Integration Guide for Network Connectivity Monitor

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-6303-01

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 guide describes Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM) and provides instructions to integrate NCM with CiscoWorks LAN Management Solution (LMS) and IP Telephony Environment Monitor (ITEM).

Audience

This guide is intended to be read by anyone responsible for integrating NCM.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font

Item	Convention
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Supplement Read Me First for Cisco Network Connectivity Center	• Printed document that was included with the product. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/cncc1_0/ncm_rmf.htm
Release Notes for Network Connectivity Monitor 1.1	• Printed document that was included with the product. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ncm11_rn.htm

Table 1 Product Documentation (continued)

Document Title	Available Formats
Integration Guide for Network Connectivity Monitor	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ncm_int.pdf
FLEXlm End Users Guide Version 9.2	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/enduser.pdf
GNU General Public License	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/gpl_ncm.pdf
InCharge Common Information Model Version 1.3 Wall Chart	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/icim.pdf
Cisco Network Connectivity Center Perl Reference Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/perl_ref.pdf
Network Connectivity Monitor Read Me First April 2004	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/rmf_ncm.pdf
Network Connectivity Monitor Documentation Roadmap April 2004	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ncm_rdmp.pdf

Table 1 Product Documentation (continued)

Document Title	Available Formats
Network Connectivity Monitor System Administration Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ncm_sys.pdf
ICIM Reference	HTML on the product CD-ROM.
Network Connectivity Monitor IP Availability Manager User's Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ipavail.pdf
Network Connectivity Monitor IP Deployment Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ip_depl.pdf
Network Connectivity Monitor IP Discovery Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ipdisco.pdf
Network Connectivity Monitor IP Management Suite Installation Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ipinst.pdf
Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/adp_plat.pdf
Network Connectivity Monitor Service Assurance Management Suite Installation Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/sa_inst.pdf

Table 1 Product Documentation (continued)

Document Title	Available Formats
Network Connectivity Monitor Service Assurance Manager Notification Adapters User's Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/sa_notif.pdf
Network Connectivity Monitor Operator's Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/ncm_op.pdf
An Introduction to Network Connectivity Monitor Service Assurance Manager	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/sa_intro.pdf
Network Connectivity Monitor Service Assurance Manager Configuration Guide	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm1_1/config.pdf
Supported Devices for Network Connectivity Monitor 1.1	On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cncc/ncm/ncm11dev.htm

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

Overview of Network Connectivity Monitor

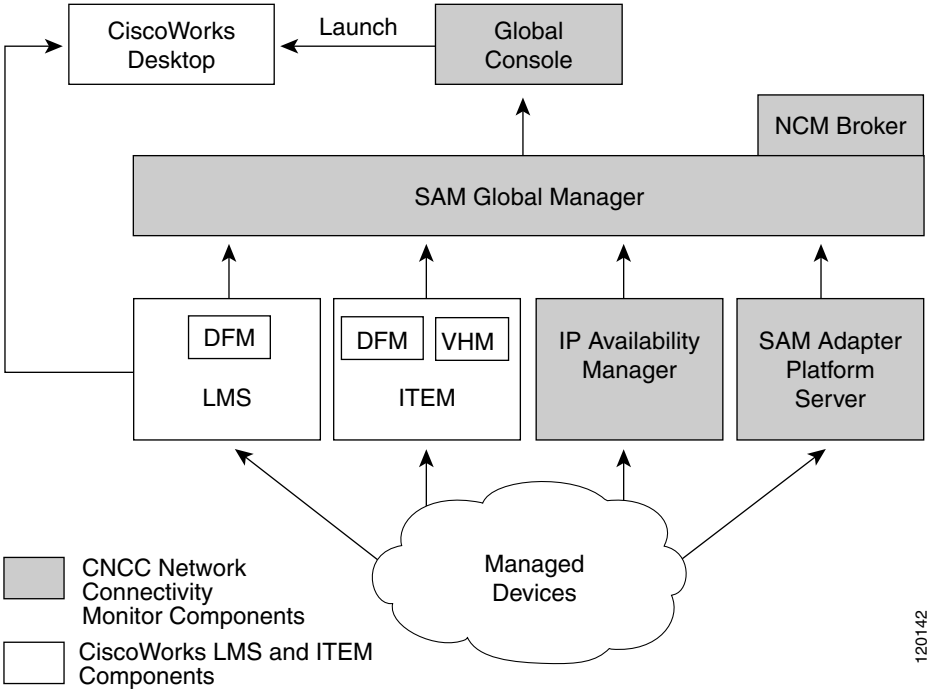
This chapter provides a brief overview of Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM). See the following topics:

Network Connectivity Monitor

NCM adds network connectivity analysis to the CNCC product family by combining the CNCC NCM IP Availability Manager (Availability Manager) and CNCC NCM Service Assurance Manager (Service Assurance Manager). NCM integrates with CiscoWorks LAN Management Solution (LMS) and/or CiscoWorks IP Telephony Environment Monitor (ITEM) to analyze and consolidate information from devices, and in real time, pinpoint device and connectivity failures in the network infrastructure.

Figure 1-1 illustrates the basic architecture and process flow of NCM when integrated with LMS and ITEM.

Figure 1-1 Network Connectivity Monitor Architecture and Process Flow



Note In Figure 1-1, LMS and ITEM reside on separate hosts.

CNCC NCM can be integrated with:

- One ITEM product suite
- One or more LMS products
- A combination of ITEM and LMS

These types of deployments are discussed in Chapter 3, "Deployment Scenarios."

CNCC Network Connectivity Monitor Components

NCM consists of two product suites:

- **CNCC NCM Service Assurance Management Suite**—A full-featured, open solution for managing multiple network infrastructure domains that support services and your business.
- **CNCC NCM IP Availability Management Suite**—A solution that automates real-time root-cause analysis of network faults and provides extensive impact analysis.

The following list describes the components that are used during the integration process:

- **CNCC NCM SAM Global Manager**—A component that serves as a central point for monitoring and managing your entire technology infrastructure by obtaining data from multiple distributed domains. The SAM Global Manager consolidates the information from underlying sources and displays notifications in its client applications, CNCC NCM Global Consoles.
- **NCM Broker**—A component that facilitates communication between the SAM Global Manager and the underlying domains such as CNCC NCM IP Availability Manager and CNCC NCM SAM Adapter Platform server.
- **CNCC NCM Global Console**—The graphical interface for all NCM products. The console enables operators to monitor the state of the managed environment and quickly respond to notifications. Administrators with appropriate privileges and access control can use the CNCC NCM Global Console to discover NCM topology and administer underlying domains, as well as administer NCM users, user profiles, program tools, and escalation policies. The CNCC NCM Global Console is typically installed on many hosts.
- **CNCC NCM SAM Adapter Platform Server**—A component that imports traps from elements in the network infrastructure, processes the traps, and transfers the information to the SAM Global Manager.
- **CNCC NCM SNMP Trap Adapter**—A component that collects and parses SNMP traps.
- **CNCC NCM IP Availability Manager (AM)**—A component that diagnoses connectivity failures, including analysis of root causes, in IP networks.

