the system after installation.

Investigate any errors or warnings. The log file is a text file with the naming convention *Install.<suite>.<productversionNumber>.log*. It is located in the ***BASEDIR****/smarts/setup/logs* directory. If the installation process fails, the log files are located in the */tmp* directory.

13 Unmount the CD-ROM after completing the installation. For more information, refer to *Unmounting the CD-ROM* on page 38.

14 Perform post-installation steps. See the Performing Post-Installation Tasks chapter.

Repeat these steps for all of the hosts in your deployment that require the installation of NCM products.

Unmounting the CD-ROM

The CD-ROM should be unmounted before starting the applications. Be sure that no processes are currently accessing the drive.

UNIX

Type the following commands:

```
# cd /
# umount /mnt/incharge/suite
# eject
```

Windows

Eject the CD-ROM from the machine.

7

Performing Migration Tasks

If you have an existing IP installation, you need to perform migration tasks before performing other post-installation tasks (such as starting products) as described in *Performing Post-Installation Tasks* on page 47.

Migration from an existing IP installation requires that you consider any customizations made in the existing installation. Customizations such as modified configuration files and custom adapters need to be evaluated in order to complete the migration. This chapter describes steps for migrating from:

- 6.0 IP Availability Manager, IP Performance Manager, and Discovery Manager
- 4.1 (4.1.1, or 4.1.2) IP Availability Manager and IP Performance Manager

Migrating From IP Management Suite 6.0

If you have received custom patches for releases earlier than 6.0, contact Cisco TAC for assistance in migrating them.

Migration Tasks

To migrate from 6.0 IP Management, you need to perform the following tasks:

- If necessary, evaluate previously installed patches. See *Reconciling Previously Installed Patches* on page 41.
- Evaluate customizations, including modified configuration files and custom adapters, as described in the *Evaluating Customizations Made in IP Management Suite 6.0* on page 41.
- Configure or combine existing licenses. See the *Network Connectivity Monitor System Administration Guide* for more information.
- Optional, modify the *runcmd_env.sh* file for each suite to set SM_INCOMING_PROTOCOL and SM_OUTGOING_PROTOCOL for encrypted connections. If you do not modify the variables, the result will be clear text communication. For information, see the *Network Connectivity Monitor System Administration Guide*.
- Encrypt existing security configuration files. Use the sm_edit utility to either add the required first line of code for encryption or merge entries from existing security configuration files into the new files located in the */local* directory. Once you have modified the files, the resulting level of encryption is equivalent to the level of default encryption.

  You can configure NCM installations with a variety of levels of security. We highly recommend that you increase your level of security. For information about the required encryption code line or how to increase your level of security, see the *Network Connectivity Monitor System Administration Guide*.
- Encrypt existing seed files. Use the sm_edit utility to add the required first line of code for encryption. For information about encrypting seed files, see the *Network Connectivity Monitor IP Discovery Guide*. For information about the sm_edit utility, see the *Network Connectivity Monitor System Administration Guide*.
- Perform validation tests as described in the *Network Connectivity Monitor IP Deployment Guide*.

Reconciling Previously Installed Patches

If applicable, evaluate any previously installed 6.0 patches which were identified during the installation process. The *Network Connectivity Monitor Release Notes* lists which patches have been incorporated into the 6.2 release. If a given patch has been incorporated into the 6.2 release, this patch can be deleted. If there are patches which are not incorporated into the 6.2 release, contact Cisco TAC. The text file supplied with a given patch also lists the files included in the patch. The text file is located in the ***BASEDIR****/smarts/setup/info* directory.

Note: The installation process identifies only 6.0 or later patches. If you received custom patches for earlier releases of any InCharge product, please contact Cisco TAC for assistance.

Evaluating Customizations Made in IP Management Suite 6.0

Customizations made to the existing 6.0 IP Management installation must be evaluated to determine:

- If they can be used "as is" in the 6.2 IP Management installation
- Or, if modifications are necessary to allow the customizations to be used in the 6.2 IP Management installation

The customized files are located in the ***BASEDIR****/smarts/local* directory and its subdirectories. You need to examine all files in these directories with respect to the 6.2 IP Management installation. Typical files included in the */local* directory are: patches (described earlier), configuration files, and custom adapters.

Note: Remember that ***BASEDIR*** includes the path to the product suite directory which, in this case, is */IP*.

