Network Connectivity Monitor IP Deployment 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-6290-01

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;

Contents

Preface

The *Network Connectivity Monitor IP Deployment Guide* describes how to deploy the Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM) IP Management Suite and related components of the CNCC NCM Service Assurance Management Suite.

This guide is intended as a comprehensive resource for deployment tasks. In many cases, you will be referred to other NCM documents for specific procedures and configuration tasks, such as:

- The *Network Connectivity Monitor Installation Guide* that accompanied your software product suite for detailed hardware requirements, platform requirements, and installation procedures
- The *Network Connectivity Monitor IP Discovery Guide* for information about discovery configuration and processing
- The *Network Connectivity Monitor IP Availability Manager User's Guide* and the *InCharge IP Performance Manager User's Guide* for information about CNCC Manager functions including polling and thresholds
- The *Network Connectivity Monitor Service Assurance Manager Configuration Guide* for information about the Global Manager Administration Console
- The *Network Connectivity Monitor System Administration Guide* for detailed administration procedures for the NCM deployment

Intended Audience

This guide is intended for the following audiences:

- Network and system administrators who aid in the design and deployment of NCM and its maintenance
- Integrators and network consultants who aid in designing NCM deployments and then install, validate, and tune the deployments
- Systems Engineers who design NCM deployments
- Cisco personnel who design, install, validate, and tune NCM deployments
- Cisco support personnel who respond to inquiries, problems, and issues that arise during NCM deployments

Prerequisites

To successfully use this guide, you should be familiar the following subjects:

- TCP/IP networking concepts
- Network administration practices
- The NCM architecture
- Concepts discussed in *An Introduction to Network Connectivity Monitor Service Assurance Manager*

Document Organization

This guide consists of the following:

1. Overview of the NCM Deployment Process	Describes the phases of the NCM deployment process
2. Gathering Information for Designing	Describes the information that must be collected before beginning the design process for an NCM deployment
3. Designing the NCM Deployment	Provides instructions, guidelines, and recommendations for designing NCM deployments
4. Planning for Discovery	Describes guidelines for designing the discovery process for NCM deployments
5. Designing Polling and Thresholds	Suggests polling and threshold configurations for NCM deployments
6. Designing Trap Processing	Describes the recommended trap processing design for NCM deployments
7. Deploying Syslog Processing	Recommends syslog processing configurations for NCM deployments
8. Designing for Administration of NCM	Describes NCM administration considerations for designing users and access to NCM deployments
9. Deploying NCM	Provides guidelines and recommendations for installing CNCC Managers, Adapters, and Global Consoles during NCM deployments
10. Validating Your Deployment (Acceptance Testing)	Describes how to ensure CNCC Managers, Adapters, and Global Consoles are properly installed in a network
11. Tuning Your Deployment to Improve Performance	Explains how to assess and tune your NCM deployment to improve performance
A. Using Discovery Manager to Obtain Network Information	Describes how to deploy Discovery Manager
B. Managing Overlapping IP Networks With NCM	Describes the NCM Overlapping IP Network functionality
C. Design and Deployment Checklists	Groups all checklists included in this guide for easy access

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 Manager	• 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

PRODUCT SUITE	INCLUDES THESE PRODUCTS	DIRECTORY
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:

- *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*

Network Connectivity Monitor Service Assurance Management Documentation

The following documents are relevant to users of the NCM Service Assurance Management product suite.

- *Network Connectivity Monitor Service Assurance Management Suite Installation Guide*
- *An Introduction to Network Connectivity Monitor Service Assurance Manager*
- *Network Connectivity Monitor Operator's Guide*
- *Network Connectivity Monitor Service Assurance Manager Configuration Guide*
- *InCharge Service Assurance Manager Business Dashboard Configuration Guide*
- *InCharge Service Assurance Manager User's Guide for Business Impact Manager*
- *InCharge Service Assurance Manager User's Guide for Report Manager*
- *InCharge Service Assurance Manager Failover System User's Guide*

The following documents are relevant to NCM Service Assurance Manager adapters.

- *Network Connectivity Monitor Service Assurance Manager Notification Adapters User's Guide*
- *InCharge Service Assurance Manager SQL Data Interface Adapter User's Guide*
- *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide*
- *InCharge XML Adapter User's Guide*
- *InCharge Service Assurance Manager User's Guide for Remedy Adapter*
- *InCharge Service Assurance Manager User's Guide for Concord eHealth Adapter*
- *InCharge Service Assurance Manager User's Guide for InfoVista Adapter*

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 of the NCM Deployment Process

This chapter provides an overview of the deployment process for the portions of the Cisco Network Connectivity Center (CNCC) Network Connectivity Monitor (NCM) architecture that monitor and diagnose network infrastructure availability and performance.

NCM Architecture

This guide describes the deployment process for the following components in the CNCC NCM IP Management Suite and the CNCC NCM Service Assurance Management Suite:

- The InCharge IP Discovery Manager (Discovery Manager) monitors and collects data for devices in a network. Discovery Manager integrates the data but does not perform root-cause analysis.
- The CNCC NCM IP Availability Manager (Availability Manager) and InCharge IP Performance Manager (Performance Manager) discover and monitor data for their corresponding NCM domains. These managers then integrate and correlate the data to perform root-cause analysis for the devices in the related NCM domain.

- The Service Assurance Manager of the CNCC NCM Service Assurance Manager (Service Assurance) correlates topology and events from various sources, including the CNCC Managers and certain NCM Adapters. The Service Assurance Manager also builds a graphical representation of these relationships in a topology map for display on the NCM Global Console.
- The NCM Global Console provides the interface for configuration and administration of NCM components and displays the root cause of any failures using notifications and the topology map.
- CNCC NCM Service Assurance Manager Adapters (SAM Adapters) and the CNCC NCM SAM Adapter Platform provide NCM with additional sources of data when monitoring a network. The SAM Adapter Platform normalizes and consolidates data from certain adapters before it is passed to Service Assurance. This guide covers deployment of the SAM Adapter Platform and two of the adapters that send data to the SAM Adapter Platform: the CNCC NCM SNMP Trap Adapter (Receiver) and the CNCC NCM Syslog Adapter.

Figure 1 shows the NCM components covered in this guide.

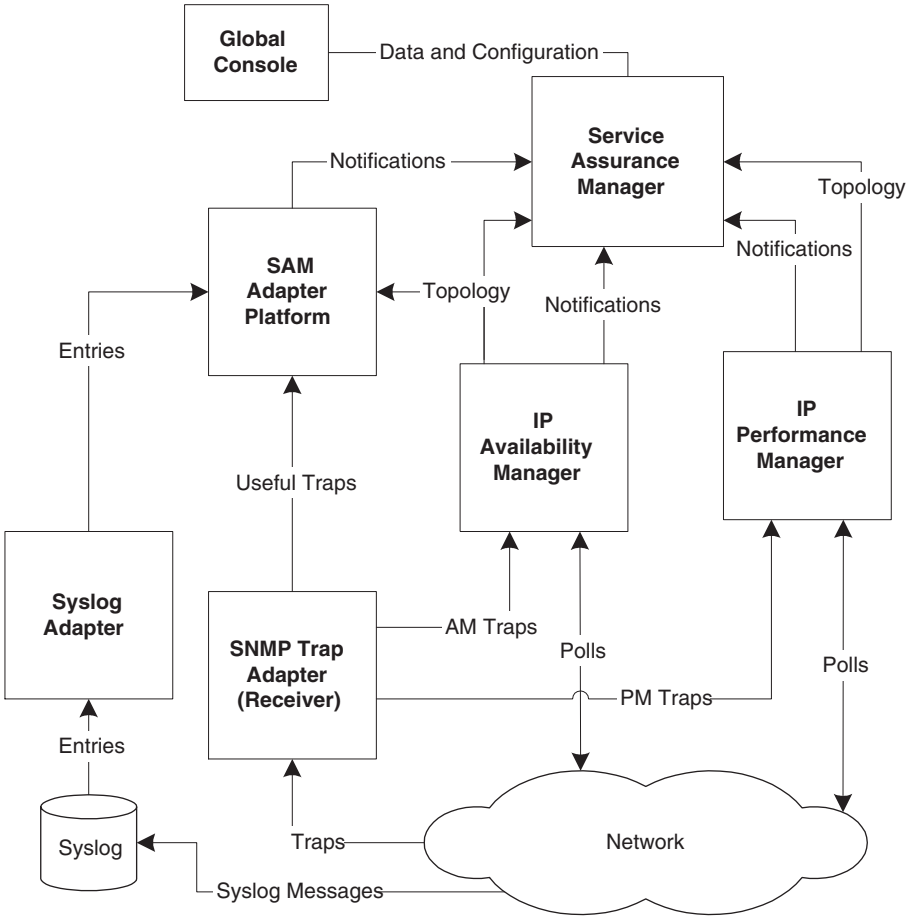


Figure 1: **NCM Components Described in this Guide**

The Deployment Process

As shown in Figure 2, the NCM deployment process can be divided into four distinct phases:

- Phase 1: Designing the NCM deployment
- Phase 2: Installing and configuring the NCM components
- Phase 3: Validating the NCM deployment
- Phase 4: Tuning and maintaining the NCM deployment to improve performance

During each phase of deployment, it is vitally important that you document all aspects of the deployment that could be required to recreate, troubleshoot, and reconfigure the NCM installation.

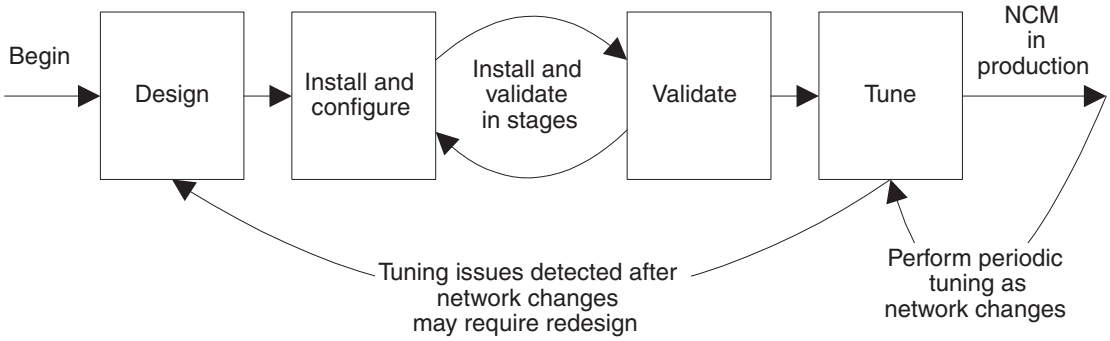


Figure 2: **The NCM Deployment Process**

Phase 1: Designing the NCM Deployment

Designing a NCM deployment consists of gathering necessary information and then using the information to develop a plan for the NCM deployment.

Gathering the information is a process that involves both the designer and the network administrators. Network administrators must provide details of their network's OSI model Layer 2 and Layer 3 infrastructure:

- List the quantities and types of devices such as routers, switches, hubs, and bridges and their ports and interfaces. Include plans for adding or removing equipment during the time period that the deployment design will cover.
- Provide IP addresses for use in discovery, including seed systems and filtering.
- Describe network geography, including locations of Network Operations Centers (NOCs) and equipment.
- Specify LAN and link speeds throughout the network and their relationship to the network geography.

This information is then applied, using sizing guidelines, to develop a NCM deployment design that will properly support the network. The design should also account for projected growth of the network.

The design is detailed in a Solution Architecture Diagram and a Deployment Build Guide. In their preliminary stages, the diagram and guide could be used in the answer to an organization's Request for Proposal (RFP) or Request for Quote (RFQ).

Once a NCM deployment is contracted, the information in the Solution Architecture Diagram can be refined and verified through meetings with network administrators. If possible, using the Discovery Manager to inventory the network can provide a highly accurate starting point for sizing the NCM deployment.

Design is covered in the following chapters:

- *Gathering Information for Designing* on page 9 (normally performed by systems engineers)
- *Designing the NCM Deployment* on page 25 (normally performed by systems engineers and Cisco)
- *Planning for Discovery* on page 37 (normally performed by Cisco)
- *Designing Polling and Thresholds* on page 49 (normally performed by Cisco)
- *Designing Trap Processing* on page 53 (normally performed by Cisco)
- *Deploying Syslog Processing* on page 61 (optionally performed by Cisco)
- *Designing for Administration of NCM* on page 65 (optionally performed by Cisco)

Phase 2: Installing and Configuring the NCM Components

Once the design is complete and has been reviewed by Cisco, the next phase is installing and configuring NCM components.

With any deployment, installation and configuration of NCM components are usually performed in stages. Each installed and configured segment is validated individually as described in the next phase of the deployment process. This phased approach eases troubleshooting.

Many organizations have specific procedural requirements that must be met before and during installation of new software products in their production environments. These requirements might include lab installations with performance validations and preproduction deployments. Lab configurations usually require the use of a testbed that is configured and equipped similarly to the production environment. Acceptance tests may be performed before the deployment to the production environment. After the production deployment, the lab or testbed may be used to test upgrades and, if required, patches.

Though this guide cannot cover organization-specific requirements, it does provide guidelines that may aid you in responding to these conditions.

Installing and Configuring NCM is covered in *Deploying NCM* on page 71. The deployment information, including software locations and all configuration choices should be recorded in the Deployment Build Guide. Normally, this phase is performed by the purchaser of the NCM deployment and Cisco.

Phase 3: Validating the Deployment

Validating the deployment ensures all installed NCM components are operational and can communicate with each other as required and that the appropriate components can properly discover and poll the network.

Logical segments of NCM are usually installed and validated to ease troubleshooting. Once all individual segments are installed and validated, the complete NCM deployment must be validated from end to end. Included in this overall validation could be acceptance tests that demonstrate the functionality of the installation. Criteria for acceptance tests should be defined during the design phase. The execution of these acceptance tests and the results are then usually included in an installation or build report.

Deploying NCM components is covered in *Validating Your Deployment (Acceptance Testing)* on page 77. Normally, this phase is performed by the purchaser of the NCM deployment and Cisco.

Phase 4: Tuning and Maintaining the Deployment

Once NCM is deployed and validated, you must ensure that it is operating at an optimal level. Tuning is the process of adjusting the configuration to improve performance. Note that this initial tuning process does not include rules writing or related maintenance: NCM does not require this type of maintenance.

This process can only be performed after *all* components are installed and validated to avoid inaccurate tuning.

The process of tuning a NCM deployment is covered in *Tuning Your Deployment to Improve Performance* on page 81. Normally, this phase is initially performed by Cisco or a partner and the knowledge is transferred to the purchasing organization's staff. As the network grows and changes, the organization's staff will take on the task of tuning the NCM deployment to deal with the network changes. If the network changes are extensive, the original design may no longer be sufficient and redesigning the NCM deployment may be required.

Before You Begin Checklist

Before you begin a NCM deployment, you must meet the requirements described in the following checklist. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

BEFORE YOU BEGIN CHECKLIST		
COMPLETE	REQUIREMENT	DESCRIPTION
☐	Possess an understanding of the NCM architecture and capabilities.	At a minimum, you must understand the concepts and NCM architecture described in the following documents: • *Network Connectivity Monitor IP Availability Manager User's Guide* • *Network Connectivity Monitor IP Discovery Guide* • *InCharge IP Performance Manager User's Guide* • *Network Connectivity Monitor Service Assurance Manager Configuration Guide* • *An Introduction to Network Connectivity Monitor Service Assurance Manager* • *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide* • *Network Connectivity Monitor System Administration Guide* • *Installation Guide* that accompanied your software product suite.
		To improve your understanding, attend NCM training courses offered by Cisco Systems. Typically, deployment requires the knowledge equivalent to what is provided in the training courses on: • CNCC NCM for IP • CNCC NCM Service Assurance Manager • CNCC NCM Service Assurance Manager Adapter Platform
☐	Obtain contact information for the deployment team.	The contact list should include titles, responsibilities, and contact methods for all team members.
☐	Get nondisclosure requirements and negotiate an agreement.	Be aware of the requirements of the non-disclosure agreements that are in place for the NCM deployment.
☐	Develop schedules and set milestones for early deliverable.	Scheduling a software deployment varies based on the size and scope of the deployment and the organization's requirements. Typical milestones might include: • Initial project meeting to define the deployment scope • Purchase of NCM software • Project development begins • Installation in test environment complete • Testing complete • Installation in production environment complete • NCM goes live Additional information on scheduling is beyond the scope of this guide.

2

Gathering Information for Designing

This chapter describes the first step in designing an NCM deployment: gathering the organizational and network-related information that is required to develop a successful NCM design.

Determine the Organization's Requirements

The design of an NCM deployment must support an organization's needs. Most Requests for Information (RFIs), Requests for Proposal (RFPs), or Requests for Quote (RFQs) will begin with a description of the overall organization and its vertical market. Understanding the organization and its market can aid in making design choices. Typical vertical markets are listed in Table 4.

TYPICAL VERTICAL MARKETS			
Communications E-Business Education	Financial General Business Government/Defense	Health Care Hosting Service Provider Network Outsourcers	Retail Transportation Wireless

Table 4: **Typical Vertical Markets**

Use an understanding of the business expectations in a vertical market to ensure a successful design. For example, each industry varies in the amount of downtime it can tolerate. As a general rule, financial organizations tolerate less downtime than organizations in the education vertical market. This can guide your design of polling and of escalation.

Obtaining Network Information

Gather information that provides the size of the network and how it is utilized to accomplish an organization's goals. A primary source for some of this information is an organization's RFI, RFP, or RFQ for the NCM deployment. The RFQ will normally contain details about a network's size and structure and deployment needs. Other sources of information include network diagrams and discussions with network administrators.

Obtain Network Diagrams

Figure 3 shows a typical network diagram. To aid in design, the network diagram should include the physical geography of the network including locations for the following:

- Network Operations Center (NOC) and LANs
- All routing, bridging, and switching devices
- Firewalls
- Lower speed WAN links such as T1 links
- Higher speed network technologies such as FDDI and Gigabit Ethernet

Important IP addresses and address ranges should be listed on the diagram. Device names and device naming conventions should also be included. Device, interface, and port naming conventions are vitally important when adding customized processing to the NCM deployment. Writing scripts to perform processing such as discovery post processing or advanced trap integration may only be practical in networks with naming conventions.