- **CNCC NCM Adapter for CiscoWorks LMS and ITEM (LMS/ITEM Adapter)**—A component that imports topology from LMS and ITEM to the CNCC NCM IP Availability Manager.
- **CNCC NCM Adapter for HP OpenView Network Node Manager** (HP OpenView NNM)—A component that imports topology and traps from HP OpenView NNM to the CNCC NCM IP Availability Manager.
- **CNCC NCM Adapter for IBM/Tivoli NetView**—A component that imports topology and traps from IBM/Tivoli NetView to the CNCC NCM IP Availability Manager.

Cisco Products that Integrate With Network Connectivity Monitor

NCM integrates with the following Cisco product suites or bundled products:

- CiscoWorks LAN Management Solution (LMS)—A solution that provides a robust set of applications for maintaining, monitoring, and troubleshooting Cisco Campus networks. One of its components is CiscoWorks Device Fault Monitor (DFM).
- CiscoWorks IP Telephony Environment Monitor (ITEM)—A suite of applications and tools that continuously evaluates and reports on the operational health of your Cisco IP telephony implementation. The suite consists of DFM, CiscoWorks Voice Health Monitor (VHM), and other Cisco applications.

In this guide, the instructions pertain to only the DFM and VHM components of LMS and ITEM.

Overview of Integration Tasks

This guide assumes that the products you want to integrate (NCM, LMS, and ITEM) and their components are properly installed, configured, and operational. For information, please refer to the installation and configuration documentation that accompanied the product.

The following list provides an overview of the tasks you must perform to integrate NCM:

1. Determine the deployment scenario you want to implement. See Chapter 3, "Deployment Scenarios."
2. Determine whether your system meets the hardware and software requirements for NCM and review the general integration considerations. See Chapter 2, "Integration Prerequisites."
3. Integrate NCM with LMS and/or ITEM.
   a. For multiple LMS installations only, you need an LMS/ITEM Adapter for each DFM. See the "Configuring the LMS/ITEM Adapter" section on page 4-2 for information.
   b. Optionally, configure the CNCC NCM Adapter for HP OpenView NNM and CNCC NCM Adapter for IBM/Tivoli NetView. See the "(Optional) Configuring the CNCC NCM Adapters for HP OpenView NNM and IBM/Tivoli NetView" section on page 4-2 for information.
   c. Edit the appropriate sections of the *ics.conf* file to reflect underlying domains. See the "Configuring Underlying Domains" section on page 4-4 for information.
   d. Configure a tool to invoke the CiscoWorks Desktop from the NCM Global Console. See the "Configuring the CiscoWorks Client Tool" section on page 4-8 for information.
   e. Configure the CNCC NCM SNMP Trap Adapter for the CNCC NCM SAM Adapter Platform server to receive traps. See the "Configuring the CNCC NCM SNMP Trap Adapter" section on page 4-10 for information.
   f. Configure the NCM Broker as a secure broker. See the "Configuring the Secure Broker" section on page 4-15 for information.
   g. Perform the necessary changes in the configurations of LMS. See the "LMS Integration Steps" section on page 4-16 for information.
   h. Perform the necessary changes in the configurations of ITEM. See the "ITEM Integration Steps" section on page 4-19 for information.
4. Ensure that the integrated components operate properly. See Chapter 5, "Validating Your Integration," for information.

Integration Prerequisites

This chapter describes the prerequisites for the integration of CNCC Network Connectivity Monitor (NCM) with the following Cisco products:

- CiscoWorks LAN Management Solution (LMS)
- CiscoWorks IP Telephony Environment Monitor (ITEM)

The chapter includes the following topics:

For installation prerequisites and specific product requirements, see the appropriate installation guide for detailed information.

Privileges Requirement

If you are integrating NCM with LMS and/or ITEM, you must have superuser or administrator access to NCM components and CiscoWorks applications.

Supported Product Versions

The following identifies the supported versions of NCM 1.1 and CiscoWorks products.

Network Connectivity Monitor

NCM 1.1 requires the following:

- CNCC NCM Service Assurance Management Suite version 1.1 CD-ROM (Disk 1)
- CNCC NCM IP Management Suite version 1.1 CD-ROM (Disk 2)

CiscoWorks LAN Management Solution

If you are integrating NCM with LMS, LAN Management Solution 2.1 or later is required.

CiscoWorks IP Telephony Environment Monitor

If you are integrating NCM with IP Telephony Environment Monitor (ITEM), one of the following is required:

- IP Telephony Environment Monitor 2.0 with the latest IDU.
- IP Telephony Environment Monitor 1.4.

General Integration Considerations

The following list highlights the general points to consider before and during the integration:

- This guide assumes that the products you want to integrate (NCM, LMS, and ITEM) and their components are properly installed, configured, and operational. For information, please refer to the installation and configuration documentation that accompanied the product.
- The products that you wish to integrate (NCM, LMS, and ITEM) and their components must use the NCM Broker. This broker is installed with NCM and is later configured as a secure broker. A secure broker enforces username/password pairs for users to log in with.
- Passwords and privileges are assigned to the various components of NCM. Passwords and privileges are required when the system is configured.
- You must have superuser or administrator access to NCM components and CiscoWorks applications.
- NCM must be installed on a host that does not have any other CiscoWorks applications installed. This is necessary to avoid potential conflicts in services, ports, and environment variables.
- Running NCM 1.0 and NCM 1.1 simultaneously on the same machine is not supported. Unpredictable results may occur.
- NCM supports the integration of multiple instances of LMS.
- NCM supports the integration of one instance of ITEM.
- You have the IP addresses of the LMS and/or ITEM machines.
- You have the IP address or DNS name of the NCM machine.
- You have CiscoWorks access to the CiscoWorks Desktop to change the trap configuration.

Standard Software Directories

This guide assumes NCM and CiscoWorks products are installed in the following standard locations. All references to files and executables are relative to these specified locations.

Location of CiscoWorks Software

It is assumed that CiscoWorks products (LMS or ITEM) are installed in a standard location specified as *NMSROOT/CSCOpx*, where *NMSROOT* is */opt* for Solaris and *C:\Program Files* for Windows. All references to files and executables are relative to these locations. When executable commands are mentioned, it is assumed that *NMSROOT/CSCOpx/bin* is present in the PATH environment variable.

Location of NCM Software

It is assumed that CNCC NCM IP Availability Manager and CNCC NCM Service Assurance Manager are installed in a standard location specified as *BASEDIR/smarts*, where *BASEDIR* is */opt/InCharge6/<productsuite>* by default on Solaris and *C:\InCharge6\<productsuite>* by default on Windows. For example on Solaris, CNCC NCM IP Availability Manager and CNCC NCM Service Assurance Manager are installed in */opt/InCharge6/IP/smarts* and */opt/InCharge6/SAM/smarts*, respectively.

Deployment Scenarios

This chapter describes several deployment scenarios for CNCC Network Connectivity Monitor (NCM). The scenarios are described in the following topics:

After you have decided on the deployment scenario you want to implement, see Chapter 2, "Integration Prerequisites," for information on hardware and software requirements.