The following sections provide information on user-modifiable files which were shipped with the 6.0 IP Management Suite. Many of these files do not require changes in order to be used with the 6.2 IP Management Suite. If necessary, use the sm_edit utility to make changes to the files. For any customized file that is in the */local* directory but is not listed in the following sections, contact Cisco TAC.

Files That Do Not Require Modifications

Repository files (<*domain_name*>.*rps*) can be copied from a 6.0 IP Management installation to a 6.2 IP Management installation without modifications. (Repository files are located in the ***BASEDIR****/smarts/local/repos/icf* directory.)

The following configuration files can be copied from a 6.0 IP Management installation to a 6.2 IP Management installation without modifications. (Configuration files are located in the ***BASEDIR****/smarts/local/conf* directory.)

- *discovery/discovery.conf*
- *discovery/partition.conf*
- *discovery/user-defined-connections.conf*
- *trapd/trapd.conf*
- *OV/server.conf*
- *NV/server.conf*

The following files can be used "as is", but you might need to modify them due to the security enhancements introduced for NCM 1.1. (These files are located in the ***BASEDIR****/smarts/local/conf* directory.)

- *seedfile*
- *brokerConnect.conf*
- *clientConnect.conf*
- *serverConnect.conf*

For any configuration file that is in the */local/conf* directory but is not listed above, contact Cisco TAC.

Files That Require Modifications

Files containing custom code must be evaluated to determine if any migration steps are needed.

These customized configuration files require modifications. (The files are located in the ***BASEDIR****/smarts/local/conf* directory.) Use the sm_edit utility to copy customizations.

- *discovery/tpmgr-param.conf*
- *discovery/oid2type_Field.conf*

Migrating From IP Applications 4.1, 4.1.1, or 4.1.2

Migration considerations for 4.1, 4.1.1, or 4.1.2 IP products are:

- Saved InCharge 4.1 Consoles, such as the Monitoring Console, are not supported.
- If your system has a 4.1, 4.1.1, or 4.1.2 broker running, a 6.2 broker with a different port number can be installed on the same system.

Migration Tasks

To migrate from 4.1, 4.1.1., or 4.1.2 IP Management, you need to perform the following tasks:

- If you have received custom patches for 4.1 releases of any InCharge product, contact Cisco TAC for assistance.
- Evaluate customizations, including modified configuration files and custom adapters, as described in the *Evaluating Customizations Made in a 4.1 IP Installation* on page 44.
- Migrate 4.1, 4.1.1, or 4.1.2 topology and create ISDN threshold groups if necessary as described in the *Migration Procedure for IP Applications 4.1* on page 45.
- Configure or combine existing licenses. See the *Network Connectivity Monitor System Administration Guide* for more information.
- Optional, modify the *runcmd_env.sh* file for each suite to set SM_INCOMING_PROTOCOL and SM_OUTGOING_PROTOCOL for encrypted connections. If you do not modify the variables, the result will be clear text communication. For information, see the *Network Connectivity Monitor System Administration Guide*.
- Encrypt existing security configuration files. Use the sm_edit utility to either add the required first line of code for encryption or merge entries from existing security configuration files into the new files located in the */local* directory. Once you have modified the files, the resulting level of encryption is equivalent to the level of default encryption.

  You can configure NCM installations with a variety of levels of security. We highly recommend that you increase your level of security. For information about the required encryption code line or how to increase your level of security, see the *Network Connectivity Monitor System Administration Guide*.

- Encrypt existing seed files. Use the sm_edit utility to add the required first line of code for encryption. For information about encrypting seed files, see the *Network Connectivity Monitor IP Discovery Guide*. For information about the sm_edit utility, see the *Network Connectivity Monitor System Administration Guide*.

Evaluating Customizations Made in a 4.1 IP Installation

Customizations made to the existing 4.1, 4.1.1, or 4.1.2 IP installation must be evaluated to determine if modifications are necessary to allow the customizations to be used in the 6.2 IP Management installation.

Note that 4.1 directory structures vary slightly from 6.2 directory structures and do not include a */local* directory for user-modifiable files.

You need to examine all files in the 4.1 directories with respect to the 6.2 IP Management installation. Typical files that might contain customizations are: patches (described earlier), configuration files, and custom adapters.

If necessary, use the sm_edit utility to open 6.2 files and copy the customizations from the corresponding 4.1 files into the 6.2 files. The sm_edit utility ensures that the files are saved to the appropriate */local* directory with the correct permissions. For information about the sm_edit utility, see the *Network Connectivity Monitor System Administration Guide*.