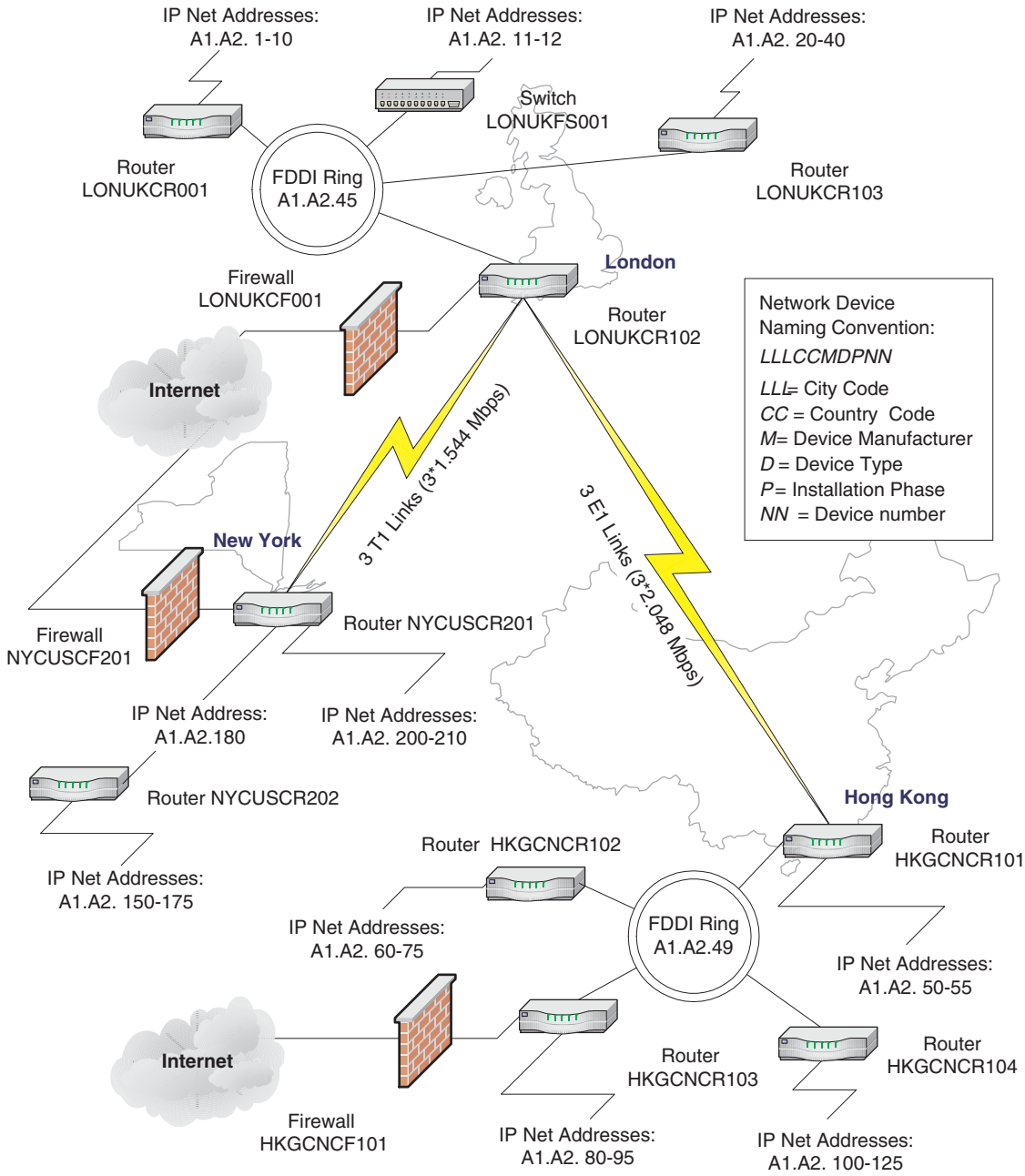


Figure 3: **Typical International Network Diagram**

Network Priorities

Organizations reflect their business priorities in their network organization. Certain parts of the infrastructure are more important and must be monitored more closely to ensure availability. This can affect polling cycles and threshold groups. Once again, the organization's RFP should describe their needs and limitations. Make notes on the network diagram to indicate the priorities that you uncover.

Identify the Types of Equipment in the Network

Create a list of all types of managed devices in your network and then compare the list with the NCM supported devices table.

Any SNMP-capable device will be discovered and monitored by NCM using generic SNMP MIB II instrumentation if it is not yet certified by Cisco: more specific instrumentation will not be available until the device is certified. Many uncertified devices can be field certified or, to provide the highest level of compatibility, certified in Cisco labs.

To certify a device, Cisco requires the following information:

- A MIB walk of the uncertified device using the IP Management Suite utility, **sm_snmpwalk**.
- Device containment information such as the IP addresses, number of cards, ports, and interfaces.
- A diagram showing how the device is connected to other devices in your network.
- MIB walks of all connected devices using **sm_snmpwalk**.

Other information specifically related to the use of the uncertified device in your network may also be required.

Cisco periodically releases SmartPacks for the CNCC NCM IP Management Suite that provide certifications of new devices. The device certifications are intended to be as extensive as possible, but they may be prioritized to meet the needs of the majority of NCM deployments. Contact Cisco Technical Support for more information.

Determine Requirements for Installing Software

Most organizations define some criteria for installing new software on their network. At a minimum, this might include software testing requirements.

In addition to responding to these requirements, plan on using a staging area before deploying. By staging the deployment, you can maintain a “clean” software distribution that does not include unwanted files, changes, and logs.

Integrating Existing Software with NCM

Integrating third-party software products with NCM requires the use of NCM adapters. Most integrations do one of the following:

- Exchange information. Determine the exact type of information (topology and/or events) that must be exchanged with any third-party software products.
- Allow access to the third-party software from the NCM Global Console. Some NCM adapters provide this capability as the Server Tools functionality.

Cisco has developed many adapters for use with NCM which may already support the integration requirements of your deployment. Itemize the integration requirements so that the suitability of existing NCM adapters can be assessed by Cisco. This guide covers only the integration capabilities provided by the CNCC NCM SNMP Trap Adapter (Receiver) and Syslog Adapter.

There are also extensive third-party software integration capabilities supported by other NCM adapters.

Determine Quantities of Network Devices

Determine the quantities of network devices that will be managed by the NCM deployment for two distinct purposes:

- The quantity of either ports and interfaces is vitally important for accurately sizing the NCM deployment. Sizing determines the number of CNCC Managers to install and the required hardware configuration for the platforms where these managers will be installed.
- The quantity of systems is needed for NCM volume licensing. The NCM discovery process will halt if the number of discovered systems or network adapters exceeds the licensed quantity.

In most cases, an organization's RFP or PFQ will estimate these quantities. This is the most common method of determining network devices: use the numbers from the RFP or RFQ as a starting point, and then improve the accuracy of those numbers by using common sense and by consulting with network administrators and other knowledgable personnel.

The most accurate method for obtaining the quantity of network devices is to use a Discovery Manager to inventory the network. Discovery Manager can be purchased with travelling license so that it can be installed on a laptop PC and then used to autodiscover an organization's network via a temporary connection. For more information on using Discovery Manager, see *Using Discovery Manager to Obtain Network Information* on page 93.

Refining the Estimate for Sizing an NCM Deployment

The network size determines the time it takes to complete discovery, the memory required, and the server hardware that should be selected to support CNCC Managers. Estimates of network size from network administrators are usually based on one of the following quantities:

- Quantity of ports and interfaces
- Quantity of routers and switches
- Quantity of devices

Ultimately, the most important quantity for sizing the server hardware in an NCM deployment is the total number of managed ports and interfaces. Managed ports and interfaces are monitored using SNMP and ICMP to determine status and connectivity.

After numerous deployments, Cisco has developed ratios that help estimate the number of managed ports and interfaces with a high degree of accuracy. These ratios provide conservative estimates, which is especially important in large and very large networks. Being conservative is imperative, because Cisco has determined that even in well-managed large networks, administrators can underestimate the number of ports and interfaces by 30% or more. Always use the multipliers in conjunction with validation, common-sense, and discussions with network administrators to improve the accuracy of the estimates.

Estimates Based on Ports and Interfaces

The most accurate method of determining network size is by retrieving the count of ports and interfaces from a network discovered by Discovery Manager.

If the network includes virtual routers, the count will include their interfaces in addition to the physical ports and interfaces. A virtual router is a software emulation of a router implemented within a physical router or switch.

Calculate the estimated managed ports and interfaces using the ratios of 90% managed for interfaces and 5% managed for ports:

ESTIMATED MANAGED PORTS AND INTERFACES	= 90% Interfaces	+ 5% Ports

For example, if the network has 2,300 interfaces and 18,000 ports, then calculate the managed ports and interfaces as follows:

ESTIMATED MANAGED PORTS AND INTERFACES	= 90% Interfaces	+ 5% Ports
	= ((90/100) * 2,300)	+ ((5/100) * 18,000)
	= 2,070	+ 900
	= 2,970	

All values that were less than one were rounded up in these calculations.

Estimates Based on Routers and Switches

When the number of ports and interfaces is not available, the next best method is to use the number of routers and switches to make an estimate:

- Obtain the total number of routers and the total number of switches in the network. Include virtual routers in this count of physical systems if they are used in the network. Cisco has developed two ratios: 25 interfaces per router and 60 ports per switch to represent the typical number of ports and interfaces for these devices. These ratios are typical in most NCM deployments.

  TOTAL PORTS = 60 * switches

  TOTAL INTERFACES = 25 * routers

- Using the total ports and total interfaces, estimate the number of managed ports and interfaces. Use the managed ratios for ports (5%) and interfaces (90%) to calculate managed ports and interfaces

  MANAGED PORTS = 5% total ports

  MANAGED INTERFACES = 90% total interfaces

- Add 30% to the estimate of managed ports and interfaces for uncertainty.

  ESTIMATED MANAGED PORTS AND INTERFACES = (managed ports + managed interfaces) + 30%

- For example, if a network has 95 routers and 305 switches, the estimate for the managed ports and interfaces is calculated as follows:

  TOTAL PORTS = 60 * switches
  = 60 * 305
  = 18,300

  MANAGED PORTS = 5% total ports
  = (5/100) * 18,300
  = 915

  TOTAL INTERFACES = 25 * routers
  = 25 * 95
  = 2,375

  MANAGED INTERFACES = 90% total interfaces
  = (90/100) * 2,375
  = 2,138

  ESTIMATED MANAGED PORTS AND INTERFACES = (managed ports + managed interfaces)+ 30%
  = (915 + 2,138) + 30%
  = 3,053 + ((30/100) * 3,053)
  = 3,053 + 916
  = 3,969

All values that were less than one were rounded up in these calculations.

Estimates Based on Devices (Level 2/Level 3)

The least accurate method for estimating the size of an NCM deployment uses only the total of level 2 and level 3 devices:

- Use the total of devices, including virtual routers, to estimate the number of ports and interfaces in the network. Cisco has developed the ratio of 50 to represent the typical number of ports and interfaces per device. This ratio assumes a split of about 30% routers and 70% switches in the network.

  TOTAL PORTS AND INTERFACES = 50 * devices

- Using total number of ports and interfaces, estimate the number of managed ports and interfaces. Assume that 35% of the total ports and interfaces are managed.

  MANAGED PORTS AND INTERFACES = 35% total ports and interfaces

- For example, if a network has 400 level 2 and level 3 devices, the estimate for the managed ports and interfaces is calculated as follows:

  TOTAL PORTS AND INTERFACES = 50 * devices
  = 50 * 400
  = 20,000

  MANAGED PORTS AND INTERFACES = 35% total ports and interfaces
  = (35/100) * 20,000
  = 7,000

All values that were less than one were rounded up in these calculations.

Note that due to the lack of specific information, this number is probably less accurate than the numbers produced by other methods and should always be discussed with network administrators.

Accounting for Sub Interface Monitoring

NCM permits performance monitoring of sub interfaces. If you intend to monitor the sub interfaces using the InCharge Performance Manager, each sub interface must be counted as an interface and added to your total of managed ports and interfaces.

The quantity of sub interfaces is very difficult to estimate: for example, some Cisco devices permit you to configure thousands of sub interfaces. If your network uses technologies such as frame relay, ATM, or ISDN, pay particular attention to the sub interface configurations. Consult network administrators to determine a reasonable maximum quantity of sub interfaces.

Accounting for Network Growth

Your NCM deployment design should account for network growth over the expected life of the design. The network growth rate will relate to the vertical market environment and the organization's plans, so the organization must provide you with growth estimates.

TOTAL MANAGED PORTS AND INTERFACES (P&I)	=	CURRENT MANAGED P&I	+	ADDITIONAL MANAGED P&I DUE TO GROWTH

Network growth planning can involve very complex calculations, but this is beyond the scope of this guide. For illustrative purposes, a simple method based on percentages is used here. For example, if a network with 5500 managed ports and interfaces was expected to grow by 10% per year, to calculate the size after one year:

TOTAL MANAGED PORTS AND INTERFACES (P&I)	=	CURRENT MANAGED P&I	+	ADDITIONAL MANAGED P&I DUE TO GROWTH
	=	5,500	+	(10/100) * 5,500
	=	5,500	+	550
	=	6,050 after one year		

To continue this example, if the design life is two years, then recalculate to add an additional 10% growth of the NCM deployment over the second year:

TOTAL MANAGED PORTS AND INTERFACES (P&I)	=	6,050	+	(10/100) * 6,050
	=	6,050	+	605
	=	6,655 after two years		

For the same network and two year design life, with an expected growth rate is 20%, the calculations are as follows:

TOTAL MANAGED PORTS AND INTERFACES (P&I)	= CURRENT MANAGED P&I	+	ADDITIONAL MANAGED P&I DUE TO GROWTH
	= 5,500	+	20% (5,500)
	= 5,500	+	1,100
	= 6,600 after one year		
	= 6,600	+	20% (6,600)
	= 6,600	+	1,320
	= 7,920 after two years		

All values that were less than one were rounded up in these calculations.

Determine Quantities of Devices for Licensing

NCM uses volume licensing to determine the size of the topology that Availability Managers are permitted to discover and manage in the deployment.

Volume licensing counts either or both of the following:

- All managed network adapters (ports and interfaces) in the topology.
- All managed systems in the topology. Systems include routers, switches, hubs, virtual routers, security devices, hosts, servers, desktop or laptop PCs, workstations, probes, terminal servers, printers, IP phones, wireless access points (WAPs), and CSUs/DSUs.

An accurate count of systems ensures that the deployment can manage all the devices appropriately. The NCM discovery process will halt if the number of discovered systems or network adapters exceeds the licensed quantity.

As the network grows and more systems are added, additional volume licenses can be obtained from Cisco.

Gather Network Security Information

Determine the level of security for the network that NCM will monitor so that NCM can be configured to a corresponding level of security. For example, the security needs of a network in a financial, defense, or health care vertical market may be greater than in the manufacturing vertical market. Enumerate security preferences, such as the use of passwords, encrypted password storage, and encrypted communications to guide you when configuring NCM security capabilities.

There are many security-related network features that will affect the NCM deployment. These include:

- Firewalls between parts of the NCM deployment. Appropriate NCM components must be able to poll the network, receive traps, and communicate with other NCM components. Certain TCP and UDP ports will need to be opened in the firewalls to facilitate these communications.
- Use of access lists. If access lists are used, the IP addresses of servers running NCM applications must be added to the access list of devices that will communicate with NCM. NCM must have full access to browse the MIBs of the devices.
- Use of SNMP versions and their respective security capabilities. The version of SNMP used to communicate with the network devices can provide dramatically different levels of security. With SNMP V1 or V2C, the security is provided through the use of SNMP community strings. To properly configure NCM, you must know the SNMP read community strings for all SNMPV1 and SNMP V2C devices that will be managed.
  For communications to devices using SNMP V3, the requirements are much greater: obtain values for these configuration parameters per SNMP V3 device:
  - SNMP V3 user name
  - SNMP engine ID (optional)
  - Authentication protocol
  - Authentication password
  - Privacy protocol and password (currently NCM does not support the use of a privacy protocol)
  - Context name, if used

What Other Network Features Affect NCM?

Other network features may affect the NCM deployment design. Consider the following questions when gathering information on the network:

- Does the organization require failover capabilities in network software?
- Is there an “out-of-band” network just for management information? For example, are certain ethernet ports just for management information? This is typical with some deployments in the financial and military/defense vertical markets.
- Who will use the Global Console and what are their needs? Who will be the operators and administrators? What are their access privileges? What network availability and performance information do they need to view?
- What are the issues related to network latency, bandwidth, and speed available for network management traffic?