Note the following deployment constraints:

- For ITEM 2.0, the DFM and VHM components must reside on the same machine.
- For ITEM 1.4, the DFM and VHM components can reside on the same machine or on separate machines.
- NCM must be installed on a host that does not have any CiscoWorks applications installed.
- Running NCM 1.0 and NCM 1.1 simultaneously on the same machine is not supported. Unpredictable results may occur.

Network Connectivity Monitor with LMS

NCM can be integrated with the CiscoWorks LAN Management Solution (LMS). Integration requires the configuration of NCM and LMS components.

The following summarizes the flow of information among the components:

- CNCC NCM IP Availability Manager uses the CNCC NCM Adapter for CiscoWorks LMS and ITEM to import topology information from the DFM component of LMS, and to synchronize its topology with LMS on a regular basis. The adapter is installed as a service named CNCC NCM DFM Topology Synchronization Adapter.
- CNCC NCM IP Availability Manager maintains communications with the devices managed by LMS, and performs root-cause analysis of device and connectivity failures.
- The DFM Trap Forwarder collects pass-through traps from the devices within the managed infrastructure, and passes the traps to LMS and the CNCC NCM SNMP Trap Adapter. The Trap Adapter forwards them to the IP Availability Manager for analysis and to the SAM Adapter Platform server for posting to the SAM Global Manager.

Note DFM collects and processes two types of traps: Analysis traps and pass-through traps. Analysis traps are used for root-cause analysis by NCM. Pass-through traps (such as linkUp/linkDown traps) are not used for the analysis of faults, but are passed on and displayed in the console to reflect certain conditions within a device (such as a loss of optical signal). Such conditions complement the analysis information.

- The SAM Global Manager imports topology information from the IP Availability Manager and the SAM Adapter Platform server, and synchronizes the information with that of the IP Availability Manager.
- The SAM Global Manager imports and consolidates event information from the IP Availability Manager, LMS, and the SAM Adapter Platform server, and displays event notifications on the Global Console(s).
- In addition to the automated corrective actions available in NCM, the CiscoWorks Desktop, used for the LMS products, can be launched from the Global Console.

In this scenario, NCM includes the CNCC NCM Adapter for CiscoWorks LMS and ITEM to seed the initial IP Availability Manager topology from LMS. The adapter provides the following functionality:

- Initial topology import of all managed devices, including managed devices not supporting SNMP.
- Periodic topology synchronization to import managed devices discovered by the DFM component of LMS since the last import. The topology synchronization is event-driven and will occur within a short period after new devices are added to LMS.

Note Any device deleted from the LMS topology is not automatically deleted from the NCM topology. It must be manually removed from the NCM topology by way of the NCM Domain Manager Administration Console or the command-line tools. If it is not manually removed, IP Availability Manager will continue to provide diagnostics for the device until it is removed from the underlying repository. For information about removing systems from the topology, see the *Network Connectivity Monitor IP Discovery Guide*.

Note CNCC NCM IP Availability Manager supports autodiscovery of all certified devices. This functionality is disabled by default. If NCM is integrated with LMS, autodiscovery must remain disabled to avoid name resolution conflicts.

CNCC NCM IP Availability Manager provides full support for certified Cisco devices and other non-Cisco devices. A noncertified device will be discovered but managed as a generic Node for connectivity analysis only.

CNCC NCM IP Availability Manager and LMS must be configured to use the NCM Broker.

Direct communication between the SAM Global Manager and the underlying domains is controlled by data exchange (dxa) files. The event information that is transferred is consolidated with the information from CNCC NCM IP Availability Manager.

In this scenario, the login page of CiscoWorks Desktop, used with LMS, can be launched from the Global Console. To enable this function, the name and address of the CiscoWorks server must be set up for the client tool that is available from the Global Console.

Network Connectivity Monitor with ITEM

NCM can be integrated with the CiscoWorks IP Telephony Environment Monitor (ITEM). Integration requires the configuration of NCM and ITEM components.

The following summarizes the flow of information among the components (see Figure 3-1):

- CNCC NCM IP Availability Manager uses the CNCC NCM Adapter for CiscoWorks LMS and ITEM to import topology information from the DFM and VHM components of ITEM, and to synchronize its topology with ITEM on a regular basis. The adapter is installed as two services, the CNCC NCM DFM Topology Synchronization Adapter and the CNCC NCM VHM Topology Synchronization Adapter.
- CNCC NCM IP Availability Manager maintains communications with the devices managed by ITEM, and performs root-cause analysis of device and connectivity failures.
- The DFM Trap Forwarder collects pass-through traps from the devices within the managed infrastructure, and passes the traps to ITEM and the NCM SNMP Trap Adapter. The Trap Adapter forwards them to the IP Availability Manager for analysis and to the SAM Adapter Platform server for posting to the SAM Global Manager.

Note DFM collects and processes two types of traps: Analysis traps and pass-through traps. Analysis traps are used for root-cause analysis by NCM. Pass-through traps (such as linkUp/linkDown traps) are not used for the analysis of faults, but are passed on and displayed in the console to reflect certain conditions within a device (such as a loss of optical signal). Such conditions complement the analysis information.

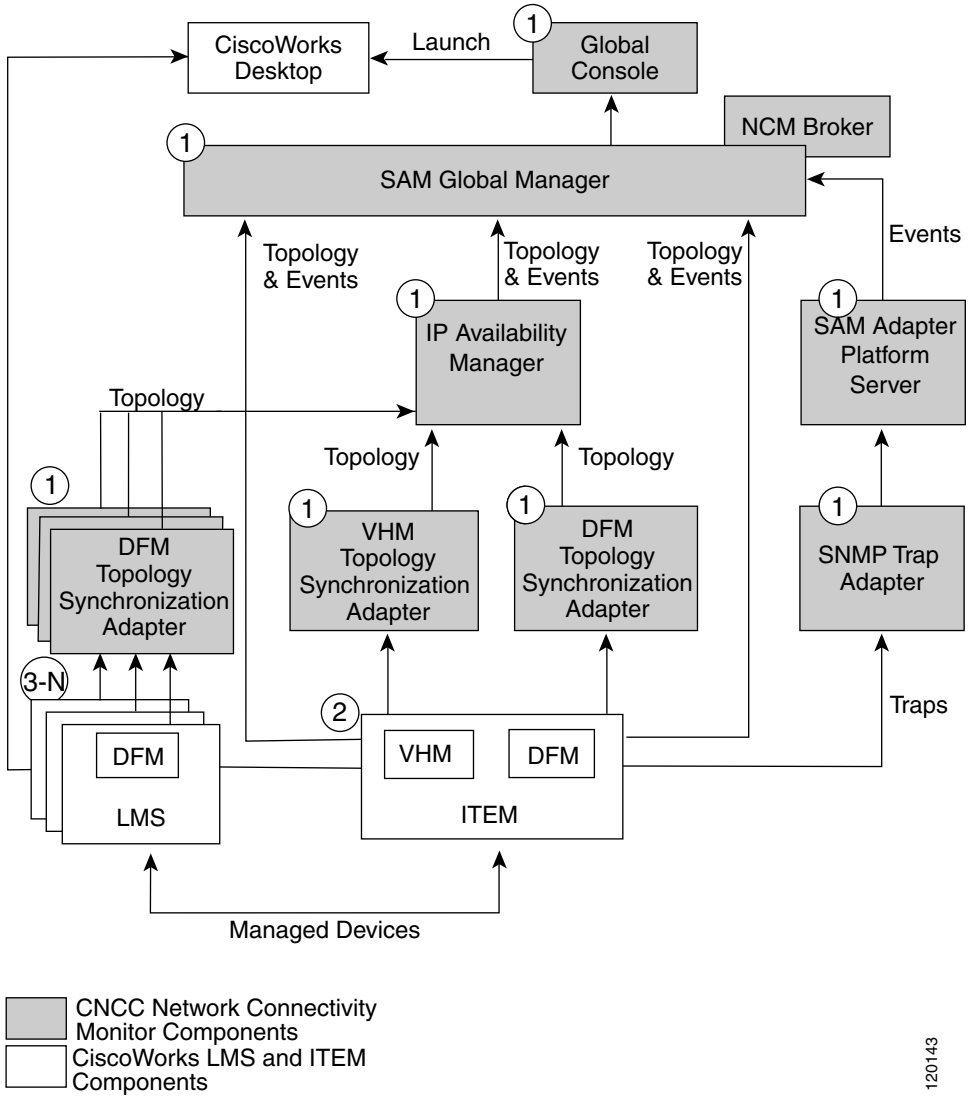
- The SAM Global Manager imports topology information from the IP Availability Manager and the SAM Adapter Platform server, and synchronizes the information with that of the IP Availability Manager.