Files That Do Not Require Modifications

The following configuration files can be copied from a 4.1 IP Management installation to a 6.2 IP Management installation without modifications. (Configuration files are located in the ***BASEDIR****/smarts/conf* directory.)

- *discovery/user-defined-connections.conf*

Files That Require Modifications

Files containing custom code must be evaluated to determine if any migration steps are needed.

Repository files (<*domain_name*>.*rps*) need to be evaluated and might require modifications. (Repository files are located in the ***BASEDIR****/smarts/repos/icf* directory.)

These customized configuration files require modifications. (The files are located in the ***BASEDIR****/smarts/conf* directory.) Use the sm_edit utility to copy customizations.

- *discovery/discovery.conf*
- *discovery/partition.conf*

- *discovery/tpmgr-param.conf*
- *discovery/oid2type_Field.conf*
- *trapd/trapd.conf*
- *icf/DEVSTAT.import*
- *icf/bootstrap.conf*
- *OV/server.conf*
- *NV/server.conf*

The following files can be used “as is”, but you might choose to modify them due to the security enhancements introduced for 6.2 InCharge. (These files are located in the ***BASEDIR****/smarts/conf* directory.)

- *seedfile*
- *clientConnect.conf*
- *serverConnect.conf*

Migration Procedure for IP Applications 4.1

Perform the following procedure to migrate 4.1, 4.1.1, or 4.1.2 topology and create ISDN threshold groups if necessary:

1. Examine files for custom modifications as described in *Evaluating Customizations Made in a 4.1 IP Installation* on page 44.
2. For IP Availability Manager and IP Performance Manager, make sure the Domain Manager’s repository file is located in the 6.2 directory ***BASEDIR****/smarts/local/repos/icf* and that it contains any necessary 4.1 customizations.

   The name of the repository file is based on the name of the Domain Manager. For example, if the Domain Manager’s name is NCM-AM, the repository file is named NCM-AM.*rps*.
3. Start the 6.2 Domain Manager for IP Availability Manager, IP Performance Manager, or Discovery Manager with the **sm_service** command. Be sure to verify that the Domain Manager was registered properly with **sm_service**, and that the command-line option of `--ignore-restore-errors` is used by the Domain Manager when it starts. When the 6.2 Domain Manager is started, the topology from the repository file is automatically loaded. For information starting and stopping services and on verifying proper registration with **sm_service**, refer to the *Network Connectivity Monitor System Administration Guide*.

4 If you manage ISDN elements, create ISDN threshold groups in your topology by executing the script *upgradeISDN4xTo60.asl*. The script resides in the ***BASEDIR****/smarts/rules/utils* directory. It creates the following thresholds groups for InCharge 6.0: ISDN Physical Interface, ISDN B Channel, and ISDN D Channel.

Execute the command to create the groups (enter the following on one line):

```
BASEDIR/smarts/rules/utils/sm_adapter -s
<6.2_domain_manager> upgradeISDN4xTo60.asl
```

Note: This command must be typed on one line.

ISDN members appear in the groups after the Domain Manager rediscovers its topology.

5 Perform validation tests as described in the *Network Connectivity Monitor IP Deployment Guide*.

8

Performing Post-Installation Tasks

This chapter explains tasks that you might want to perform after installation. The tasks are intended for all IP Management installation scenarios. They are:

- Start products or components (for example, the broker or Domain Manager) as services.
- Verify product status
- If adapters for these third-party applications are installed, restarting HP OpenView NNM and IBM/Tivoli NetView
- Start the Global Console

Starting NCM Products

Note: If you are migrating from a previous version of InCharge, read *Performing Migration Tasks* on page 39 before starting any products.

If you installed the products (or components) as services, you need to start them for the first time. We recommend installing products as services.

NCM programs installed as services start automatically upon system reboot; those not installed as services (manual processes or disabled processes) require that you issue commands to start and stop them as necessary.

Use the method appropriate for your platform.

Starting Services on UNIX

Start the sm_serviced process to restart the services. Issue the command:

```
# <system-dependent path>/ic-serviced start
```

The script is stored in a system-specific location: */etc/init.d* on Solaris and Linux; and */sbin/init.d* on HP-UX.

Starting Services on Windows

To restart all of the services, reboot your system.