Architectural Information Checklist

Use the following checklist to aid in gathering information for your architectural design. The checklist includes space for writing information; record the information here or in your design documentation. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105

ARCHITECTURAL INFORMATION CHECKLIST			
COMPLETE	TASK	DESCRIPITON	RELATED DOCUMENTATION
☐	Describe the organization's requirements and expectations.	Organization's vertical market: _____ (Reference to an organization's documentation) _____ _____ _____	*Determine the Organization's Requirements* on page 9
☐	Obtain network diagrams.	Ensure the diagrams include the locations of the following: • Network Operations Center (NOC) and LANs • Routing and switching devices • Firewalls • WAN links • High speed network technologies such as FDDI and Fast or Gigabit Ethernet In addition, important IP addresses and address ranges should be indicated.	*Obtain Network Diagrams* on page 10
☐	If possible, schedule and discover the network.	If you intend to use the Discovery Manager to inventory the organization's network, schedule a time to perform the process and then discover the network as scheduled.	*Obtaining Network Information* on page 10
☐	Describe the organization's network priorities.	Document these priorities in the Deployment Build Guide.	*Network Priorities* on page 12
☐	Get the organization's testing/acceptance requirements.	Your design may be required to meet test and acceptance requirements. Obtain any specifications that cover integration testing, user acceptance testing, and operational acceptance testing. You may be required to write an installation or deployment report that follows an organization's particular standards.	*Determine Requirements for Installing Software* on page 13
☐	Describe the organization's requirements for installing new software.	☐ Lab installation and testing ☐ Staging (*strongly* recommended) ☐ Preproduction deployment ☐ Shadow operation period (existing MoM still used) ☐ Other _____ Document these requirements and how the design meets them in the Deployment Build Guide.	*Determine Requirements for Installing Software* on page 13

ARCHITECTURAL INFORMATION CHECKLIST			
COMPLETE	TASK	DESCRIPITON	RELATED DOCUMENTATION
☐	List the products that currently monitor the network and will be integrated with NCM.	NCM's open architecture allows easy integration with third-party software. Many networks have at least a rudimentary network availability monitoring or a legacy system such as HP OpenView or IBM NetView. Document the products (including version) in deployment Build Guide.	*Integrating Existing Software with NCM* on page 13
☐	List device types to manage.	To ensure devices are certified in NCM, obtain a list of the manufacturers and models for all devices in the network. Document the types of managed devices in the Deployment Build Guide.	*Identify the Types of Equipment in the Network* on page 12
☐	Determine the number of managed ports and interfaces in the network.	Document all quantities and calculations used to determine the number of managed ports and interfaces in the Deployment Build Guide.	*Determine Quantities of Network Devices* on page 13
☐	Estimate potential growth in quantity of managed devices.	The NCM deployment must support potential network growth. Estimate the growth over a specific time period. Document the calculations in the Deployment Build Guide.	*Accounting for Network Growth* on page 18
☐	Estimate number of managed systems and network adapters for licensing.	The NCM deployment can only discover and manage the quantity of systems and network adapters that are licensed. Document the quantities in the Deployment Build Guide.	*Determine Quantities of Devices for Licensing* on page 19
☐	Describe the network security.	Describe security features such as the firewalls that will be between parts of the NCM deployment and if access lists are used. Obtain SNMP security parameter values for each device where they are used: for SNMP V1 and V2C, obtain community strings; for SNMP V3, obtain the user name, SNMP engine ID (optional), authentication protocol and password, privacy protocol and password (currently NCM does not support the use of a privacy protocol), and context name, if used. Document the security features in the Deployment Build Guide.	*Gather Network Security Information* on page 20
☐	List any other network requirements or features that may affect NCM.	Document the features in the Deployment Build Guide.	*What Other Network Features Affect NCM?* on page 21

3

Designing the NCM Deployment

This chapter provides guidelines for producing an initial design of the NCM deployment using the organization and network information that you have gathered. This design usually takes the form of a Solution Architecture Diagram and a Deployment Build Guide.

Documenting the Deployment

The most useful way to document the design of your NCM deployment is to create a Solution Architecture Diagram and record implementation details in a Deployment Build Guide.

The Solution Architecture Diagram

Based on the complexity of the NCM deployment, a Solution Architecture Diagram may actually be a set of diagrams documenting various levels of the architecture.

The diagram relates both physical and logical choices for your NCM architecture in an easily understood manner. This diagram graphically reflects your design choices and will be an important part of the review and approval process for your design.

The Solution Architecture Diagram should always include:

- A logical representation of the NCM components that will be installed
- Locations for each NCM component including the name and IP address of the host and the geographical location of the host
- Connections between NCM components and the ports that are used for communications
- Connections, including port numbers, between NCM and external sources such as networks and third-party software products

This chapter describes how to start the Solution Architecture Diagram. This diagram cannot be completed until the design is complete, so the design portion of the guide includes directions for adding information to the diagram.

The Deployment Build Guide

To record the specifics of the NCM deployment design and implementation, create a document called a Deployment Build Guide. As with the Solution Architecture Diagram, this chapter describes information that you should add to the Deployment Build Guide. The Deployment Build Guide should include the complete design and all installation specifications, validation results, and tuning activities.

Start the Deployment Build Guide by recording all the information that you have gathered on the network. Include a copy of the network diagram that you have already obtained. As you continue the deployment process, this guide will include recommendations for adding other information to the Deployment Build Guide.

Determine the Required Size of the NCM Deployment

The size of a NCM deployment is directly related to quantity of managed ports and interfaces that the deployment must support. Based on the values for managed ports and interfaces that you developed using the formulas in *Determine Quantities of Network Devices* on page 13, you can begin to determine how many Availability Managers and Performance Managers are needed.

As a first step, work with the network administrators to choose the platform equipment tier that is appropriate for the organization's resources and personnel. For example, familiarity with the operating system or with a vendor's equipment may direct the choice. Typical hardware for the equipment tiers and operating systems is listed in Table 5.

Operating System	Platform Equipment Tier			
	Small (1-2 low end CPUs, 1 GB RAM) *	Medium (2 CPUs, 2 GB RAM)	Large (2 CPUs, 4 GB RAM)	Extra Large (4 CPUs, 8 GB RAM)
Solaris	SunFire V120 or V210	SunFire V280	SunFire V280 with fastest CPU	SunFire V480 with fastest CPUs
HP-UX	HP rp2430 or rp2470	HP rp5430	HP rp7410 with fastest CPU	HP rp7410 with fastest CPUs
Linux	Any vendor, 1-2 Xeon 1.4GHz	Any vendor, 2 Xeon 2.0 GHz	Any vendor, 2 Xeon 2.4 GHz	Any vendor, 4 Xeon 3.0 GHz
Windows				
AIX	IBM pSeries 615 Model 6C3	IBM pSeries 650	IBM pSeries 650 with fastest CPU	IBM pSeries 655 with fastest CPUs
* The small tier configurations are less than the minimum requirements listed in the NCM installation guides. These configurations are not recommended unless you are very experienced with NCM deployments and have very reliable network size information. Contact Cisco Technical Assistance Center for the latest hardware equipment specifications.				

Table 5: **Typical Hardware for the Equipment Tiers**

Advantages of Larger Platform Equipment Tiers

The larger the tier, the larger portion of the network that a single CNCC Manager installed on that hardware can support. Advantages and disadvantages of using a single CNCC Manager on larger platforms are listed in Table 6.

ADVANTAGE:	DISADVANTAGE:
• Easier to maintain. • Split topology is not required. Splitting a topology into multiple domains is a complex process that must be updated as the network topology changes. • Saves bandwidth for discovery: separate Availability or Performance Managers must each discover the network. Multiple Availability Managers in a split topology must discover parts of the network twice. • If Availability and Performance Manager are installed as a single process, synchronizing the topology between them is not necessary.	• Scalability is limited. • Requires tuning. • Increased risk of encountering single-threaded bottlenecks. • The memory required by the process may reach or exceed operating system limits. • Requires expensive hardware.

Table 6: **Advantages and Disadvantages of a Single Process on Larger Platforms**

After choosing the equipment tier that best suits the organizational requirements, determine how many CNCC Managers are required. Dividing your estimate of the total managed ports and interfaces by one of the values in Table 7. Select the functionality required: Availability Manager, Availability Manager/Performance Manager (single process), or Performance Manager.

When Availability Manager and Performance Manager are installed as a single process rather than two separate processes on the same platform, the single process supports a more limited number of network device ports and interfaces. This is caused by the additional attributes that Performance Manager must track per port or interface (10 times more than Availability Manager). Performance Manager also tracks five more attributes per system.

SIZING CONSIDERATIONS		PLATFORM EQUIPMENT TIER			
		SMALL	MEDIUM	LARGE	EXTRA LARGE
Managed Ports and Interfaces (P&I) supported	AM only:	10,000	25,000	50,000	100,000
	AM/PM or PM only:	5,000	15,000	25,000	50,000
AM = Availability Manager; PM = Performance Manager					

Table 7: **Port and Interface Support by Platform Equipment Tiers**

For example, if NCM must support 30,000 managed ports and interfaces in an availability-only deployment, you would require:

- Three Availability Managers with each one on a small-tier platform
- Two Availability Managers with each one on a medium-tier platform
- One Availability Manager on a single, large-tier platform

Partitioning Networks

To avoid processing bottlenecks such as reconfiguration in a very large network, it may be necessary to partition the network. Splitting a very large topology into multiple NCM domains is a complex process. Cisco can perform this process for any deployment.

Multiple CNCC Managers on a Single Platform

When splitting the topology is necessary or desired, you can install multiple CNCC Managers on a single platform. Simply add the CPUs and memory requirements for each CNCC Manager you wish to install on a platform to determine if the platform can support the configuration.

Adding Information to the Solution Architecture Diagram and Build Guide

Include the appropriate number of Availability Managers and Performance Managers on the Architecture Solution Diagram. Enclose the managers in a box to represent the appropriate host as shown in Figure 4.

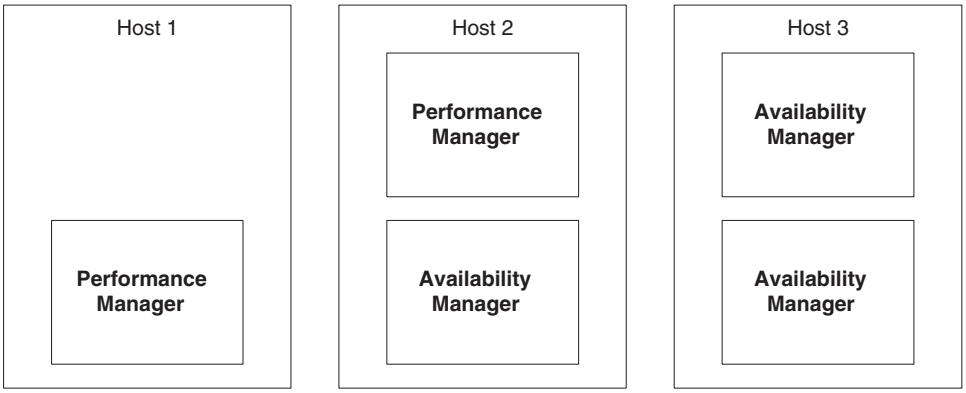


Figure 4: **Typical Start for Solution Architecture Diagram showing Hosts and Underlying Domain Managers.**

For the Deployment Build Guide, document equipment choices and start a table to document NCM components on each host.

Locating CNCC Managers and Platforms

In choosing locations for the platforms that support CNCC Managers, there may be restrictions on locations that are not related to network and application efficiency:

- Locating CNCC Managers might be based on geographical requirements. Some organizations might require all CNCC Managers to be based in a single Network Operations Center (NOC). Others might have the Service Assurance Manager in the NOC and the underlying CNCC Manager located in regional data centers.
- Locating CNCC Managers might be based on corporate organizational requirements. For example, organizations with distributed management might require that the NCM deployment is partitioned to support a portion of a network that is split along bureaucratic rather than technical lines.
- Locating CNCC Managers might be based on the network's security design. For example, if parts of the network are highly secured and SNMP or ICMP polling between these network segments is not allowed, separate Availability Managers would have to support each segment.

Polling and discovery are influenced by network speed and latency. If possible, consider network efficiency when locating CNCC Managers. Avoid configurations that require NCM to discover or poll large portions of the network across lower speed WAN links or other network bottlenecks. Consider placing CNCC Managers on higher speed LAN networks.

Add system names and CNCC Manager names to your Solution Architecture Diagram. Define IP addresses and dedicated port numbers when needed.

Establish a host naming convention and a CNCC Manager naming convention before you settle on any names. For example, a service provider using separate NCM domains to support each of their customers chose the to use the name of the customer as part of the name of any CNCC Manager that supported the customer.

Specify the locations for the hosts that support the IP Availability Manager and IP Performance Managers on the Architecture Solution Diagram as shown in Figure 5.

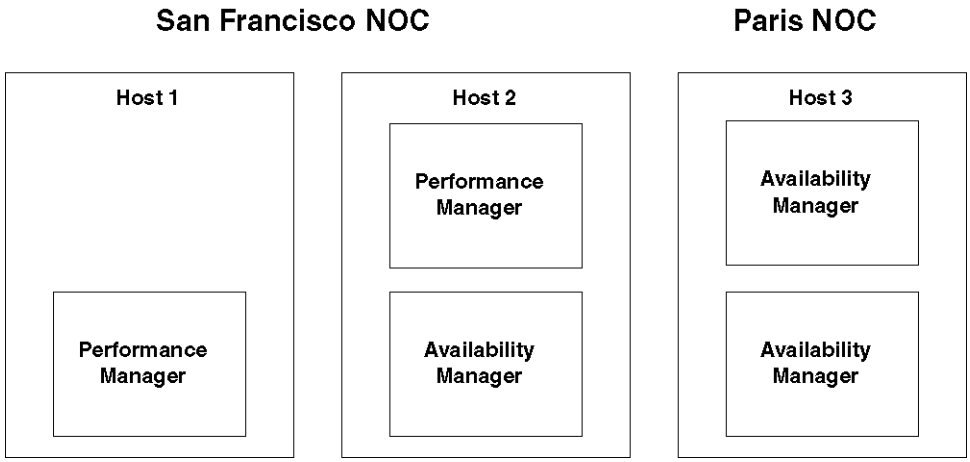


Figure 5: **Adding Locations to the Solution Architecture Diagram**

Considering Volume Licensing Configurations

In certain cases, you may use multiple license servers in your network for the same reasons that you split a topology or choose different locations for CNCC Managers: geographical requirements, corporate organizational requirements, or the network's security design. Using multiple license servers requires the corresponding number of NCM licenses from Cisco.

When multiple license servers are used, each NCM Domain will use blocks of licenses from a specific license server. Therefore, the license blocks must be divided among multiple licenses and the appropriate license must be deployed to each license server. Then, Availability and Performance Managers that rely on a specific license server will have the appropriate licenses to support the systems that they must manage.

Considering Security and Firewalls

Based on the security information you obtained earlier, you must plan designing solutions so that NCM can function properly in the network's security environment:

- For communication between CNCC Managers across firewalls, plan on opening a "hole" in the firewall for the NCM communications. Certain UDP and TCP ports must be opened for proper communications:
  - SNMP Polls: Port 161
  - SNMP Trap: Port 162
  - NCM Broker: Port 426
  - NCM License Manager: Port 1744
  - CNCC Manager: one port each, which can be configured.
  - NCM adapters, including SNMP Trap Adapter (Receiver) and Syslog Adapter: See *Deploying Syslog Processing* on page 61 and *Designing Trap Processing* on page 53.

- If access lists are used, plan on deploying the IP addresses of hosts that include CNCC Managers to the access list of devices that will be managed. NCM must have full access to browse the MIBs of the devices. (The specific MIBs are listed in the *Network Connectivity Monitor IP Availability Manager User's Guide* and/or the *InCharge IP Performance Manager User's Guide*.) Depending on the network size and complexity, this may require scheduling to obtain support from the organization's network personnel.
- You must have a listing of SNMP versions and related security parameter values that are used by specific devices in the organization's network. Due to security concerns, it may not be appropriate to include them in the Deployment Build Guide.

In addition, consider the level of security to configure for NCM applications. The NCM security mechanisms support various levels of user authentication and both authentication and encrypted communication between NCM applications. Ensure that you understand the capabilities described in the *Network Connectivity Monitor System Administration Guide* and then choose a level of security that is appropriate for the deployment.

Considering High Availability Configurations

Failover is a complex configuration that currently requires aid from Cisco. Consult with Cisco if your installation requires this capability.

Designing for Overlapping (Duplicate) IP Networks

NCM allows service providers who offer managed IP network services to centrally manage the private IP networks of customers who use identically-numbered IP address spaces. Enterprise users facing similar issues due to acquisitions of new networks can also use this ability. For more information, see *Managing Overlapping IP Networks With NCM* on page 97.

Designing Acceptance Tests

Acceptance tests may be required for different portions of NCM functionality. Be aware of the requirements and develop acceptance criteria with the aid of the network administrators and other organization personnel. Include all necessary acceptance tests in the Deployment Build Guide for the NCM deployment. At a minimum, you must develop completion criteria that the organization's project managers approve. Document these completion criteria in the Deployment Build Guide and use them in validation.

Solution Architecture Diagram Checklist

Use the Solution Architecture Diagram to document your initial overall design of the NCM deployment. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105

SOLUTION ARCHITECTURE DIAGRAM CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	List important device quantities on the Solution Architecture Diagram and in the Deployment Build Guide.	Start the Solution Architecture Diagram by listing the totals for Routers, Switches, Hubs, Bridges, Hosts, Ports and Interfaces. Include expected growth rate and estimates for managed ports and interfaces. Also document the quantities in the Deployment Build Guide.	*Documenting the Deployment* on page 25
☐	Choose a tier size for platforms supporting CNCC Managers.	Small (P&I:10K/AM or 5K/AM PM) Medium (P&I:25K/AM or 15K/AM PM) Large:(P&I:50K/AM or 25K/AM PM) Very Large:(P&I:100K/AM or 50K /AM PM) Document the choice in the Deployment Build Guide.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Determine quantity of NCM IP Managers required.	Include representations on the Solution Architecture Diagram.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Document equipment supporting NCM components.	Document the hardware and operating system supporting each of the NCM components. Start a chart for each host in the Deployment Build Guide and list the NCM components on the host.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Locate the hosts supporting the NCM components.	Document choices on the Solution Architecture Diagram and in the Deployment Build Guide.	*Locating CNCC Managers and Platforms* on page 30

SOLUTION ARCHITECTURE DIAGRAM CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine license server and licensing configuration requirements.	Document requirements on the Solution Architecture Diagram and in the Deployment Build Guide.	*Considering Volume Licensing Configurations* on page 32
☐	Determine security requirements.	Document requirements in the Deployment Build Guide.	*Considering Security and Firewalls* on page 32
☐	Is Failover Capability Required for NCM?	☐No ☐Yes: Contact Cisco. Document choices on the Solution Architecture Diagram and in the Deployment Build Guide.	*Considering High Availability Configurations* on page 33
☐	Determine if overlapping IP networks are used.	Document needs in the Deployment Build Guide.	*Designing for Overlapping (Duplicate) IP Networks* on page 33
☐	Plan acceptance tests and completion criteria.	Document in the Deployment Build Guide as each portion of NCM functionality is designed. Use them in validation.	*Designing Acceptance Tests* on page 34

4

Planning for Discovery

This chapter provides guidelines for designing the discovery process for your NCM deployment. Before beginning the design of your discovery process, read the comprehensive description in the *Network Connectivity Monitor IP Discovery Guide*.

Designing Discovery

Discovery is the process of creating a representation of the managed network topology within a Domain Manager's repository. Data is collected by SNMP to create instances of the managed systems, their dependencies, and their internal components. Discovery is an expensive process in terms of required processing and network resources, so making the appropriate choices during design is imperative. The NCM discovery implementation is very flexible and allows many variations.