- The SAM Global Manager imports and consolidates event information from the IP Availability Manager, ITEM, and the SAM Adapter Platform server, and displays event notifications on the Global Console(s).
- In addition to the automated corrective actions available in NCM, the CiscoWorks Desktop, used for the ITEM products, can be launched from the Global Console.

Optionally, you can also integrate one or more LMSs with NCM and ITEM. Each LMS resides on a separate host and has its own CNCC NCM Adapter for CiscoWorks LMS and ITEM to pass topology and event information to the IP Availability Manager. See the "(Optional) Multiple LMSs with NCM and ITEM" section on page 3-8.

Figure 3-1 illustrates the deployment of NCM with ITEM and multiple LMSs. The numbers **1**, **2**, and **3-N** refer to separate hosts.

Figure 3-1 Network Connectivity Monitor with LMS and ITEM



In this scenario, NCM includes CNCC NCM Adapter for CiscoWorks LMS and ITEM to seed the initial IP Availability Manager topology from ITEM. The adapter provides the following functionality:

- Initial topology import of all managed devices, including managed devices not supporting SNMP.
- Periodic topology synchronization to import managed devices discovered by the DFM and VHM components of ITEM since the last import. The topology synchronization is event-driven and will occur within a short period after new devices are added to ITEM.

Note Any device deleted from the ITEM topology is not automatically deleted from the NCM topology. It must be manually removed from the NCM topology by way of the NCM Domain Manager Administration Console or the command-line tools. If it is not manually removed, IP Availability Manager will continue to provide diagnostics for the device until it is removed from the underlying repository. For information about removing systems from the topology, see the *Network Connectivity Monitor IP Discovery Guide*.

Note CNCC NCM IP Availability Manager supports autodiscovery of all supported devices. This functionality is disabled by default. If NCM is integrated with ITEM, autodiscovery must remain disabled to avoid name resolution conflicts.

CNCC NCM IP Availability Manager provides full support for supported Cisco devices and other non-Cisco devices. An unsupported device will be discovered but managed as a generic node for connectivity analysis only.

CNCC NCM IP Availability Manager and ITEM must be configured to use the NCM Broker.

Direct communication between the SAM Global Manager and the underlying domains is controlled by data exchange (dxa) files. The event information that is transferred is consolidated with the information from CNCC NCM IP Availability Manager.

In this scenario, the login page of CiscoWorks Desktop, used with ITEM, can be launched from the Global Console. To enable this function, the name and address of the CiscoWorks server must be set up for the client tool that is available from the Global Console.

(Optional) Multiple LMSs with NCM and ITEM

NCM can be deployed with multiple LMSs and one ITEM installation. In this case, the functionality and process flow are the same as in the preceding scenario. However, note the following:

- The topologies collected by multiple LMSs are imported into, and monitored by, one CNCC NCM IP Availability Manager.
- The topologies imported into the IP Availability Manager are, in turn, sent to the SAM Global Manager.
- All of the pass-through traps from multiple LMSs are sent to the SAM Adapter Platform server.

When multiple LMSs are deployed with NCM, each DFM must be configured with a unique domain name. It is recommended that the domain names of the DFMs follow a naming convention. For example, use a numerical scheme (DFM1, DFM2, DFM3), the names of geographical regions (NE-DFM, SW-DFM), or perhaps the names of network centers or campuses (Dallas-DFM).

Note Do not change the name for the DFM component used by ITEM. The DFM component *must* retain its original name, *DFM*, in order to communicate with the VHM component of ITEM.

Integration Instructions

This chapter describes the various integration tasks that you must perform after installing NCM.

This chapter contains:

CNCC NCM IP AM Integration Steps

The following sections describe the steps to integrate adapters that are provided on the CNCC NCM IP Management Suite version 1.1 CD-ROM.

The topics include:

Note The term BASEDIR represents the location where CNCC NCM IP Availability Manager and its components are installed. By default, BASEDIR represents the */opt/InCharge6/IP* directory for Solaris, the *C:\InCharge6\IP* directory for Windows, or your specified path.

Configuring the LMS/ITEM Adapter

The CNCC NCM Adapter for CiscoWorks LMS and ITEM (LMS/ITEM Adapter) imports topology from LMS and ITEM to the CNCC NCM IP Availability Manager. The adapter is specified during the CNCC NCM IP AM installation process and is installed as a service. The service for the adapter is started as a post-installation task or is automatically started when the NCM machine restarts. For ITEM, two services are installed for the adapter: one for its DFM component, another for its VHM component.

For a single LMS or ITEM installation, no additional configuration is required for the LMS/ITEM Adapter.

For multiple LMS installations, you need an LMS/ITEM Adapter for each DFM.

To integrate NCM with multiple LMSs, you need to download and install the Multiple DFM Integration Package.

To download the package and the accompanying Readme file, which describes how to download and install the package, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-ncm.

(Optional) Configuring the CNCC NCM Adapters for HP OpenView NNM and IBM/Tivoli NetView

This section is applicable only if the following NCM adapters are installed:

- CNCC NCM Adapter for HP OpenView NNM
- CNCC NCM Adapter for IBM/Tivoli NetView

These adapters are specified during the CNCC NCM IP AM installation process and are installed as services. They must run on the same host as OpenView NNM or IBM/Tivoli NetView, respectively. The services for these adapters are started as a post-installation task or are automatically started when the NCM machine restarts.

To configure these adapters, you must execute the *NMSAttachToNCM.pl* script. The script changes:

- The name of the DFM, while attaching DFM to NCM.
- The values of the DFM broker hostname and port to the NCM Broker hostname and port.

To download the *NMSAttachToNCM.pl* script and the accompanying Readme file, which describes how to download and install the package, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-ncm.