Starting Individual Services

To start or stop a service manually, use the sm_service utility. Issue the command:

```
sm_service start <service_name> [<service_name> ...]
```

For example, to start a service for the CNCC NCM IP Availability Manager product, issue:

```
# BASEDIR/smarts/bin/sm_service start ic-am-server
```

To start the service for the DFM component of CiscoWorks LMS, issue:

```
# BASEDIR/smarts/bin/sm_service start ic-dfm-adapter
```

To start the services for the DFM and VHM components of CiscoWorks ITEM, issue two commands:

```
# BASEDIR/smarts/bin/sm_service start ic-dfm-adapter
```

```
# BASEDIR/smarts/bin/sm_service start ic-vhm-adapter
```

For products that are not installed as services, you need to install them either as services (`--startmode=runonce`) or manual processes (`--startmode=manual`) with **sm_service**, and start them as needed with the **sm_service start** command.

For information about starting services, refer to the *Network Connectivity Monitor System Administration Guide*.

Verifying the NCM Product Status

You can determine the current state of the Broker, Global Managers, and Domain Managers by issuing the following command:

```
# BASEDIR/smarts/bin/brcontrol
```

This command displays a list of Managers registered with the broker, their states (RUNNING, DEAD, UNKNOWN), process IDs, port numbers, and the last time their states changed.

Verifying the NCM Version Number

To verify the version number of your NCM products, issue the following command:

```
# BASEDIR/smarts/bin/sm_server --version
```

The platform version number should say V6.2 (There may be some additional identification numbers included after the version number). For example, the output might look like:

```
sm_server.exe: V6.2(43968), 08-Mar-2004 12:25:47 - Build 6219
Copyright (C) 1995-2004, System Management ARTS Inc.
```

You can also verify that the version number is correct for the suite product(s) by running the following script:

```
# BASEDIR/smarts/script/ic-products.pl
```

For example, this partial script output is for the CNCC NCM IP Management Suite:

```
Installed in C:/InCharge6/IP

PACKAGE                          6.2
C:/InCharge6/IP                  1=ICIP_OV-pkg
-------------------------------------------
PACKAGE                          6.2
C:/InCharge6/IP                  1=ICIP_PM-pkg
-------------------------------------------
PACKAGE                          6.2
C:/InCharge6/IP                  1=ICIP_CORE-pkg
-------------------------------------------
Adapter for HP OpenView NNM      6.2
C:/InChargeTest6/IP              1=ICIP_OV
-------------------------------------------
PACKAGE                          6.2
C:/InCharge6/IP                  1=ICIP_NV-pkg
-------------------------------------------
```

```
Availability Manager          6.2
C:/InCharge6/IP               1=ICIP_AM
```

HP OpenView and IBM/Tivoli NetView

If you installed the CNCC NCM Adapter for HP OpenView NNM or the CNCC NCM Adapter for IBM/Tivoli NetView, prior to using the adapters, you should do one of the following:

- Stop and restart OpenView or NetView.
- If OpenView or NetView was running during the installation, start the adapters by issuing the following command:

  OpenView:

  ```
  \opt\OV\bin\ovstart
  ```

  NetView:

  ```
  \usr\OV\bin\ovstart
  ```

For more information about adapters for OpenView or NetView, refer to the *InCharge IP Adapters User's Guide*.

Starting the Global Console

Start the Global Console after you have installed the CNCC NCM IP Management Suite. To start the console, select it from the Start Menu or use the **sm_gui** command:

```
# BASEDIR/smarts/bin/sm_gui
```

The Global Console must be installed from the CNCC NCM SAM CD-ROM. For console installation instructions, see the *Network Connectivity Monitor Service Assurance Management Suite Installation Guide*. For information about using the Global Console, see the *Network Connectivity Monitor Operator's Guide*.

9

Uninstalling the IP Management Suite

This chapter describes instructions for uninstalling this product suite or individual products. The uninstall process (**uninstaller** command) removes selected products or an entire suite using the same interactive program as the install procedure. After uninstalling, your customized files remain saved in ***BASEDIR****/smarts/local*. For Windows, you can also use Add/Remove Programs from the Control Panel to uninstall a suite.

WARNING: NCM uses standard install software to install and uninstall product suites. You must use either the **uninstaller** command or, for Windows, Add/Remove Programs to uninstall NCM software. Failure to use either method will result in an unstable system and/or inconsistent product directories. Do not manually delete the installed product directories.

WARNING: Before you uninstall an NCM product, you should stop all NCM processes, consoles, and any adapters that interface with it.