To simplify discovery design, consider discovery in two separate stages:

- Initial topology discovery
- Maintenance and subsequent topology discovery

Initial Discovery

The initial discovery of the network topology is usually the most time consuming and expensive in terms of network resources, so scheduling the initial discovery is very important. Accurately predicting the duration of the initial discovery is virtually impossible due to network variance, so assume the discovery will take a considerable period during this initial discovery.

This is due to the time-consuming process of creating objects with defined relationships for every device in the topology. Discover the network over a long period of low utilization, such as a weekend or holiday. Plan on this even if NCM is deployed in a test environment, because discovery can be adversely affected by heavy network utilization.

The initial discovery requires use of one of the following methods:

- Use a comprehensive seed file without autodiscovery. This method provides the greatest level of control of the discovery process with the simplest discovery design. This is the quickest method for discovering a network because all systems are discovered using the IP addresses or system names that are already in the seed file. Typically, this is the method used in well-documented networks by organizations such as service providers. A comprehensive seed file can only be created if the network topology information is complete and accessible.
- Use autodiscovery with an agent or seedfile. This method requires more resources than the other methods. Normally, autodiscovery is used for a network that has limited documentation, emphasizes flexibility, or is constantly in flux. This method requires appropriate autodiscovery filters and configuration. Consider using a Cisco Discovery Protocol (CDP)-enabled device as an agent or in the seed file when possible to improve autodiscovery processing. Autodiscovery can take advantage of CDP tables in one of its probes. At the very least, use a device that is not at a network edge as an agent. Note that autodiscovery can not be used to discover devices that use SNMP V3.

When Should You Use AutoDiscovery?

Other than scheduling, the most basic choice in the discovery design is whether or not to use autodiscovery. With autodiscovery, NCM automatically discovers your network from one or more seed systems. During an initial discovery, using autodiscovery can be timesaving, particularly when topology information is incomplete.

With appropriate discovery filtering, autodiscovery is very efficient and requires little in additional resources. In addition, autodiscovery can be limited and controlled by specifying manual addition of discovered systems to the topology and setting an appropriate topology system limit.

But using autodiscovery is not advised in the following deployment configurations:

- New network devices are constantly being phased in. During the phase in period, the devices are accessible on the network, although not fully operational and are being tested. Though you intend to eventually add the devices to the topology, adding the devices at this point would cause spurious notifications or fill the device pending list and obscure devices that should be discovered.
- Specific devices are accessible on the network but will never be managed. For example, ISPs might want to discover a router and its interfaces, but not the devices connected to the router from the ISP's client side. If the connecting devices do not follow a naming convention or can change without notice, it may be very difficult to define autodiscovery filters and exclude filters that ensure that the devices are not discovered or placed in the pending list.
- The network uses many SNMP read community strings. Currently, autodiscovery allows four and you can increase the number by reconfiguring *discovery.conf*, but in some situations dozens or more strings may be used and filtering becomes impractical. In addition, you may not want to use the community strings in a secure environment—devices may write community strings to syslog files when the devices are polled with strings do not match.
- The network uses an inventory database and devices are being commissioned through the use of the database.

In addition, autodiscovery cannot be used with devices that use SNMP V3.

Using Autodiscovery During Initial Discovery

Autodiscovery is particularly useful when topology information is incomplete. Even in network environments where autodiscovery is not recommended, autodiscovery can sometimes be used during an initial discovery to inventory the network and create a comprehensive topology. After the initial discovery, autodiscovery could be disabled so that it is not triggered by subsequent full discoveries or pending list discoveries.

If you determine it is inappropriate to use autodiscovery on a regular basis, but want to take advantage of autodiscovery during the initial discovery, configure autodiscovery carefully. Ensure that the autodiscovery filters and the exclusion filters in the *discovery.conf* file are properly configured. Consider using the *Ask before adding new systems* option with each discovery filter to ensure the greatest control of the discovery process.

When the discovery process is complete, review the topology and discover appropriate devices on the device pending list. Remember that discovering devices on the pending list will trigger autodiscovery to restart. After completing discovery, create a comprehensive seed file using **sm_tpmgr --dump-agents**.

If necessary, disable autodiscovery after the initial topology discovery is complete.

Topology Maintenance and Subsequent Discovery

After the initial discovery of the network topology, you must choose a schedule for subsequent discovery processes to maintain an accurate topology:

- Full discovery of the existing topology should be scheduled to occur at least once per week. Once again, scheduling full discovery during a long period of low network utilization such as a weekend is very important.

  For example, a large multinational bank discovers devices for a domain on Saturdays at 1:00 pm. Specific times are scheduled using **cron** or **sm_sched** to invoke **sm_tpmgr --discover-all** for the domain. The Global Console allows you to specify an interval between full discoveries, but not a specific time.

- Pending discovery should be scheduled to occur at least once per day. This is the discovery of any devices that were placed in the Pending Devices list. Like full discovery, schedule the pending discovery during a period of low network utilization. The duration of a pending discovery is usually much shorter than full discovery, so schedule it during a relatively idle work shift.

  For example, a regional service provider discovers pending devices on weekdays at 2:00 am. As with full discovery, specific times are scheduled using **cron** or **sm_sched** to invoke **sm_tpmgr --discover-pending** for the domain. The Global Console only allows you to specify an interval since the pending list was last discovered, but not a specific time.

Note: If you use **cron** or **sm_sched** to schedule full and pending discoveries, uncheck the Enable Full Discovery option and use 99 days for Discover Pending Interval at the Domain Manager Administration Console.

Running the discovery processes more often will provide a more accurate network topology, but you must consider both your needs and the cost in terms of resources. If your network changes more often than the recommended discovery schedules, then you must shorten the time between discoveries. Typical network changes include anything from hardware changes, such as adding cards or devices, to configuration changes such as reassigning IP addresses or modifying a VLAN.

Adding New Systems to an Existing Topology

Remember that new devices will only be added to the topology if you do one of the following:

- Enable autodiscovery and create an appropriate filter configuration for automatic addition. New systems are NOT automatically found during discovery (or added) unless autodiscovery is enabled. If enabled, autodiscovery occurs *whenever* either a full discovery occurs or a pending device is successfully discovered. When full discovery takes place, all the devices already in the topology will be probed during discovery in an attempt to autodiscover new devices. If a topology is unstable, autodiscovery is a very useful feature.
- Use the add agent or import from seedfile functions at the Global Console to discover new devices by name or IP address. Using comprehensive seed files is the typical way to add systems to networks with stable topologies that are well documented. Service providers who manage devices under contract will typically use this approach to avoid discovering and managing devices that they are not paid to manage.

These two methods of adding new devices can be used separately or combined. When combined, adding a system manually using a seedfile or add agent will trigger autodiscovery on the system if it is successfully discovered.

Controlling Autodiscovery with Filters

Control autodiscovery with autodiscovery filters. Use the filters to add devices automatically or select the **Ask before adding new systems** option. When selected, this option places new devices in the Pending Devices list to be reviewed and then added manually.

You can further customize autodiscovery by making some filters automatic and some manual when adding systems to the topology. For example, automatically add routers and switches on subnets in a new phase of network expansion but continue to manually add all other devices. This use of autodiscovery filtering works best in networks that have consistent, well-defined naming conventions.

Autodiscovery filters are inclusive filters, so to prevent specific devices from being discovered, you must configure exclude filters. Use the ipExlcudeList in the *discovery.conf* file to create these filters.

Note that seed file and agent devices are not subject to the autodiscovery filters, but devices found by autodiscovery probing of the seed file or agent devices will be subject to the autodiscovery filters.

Automating Manual Discovery

Using the seed file or add agent without autodiscovery provides complete control over the discovery process while avoiding the additional autodiscovery probing. Though this method is usually a manual one, you can automate it: first, generate a seed file from an inventory system on a regular basis as the network changes. Then, import the file by invoking **sm_tpmgr --seed=<*seedfile*>** for the domain using **cron** or **sm_sched**. Other more sophisticated approaches can also be programmed.

Discovery and Third-Party Software

Another way to add systems to the topology without discovering them is to import topology into NCM from third-party software. CNCC NCM can import topology information from many sources, including HP OpenView NNM and IBM/Tivoli Netview. This method requires an NCM adapter such as the Adapter for HP OpenView Network Node Manager or the Adapter for IBM/Tivoli NetView described in the *InCharge IP Adapters User's Guide*. To use these adapters, you must define at least one discovery filter. Ensure the filter is defined broadly enough to accept the possible device names and addresses that are provided by the third-party software.

Discovery and Security

When planning discovery, consider the following network security-related features:

- Firewall Ports: If there is a firewall between any portions of the management infrastructure, certain TCP and UDP ports in the firewall must be opened for proper communications during discovery and for other NCM communications:
  - SNMP polls: 161
  - SNMP traps: 162
  - NCM Broker: 426
  - NCM License Manager: Port 1744
  - CNCC Manager: one port each, which can be configured.
  - NCM adapters, including SNMP Trap Adapter (Receiver) and Syslog Adapter: See *Deploying Syslog Processing* on page 61 and *Designing Trap Processing* on page 53.

  Document the ports that are opened in the Deployment Build Guide.
- Use of access lists. If access lists are used, the IP addresses of servers running NCM applications must be added to the access list of devices that will communicate with NCM. NCM must have full access to browse the MIBs of the devices.
- Use of SNMP versions and their respective security capabilities. The version of SNMP used to communicate with the network devices can provide dramatically different levels of security. With SNMP V1 or V2C, the security is provided through the use of SNMP community strings. To properly configure NCM, you must know the SNMP read community strings for all devices that will be managed.
  For communications to devices using SNMP V3, the requirements are much greater: in addition to the community string, obtain values for these configuration parameters per SNMP V3 device:
  - SNMP V3 user name
  - SNMP engine ID (optional)
  - Authentication protocol
  - Authentication password

- Privacy protocol and password (currently, NCM does not support the use of a privacy protocol)
- Context name, if used

Discovery and Certified Device Types

To ensure devices are certified in NCM, obtain a list of the manufacturers and models for all devices in the network. In some cases, it might be necessary to obtain a device MIB for certification. Cisco certifies many devices, but some may be specialty devices for the particular organization (for example, private MIBs for SNMP agents in point of sales terminals) Document the types of devices to manage in the Deployment Build Guide.

Discovery and the Domain Name System

NCM relies on DNS as part of the automatic name resolution process for devices discovered in the topology. If DNS is not properly configured, the discovery process can be slowed considerably as NCM waits for DNS requests to time-out.

Both the forward *and* the reverse DNS lookup files must be complete and properly configured. Improper configuration of the reverse lookup pointer records is a common problem. As part of the discovery design, determine if the network administration will ensure the accuracy of the DNS configuration.

If you cannot rely on DNS, you must use the seed file to name devices in your network. This requires that you set the value of NameFormat in the *discovery.conf* file to “TM_USESEEDNAME”. Plan on creating a comprehensive seed file that includes all necessary names. In this configuration, if autodiscovery is enabled, seed names are not available for devices that are autodiscovered. The IP address will be used as the name for the autodiscovered device.

Advanced Discovery Post-Processing

If needed, customized processing can be added to discovery post-processing using ASL rulesets. Additional post-processing steps are added by editing one of the supplied ASL rule sets. Each ASL rule set is configured in such a way that it is invoked during a specific phase of the discovery:

- Before a full discovery (*custom-start-fulldisc.asl*)
- Before a system is discovered (*custom-start-system.asl*)
- After a system is discovered (*custom-end-system.asl*)

- Before discovery post-processing (*custom-start-post.asl*)
- After discovery post-processing (*custom-end-post.asl*)

Typical applications of custom discovery post-processing include:

- A post-processing script could unmanage devices in IP address ranges or with specific name patterns before post-processing. If there are groups of IP Addresses that are not normally reachable, a list of IP ranges or some matching criteria could be used during post processing to ensure NCM will not unnecessarily ping these addresses. Devices can also be unmanaged individually from the Global Console.
- A post-processing script could rename devices after a system is discovered.

Discovery Design Checklist

Before discovering the network using NCM, the requirements in the following checklist must be completed. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
Initial Discovery			
☐	Define a method for the initial topology discovery.	☐ Use a comprehensive seed file without autodiscovery. ☐ Use autodiscovery with an agent or seedfile. Document the method in the Deployment Build Guide.	*Initial Discovery* on page 38
Topology Maintenance and Subsequent Discovery			
☐	Define a schedule for Full Discovery.	Define a regular schedule for full discovery. Choose a time of relative inactivity. Document the schedule in the Deployment Build Guide. Include *crontab* or *sm_sched* control file entries if used.	*Topology Maintenance and Subsequent Discovery* on page 40
☐	Define a schedule for Pending Discovery.	Define a regular schedule for pending discovery. Choose a time of relative inactivity. Document the schedule in the Deployment Build Guide. Include *crontab* or *sm_sched* control file entries if these utilities are used.	*Topology Maintenance and Subsequent Discovery* on page 40

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine if Autodiscovery is appropriate.	Document choice in the Deployment Build Guide.	*Topology Maintenance and Subsequent Discovery* on page 40
☐	Choose a method for adding devices to the topology.	☐ Agent without autodiscovery. ☐ Seed file without autodiscovery. ☐ Use autodiscovery with an agent or seedfile. Document choice in the Deployment Build Guide.	*Adding New Systems to an Existing Topology* on page 41
☐	Prepare Seed File or Choose Agent.	If a seed file will be used to add devices to the topology, obtain a list of devices with names or IP addresses. Document how to obtain the list or the location of the list in the Deployment Build Guide. If an agent will be used instead, document the IP address or name of the agent.	*Topology Maintenance and Subsequent Discovery* on page 40
☐	Define Autodiscovery Filters.	If autodiscovery is enabled, configure autodiscovery filters. These are inclusive filters that add devices to the topology. Document the autodiscovery filter criteria in the Deployment Build Guide.	*Controlling Autodiscovery with Filters* on page 41
☐	Define an Exclude Filter.	To exclude specific devices, use the exclude filter in the *discovery.conf* file. This simplifies creation of the autodiscovery filters. Document exclude filter entries in the Deployment Build Guide.	*Controlling Autodiscovery with Filters* on page 41
☐	Obtain SNMP security parameters per device.	NCM Domain Managers use SNMP to poll the device agents. In order to do this, the Domain Manager needs the appropriate security information for the SNMP version: V1 and V2C use READ community strings for every device that will be managed; V3 uses the user name, SNMP engine ID, authentication protocol and password, privacy protocol and password and the context name. These parameters will be needed during discovery. Document in the Deployment Build Guide if permitted.	*Discovery and Security* on page 43
☐	Open necessary firewall ports.	If there is a firewall between any portions of the management infrastructure, certain TCP and UDP ports in the firewall must be opened for proper communications: • SNMP polls: 161 • SNMP traps: 162 • NCM Broker: 426 • NCM License Manager: 1744 • CNCC Managers (1 per manager): configurable • NCM adapters, including SNMP Trap Adapter (Receiver) and Syslog Adapter: configurable Document the ports that are opened in the Deployment Build Guide.	*Discovery and Security* on page 43

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Provide access to network devices to manage.	For each device that NCM will monitor, the device's access list must include the IP address of the hosts where CNCC Managers are installed. NCM must have full access to browse the MIBs of the devices. Document in the Deployment Build Guide.	*Discovery and Security* on page 43
☐	Ensure DNS is properly configured.	For NCM to correctly name devices in its topology, the DNS needs to be clean (proper forward and reverse lookup). If DNS is not used, use of an */etc/hosts* file or not doing any name resolution at all can be considered.	*Discovery and the Domain Name System* on page 44
☐	Determine if Discovery post processing is required.	Determine if discovery post processing using ASL rulesets will be used. Document in the Deployment Build Guide.	*Advanced Discovery Post-Processing* on page 44
☐	List unreachable IP Addresses	If there are groups of IP addresses that are NOT normally reachable, assemble a list of IP ranges or some matching criteria so NCM will not unnecessarily ping these addresses. Document these addresses in the Deployment Build Guide.	*Advanced Discovery Post-Processing* on page 44

5

Designing Polling and Thresholds

This chapter describes polling and thresholds design considerations. For a complete discussion of polling and threshold groups, parameters, and default values, see the Groups and Setting chapters of the *Network Connectivity Monitor IP Availability Manager User's Guide* and/or *InCharge IP Performance Manager User's Guide*.

Designing Polling and Thresholds

Organizations reflect their business priorities in their network organization. Certain parts of the infrastructure are more important and must be monitored more closely to ensure availability and performance. Critical systems may need to be polled more frequently to uncover problems sooner. This is reflected in polling and threshold groups.

Settings and groupings are determined by assessing the operational requirements for the delivery of timely analysis data and the impact of polling on network infrastructure components.

Modifying Polling and Polling Groups

Before modifying any polling groups, determine if the organization enforces any limitations on polling frequency. Note that some limitations may be based on CPU utilization limits or router traffic limits that no longer apply in the current network. Be sure that you understand how the limitations were determined and, if necessary, suggest that network administrators modify the limits.

Make changes to polling by changing existing polling groups or by creating new groups. Before modifying polling parameters for existing polling groups, ensure the changes are appropriate for all members in the polling group. If the polling changes affect only a limited number of devices and the current polling groups adequately support most devices, then create new polling groups for the devices with the unique polling requirements.

When creating new polling groups, consider device types and roles such as core devices and edge devices. Consider functional roles such as routers supporting particular organizations or departments. For example, a Service Provider could provide various support levels that include different polling cycles. The Service Provider could charge more for more frequent polling assuming that it will result in an earlier resolution of root cause analysis.

Whenever new groups are created with more specific matching criteria than the existing groups, pay particular attention to the polling group priority. More specific groups should always be higher in priority than similar less specific groups because the first match is always used: a device is compared against each polling group's matching criteria and when a set of criteria corresponds, that group's polling parameters are used. No further comparisons are performed for the device.

Note that whenever you increase the polling time-out, pay attention to the effect on the cumulative value for the polling time-out. On each successive retry, the polling time-out is doubled. The cumulative polling time-out should always be less than the polling interval or the device could be polled excessively. Consider reducing the number of retries when increasing the polling time-out.