CNCC NCM SAM Integration Steps

The following sections describe the steps to perform to integrate CNCC NCM Service Assurance Manager with LMS and ITEM.

The topics include:

Note The term BASEDIR represents the location where CNCC NCM Service Assurance Manager and its components are installed. By default, BASEDIR represents the */opt/InCharge6/SAM* directory for Solaris, the *C:\InCharge6\SAM* directory for Windows, or your specified path.

Note In this section, remember to use the sm_edit utility to edit the CNCC NCM SAM files for the SAM Global Manager, the SAM Adapter Platform server, the NCM SNMP Trap Adapter, and the Secure Broker. See the "Configuring Underlying Domains" section on page 4-4 for an example of the command. The sm_edit utility is used to edit all types of NCM configuration files. For complete information, see the *Network Connectivity Monitor System Administration Guide.*

Configuring Underlying Domains

Configuring CNCC NCM SAM includes creating user profiles, configuring settings for the underlying domains, and setting system parameters for the SAM Global Manager.

The following section discusses how to configure settings for the underlying domains specifically for integration. See the *Network Connectivity Monitor Service Assurance Manager Configuration Guide* for other configuration tasks such as creating user profiles and setting system parameters.

To configure settings for the underlying domains, use the sm_edit utility to modify the *ics.conf* configuration file. Depending on your deployment scenario, you will have to uncomment existing code and possibly insert additional domain names for your underlying applications.

Step 1 Open the *ics.conf* configuration file for the SAM Global Manager to modify it. For example, invoke:

```
# /opt/InCharge6/SAM/smarts/bin/sm_edit conf/ics/ics.conf
```

The sm_edit utility automatically creates a copy of the *ics.conf* file in the *BASEDIR/smarts/local/conf/ics* directory, if necessary, and opens the file in a text editor. If a local version of the file already exists, the sm_edit utility opens the local version in a text editor. For complete information about the sm_edit utility, see the *Network Connectivity Monitor System Administration Guide*.

Caution You should never modify configuration files manually—use the sm_edit utility to do so.

Step 2 Modify the DomainType definitions that are applicable to your NCM deployment scenario. (See the "ics.conf Configuration File" section on page 4-5 for examples of the DomainType entries.)

- You *must* uncomment (remove the # characters) the "DomainType definition for NCM-OI" entry for the SAM Adapter Platform server for all NCM deployment scenarios.
- If you are integrating NCM with LMS, you *must also* uncomment the "DomainType definition for DFM" entry.

- If you are integrating NCM with multiple LMSs, in the "DomainType definition for DFM" entry, you must insert an additional Name field with the name of each additional LMS/ITEM Adapter. Values for the Name field must be unique. See the "Configuring the LMS/ITEM Adapter" section on page 4-2 for more information.
- If you are integrating NCM with ITEM, you *must* uncomment two entries: the "DomainType definition for DFM" entry and the "DomainType definition for VHM" entry.
- If you are integrating NCM with ITEM *and* LMS, in addition to uncommenting the "DomainType definition for DFM" entry and the "DomainType definition for VHM" entry, you must specify unique values for the DFM names:
  - The value of the Name field for the DFM component of ITEM *must* remain DFM in order to communicate with the VHM component of ITEM.
  - Insert an additional Name field for the DFM component used by LMS and specify a unique name for that DFM.

ics.conf Configuration File

CNCC NCM SAM includes data exchange files. The files enable direct communications between the underlying domains (CNCC NCM IP Availability Manager, SAM Adapter Platform server, DFM, and VHM) and the SAM Global Manager.

A domain refers to an underlying application, such as NCM IP Availability Manager, SAM Adapter Platform server, DFM, and/or VHM, that serves as a source of event and topology data. You specify the domains and the parameters that control the import of event and topology data in the DomainSection of the *ics.conf* configuration file.

The DomainSection is divided into DomainType subsections, each of which defines the configuration for one or more underlying domains. The following example shows the syntax of a DomainSection when the underlying domains are SAM Adapter Platform server, DFM, and VHM. Table 4-1 describes the fields of DomainType subsections.

Note *Only* uncomment the lines that are **bolded**.

```
DomainSection
{
#   DomainType definition for NCM-OI
#    DomainType
#    {
#        ConfFile          = "dxa-oi.conf";
#        MinimumCertainty  = 0.24;
#        SmoothingInterval = 65;
#        HookScript        = "ics/dxa-sample-hook.asl";
#        Name              = "NCM-OI";
#    }
#   DomainType definition for DFM
#    DomainType
#    {
#        ConfFile          = "dxa-dfm.conf";
#        MinimumCertainty  = 0.24;
#        SmoothingInterval = 65;
#        HookScript        = "ics/dxa-sample-hook.asl";
#        Name              = "DFM";
#    }
#   DomainType definition for VHM
#    DomainType
#    {
#        ConfFile          = "dxa-vhm.conf";
#        MinimumCertainty  = 0.24;
#        SmoothingInterval = 65;
#        HookScript        = "ics/dxa-sample-hook.asl";
#        Name              = "VHM";
#    }
}
```

Table 4-1 describes the fields of DomainType subsections in the *ics.conf* configuration file.

Table 4-1 Fields Defining the DomainSection

Field	Description
ConfFile	The data exchange file that corresponds to the underlying domain. A data exchange file ensures that SAM Global Manager receives the correct event and topology data. These files should not be edited: • *dxa-conn.conf* for CNCC NCM IP Availability Manager. • *dxa-dfm.conf* for CiscoWorks Device Fault Manager (DFM). • *dxa-vhm.conf* for CiscoWorks Voice Health Monitor (VHM). • *dxa-oi.conf* for the SAM Adapter Platform server.
MinimumCertainty	Minimum value the Certainty attribute must have before an event is sent to the SAM Global Manager from the underlying domain. Events with a Certainty value below the threshold are discarded. This value must be a number between 0.0 and 0.99. The default value is 0.24.
SmoothingInterval	Time, in seconds, an event must be active before it is sent to the SAM Global Manager. The default value is 65 seconds. Note that the smoothing interval does not apply to underlying SAM Adapter Platform servers or other SAM Global Managers.
HookScript	*Optional*—Name of an ASL script that modifies a notification. Typically, this is used to add information to one of the user-defined fields of a notification. Hook scripts must be located in the *BASEDIR/smarts/local/rules/ics* directory. You must prefix the name of the script with the directory in which it is located; typically this is the *ics* directory.

Table 4-1 Fields Defining the DomainSection (continued)

Field	Description
Name	Name of the underlying domain. You can specify multiple domains with the same configuration by adding Name fields to the DomainType subsection. However, the value of each Name field within a DomainSection must be unique.

Configuring the CiscoWorks Client Tool

The login page of the CiscoWorks Desktop can be launched from the NCM Global Console.

To enable this function, use the Global Manager Administration Console from the Global Console to configure the tool. You must also specify the variables for your browser and the CiscoWorks Server in the ciscoworks script that is provided with the Global Console.

- Configuring the CiscoWorks Client Tool with the Global Manager Administration Console, page 4-8
- Modifying the ciscoworks Script on Solaris, page 4-9
- Modifying the ciscoworks Script on Windows, page 4-10

When users right-click in the Global Console, the CiscoWorks client tool is listed in the Client Tools submenu.