WARNING: For UNIX only, for a complete uninstallation, if you intend to uninstall multiple suites from the same host, the last suite you should uninstall is the suite you installed first. During the installation of the first suite, the Service Database is also installed and the other suites subsequently access it. Uninstalling the Service Database prior to uninstalling other suites will disable the **sm_service** command for those products and interrupt products running as services. To identify which suite was installed first, examine the directory path listed in the init.d table. The Service Database resides in the */var/smarts* directory.

Uninstallation Steps

This section describes how to uninstall a suite or individual products.

Stopping NCM Services

We recommend that you stop the NCM services that are running (including the FLEXlm License Server) for the suite. For more information on stopping NCM services, refer to the *Network Connectivity Monitor System Administration Guide*.

Note: For UNIX only, before uninstalling suites or individual products, check that the status of the sm_serviced process is running with the **ic_serviced status** command. The sm_serviced process must be running for uninstallation. If the process is not running, use the **ic_serviced start** command to start it. These commands are described in the *Network Connectivity Monitor System Administration Guide*.

Uninstalling the FLEXlm Server

When uninstalling your NCM products, you must also uninstall the FLEXlm License Server from your system. The FLEXlm License Server runs as a daemon on UNIX and as a service on Windows. These automatically start the license server. If you uninstall NCM products without uninstalling the FLEXlm License Server, a message displays that the FLEXlm (lmgrd) service is still running. Keep in mind that an NCM application will not start if it is unable to contact the license server.

To stop and uninstall the FLEXlm License Server, execute the *install_license* script with the **uninstall** command from the ***BASEDIR****/smarts/script* directory.

UNIX

```
# BASEDIR/smarts/script/install_license.sh uninstall
```

Windows

```
BASEDIR\smarts\script\install_license.cmd uninstall
```

Uninstalling From the Control Panel (Windows Only)

Note: If you installed the same suite in two or more directories on your system, do not use Add/Remove Programs; use the **uninstaller** command instead. Add/Remove Programs does not support multiple instances of the same suite.

To use the Windows Control Panel to uninstall a product suite, perform these steps:

1. Click *Start* > *Settings* > *Control Panel*
2. Double-click **Add/Remove Programs**
3. From the Add/Remove Programs window, select the appropriate service for your product suite.
4. Click **Change/Remove**.

Running the Uninstallation Program

You can uninstall a suite or individual products from the local host.

1. Execute the **uninstaller.bin** command for UNIX or the **uninstaller.exe** command for Windows. For example:

   ```
   BASEDIR/_uninst/uninstaller.bin
   ```

2. Click **Next** in the Welcome screen to continue.
3. In the Product Selection screen, click **Next** to uninstall the entire suite of products (by default, all products are selected) or deselect products that should remain installed.
4. Review the list of products that will be uninstalled and the target installation directory. Once you click **Next**, you cannot cancel the uninstallation process.

   If necessary, click **Back** to return to the Product Selection screen to revise your selections.

   To uninstall the products, click **Next** and the Uninstallation Progress screen displays.

5 Upon completion, the Uninstallation Summary displays informational messages such as successful confirmations, error messages, and warnings. If **Next** displays, your system needs to be rebooted. Click it and then reboot your system. Otherwise, click **Finish** to exit the uninstallation.

The log file is a text file with the naming convention *Uninstall.<suite>.<productversionNumber>.log*. It is located in the ***BASEDIR****/smarts/setup/logs* directory. If the uninstallation process fails, the log files are located in the */tmp* directory.

6 Examine any remaining directories if you plan to re-install NCM and save customized files located in the */local* directory. Depending upon the suite, some or all of the following subdirectories will remain in the ***BASEDIR****/smarts* directory after uninstallation, because they contain user-modified files:

- */classes*
- */local*
- */bin*
- */setup*

A

Installing the IP Management Suite Using CLI Mode

This appendix briefly describes how to install and uninstall the CNCC NCM IP Management Suite using the Command Line Interface (CLI) mode.

Cisco provides this text-mode alternative to the InstallShield Wizard method for UNIX users.

CLI-mode installation offers the following advantages: X display, fixed ports to permit communication through firewalls, and special access to production systems are not required.

The process flow for CLI-mode is identical to that of the InstallShield Wizard:

- To install, satisfy previously-described requirements, stop the NCM services for the suite, and, afterwards, perform migration and post-installation tasks, if applicable.
- To uninstall, stop NCM services, including the service for the FLEXlm License Server.

The log files are located in the ***BASEDIR****/smarts/setup/logs* directory. If the installation process fails, the log files are located in the */tmp* directory.

User selections and the navigation method for CLI-mode are described in a subsequent section.