Considering Network Latency

Polling groups are especially important in multi-site environments from a single IP Availability Manager or Performance Manager. You must consider connection speeds and latency that may differ based on network location.

Refer to the network diagram to locate WAN links that NCM polls must cross to reach devices. Based on the latency of the links, you may have to adjust the polling cycles. These types of modifications are difficult to perform accurately before the actual deployment because the traffic load across the links that NCM polls may not be readily available. Expect to revisit the polling settings during the validation and tuning phase.

If latency becomes an issue that cannot be overcome with realistic polling groups, you must reconsider your design. If the network includes many lower speed links, it may be necessary to physically relocate one or more CNCC Managers or even increase the number of CNCC Managers to reduce the latency.

Modifying Threshold Values and Threshold Groups

Judicious choice for thresholds can allow proactive rather than reactive network management, but poor choices can result in hundreds of inappropriate notifications.

It is difficult to adjust performance thresholds before gaining experience with the deployment and the network components being monitored.

Analyze failures of network components to determine if performance degradation was a precursor to failures. Based on the analysis, adjust the thresholds accordingly. This analysis should become a constant ongoing process with constant adjustment as performance notifications and failures occur.

In many cases, threshold values may be adjusted in response to inappropriate notifications.

Notifications from backup interface support thresholds and dial-on-demand interface support thresholds are some of the more common issues as these threshold groups are particularly unique to an individual network and its administrators.

Polling and Threshold Checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

POLLING AND THRESHOLD CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine if polling changes are needed.	Design polling groups based on importance of network device performance both to the network and to the various parts of the organization. Also consider network latency to determine if changes are needed. Document choices in the Deployment Build Guide.	*Modifying Polling and Polling Groups* on page 50
☐	List all polling changes by polling group.	Modify polling parameters based on importance of network device performance. Additional modifications may be necessary if polling does not present an accurate picture of network availability during validation. Document new polling parameters in the Deployment Build Guide.	*Modifying Polling and Polling Groups* on page 50
☐	Determine if threshold changes are needed.	Design threshold groups based on importance of network device performance both to the network and to the various parts of the organization. Document choices in the Deployment Build Guide.	*Modifying Threshold Values and Threshold Groups* on page 51
☐	List all threshold changes by threshold group.	Modify threshold parameters based on the expected effect of degraded performance on network operations. Additional modifications may be necessary during validation and as the organization gains experience with the performance indicators. Document new threshold parameters in the Deployment Build Guide.	*Modifying Threshold Values and Threshold Groups* on page 51

6

Designing Trap Processing

NCM includes very flexible and capable trap processing. This chapter describes the considerations required to deploy effective NCM trap processing.

Recommended Trap Processing Design

Though there are many possible trap configurations, we recommend the trap processing design as shown in Figure 6. This configuration relies on two instances of the CNCC NCM SNMP Trap Adapter (Receiver) to handle trap processing and performs well under the stress of high volumes of traps.

The first instance (Instance 1) of the adapter is configured as a “trap exploder” which receives and forwards traps. In this configuration, the trap exploder does not process traps into notifications or use any ASL scripts for sophisticated trap processing. The trap exploder’s sole function is to filter and forward traps:

- Availability Manager-required traps are forwarded to Availability Managers.
- Performance Manager-required traps are forwarded to Performance Managers.
- Useful traps are forwarded to second instance (Instance 2) of the CNCC NCM SNMP Trap Adapter (Receiver) for processing into notifications. Useful traps are traps that are meaningful to the administrators of the network.
- Useless or unneeded traps are forwarded to a nonexistent address to reduce overhead at the CNCC NCM SNMP Trap Adapter (Receiver). If the adapter receives a trap that is not processed or forwarded, an error message is logged, so this practice impacts processing.

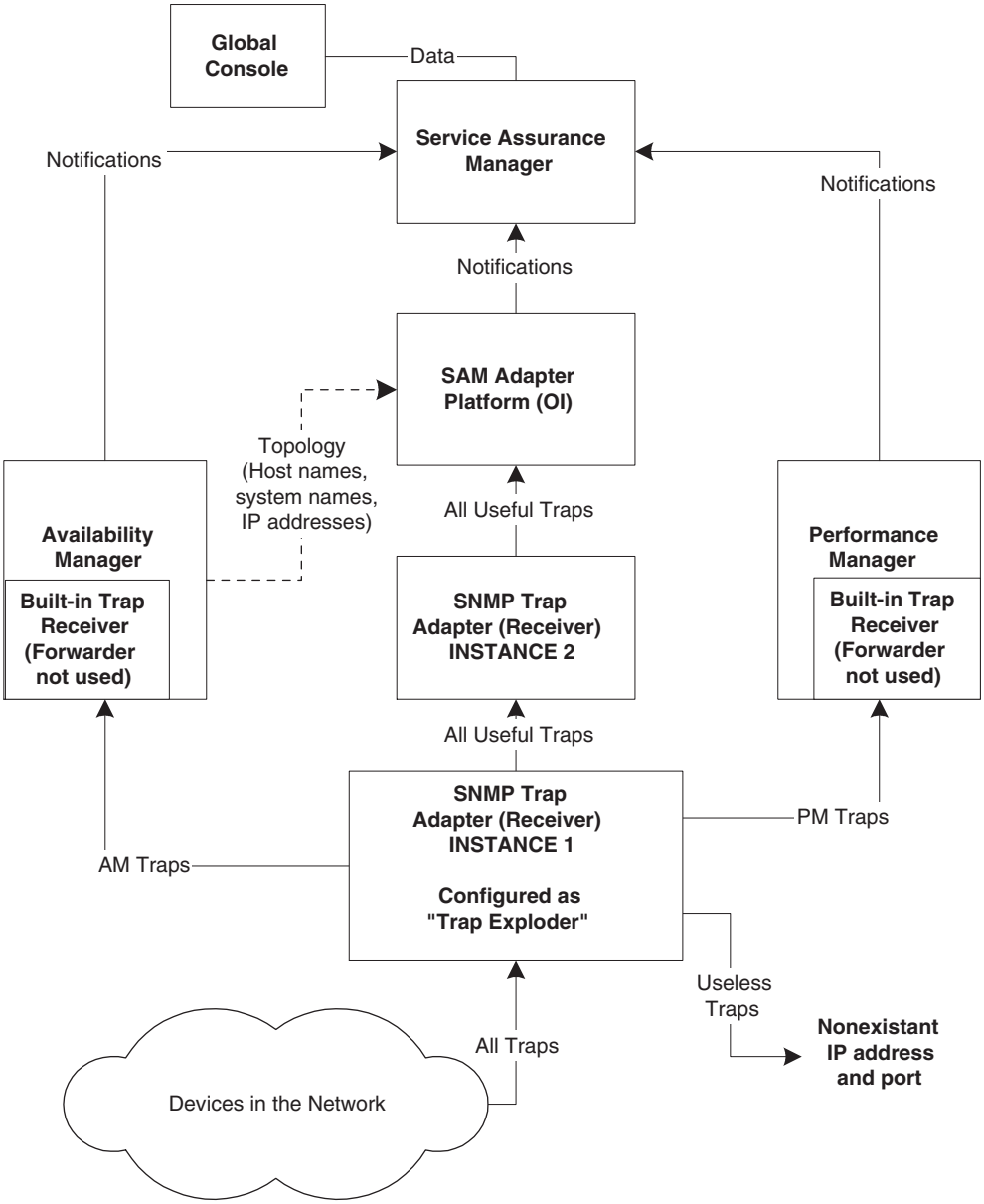


Figure 6: **Recommended Trap Processing Design**

The instance 2 of the CNCC NCM SNMP Trap Adapter performs the typical processing of traps into notifications and may invoke ASL scripts for advanced processing. This instance does not forward any traps.

The two SNMP Trap Adapter instances are invoked using different configurations. The typical configuration when the instances are on a single host is the following:

- The trap exploder (instance 1 of the SNMP Trap Adapter) uses ***BASEDIR****/smarts/local/conf/trapd/trapd.conf*. (In this case, ***BASEDIR*** is the location where the Service Assurance Management suite is installed.) This *trapd.conf* file includes trap forwarding statements and indicates the port to use when listening for traps.
- Instance 2 of the SNMP Trap Adapter processes traps into notifications and uses ***BASEDIR****/smarts/local/conf/icoi/trapd.conf* and ***BASEDIR****/smarts/local/conf/icoi/trap_mgr.conf*. (As with the trap adapter, ***BASEDIR*** is the location where the Service Assurance Management suite is installed.) This *trapd.conf* configuration file does not include trap forwarding statements. The *trap_mgr.conf* file includes definitions for all traps that will be forwarded as notifications.

Note: The *trapd.conf* files installed with IP Availability Manager and IP Performance Manager can be configured to permit Availability Manager and Performance Manager to forward traps using their built-in trap receivers. This capability should not be used except for testing deployments or when migrating traps from multiple locations to one destination.

For a complete description of the CNCC NCM SNMP Trap Adapter (Receiver) see the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide*.

For split topologies in a Service Provider (SP) environment, a variation on the recommended design is shown in Figure 7. In this design, individual domains support different customers of the SP. The SP provides each customer with a Global Console that monitors only an individual customer's portion of the network. A common trap exploder forwards Availability Manager-related traps to the appropriate domain. If the trap processing demands are too high to support the two SNMP Trap Adapter (Receiver) instances on a single host, install a CNCC NCM SNMP Trap Adapter (Receiver) and CNCC NCM SAM Adapter Platform pair on separate hosts and configure one pair as a trap exploder.

Batching to Improve Performance

In a deployment where a high frequency of traps is expected, plan on using the batching capability of the CNCC NCM SNMP Trap Adapter (Receiver) to improve performance of clients that process the notifications. The *BATCH_NOTIFY_INTERVAL* in the *trap_mgr.conf* configuration file determines the length of the interval. It may be necessary to fine tune this value under the typical trap load, so plan on monitoring the client performance and adjusting this value.

Listening for Traps

The SNMP Trap Adapter (Receiver) configured as the trap exploder should listen for traps on the standard port that network devices use when forwarding traps. Typically, this is 162 for UNIX: by default, NCM uses 9000 for Windows.

If another application is listening for traps at this port, the application should be moved and the trap exploder can forward needed traps to the application's new location. The CNCC NCM SNMP Trap Adapter (Receiver) is usually a better choice for forwarding traps than other third-party software applications because the adapter can be limited to the forwarding function.

The second instance of the SNMP Trap Adapter (Receiver) can listen on any port, but the trap exploder must be configured to forward the appropriate traps to this port.

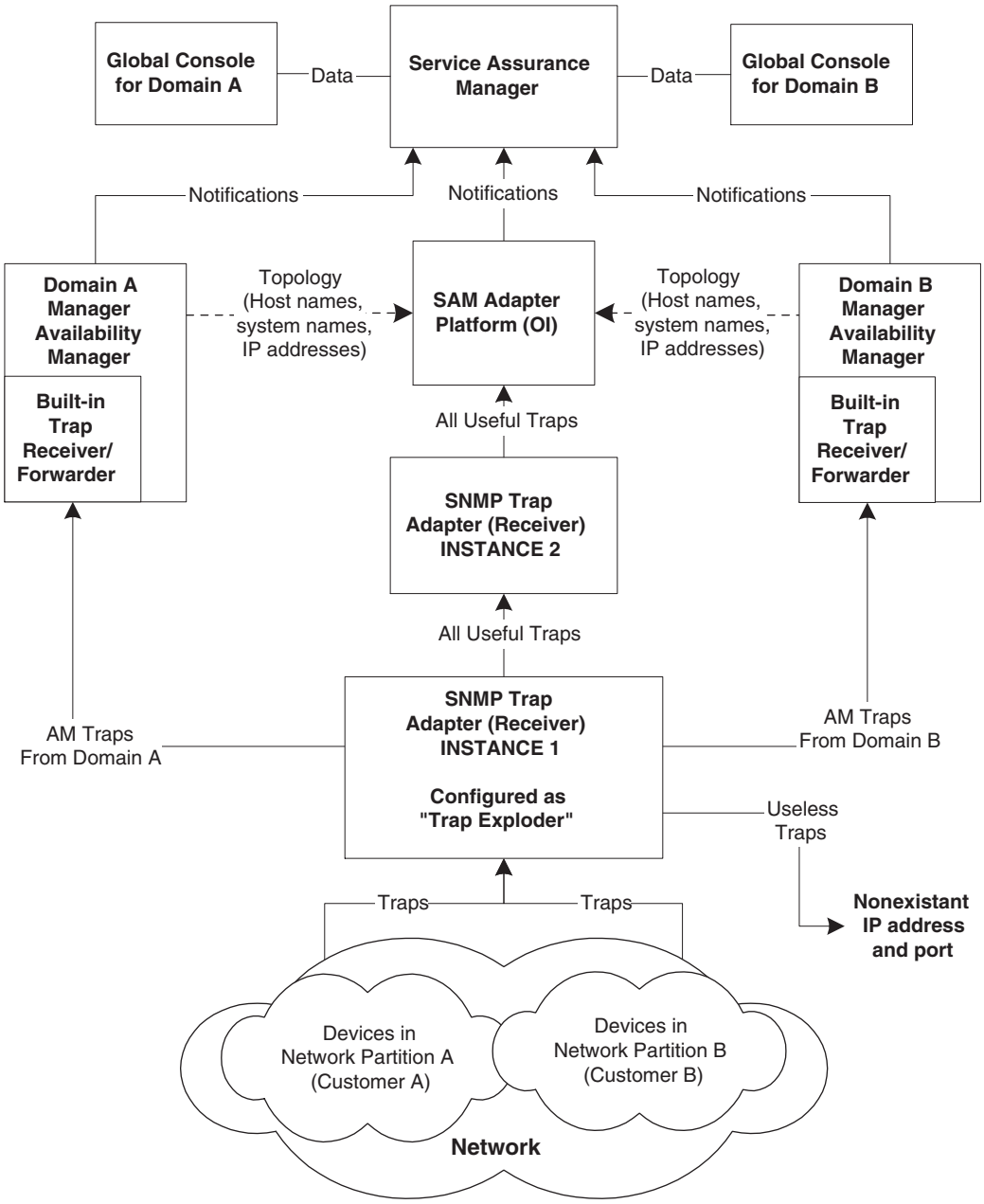


Figure 7: *Typical Trap Design in a Split Topology NCM Deployment*

Trap Forwarding

When defining trap forwarding, traps required by CNCC NCM IP Availability Managers and InCharge IP Performance Managers are already defined in the *trapd.conf* file. The only changes to the files that you must configure is to specify the specific destination hosts and ports where the Availability Managers and Performance Managers listen for traps. This change is only necessary in the *trapd.conf* file for the trap exploder instance of the SNMP Trap Adapter (Receiver).

Always try to minimize the volume of traps that are forwarded from the trap exploder to the second instance of the CNCC NCM SNMP Trap Adapter (Receiver). If network administrators do not use the traps, discard them by sending them to a nonexistent address. Judicious forwarding of traps can reduce or eliminate stressful trap processing loads. Administrators of the NCM deployment should be aware of how traps are discarded so that they can choose to discard other useless traps as their experience with the network grows.

Each trap that is transformed into a notification will require an entry in the *trap_mgr.conf* file. If an entry does not exist, then the trap should not be forwarded to the second instance of the CNCC NCM SNMP Trap Adapter (Receiver).

Traps and Notifications

When configuring the CNCC NCM SNMP Trap Adapter (Receiver) to process traps, you must decide which trap should become notifications and how the notifications should appear at the Global Console. This is defined in the *trap_mgr.conf* configuration file which is described in the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide*.

Some of the more commonly used configuration parameters include the following:

- EventText which is used to provide descriptions of the event that caused the trap.
- Expiration which defines how long the notification will remain in the Notification list until cleared.
- UserDefined1 through UserDefined10 which can include any useful information, including information retrieved from databases or other third-party sources using ASL scripting as described in *Advanced Trap Processing Using ASL Scripts* on page 59.

- Aggregate which is used to identify closely-related traps that will be combined into a single aggregate notification. Aggregating traps can reduce an operator's workload and improve an operator's ability to interpret many related traps. These traps are processed into individual component notifications and sent to the Notification List at the Domain Manager level, but in addition, an aggregate notification will appear in the list. At the Global Console, the operator will only see the aggregate notification, but can retrieve information about individual notifications by checking the aggregate tab of the notification.

Include as much of the trap processing information as possible, including the *trap_mgr.conf* configuration file, in the Deployment Build Guide.

Advanced Trap Processing Using ASL Scripts

See the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide* for specific information on advanced SNMP Trap Integration. Typically, the ASL scripts (hook scripts) will extract event text or other important information from network sources to populate the User Defined fields in the notification.

Include as much of the ASL processing definition as possible in the Deployment Build Guide. When the ASL scripts are complete, the code should be documented in the Deployment Build Guide.

Trap Processing in Overlapping IP Networks

To configure Trap Processing in overlapping IP Networks, see *Configuring Devices to Send SNMP Traps* on page 103.

Trap Processing Checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

TRAP PROCESSING CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Adapt the recommended trap processing design to the NCM deployment.	Use the recommended trap processing design whenever possible. If you must use a different design, ensure that Cisco TAC approves of the design. Add the trap processing design to the Solution Architecture Diagram.	*Recommended Trap Processing Design* on page 53
☐	Determine IP address:port locations to forward Availability Manager and Performance Manager traps.	For the trap exploder instance of the CNCC NCM SNMP Trap Adapter, the *trapd.conf* file must be modified to specify destinations for the Availability Manager and Performance Manager traps. Document in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Determine where network devices send traps.	In most cases, the trap exploder should be configured to listen for traps at the location where network devices already send traps. Document port locations in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Determine which traps will be discarded.	The design will use the trap exploder instance of the CNCC NCM SNMP Trap Adapter to forward useless traps to a nonexistent IP address:port. Document these traps in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Choose traps to process into notifications and define notification properties.	Use parameters in the *trap_mgr.conf* configuration file to choose the appropriate traps to process into notifications and to define the characteristics of the corresponding notifications. Document the traps and notifications properties in the Deployment Build Guide.	*Traps and Notifications* on page 58
☐	Choose traps to aggregate into a common notification.	Use aggregate notifications to combine related traps and reduce the workload of NCM operators. Document the aggregated notifications in the Deployment Build Guide.	*Traps and Notifications* on page 58
☐	If needed, plan for advanced processing of traps using ASL scripts.	Define the desired trap processing that requires ASL scripts. Document the purpose of this processing purpose and explain the code in the Deployment Build Guide.	*Advanced Trap Processing Using ASL Scripts* on page 59

7

Deploying Syslog Processing

The CNCC NCM Syslog Adapter reads the contents of any system log file and generates notifications based on the file contents. This chapter describes the choices that must be made when designing syslog processing. Complete configuration details are included in the *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide*.