Configuring the CiscoWorks Client Tool with the Global Manager Administration Console

Step 1 Open the Global Console. For Solaris, type:

```
# <BASEDIR>/smarts/bin/sm_gui
```

For Windows, select **Start > Programs > Cisco Network Connectivity Monitor (NCM) > Global Console**.

Step 2 From the Global Console, select **Configure > Global Manager Administration Console**.

Step 3 Select **Edit > New Client Tool**.

Step 4 Specify the display name of the client tool. In the Client Tool field, type CiscoWorks. The Create New button is selected by default. Click **Next**.

Step 5 Specify the script, tool parameters, and user profiles. Select the following:

- Program pull-down menu—Select the ciscoworks script.
- Display Output—Select FALSE. (You do not have to change the default values for Timeout Interval and Trace, 30 seconds and FALSE, respectively.)
- Current—Specify the user profiles that will include the tool. To do so, move the user profiles listed in the Unused list to the Current list. Select the user profile and click **Add**. (To select multiple profiles, press the **Ctrl** key while making your selections.)
- Click **Next**.

Step 6 For context criteria, click **Next**.

Step 7 For status criteria, click **Next**.

Step 8 Verify that the CiscoWorks tool is listed in the Client tree and click **Finish**.

For more information about tools and tool parameters, see the *Network Connectivity Monitor Service Assurance Manager Configuration Guide*.

Modifying the ciscoworks Script on Solaris

Step 1 Edit the *ciscoworks.sh* file in the *BASEDIR/smarts/actions/client* directory. For example:

```
# cd /opt/InCharge6/SAM/smarts
# bin/sm_edit actions/client/ciscoworks.sh
```

Step 2 Change the BROWSER entry to point to the Netscape executable on your machine. For example:

```
BROWSER=/opt/misc/netscape/netscape-7.0/netscape
```

Step 3 Change the CISCOWORKS_URL entry to point to the CiscoWorks location, on a remote machine, to which you want to connect. For example:

```
CISCOWORKS_URL=http://cw_host:1741
```

where *cw_host* is the IP address or DNS name of the CiscoWorks machine running LMS or ITEM.

Modifying the ciscoworks Script on Windows

Step 1 Edit the *ciscoworks.cmd* file in the *BASEDIR/smarts/actions/client* directory. For example:

```
cd C:\InCharge6\SAM\smarts
bin\sm_edit actions\client\ciscoworks.cmd
```

Step 2 Change the <host> entry to the host where CiscoWorks is running. For example:

```
set CISCO_HOST=cw_host
```

where *cw_host* is the IP address or DNS name of the CiscoWorks machine running LMS or ITEM.

Note It is not necessary to indicate the Internet Explorer path.

Configuring the CNCC NCM SNMP Trap Adapter

Note If you are integrating NCM with LMS or ITEM, you must stop the SNMP TrpSvc service (on Windows) or stop any other running trap receivers (on Solaris) on the NCM machine.

The CNCC NCM SNMP Trap Adapter collects and parses SNMP traps sent from LMS and ITEM and generates notifications to the SAM Global Manager based on the contents of the traps. The Trap Adapter is specified during the CNCC NCM SAM installation process and is installed as a service.

See the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide* for complete information about the Trap Adapter.

SNMP Trap Receiving

Trap definitions are available for most Cisco MIBs. They are defined in the file *BASEDIR/smarts/conf/icoi/trap_mgr.conf*.

For NCM 1.1, a new trap definition (.1.3.6.1.4.1.9.9.311.0.1 6 1) from MIB: CISCO-EPM-NOTIFICATION-MIB is included in the file. *No user action is required.* By default, UnknownAgent is set to IGNORE, which means the ITM (IP Telephony Monitor) device needs to be available in the CNCC NCM SAM Adapter Platform server's topology.

If you want to create this device, then you need to use the sm_edit utility to edit the file *BASEDIR/smarts/conf/icoi/trap_mgr.conf* during discovery. Change the value of UnknownAgent to CREATE (UnknownAgent = CREATE) and make sure you specify the ElementClassName and ElementName. For more information about modifying the *trap_mgr.conf* file, see the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide*.

Changing the Port Setting for Trap Receiving

If necessary, you can change the port setting of the CNCC NCM SNMP Trap Adapter so that it receives traps on a different port other than the default port (162).

To do so, for Solaris and Windows, perform all of the following steps.

Note The following instructions assume that the desired port is already configured on the DFM machine for trap forwarding to the NCM machine.

Step 1 On the NCM machine where SAM is running, use the sm_edit utility to modify the file *BASEDIR/smarts/conf/icoi/trapd.conf*.

For example, on Windows, enter the command:

```
cd C:\InCharge6\SAM\smarts
bin\sm_edit conf\icoi\trapd.conf
```

In the file, locate the PORT parameter setting and change the 9000 value to the desired port number. In this example, the port number changed to 9020.

```
# Set the parameters here.

PORT: 9020
```

Step 2 Change the directory to *BASEDIR/smarts/bin*.

Step 3 Stop the service for the CNCC NCM SNMP Trap Adapter. Enter the command:

```
<BASEDIR>/smarts/bin/sm_service stop ic-trapd-receiver
```

For example, on Windows, enter:

```
C:\InCharge6\SAM\smarts\bin\sm_service stop ic-trapd-receiver
```

Step 4 Remove the existing CNCC NCM SNMP Trap Adapter service. Enter the command:

```
<BASEDIR>/smarts/bin/sm_service remove ic-trapd-receiver
```

For example, on Windows, enter:

```
C:\InCharge6\SAM\smarts\bin\sm_service remove ic-trapd-receiver
```

Step 5 Reinstall the service for the CNCC NCM SNMP Trap Adapter *without* the --port option. Enter the command:

```
<BASEDIR>/smarts/bin/sm_service install
        --startmode=runonce --description="CNCC NCM SNMP Trap Adapter"
        ic-trapd-receiver <BASEDIR>/smarts/bin/sm_trapd
        --name=TRAP-NCM-OI --server=NCM-OI --config=icoi --ascii
        --model=sm_actions --output icoi-trapd/trap_mgr_parse.asl
```

For example, on Windows, enter:

```
C:\InCharge6\SAM\smarts\bin\sm_service install
        --startmode=runonce --description="CNCC NCM SNMP Trap Adapter"
        ic-trapd-receiver C:\InCharge6\SAM\smarts\bin\sm_trapd
        --name=TRAP-NCM-OI --server=NCM-OI --config=icoi --ascii
        --model=sm_actions --output icoi-trapd\trap_mgr_parse.asl
```

Note The sm_service install command must be typed as one line.

Step 6 Restart the service for the CNCC NCM SNMP Trap Adapter. Enter the command:

```
<BASEDIR>/smarts/bin/sm_service start ic-trapd-receiver
```

For example, on Windows, enter:

```
C:\InCharge6\SAM\smarts\bin\sm_service start ic-trapd-receiver
```

Configuring SNMP Trap Forwarding

To configure trap forwarding, you can do one of the following:

- Use the *AttachToNCM.pl* script and perform Step 3 of the following procedure. (See the "AttachToNCM Script" section on page 4-16 for additional information.)
- Manually configure trap forwarding (perform all of the steps in the following procedure).