Running the CLI-Mode Installation

To start the CLI-Mode installation program, execute the **Setup** command with the `-console` option. The syntax is:

`<`***`setup-executable`***`> -console`

where ***<setup-executable>*** is one of the following:

OPERATING SYSTEM	EXECUTABLE
Solaris	`setup-solaris.bin`
HP-UX	`setup-hpux.bin`
AIX	`N/A`
Red Hat Linux	`setup-linux.bin`

Table 19: **The Setup Commands**

For example, to start the CLI-Mode installation on Solaris, execute:

```
# ./setup-solaris.bin -console
```

Running the CLI-Mode Uninstallation

To uninstall a product suite or individual products using CLI-Mode, execute the **uninstaller.bin** command with the `-console` option. The syntax is:

`BASEDIR``/_uninst/uninstaller.bin -console`

User Selections and Navigation

During the installation and uninstallation processes, you are prompted with a series of steps and menus. You can either accept the default value or select another choice.

Default Values

The default values are indicated in brackets or as pre-defined selections (check marks) in menus. To accept the default value, press **Enter**.

Replying to Prompts

When replying to a prompt, you can either accept the default value or select another choice. To reply “yes,” enter y or Y; to reply “no,” enter n or N. Do not press **Delete**; this causes the process to terminate with an error message.

Menu Selections

For selections in menus, you can accept default selections or type the number of the item and press **Enter**. A check mark (X) displays next to the item. When you are finished making selections, type zero (0) and press **Enter**.

If you incorrectly type an entry, press **4** to repeat the prompt and select the correct value. Arrow keys and the Backspace key are not supported.

Navigation Method

To navigate between the steps, use the following keys:

KEY	FUNCTION
1	Next, continue to the next step
2	Previous, go back to the previous step
3	Cancel, terminates the program
4	Redisplay, repeats the step

B

Unattended Installation for the IP Management Suite

This appendix briefly describes how to install and uninstall the CNCC NCM IP Management Suite using command line options from a user-modifiable file.

Unattended installation, an alternative to the InstallShield Wizard method, is available for all supported platforms.

Unattended installation offers the following advantages: It is useful for performing multiple installations in a large deployment and, for UNIX users, the X protocol is not required. NCM installations are typically performed using the InstallShield Wizard, but some organizations have security-based policies for UNIX users that prohibit the transmission of the X protocol.

For an unattended installation, you need to:

- For an installation, modify a response file as described in *About Response Files* on page 60. You also need to satisfy previously-described requirements, stop the NCM services for the suite, and, afterwards, perform migration and post-installation tasks, if applicable.
- For an uninstallation, stop NCM services including the service for the FLEXlm License Server.

The log files are located in the ***BASEDIR****/smarts/setup/logs* directory. If the installation process fails, the log files are located in the */tmp* directory. A non-zero status indicates a failure.

Running the Unattended Installation

To start an unattended installation, execute the **Setup** command with the `-options` option and a fully-qualified directory path for the response file. The command can only be invoked from the command-line environment. The syntax is:

`<`***`setup-executable`***`> -options <path>/<suite-response.txt>`

where ***<setup-executable>*** is one of the following:

OPERATING SYSTEM	EXECUTABLE:
Solaris	`setup-solaris.bin`
HP-UX	`setup-hpux.bin`
AIX	`N/A`
Red Hat Linux	`setup-linux.bin`
Windows	`setup-winnt.exe`

Table 20: **The Setup Commands**

For example, to start the unattended installation on Solaris for the IP Management Suite, execute:

```
# ./setup-solaris.bin -options /home/IP_SUITE-response.txt
```

Running the Unattended Uninstallation

To uninstall all of the products for a suite using the unattended uninstallation, execute the **uninstaller.bin** command with the `-silent` option. The syntax is:

```
BASEDIR/_uninst/uninstaller.bin -silent -G
replaceNewerResponse="Yes to All"
```

Note: The command must be typed as one line.

About Response Files

Each suite has a response file located on the CD-ROM in the */utils* directory. Its naming convention is *<suite>-response.txt*.

The response file provides instructions and examples of command line options that are passed to the unattended installation program. The command line options are organized by process flow. For example, there are sections for product selection and services. The process flow is almost identical to that of the InstallShield Wizard.

Before you execute the unattended installation program, you need to:

1. Copy the response file to the */tmp* directory on your system.
2. Modify the values for the command line options to select the products and services you wish to install and to ensure that the values reflect your environment. User input must be acceptable values and fully-qualified directory paths.