Syslog Processing Applications

The CNCC NCM Syslog Adapter can read any text file in the proper format and parse the file to generate notifications for the CNCC NCM Service Assurance Manager. Typical applications use the CNCC NCM Syslog Adapter to monitor security violations at specific servers or monitor routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) protocol.

For example, the CNCC NCM Syslog Adapter can listen to a system log (syslog) file that represents the combined syslog files for a group of similar routers. Then, when specified messages such as BGP adjacency changes are written in the syslog file, the CNCC NCM Syslog Adapter generates notifications to the CNCC NCM Service Assurance Manager via the CNCC NCM Service Assurance Manager Adapter Platform.

The syslog messages that generate notifications and the corresponding notification's attributes are defined in the files *my_hook_syslog.asl* and *syslog_mgr.asl* in **BASEDIR/***smarts/rules/icoi-syslog*.

Creating the Syslog File

You must answer the following questions for syslog processing before moving to NCM-specific deployment design:

- How will the syslog file be created? If the syslogs for a number of systems must be monitored, a typical application has the systems send the syslog messages to a UNIX or Linux host running a syslog daemon as a receiver for systems' messages. The syslog daemon then writes the messages to a combined syslog file. Applications other than syslog daemon can create files that the CNCC NCM Syslog Adapter can read, such as the Event Log file for Cisco products on a Windows host.
- Where will the syslog file be located? The CNCC NCM Syslog Adapter must be able to access the file. The monitored devices must be able to send messages to the system where the file will be compiled.

Processing the Syslog File

In normal processing, the CNCC NCM Syslog Adapter will tail the contents of a syslog file. When tailing a file, the adapter processes only new messages added to the file. Tailing provides constant monitoring of the syslog file while the adapter is running. If tailing is disabled, the CNCC NCM Syslog Adapter parses and processes the file once.

Determine which messages in the syslog file are important in the deployment. Network administrators can explain any practices in their network that result in syslog messages and can recommend which syslog messages are appropriate for processing. Note that by default, only messages related to devices in the topology are used by the Syslog Adapter: all other messages are ignored. This behavior can be reconfigured, but processing other syslog messages may add to processing time significantly.

To expand syslog processing, choose additional messages that will generate notifications and determine what information the notifications will contain. Messages can be selected based on source and content to create notifications. With appropriate logic in the *my_hook_syslog.asl* file, information retrieved from the messages can be used to customize the notifications. You can use the Adapter Scripting Language (ASL) to modify *my_hook_syslog.asl* and specify the appropriate processing.

If more extensive customization of notifications is considered, remember that Syslog Adapter hook script processing is single-threaded: the more logic performed on each notification, the longer the processing time and potential bottleneck.

Revise your solution architecture diagram to respond to your syslog processing design. See Figure 8 for a typical example.

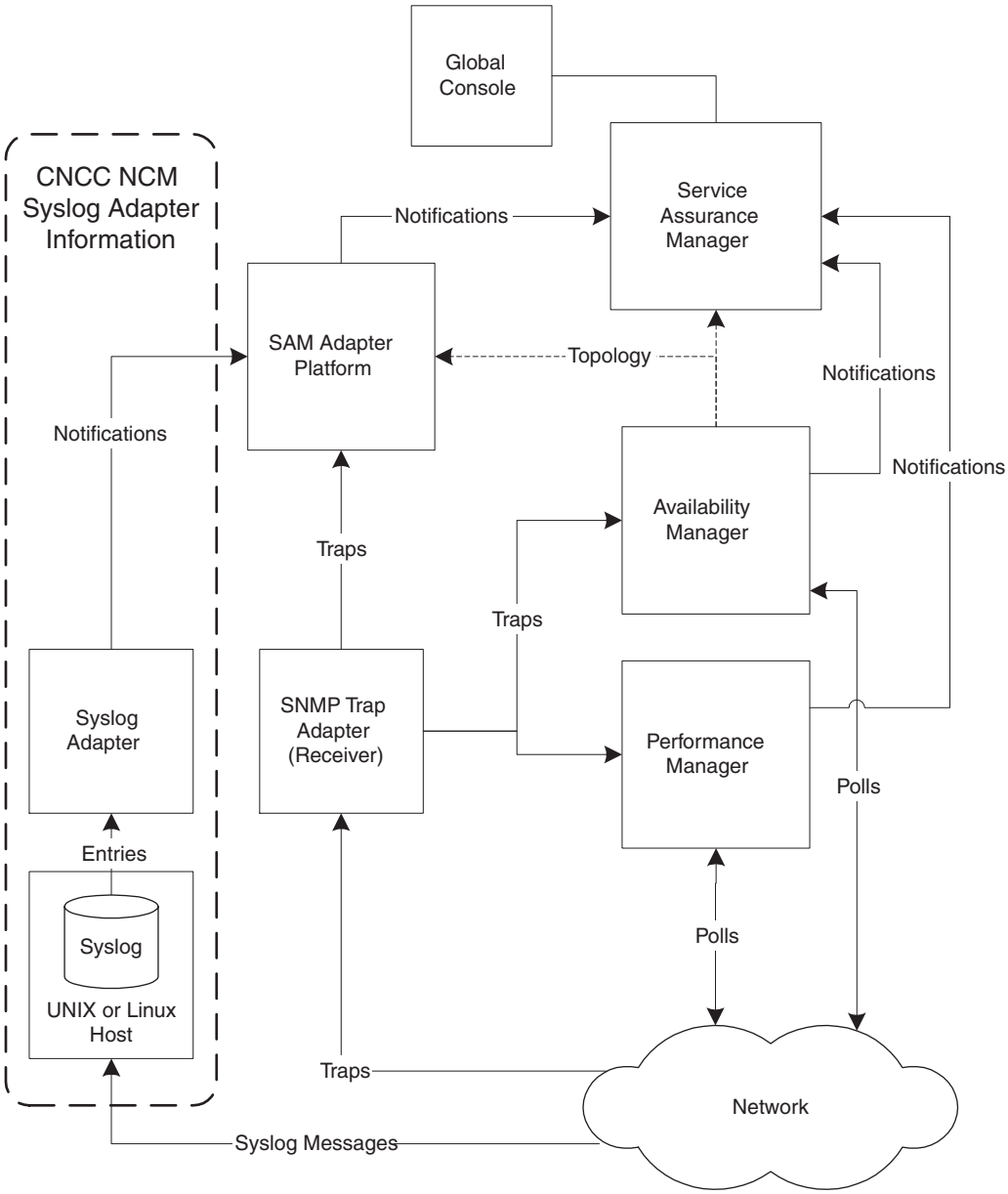


Figure 8: **Syslog Adapter added to the Solution Architecture Diagram**

Syslog Processing Checklist (Optional)

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

SYSLOG PROCESSING CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine how to create the file for processing by the CNCC NCM Syslog Adapter.	A file must be created that the CNCC NCM Syslog Adapter can parse. Determine which devices will contribute messages to the file. Consistent layout of the messages in the file is required for CNCC NCM Syslog Adapter processing. Include all details in the Deployment Build Guide.	*Creating the Syslog File* on page 62
☐	Determine the location of the file that the Syslog Adapter will process.	The process that is creating the file must be able to receive messages from source applications and the created file must be accessible by the CNCC NCM Syslog Adapter. Include all details in the Deployment Build Guide, including location, host and path.	*Processing the Syslog File* on page 62
☐	Choose the messages that are most important for processing.	Choose the messages that are most important for processing. Include all details in the Deployment Build Guide.	*Processing the Syslog File* on page 62
☐	Determine the characteristics of the notifications that are generated.	For each message that generates a notification, determine the notification format. These characteristics will be used to develop the hook script for the NCM syslog processing deployment. Include all details in the Deployment Build Guide.	*Processing the Syslog File* on page 62
☐	Add Syslog Processing to the Solution Architecture Diagram.	Add Syslog Processing to the Solution Architecture Diagram.	*Processing the Syslog File* on page 62

8

Designing for Administration of NCM

This chapter describes how to categorize NCM users, choose their access rights, and then assign administrative or monitoring capabilities.

See the *Network Connectivity Monitor Service Assurance Manager Configuration Guide* for information about configuration and implementation of NCM access.

Who are the NCM Global Console Users?

When designing your NCM deployment, you must determine who will use the NCM Global Consoles and for what purposes. Initially, it is not necessary to define individual NCM users—consider, instead, broad functional categories of users with similar needs and characteristics.

Name these categories and list their requirements in the deployment's Build Guide. Using specific position names as categories can make the process easier. For example, you might create one or more of these categories: network engineer, network administrator, network support specialist, technical specialist, NOC manager, NOC operator, LAN administrator, and IT management. Once you choose categories, determine the typical NCM-related duties that are performed by the personnel in these categories. You may find that as you list the duties, you may have to expand or combine certain categories. Once the categories are completely defined, list them in the Deployment Build Guide.

For example, Table 8 defines two typical NCM user categories.

USER CATEGORY	DESCRIPTION OF NEEDS/DUTIES
Field Engineer	Administers and maintains local and wide area networks and related hardware. Monitors daily activity, enforces licensing agreements, and provides front line support, including both software and hardware support. • Needs monitoring access to all NCM domains. • Needs to see all important traps, notifications, and network outages.
Local Area Network Administrator supporting a Customer of a Service Provider	Directs the daily operational availability of the hardware and software systems required to support facility operations. Directs and oversees scheduled testing and review of hardware and software to ensure potential problems are identified at the earliest point possible. Analyzes, evaluates and builds cost effective LAN solutions that leverage resources and technology to meet business requirements. Designs, creates and distributes user documentation relating to installation of software. • Needs monitoring access to the NCM domain that supports the customer, but not access any other domains. • Needs to see all important traps, notifications, and network outages for the customer's NCM domain.

Table 8: **Typical NCM User Categories**

Users and Security

When defining your functional groupings for users, you must consider NCM's security implementation. NCM is designed so that users fall into these access levels:

- All, a level where users can access all Global Console functionality available for one or more CNCC Managers, if their user profile permits it
- Monitor, a level where users can access only Global Console monitoring functionality, not administrative functionality, at one or more CNCC Managers, if their user profile permits it
- Ping, a level normally reserved for NCM processes, where processes will ping hosts where other NCM processes are installed to determine if the hosts are running.
- None, a level that specifically excludes access to the NCM Global Console

Also consider which CNCC Managers should be accessed by which users. You can define this access in the *serverConnect.conf* file on the servers where NCM is installed.

Password Configurations

Determine how you will configure NCM passwords. You can do any or all of the following:

- Allow the host operating system to validate users. This method provides the highest level of security and is easy to manage because it relies on the security implementation that is already in place. There are two variations: any valid user can access one of the NCM levels (All, Monitor, Ping) or specific users can access a specific NCM security level. Defining specific access requires more maintenance because you must list the user names in NCM configuration files (*serverConnect.conf* and *clientConnect.conf*). See the *Network Connectivity Monitor System Administration Guide* for methods to configure and to secure access for these files.
- Specify unique NCM passwords for individual users. Consider this method only when there are very few users because it requires a high level of maintenance. Note that it is less secure than permitting the host to validate users.
- Specify a common NCM username with a common password. This method is the least secure, but very easy to maintain.

Note that you can combine these methods, for example, you could restrict administration (All) capabilities to specific users validated by the operating system. In addition, you could provide Monitor level abilities to a general NCM user named “Monitor.”

Designing User Profiles

The functional grouping of users and their requirements form the basis of NCM user profiles. These profiles combine access to notification lists, console operations, custom console layouts, and specific tools.

Create a profile for each category of user that you must support. Groups of NCM users with similar needs can then be assigned the same user profile.

If needed, you can further customize a generic user profile by copying it and then modifying it for more specific needs. For example, an administration user profile could be customized for less experienced administrators by restricting access to some administrative console operations and tools. Other possible user profiles could include regional or customer-specific consoles.

Designing Notification Lists

A Notification List determines the events that are forwarded to a user. Essentially, the list filters the notifications that are sent from the Service Assurance Manager and can be assigned to one or more users. The lists can be organized by:

- Business units
- Geographical regions
- Groups of resources

For example, a notification list can be defined to allow only notifications from the subnetworks devoted to a specific ISP customer to reach the Global Console of the customer's network administrator.

Restricting Console Operations

Most operations that can be performed at the NCM Global Console can be individually enabled or disabled in the user profiles. When used with the security levels, restricting console operations can fine tune the abilities of users and further protect the NCM deployment.

For example, consider two users who have the Monitor security level that allows access to Global Console monitoring functionality, but not administrative functionality, for a CNCC Manager. You can further restrict one of the viewers to see only the summary view and the IP Network map while restricting the other user to the notification log and the topology browser.

Designing Consoles

The default NCM notification console is unfiltered, so NCM users may be overwhelmed by potentially enormous amounts of information. Properly configured filters can be used to customize notification consoles for groups of users. In addition, specific views can be automatically provided to match user needs.

Planning for Tools and Tool Deployment

Many types of client and server tools can be designed and developed. Typically, tools will require different levels of programming skills based on their complexity. Plan to have personnel with the appropriate skills available.

In addition, determine which tools should be available to users through their user profiles.

Administration Design Checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in *Design and Deployment Checklists* on page 105.

ADMINISTRATION DESIGN CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Define functional groups for users.	List the broad functional groups that users will belong to and then define the needs and duties of each group. Add this information to the Deployment Build Guide.	*Who are the NCM Global Console Users?* on page 65
☐	Define how you will implement user security.	Document in the Deployment Build Guide.	*Who are the NCM Global Console Users?* on page 65
☐	Define User Profiles.	Document in the Deployment Build Guide.	*Designing User Profiles* on page 67
☐	Define notification lists.	Document in the Deployment Build Guide.	*Designing Notification Lists* on page 68

ADMINISTRATION DESIGN CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Design console operations access.	Document in the Deployment Build Guide.	*Designing Consoles* on page 68
☐	Design console layouts.	Document in the Deployment Build Guide.	*Designing Consoles* on page 68
☐	Design client and server tools.	Document in the Deployment Build Guide.	*Planning for Tools and Tool Deployment* on page 69
☐	Associate notification lists, console operations, console layouts, tools, and users with user profiles.	Document in the Deployment Build Guide.	*Administration Design Checklist* on page 69

9

Deploying NCM

This chapter describes important design considerations when installing NCM. This chapter should be considered as a supplement, not a replacement, for the Installation Guides included with the NCM software and for the *Network Connectivity Monitor System Administration Guide*. Consult the Installation Guides for detailed installation procedures and consult the *Network Connectivity Monitor System Administration Guide* for detailed configuration procedures.

General Installation/Deployment Guidelines

Many organizations have strict rules for deploying enterprise-level software which may include deployment of staging areas whenever possible. A staging area is a copy of the installation.

Never install a deployment during a normal production shift; instead, choose a period of low utilization for installation. If a testbed is not available, create a staging area and make and test all changes in the staging area.

If possible, install the deployment in stages to reduce the size and complexity of each step in the overall process. Doing so makes debugging easier. Verify each stage of the deployment as described in the *Validating Your Deployment (Acceptance Testing)* on page 77.

Allow Access to MIBs in Network Devices

The IP addresses of servers running NCM applications must be added to the access list of devices that will communicate with NCM. NCM must be given full access to browse the MIBs that are listed in the *Network Connectivity Monitor IP Availability Manager User's Guide* and/or the *InCharge IP Performance Manager User's Guide*.

Licensing

For permanent licensing, NCM products rely on FLEXlm licensing software from Macrovision and a license file provided by Cisco after NCM is purchased.

The FLEXlm software is installed with the software, but a license file from Cisco is also required. The license file must be installed using the *install_license* script as described in the *Network Connectivity Monitor System Administration Guide*. To generate the license, Cisco needs the following information for the computer where the FLEXlm license server is running:

- The host ID (For Windows systems, use the Ethernet address)
- The hostname
- The operating system and version
- The number of systems that will be managed by NCM. Managed systems include routers, switches, hubs, virtual routers, security devices, hosts, servers, desktop or laptop PCs, workstations, probes, terminal servers, printers, IP phones, wireless access points (WAPs), and CSUs/DSUs

Note: An accurate count of systems ensures that the deployment can manage all the devices appropriately. The NCM discovery process will halt if the number of discovered systems exceeds the licensed quantity.

Send this information to Cisco as soon as possible after purchasing NCM to ensure that an appropriate license is available for the deployment.

When multiple license servers are used, each NCM Domain will use blocks of volume licenses from a specific license server. Therefore, the license blocks must be divided among multiple licenses and the appropriate license must be deployed to each license server. Then, Availability Managers that rely on a specific license server will have the appropriate volume licenses to support the systems that they must manage. If multiple license servers are used, ensure Cisco is aware of the configuration details.

NCM Installation

The general rule is to install and configure items from the bottom of the hierarchy first, moving up to the Service Assurance Manager. The installation order is as follows:

1. NCM Broker (normally installed and configured when the first NCM components are installed)
2. NCM Adapters
3. Underlying Domains (IP Availability Manager and IP Performance Manager)
4. Global Manager (Service Assurance Manager)
5. Global Console

After the Service Assurance Manager is installed and configured, you can install the components that use the Service Assurance Manager as a server, such as the Global Console.

To ease the troubleshooting of initial deployment, install more limited segments of the deployment first, such as an Availability Manager and then Service Assurance Manager. Always validate a segment before installing the next segment.

By default, all NCM applications are installed as services and are started immediately after installation. During deployment, you should set the services to start manually until your installation and validation are complete.

Setting Environment Variables

Setting inappropriate values for environment variables is a common cause of post-installation problems. Detailed descriptions of the environment variables used by NCM, including methods for setting them, are described in detail in the *Network Connectivity Monitor System Administration Guide*.

Configure Security

For initial validation, use the default administration user name and password (*admin* and *changeme*). Once you have validated your installation, change the default administration user name and password.