Note Perform Step 1 and Step 2 on the DFM machine; perform Step 3 on the NCM machine where SAM is running.

Note If you are using the *AttachToNCM.pl* script (see the "AttachToNCM Script" section on page 4-16 for additional information), then you need to perform only Step 3 of the following procedure, because the script automatically configures DFM trap forwarding.

To configure the SNMP trap forwarding manually, perform all of the following steps:

Step 1 On the DFM machine, select **Device Fault Manager > Administration > Trap Configuration > Trap Forwarding** from the CiscoWorks Desktop.

Step 2 In the configuration dialog box, make sure Forwarding is set to ON, and that the Add Recipient field contains the name or the IP address of the host running NCM; the port should be set to 162. Make sure that the Restart DFM Server checkbox is selected and click **OK**. After the DFM server is restarted, all traps will be forwarded to the CNCC NCM SNMP Trap Adapter listening on port 162.

Step 3 On the NCM machine where SAM is running, you must configure the CNCC NCM SNMP Trap Adapter to forward selected traps to CNCC NCM IP AM. To enable NCM trap forwarding, the file *BASEDIR/smarts/conf/icoi/trapd.conf* needs to be edited. Use the sm_edit utility to edit the file.

For example:

```
cd C:\InCharge6\SAM\smarts
bin\sm_edit conf\icoi\trapd.conf
```

The file contains forwarding statements for different types of traps. They are commented out by default (with #). To uncomment a statement, remove the # character.

In the file, uncomment all FORWARD statements *except* for this statement:

```
#
#FORWARD: *.*.*.* .* * * host:port
```

Also, in the uncommented FORWARD statements, change *host:port* to *localhost:9000*.

The following are two examples of modified FORWARD statements:

```
# Generic: coldStart, warmStart, LinkUp, LinkDown
FORWARD: *.*.*.* .* <0-3> * localhost:9000

# Cisco: STACK module inserted, removed
FORWARD: *.*.*.* .1.3.6.1.4.1.9.5 6 <3-4> localhost:9000
```

Note NCM is automatically configured to receive traps on port 162. If you have any third-party SNMP trap receivers installed on the NCM machine, then you must disable them.

Configuring the Secure Broker

By default, NCM is installed with a secure broker. All NCM internal components authenticate each other, which prevents unauthorized access. Using a secure broker results in the following:

- Consoles prompt for a username and password to connect to the broker.
- Other NCM servers and clients use their respective credentials and send them to the broker and to each other.

Note The default NCM username is *admin*; the default NCM password is *changeme*. It is highly recommended that you change the default NCM password, as well as other internal NCM credentials.

In addition, you can add username and password pairs for more users. For information about username-password pairs and securing access to NCM, see the *Network Connectivity Monitor System Administration Guide*. For information about adding user profiles, see the *Network Connectivity Monitor Service Assurance Manager Configuration Guide*.

If LMS or ITEM has already been deployed, the existing DFM username and password pair can be configured within the NCM secure broker. To obtain the existing username and password pair, you can use the *DFMConnect.pl* command, provided on the DFM product CD-ROM, on the CiscoWorks machine. For more information about the *DFMConnect.pl* command, refer to the *User Guide for CiscoWorks Device Fault Manager*. You need the following information:

- adminUser and adminPassword—Credentials to log in to NCM.
- brokerUser and brokerPassword—Credentials, such as the username and password, used by DFM, VHM, and NCM services when sending requests to the NCM broker.
- pingUser and pingPassword—Credentials, such as the username and password, used by the NCM Broker when sending requests to DFM, VHM and NCM services.

LMS Integration Steps

The following sections describe the steps to perform on the LMS machine, to integrate LMS with Network Connectivity Monitor.

The topics include:

AttachToNCM Script

Changing the DFM and/or VHM broker location can be performed automatically by using the *AttachToNCM.pl* script.

The script, which can be executed for any LMS or ITEM domain, automatically performs the following:

- Changes the name of the DFM, while attaching DFM to NCM.
- Changes the values of the DFM broker hostname and port to the NCM Broker hostname and port.

- Changes DFM and VHM authentication parameters to match the default values in NCM, which are the username *admin* and password *changeme*.
- Configures and enables DFM trap forwarding to the NCM machine.

After running the script, the machine running LMS or ITEM must be restarted.

An *AttachToNCM.pl* Perl script is available from Cisco.com. To download the script and the accompanying Readme file, which describes how to download and install the script, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-ncm.

Multiple DFM Integration Package

To integrate NCM with multiple LMSs, you need to download and install the Multiple DFM Integration Package.

To download the package and the accompanying Readme file, which describes how to download and install the package, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-ncm.

Manually Changing the Broker Location

Note Skip this procedure if you are using the *AttachToNCM.pl* script.

On the LMS machine, in order for notifications from LMS to be viewed in the SAM Global Manager, the value of the SM_BROKER_DEFAULT or SM_BROKER (for Windows) variable needs to be changed from the default value of localhost:426 to the server on which the SAM Global Manager is installed.

To manually change the broker location, perform the following steps:

Step 1 Change the value of the SM_BROKER_DEFAULT (or SM_BROKER for Windows) variable using either the *runcmd_env.sh* script on Solaris, or the Windows Control Panel (for Windows). The broker location must always contain the hostname running the Global Manager with an optional port specification, if the NCM Broker uses a port other than the default port (426).

Step 2 Restart the computer running LMS to make sure the variable change is propagated to all needed processes.

When multiple LMSs are integrated with NCM, repeat these steps to reconfigure all of the DFM Brokers to use the NCM Broker.

Manually Configuring Authentication

Note Skip this procedure if you are using the *AttachToNCM.pl* script.

Before configuring authentication, the usernames and passwords should be chosen for securing access to the NCM Broker, SAM Global Manager, CNCC NCM IP Availability Manager, and DFM server. If the DFM component of LMS installation has already been deployed, the existing DFM name and password pairs can be used to configure NCM security. However, it is not required. To obtain the existing DFM name and password pairs, the existing *DFMConnect.pl* script can be used. Since DFM uses the same name and password to authenticate the broker and the DFM Server, the NCM security configuration should always use identical name and password pairs for all servers and the broker.

Optionally, if DFM uses the --accept option to limit access to the server to only a range of IP addresses, configure DFM to make sure the IP addresses of the NCM Broker, the SAM Global Manager, and the LMS/ITEM Adapter are accepted.

See the "Configuring the Secure Broker" section on page 4-15 for additional information about configuring authentication.

ITEM Integration Steps

The following sections describe how to integrate ITEM with Network Connectivity Monitor. ITEM consists of DFM, VHM, and other Cisco applications. The following procedures apply to DFM and VHM only.

The topics include:

- For DFM and VHM, Manually Changing the Broker Location, page 4-19
- For DFM and VHM, Manually Configuring Authentication, page 4-20

Note Changing the broker location and configuring authentication can be accomplished automatically. See AttachToNCM Script, page 4-16 for additional information.