Use and Guard Your NCM Secret Phrase

NCM components are installed using a default secret phrase. This phrase can be used to encrypt NCM passwords used in authentication and to encrypt communications between NCM components.

Cisco recommends that you take advantage of the added level of security provided through the secret phrase and its related security mechanisms. To do this, you must change the secret phrase using sm_rebond and make it consistent at all your NCM installation sites. Due to the sensitive and vital nature of this secret phrase, store and guard the phrase as you would do with the root passwords of the most sensitive servers in your network.

Under certain circumstances, the loss of the secret phrase can force extensive reconfigurations and require reinstallations of all NCM components.

Deploy Trap Processing

In the recommended trap processing configuration, two SNMP Trap Adapter (Receiver) instances are invoked using different *trapd.conf* files. The *trapd.conf* for the "trap exploder" instance includes trap forwarding statements and indicates the port to use when listening for traps. In contrast, the *trapd.conf* for the other instance of the SNMP Trap Adapter does not include trap forwarding statements.

In the following procedure, ***BASEDIR*** is the location where the Service Assurance Management Suite is installed. Deploy the trap processing as follows:

1. Install the SNMP Trap Adapter (Receiver) as a service. The default configuration will use ***BASEDIR****/smarts/local/conf/icoi/trapd.conf*, the version of the *trapd.conf* file that is *not* configured to forward traps.
2. Create the startup configuration for the trap exploder instance of the SNMP Trap Adapter (Receiver) using **sm_service**. The trap exploder instance will use ***BASEDIR****/smarts/local/conf/trapd/trapd.conf*, the version of the *trapd.conf* file configured to forward traps. Typically, the startup configuration would look like this (enter the following on one line):

```
# BASEDIR/smarts/bin/sm_service install
--startmode=runonce
--description="SMARTS Trap Exploder" ic-trapd-exploder
BASEDIR/smarts/bin/sm_trapd
--name=EXPLODER-NCM_OI --config=trapd
--port=<number> --ascii --output --rules=default
```

   In this case, the value for - *-port* should be the port number where network devices send traps. For complete details on **sm_service**, see the *Network Connectivity Monitor System Administration Guide*.

3. Use **sm_edit** to configure the two different versions of the *trapd.conf:*
   - The SNMP Trap Adapter (Receiver) instance will use ***BASEDIR****/smarts/local/conf/icio/trapd/trapd.conf*. The file should not include trap forwarding statements.

- The trap exploder instance will use ***BASEDIR****/smarts/local/conf/trapd/trapd.conf*. This file should include all trap forwarding statements. Traps that must be processed into notifications should be forwarded to *host:port* where the SNMP Trap Adapter (Receiver) instance listens for traps.

4. Use **sm_edit** to configure the *trap_mgr.conf* file for the SNMP Trap Adapter (Receiver) instance.
5. Start both the SNMP Trap Adapter (Receiver) and the trap exploder.

Deploy NCM User Configurations

Deploying the NCM user configurations consists of two tasks:

- Configure access to NCM by adding user names and passwords to the security files (*clientConnect.conf* and *serverConnect.conf*) as described in the *Network Connectivity Monitor System Administration Guide*. These files define the security level for each user, including user capabilities, servers that can be accessed, and passwords.
- Configure NCM users:
  - Deploy and configure tools. Server tools must be copied to the server where Service Assurance is installed and client tools must be copied to all systems where Global Consoles are installed.
  - Create console configurations and then save them on the server where Service Assurance is installed. Create each console configuration by opening the Global Console and then arranging the layout and customizing preferences. Save the customized console with an appropriate name in an **.iccon* file. Each console file can then made available to all users by copying it from ***BASEDIR****/smarts/local/consoles/<user>* to ***BASEDIR****/smarts/local/consoles*.
  - Define customized notification lists.
  - Create user profiles which associate individual users with access to specific tools, consoles, and a notification list.

10

Validating Your Deployment (Acceptance Testing)

This chapter describes how to ensure that your NCM deployment operates as intended.

Validation Techniques

When validating, begin by dividing the deployment into manageable, logical segments. Ensure each of the segments function properly and then perform end-to-end testing. Check data flow and then check the accuracy of the data itself. Validate as much as possible before discovering the topology so that you reduce complexity.

Initial Validation

To start validation, ensure that the NCM Broker has access to all the CNCC Managers and that the CNCC Manager processes are registered and running. Use **brcontrol**, as described in the *Network Connectivity Monitor System Administration Guide*, to list the NCM processes registered with the NCM Broker and their status.

Validating Discovery

Discover the topology of the network. If the deployment includes a single Availability Manager on a large or extra large platform, discover the network in limited portions: for example, discover groups of one thousand managed network devices. Monitor the discovery process and review the discovered topology after each discovery.

If the network includes Hot Standby Router Protocol (HSRP) groups or virtual routers, ensure they are discovered.

For Availability Manager and Performance Manager, validate the discovered topology by reviewing a segment of the network that is well known. Always confirm possible discovery errors: if an expected device does not appear in the topology, ping the device to ensure it is accessible. It is not unusual for discovery to find more devices than you expect; if this is the case, confirm that the devices exist.

Validating Polling and Events

To validate polling and thresholds, do the following using the Polling and Thresholds Console:

- Cause a failure by physically removing a cable in a discovered portion of the network. Check that the correct notification is received at the Global Console and that the topology map indicates the failure. Note that you may have to wait a few polling cycles to see the correct root-cause analysis.
- Reduce threshold settings to very low levels or zero. Typically, reducing port or interface performance settings works well for validating Performance Manager deployments. For Availability Manager deployments, reduce the RestartTrapThreshold connectivity setting for a router or switch and cause a warmstart on the corresponding type of system. Obviously, choose equipment and a time frame when you will not interrupt your network users. Verify that the correct notification is received at the Global Console indicating that the threshold was exceeded.

Validating that the levels that you chose for the thresholds are appropriate for your deployment is much more difficult. Start by using the defaults and adjust them upward or downward as you gain experience with the equipment. When failures occur, particularly failures with little or no warning, determine if the failures were preceded by symptoms that could have been detected by lower threshold values. Then adjust the thresholds appropriately. This evaluation should be performed after all failures.

Validating Trap Processing

Use **sm_snmp** to generate traps to the SNMP Trap Adapter (Receiver) functioning as the trap exploder.

Ensure that you send traps that cause notifications from the underlying analysis servers as well as from the SAM Adapter configuration. Create a trap for each trap processing statement in the *trap_mgr.conf* file. If ASL scripting is included in the trap processing, ensure the scripts function as intended.

Validating Users and Capabilities

To validate users and their capabilities, test each user profile. You must create a temporary user for each of your user profiles. Log onto the NCM Global Console as each user in turn and review the associated console capabilities including access to console operations, access to tools, configuration of the notification list, and layout of the console. Ensure the capabilities match your expectations for each user profile.

11

Tuning Your Deployment to Improve Performance

This chapter describes methods for identifying performance problems in a NCM deployment and the steps that you can take to correct these problems.

Performance Tuning Guidelines

Whether tuning NCM is required is directly related to the capabilities of the equipment where the NCM applications are installed.

When an NCM deployment is installed on equipment from the small and medium platform equipment tiers, defined in *Determine the Required Size of the NCM Deployment* on page 26, tuning is usually not required. But performance should be monitored to ensure that there are no issues.

When the NCM deployment is installed on equipment from the large or extra large platform equipment tiers, tuning for peak performance is almost always required. For these large and complex deployments, expect that you will require aid from the Cisco for the tuning process.

General tuning recommendations and details on network sizing are described in Table 9.

Platform Equipment Tier Size	Small	Medium	Large	Extra Large
Managed Ports and Interfaces	AM: 10K AM+PM: 5K	AM: 25K AM+PM: 15K	AM: 50K AM+PM: 25K	AM: 100K AM+PM: 50K
Hardware Configuration	1-2 CPUs (low-end) 1GB RAM	2 CPUs 2GB RAM	2 CPUs 4GB RAM	2-4 CPUs (high-end) 8GB RAM
Fine-tuning required?	Usually never	Possibly	Yes	Absolutely
Additional Sizing Comments	Add a second CPU for growth or if collocating a PM.		Use high-end CPUs for growth or if collocating a PM.	Consider splitting your topology into multiple domains.

AM = Availability Manager
PM = Performance Manager
AM+PM = Availability Manager and Performance Manager as a single process

Table 9: **Tuning Recommendation for Various Sized NCM Platforms**

Regardless of the size of your NCM deployment, always monitor its performance. If tuning is required, remember that tuning your deployment is an ongoing process that should be performed regularly. Network changes can potentially affect the performance of NCM: if you add, remove, or relocate network equipment, review the performance metrics.

Never waste resources by tuning a partial deployment—adjustments made during a partial deployment will usually be inappropriate for a complete deployment.

Assessing Performance

For NCM, assess performance by checking the resources required by NCM processes against the operating system limits and by reviewing NCM performance metrics.

Checking Resource Requirements Against Operating System Limits

The memory limit is an operating system limit that indicates the maximum process size permitted in memory. This limit may become an issue for very large NCM topologies. The process size limits are shown in Table 10.

OPERATING SYSTEM	MEMORY LIMIT
Solaris	3.75 GB
HP-UX	2 GB
Linux	3.8 GB
Windows	2 GB
AIX	3.75 GB
See the appropriate installation Guide for specific operating system version and patch information. For more information on operating system limits, consult the operating system's documentation.	

Table 10: **Operating System Limits on Total Process Size in Virtual Memory**

To find the total size in memory for various NCM processes, use the following commands:

- For Linux or UNIX systems, use **ps -l -p** ***proclist*** where **proclist** is one or more IDs for the NCM processes. Review the total size of the processes in virtual memory (usually the SZ column).
- For Windows systems, open the Windows System Information tool and find the process size in the Software Environment, Running Tasks folder.

If a NCM process is approaching the memory limit, consult with Cisco for further evaluation.

Reviewing License Metrics

To determine if your deployment has sufficient licenses, Availability Manager and Performance Manager provide the **sm_tpmgr** utility. Use this utility with the following syntax to generate a complete list of performance metrics and deployment size information:

```
sm_tpmgr -s servername --sizes
```

For example, lines similar to the following would appear in the output:

```
Total System Volume License Checked Out:         150
Total Systems in Topology:               105
Remaining Blocks of System Licenses in License Server: 5
Maximum Number Of Systems: 1500
```

In this example, licenses for 1395 additional systems are available.

Reviewing Performance Metrics

To assess performance, Availability Manager and Performance Manager provide the **sm_tpmgr** utility. Use this utility as follows to generate a complete list of performance metrics:

```
sm_tpmgr -s servername --show-dm-processes
```

The output of this command lists the duration of most tasks performed by the Domain Manager, including:

- Codebook tasks
- Discovery cycles, including post processing, reconfiguration, and saving the repository
- ICMP statistics
- SNMP statistics

Note that when collecting performance statistics for Availability Manager, useful statistics are only available after Availability Manager is in a steady state for two to three hours.

Codebook Tasks

The codebook tasks are single-threaded and CPU-bound. These tasks occur each time discovery is completed, when reconfiguration occurs, or when topology changes are made. The tasks may also be triggered manually.

The codebook task durations are listed at the beginning of the output from the **sm_tpmgr** utility and will be similar to Figure 9.

```
    Last Consistency Phase One Update = 1
      Last Offline Consistency Update = 1
               Last Consistency Update = 0

    Last Offline Codebook Computation = 2
            Last Codebook Computation = 2

                     Last Correlation = 0

                       codebookRadius = -1
                  correlationInterval = 30
                    correlationRadius = 4

  Process                 Last Start Time                Last End Time          Duration
Phase One Consistency  03-Nov-2003 19:15:00 EST   03-Nov-2003 19:15:01 EST         1
 Offline Consistency   03-Nov-2003 19:15:03 EST   03-Nov-2003 19:15:04 EST         1
        Consistency    03-Nov-2003 19:15:06 EST   03-Nov-2003 19:15:06 EST         0

  Offline NewMatrix    03-Nov-2003 19:15:06 EST   03-Nov-2003 19:15:08 EST         2
          NewMatrix    03-Nov-2003 19:15:06 EST   03-Nov-2003 19:15:08 EST         2

       Correlation     03-Nov-2003 19:15:18 EST   03-Nov-2003 19:15:18 EST         0
```

Do not use this value.

Refer to these codebook task values.

Figure 9: **The sm_tpmgr Utility: Codebooks Tasks**

Look for these codebook task values to evaluate performance:

- Consistency: The time (seconds) required to recalculate aggregations.
- NewMatrix: The time (seconds) required to re-compute the codebook.
- Correlation: The time (seconds) required to perform the correlation

Table 11 indicates the acceptable and unacceptable values for the codebook tasks.

Performance Category	Performance Assessment			How to Improve
	Good	Acceptable	Unacceptable	
Consistency	< 10 sec	10-30 sec	> 30 sec	Use a faster CPU or split the topology.
NewMatrix	< 10 sec	10-30 sec	30 sec	Use a faster CPU or split the topology.
Correlation	0	0-20 sec	20 sec	Use a faster CPU or split the topology.

Table 11: **Evaluating Codebook Task Durations**

Duration of Last Discovery

When assessing discovery performance, do not use the numbers from an initial discovery process because it is not representative of typical discovery processes and is usually very costly. In addition, discovery durations vary dramatically based on the type of discovery processing:

- Discover all
- Discover pending
- Discover one device
- Discover many devices using a seed file

The Topology Manager section of the output from the **sm_tpmgr** utility list discovery times and will be similar to Figure 10.

```
Topology Manager:
                durationOfLastProbe = 0 00:09:00
                 lastProbeFinishedAt = 03-Nov-2003 07:15:00 PM EST
                  lastProbeStartedAt = 03-Nov-2003 07:06:00 PM EST
        lastProbeStartedAt_pending = 03-Nov-2003 07:06:00 PM EST
                     numberOfAgents = 0
                  numberProbeThreads = 10
                     probeQueueSize = 0
```

Length of Discovery

Figure 10: **The sm_tpmgr Utility: Discovery Information in the Log File**

If a full discovery takes more than eight hours (including post-processing and reconfiguration), it may affect normal business operations. In an environment where full discovery can be scheduled over a weekend, eight hours or more might be acceptable, but between two and five hours is often required to avoid interfering with possible third shift work.

Note: In addition to the **sm_tpmgr** utility, the DiscoveryInProgress event could be used with ASL scripting to determine the length of the task.

Discovery Post Processing

The log files provide the most accurate source of information for discovery post processing. In the ***BASEDIR****/smarts/local/logs* directory of the Availability Manager, Performance Manager, or Discovery Manager, there is a *server_name.log* file where *server_name* is name of the CNCC Manager.

Search the log file for the most recent “Started basic post-processing” statement and the most recent “Finished partitioning” statement. The duration between the times of these statements is the length of time required for discovery post-processing.

Do not use the discovery postprocessing duration when a large number of new devices are discovered and added to the topology because the post-processing required to create a new topology is much higher than under normal circumstances.

Additionally, in large or very meshed topologies, the greatest cost of partial discoveries, even of a single device, is in discovery post-processing. If discovery post processing is taking too long, review any custom post processing. If it is poorly designed or implemented, it should be reconsidered before splitting the topology or adding CPUs.

Performance Category	Performance Assessment			How to Improve
	Good	Acceptable	Unacceptable	
Post-Processing	< 5 min	5-10 min	> 10 min	Use a faster CPU or split topology. Review any custom post-processing.

Table 12: **Evaluating Codebook Task Durations**

Reconfiguration and Saving the Repository

Reconfiguration is single-threaded and CPU-bound. Saving the repository is also single-threaded, but is mostly I/O-bound. These task durations appear in the output from the **sm_tpmgr** utility and will be similar to Figure 11.

```
Policy Manager:                                          Reconfiguration
            durationOfLastReconfigure = 0 00:00:07

Persistence Manager:                                     Repository Save Duration
            lastCheckpointFinishedAt = 03-Nov-2003 07:15:02 PM EST
            durationOfLastCheckpoint = 0 00:00:01
```

Figure 11: **The sm_tpmgr Utility: Reconfiguration and Repository Save Tasks**

Table 13 indicates the acceptable and unacceptable values for these tasks.

Performance Category	Performance Assessment			How to Improve
	Good	Acceptable	Unacceptable	
Reconfigure	< 5 min	5-8 min	> 8 min	Use a faster CPU or split the topology.
Repository Save	< 1 min	1-3 min	> 3 min	Use a faster CPU or split the topology.

Table 13: **Evaluating Reconfiguration and Repository Save Tasks Durations**

ICMP Processing Statistics

ICMP processing statistics appear in the output of the **sm_tpmgr** utility and will be similar to Figure 12.

Look for these statistics to evaluate performance:

- avg_get_time, max_get_time, min_get_time: The average, maximum, and minimum duration (seconds) of a ping cycle.
- avg_late_polling: The amount of time (seconds) that the ICMP pinger is falling behind. If the value is negative, the pinger is ahead of schedule.

```
Pinger Accessor Interface:
                    avg_late_polling = -0.01840490847826
                        bytesPerPing = 64
      gets_causing_request_percentage = 0
           gets_from_cache_percentage = 100
                     icmpNumberOfPolls = 90
                  icmpNumberOfResponse = 90
                    icmpPollerTimeSkew = -0.0184049
                         icmpStartTime = 31-Oct-2003 10:10:44 EST
                    num_other_failures = 0
                           num_threads = 1
                          num_timeouts = 0
                        operation_size = 1
             periodic_gets_per_second = 0
           total_active_poll_actions = 0
                      total_get_nexts = 0
                total_gets_from_cache = 162
    total_instrumentation_get_requests = 0
                 total_on_demand_gets = 0
                  total_periodic_gets = 0
                   total_poll_actions = 0
                     total_repos_gets = 162
```

Average Late Polling

Figure 12: **The sm_tpmgr utility: ICMP Statistics**

Table 14 indicates the acceptable and unacceptable values for these statistics.

ICMP Performance Category	Performance Assessment			How to Improve
	Good	Acceptable	Needs Improvement	
avg. get time, max get time, min get time	<1 msec		>1 msec	Increase polling interval or split the topology.
avg. late polling	Negative	0-0.5 sec	> 0.5 sec	Increase polling interval or split the topology.