If you are integrating one or more LMSs with NCM and ITEM, see the "LMS Integration Steps" section on page 4-16.

Manually Changing the Broker Location

Note Skip this procedure if you are using the *AttachToNCM.pl* script.

If you are not using the *AttachToNCM.pl* script, you need to manually change the broker location for both DFM and VHM. Perform the following steps:

Step 1 Change the default values of the hostname and port (localhost:426) to the server on which the SAM Global Manager is installed. The broker location must always contain the hostname running the SAM Global Manager with an optional port specification, if the NCM Broker uses a port other than the default port (426).

- On the DFM machine, change the default value of the SM_BROKER_DEFAULT (or SM_BROKER for Windows) variable using either the *runcmd_env.sh* script on Solaris, or the Windows Control Panel (for Windows).
- On the VHM machine, change the broker location using the VHM tool **changeHostName**.

Step 2 Restart the DFM machine and the VHM machine to make sure the change is propagated to all needed processes.

Manually Configuring Authentication

Note Skip this procedure if you are using the *AttachToNCM.pl* script.

Before configuring authentication, the usernames and passwords should be chosen for securing access to the NCM Broker, SAM Global Manager, CNCC NCM IP Availability Manager, DFM, and VHM.

If the DFM and VHM components used by ITEM have already been deployed, the existing DFM/VHM name and password pairs can be used to configure NCM security. However, it is not required.

To obtain the existing name and password pairs, you can use:

- For DFM, the existing *DFMConnect.pl* script.
- For VHM, the existing VHM tools. Or, the information can be extracted directly from the configuration files. See the *Voice Health Monitor User Guide* for additional information about configuring authentication.

Since DFM and VHM use the same name and password pairs to authenticate the broker and the DFM/VHM servers, the NCM security configuration should always use identical name and password pairs for all servers and the broker.

Optionally, if DFM or VHM uses the --accept option to limit access to the server to only a range of IP addresses, configure DFM to make sure the IP addresses of the NCM Broker, the SAM Global Manager, and the LMS/ITEM Adapter are accepted.

See the "Configuring the Secure Broker" section on page 4-15 for additional information about configuring authentication.

CHAPTER 5

Validating Your Integration

This chapter describes how to ensure that your integrated components operate as intended.

This chapter contains:

Note The term BASEDIR represents the location where CNCC NCM IP Availability Manager and its components are installed. By default, BASEDIR represents the */opt/InCharge6/IP* directory for Solaris, the *C:\InCharge6\IP* directory for Windows, or your specified path.

Note The term BASEDIR represents the location where CNCC NCM Service Assurance Manager and its components are installed. By default, BASEDIR represents the */opt/InCharge6/SAM* directory for Solaris, the *C:\InCharge6\SAM* directory for Windows, or your specified path.

Verifying that Processes Are Registered with the Broker

Ensure that the NCM Broker has access to all of the CNCC NCM (SAM and AM), LMS (DFM), and ITEM (DFM and VHM) applications and that the processes are registered and running. To do so, issue the following command:

```
# <BASEDIR>/smarts/bin/brcontrol
```

This command displays a list of processes registered with the broker, their states (RUNNING, DEAD, UNKNOWN), process IDs, port numbers, and the last time their states changed. For additional information about the broker, see the *InCharge System Administration Guide*.

Verifying the Services for the LMS/ITEM Adapter

The CNCC NCM Adapter for CiscoWorks LMS and ITEM (LMS/ITEM Adapter) imports topology from LMS or ITEM to the CNCC NCM IP Availability Manager.

Ensure that services for the LMS/ITEM Adapter are running:

- For LMS, the service is ic-dfm-adapter and is named CNCC NCM DFM Topology Synchronization Adapter.
- For ITEM, two services, ic-dfm-adapter and ic-vhm-adapter, should be running; their names are CNCC NCM DFM Topology Synchronization Adapter and the CNCC NCM VHM Topology Synchronization Adapter, respectively.

To display the status of the installed services on Solaris or Windows, use the sm_service show command. For example, on Solaris, issue:

```
# /opt/InCharge6/SAM/smarts/bin>./sm_service show
```

Alternatively, on Windows, you can select **Settings > Control Panel > Administrative Tools > Services** to view the status of services.

Usually, the service for the adapter is started as a post-installation task or is automatically started when the NCM machine restarts. If the service is not running, you can start an individual service.

Starting the Adapter Service for LMS

If necessary, on Solaris, to start the adapter service for the DFM component of LMS, issue:

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

On Windows, you can start the adapter service from Services in the Control Panel.

Starting the Adapter Services for ITEM

If necessary, on Solaris, to start the adapter services for the DFM and VHM components of ITEM, issue these commands:

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

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

On Windows, you can start the adapter services from Services in the Control Panel.

Checking the LMS/ITEM Adapter Service Installation Parameters (Optional)

To view the default parameters and their values of an existing service installation invocation, you can use the sm_service show command. For example, issue:

```
# sm_service show ic-dfm-adapter --cmdline
```

The default parameters for the adapter service for the DFM component are:

```
<BASEDIR>/smarts/bin/sm_service install ic-dfm-adapter
--startmode=runonce
  --description="CNCC NCM DFM Topology Synchronization Adapter"
     <BASEDIR>/smarts/bin/sm_adapter
     --name=NCM-DFM-ADAPTER
     --logname=ncm-dfm-adapter
     -DciscoServerName=DFM
     -DamServerName=NCM-AM
     -DdiscoverPending=YES
     --output
     nfm/nfm-start.asl
```

The default parameters for the adapter service for the VHM component are:

```
<BASEDIR>/smarts/bin/sm_service install ic-vhm-adapter
--startmode=runonce
  --description="CNCC NCM VHM Topology Synchronization Adapter"
     <BASEDIR>/smarts/bin/sm_adapter
     --name=NCM-VHM-ADAPTER
     --logname=ncm-vhm-adapter
     -DciscoServerName=VHM
     -DamServerName=NCM-AM
     -DdiscoverPending=YES \
     --output
     nfm/nfm-start.asl
```

For additional information about services, see the *Network Connectivity Monitor System Administration Guide*.

Opening the Global Console and Verifying Devices

Open the Global Console and check your topology. Verify that devices are imported.

Step 1 To open the Global Console for Solaris, type:

```
# <BASEDIR>/smarts/bin/sm_gui
```

For Windows, select **Start > Programs > Cisco Network Connectivity Monitor (NCM) > Global Console**.

Step 2 Select **File > New > Topology Browser Console** to open the Topology Browser Console. In the left panel, expand each object in the topology tree and check its contents.

For information about using the Global Console, see the *Network Connectivity Monitor Operator's Guide*.

Verifying Traps

In the Global Console, verify that you are receiving traps as notifications.

Step 1 To open the Global Console for Solaris, type:

```
# <BASEDIR>/smarts/bin/sm_gui
```

For Windows, select **Start > Programs > Cisco Network Connectivity Monitor (NCM) > Global Console**.

Step 2 The Notification Log Console opens by default or select **File > New > Notification Log Console**. In the console, examine the notifications that display.

A

B

C

D

G

H

I

L

M

N

O

P

S

T

V