Table 14: **Evaluating ICMP Statistics**

SNMP Processing Statistics

SNMP processing statistics appear in the output of the **sm_tpmgr** utility and will be similar to Figure 13. Look for these statistics to evaluate performance:

- avg_get_time: The average time (seconds) that an SNMP get cycle takes on a per-thread basis (that is, the round-trip delay). The value varies based on the network configuration and will serve as a guideline when configuring polling threads.
- avg_late_polling: The amount of time (seconds) that the SNMP poller is falling behind.
- avg_request_size: The average number of variable bindings in a get request. Higher values indicate more efficient polling.
- num_threads: The current number of polling threads that are configured. Check this value after reconfiguring to ensure accuracy.
- periodic_gets_per_second: The actual throughput of the poller across all threads.

```
SNMP Accessor Interface:
            avg_active_processing_time = 0.0973929232857143
                          avg_get_time = 0.0412507578666667
                     avg_late_polling = 0.188394353857143
                        avg_lock_wait = 0.00014787585714285 7
                     avg_request_size = 14
       gets_causing_request_percentage = 0
            gets_from_cache_percentage = 100
            max_active_processing_time = 0.369101803
                          max_get_time = 0.091588776
                     max_late_polling = 0.805186757
                        max_lock_wait = 0.000490496
                          min_get_time = 0.001716586
                   num_other_failures = 0
                          num_threads = 10
                          num_timeouts = 0
             on_demand_gets_percentage = 0
                        operation_size = 19
             periodic_gets_per_second = 5.13920718548761E-05
             periodic_gets_percentage = 100
             total_active_poll_actions = 7
                       total_get_nexts = 0
                  total_gets_from_cache = 744
    total_instrumentation_get_requests = 15
                   total_on_demand_gets = 0
                    total_periodic_gets = 15
                     total_poll_actions = 7
                       total_repos_gets = 744
```

Figure 13: **The sm_tpmgr Utility: SNMP Statistics**

Table 15 indicates the acceptable and unacceptable values for the SNMP average late polling and average cycle statistics.

SNMP Performance Category	Performance Assessment			How to Improve
	Good	Acceptable	Unacceptable	
avg. late polling	< 5 secs	5-60 secs	> 60 secs	Add polling threads or split the topology.
avg. get time	< 150 msec	150-300 msec	> 300 msec	Add polling threads.

Table 15: **Evaluating SNMP Statistics**

Improving Performance

If the performance metrics indicate a performance degradation, try the following tactics to improve performance:

- Add polling threads. This tactic is one of the best and simplest methods for improving performance. Increasing threads to 20, 30 or even 50 discovery threads is acceptable, but keep in mind that more threads may require additional or more capable CPUs and that the IO requirements during discovery will increase.
- Split topology into multiple domains. Currently, Cisco can aid in efficiently splitting a network topology across multiple NCM Domain Managers.
- Improve the capabilities of the equipment where the NCM process is installed: Use a faster CPU or reinstall NCM on more capable equipment. Before resorting to this hardware upgrade, consider the previous options.

Other Tuning Issues

Adjust Performance Thresholds to Reduce Inappropriate Alarms

After gaining experience with the NCM deployment, adjusting performance thresholds may reduce the number of inappropriate alarms. Devices may trigger alarms during normal operation because performance thresholds set inappropriately low. Review all performance-related alarms that were triggered by conditions that did not represent actual or potential failures and adjust the threshold to avoid repetition of the alarm.

Conversely, failures of some devices may be preceded by performance degradation that does not trigger an alarm. Once again, review any failures that may be preceded by degraded performance and adjust the thresholds to detect these changes appropriately.

Use Batching to Improve Trap Processing Performance

In a deployment where a high frequency of traps is expected, plan on using the batching capability of the CNCC NCM SNMP Trap Adapter to improve performance of the clients that process the notifications. The *BATCH_NOTIFY_INTERVAL* in the *trap_mgr.conf* configuration file determines the length of the interval between sending batches of notifications based on traps. It may be necessary to tune this value under the typical trap load, so plan on monitoring the client performance and adjusting this value.

Global Console Performance

To ensure appropriate performance at the Global Console, limit the total number of Global Console users attached to the same Service Assurance Manager to fifty. This is typically a safe limit, but more users are possible. Check processor utilization to ensure it is not too high before adding additional users.

A typical Global Console tuning task is to optimize notification list filters for the operators. The operator should not see more (or less) than needed. Avoid needless processing whenever possible.

A

Using Discovery Manager to Obtain Network Information

This appendix explains how to deploy the InCharge IP Discovery Manager to obtain the network information needed when designing an NCM deployment.

Deploying Temporarily

Cisco offers a traveling license for the Discovery Manager which allows you to deploy the Manager on a laptop. The laptop can then be connected to an organization's network and be used to discover IT objects in the networks.

You may also use the travelling license to temporarily install the Discovery Manager on a platform in an organizations's network. This is more cumbersome as it requires installation and configuration each time it is used in a new network. In addition, you must uninstall the Discovery Manager before moving on to another network.

Typically, the Discovery Manager is used as a due diligence tool in a temporary deployment.

Deploying Permanently

The Discovery Manager can also be deployed in a network permanently using a static license. This deployment is beyond the scope of this Appendix.

Discovery Process

Note that this method still requires that you design a discovery process as explained in *Planning for Discovery* on page 37.

Exporting topology

The topology can be retrieved with **dmctl** or by using an ASL script. In general, users need to develop their own tool to export the topology in the format they want. Users can also use **sm_topodump** to dump a subset of the topology or they can export the quantities of various network components using the **sm_tpmgr**.

Using sm_tpmgr

After discovering the network, use **sm_tpmgr --sizes** to retrieve data on the topology. **sm_tpmgr --sizes** breaks down topology by major classes of objects (Routers, Switches, Interfaces, Ports, Cables, etc.) and identifies what is instrumented (that is, monitored) and for what application (ICAM, ICPM or both).

For example, from ***BASEDIR/****smarts/bin*, enter:

```
% ./sm_tpmgr -s NCM-AM --sizes
```

Typically the output from *sm_tpmgr -- sizes* is as follows:

```
Total System Volume License Checked Out:         150
Total Systems in Topology:               105
Remaining Blocks of System Licenses in License Server: 5
Maximum Number Of Systems: 1500

Number of Systems [Instrumented for Connectivity/Performance]
Total Number of Systems: 105 [105/0]
        Number of Node: 10 [10/0]
        Number of Probe: 1 [1/0]
        Number of Switch: 11 [11/0]
        Number of Host: 78 [78/0]
        Number of Router: 4 [4/0]
        Number of Hub: 1 [1/0]

Total Number of IPs: 172 [170/0]
Total Number of Ports: 427 [91/0]
        Number on Switch: 427 [91/0]

Total Number of Interfaces: 160 [157/0]
        Number on Node: 11 [11/0]
        Number on Probe: 10 [10/0]
```

```
        Number on Switch: 26 [25/0]
        Number on Host: 94 [94/0]
        Number on Router: 18 [16/0]
        Number on Hub: 1 [1/0]

Total Number of Links: 76
        Number of NetworkConnections: 1
        Number of Cables: 71
        Number of TrunkCables: 4

Total Number of MACs: 648
Total Number of STPNodes: 43
```

B

Managing Overlapping IP Networks With NCM

NCM enables service providers who offer managed IP network services the ability to centrally manage the private IP networks of customers who deploy identically-numbered IP address spaces.

To provide this capability, NCM must be deployed in an environment where the following criteria are met:

- The system hosting the NCM application supports virtual IP interfaces.
- A policy-based router between the system hosting NCM and the customer networks that supports policy routing based on a packet's source address.

Using IP Management Domains to Manage Overlapping IP Networks

To use NCM to manage overlapping IP networks, you must establish separate IP Management Domains. An IP Management Domain is a set of IP networks that do not contain overlapping addresses.

Consider two customers, A and B, that both use the private IP network number 10.0.0.0/8 (subnet 255.0.0.0). In this case, customer A is one management domain, Domain A, and customer B is a second domain, Domain B. The combination of A and B cannot be a domain because they both use the 10.0.0.0/8 network number. As the administrator of the NCM application, you map each customer network to a different management domain when configuring the NCM applications.

NCM assumes that IP addresses within a domain are unique (except for cases such as Hot Standby Routing Protocols where it is possible for two devices to share the same virtual IP address so long as only one device actually uses it at any one time). IP addresses do not have to be unique across all of the management domains.

Topology and event information for the systems and networks in each IP Management Domain are kept isolated by running separate NCM applications on the same host system. Because the topology and event information for each domain is separated, NCM does not display phantom connectivity between devices in different domains, even if they share the same IP network numbers. You can manage each domain from the same Administration Console, but the settings for each domain are separately configurable.

An IP Management Domain provides the structure into which the different customer networks are placed. But to actually discover the networks and then to subsequently poll them and process traps requires specialized support provided by the NCM application, as well as configuration support from the host operating system.

To manage networks with overlapping IP addresses, you need to complete the following steps.

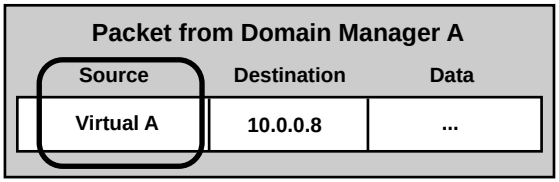
- Configure the NCM applications, one per IP Management Domain, by binding a virtual IP interface to each domain manager.
- Configure a policy-based router, or use source routes, to properly route packets sent from the NCM applications to the appropriate IP Management Domain.
- Configure the devices in each IP Management Domain to send SNMP traps to the virtual IP address for which the respective NCM application is listening for traps.

Using Virtual IP Interfaces to Direct Management Traffic

You bind an NCM application, and thus an IP Management Domain, to a virtual IP interface on the host operating system. Consider again the example from the previous section that defined two domains, Domain A and Domain B. To discover and poll these networks, the administrator must configure a separate virtual IP interface—Virtual A and Virtual B in this example—for each domain. Then, as part of the definition of the domain within the NCM application, you bind a domain to a particular virtual interface. In this case, Domain A may be bound to Virtual A and Domain B to Virtual B.

The domain-to-interface binding has the following effect on the requests coming into and going out of the NCM application:

- All SNMP and ICMP requests from Domain Manager A specify Virtual A as the source address. Requests from Domain Manager B specify Virtual B as the source address. Because of this, two packets destined for identically addressed devices in Domain A and Domain B are differentiated by the packet source address, as shown in Figure 14.



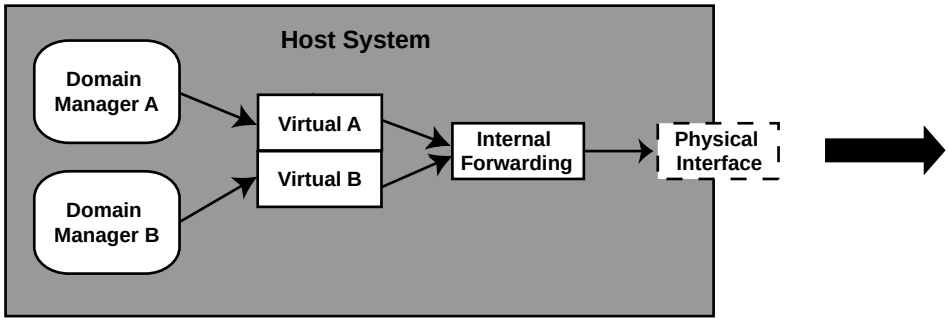


Figure 14: **Path of Packets Delivered to NCM Applications**

- An SNMP response or trap whose destination address is Virtual A is interpreted in the context of Domain A. The response or trap whose destination is Virtual B is interpreted in the context of Domain B. Incoming traps from identically addressed devices in Domain A and Domain B are distinguishable by the packet destination address as shown in Figure 15.

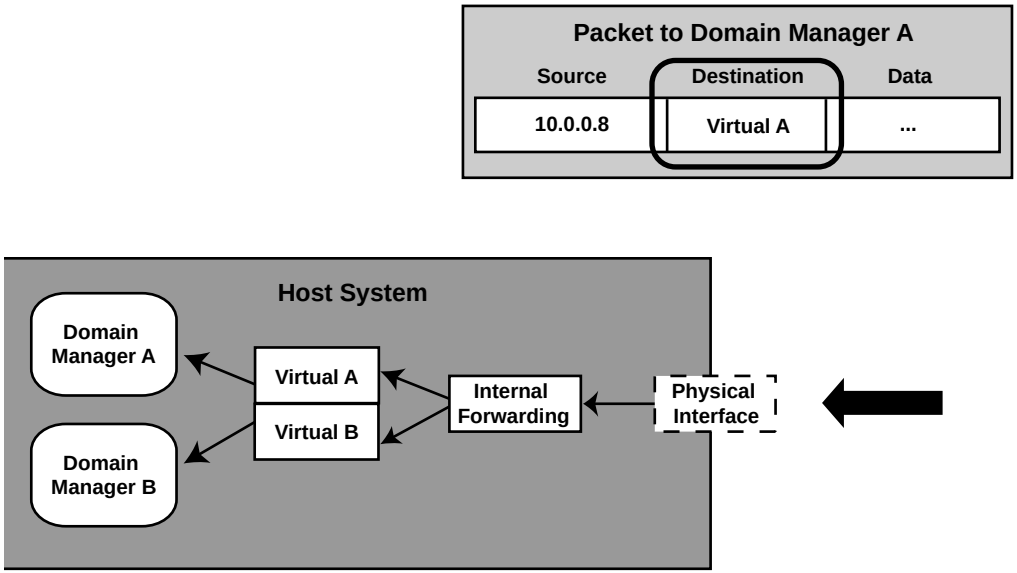


Figure 15: **Path of Packets Delivered to NCM**

Proper trap processing support requires that devices in customer A's network are configured to send traps to Virtual A. Devices in customer B's network must be configured to send traps to Virtual B. Because responses are sent to the source address of the query that initiated them, the rules for sources described previously ensure that responses are automatically sent to the right destination.

Binding an NCM Application to a Virtual Interface

You first need to create one or more virtual IP addresses on the host where the NCM applications are running. After you have created the virtual interfaces, you can bind each NCM application to a virtual interface. The domain manager is bound to the IP address at startup. Because of this, you will need to modify the startup script for each domain manager.

The sm_server command, which is used to start a domain manager, provides a special option, `--useif`, for binding the domain manager to a particular interface. The following example illustrates this option by binding the domain manager NCM_A to the IP address 192.168.1.2.

```
# BASEDIR/smarts/bin/sm_server -n NCM_A --useif=192.168.1.2
```

Routing Management Traffic To and From the Management Domains

In addition to binding each NCM applications to a virtual IP interface, you need to configure a router to route packets to and from each NCM application to the appropriate managed domain. You can use one of two methods to route management traffic.

- A policy-based router that routes traffic from each virtual interface through interfaces that are only connected to each managed domain.
- Source routing where routing instructions are added to the packets leaving each NCM application.

Using a Policy-Based Router to Route Management Traffic

A policy-based router using methods such as Multiprotocol Label Switching (MPLS) or Border Gateway Protocol (BGP) is required to properly route the packets coming out of the NCM applications. Figure 16 shows this example, where such a router must have two interfaces, Interface A and Interface B, through which there is unambiguous connectivity to networks of customers A and B, respectively.

A policy route must be defined such that a packet, originating from Domain Manager A whose source address is Virtual A, is forwarded out of Interface A. Similarly, a second route must be defined such that a packet, whose source address is Virtual B, is forwarded out of Interface B. Packets returning from the customer networks through Interface A and Interface B are routed back to the appropriate interface and NCM application using standard IP routing.

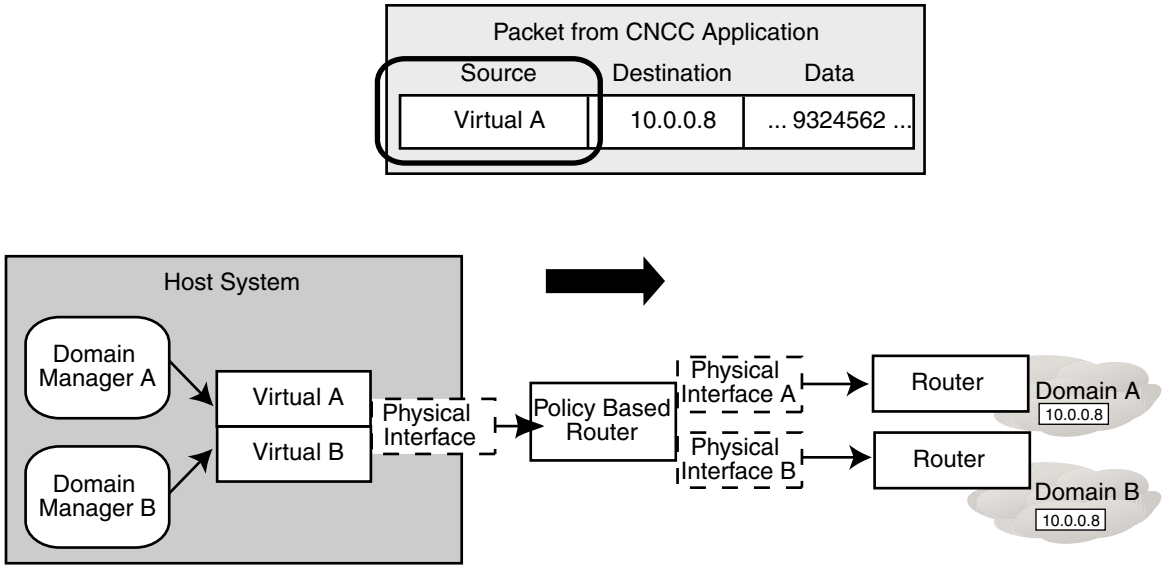


Figure 16: **Packets Routed Through a Policy-Based Router**

Using Source Routes To Route Management Traffic

You can also use either loose or strict source routes to route management traffic. The advantage of source routing is that it you do not have to configure the routers. However, not all routers support source routes. Figure 17 shows an example where routing instructions are added to the packets leaving the NCM application. Each packet arrives at a router with instructions about the packet's next destination. When the instructions are exhausted, the packet will be in a location where standard routing can complete the packet's delivery.

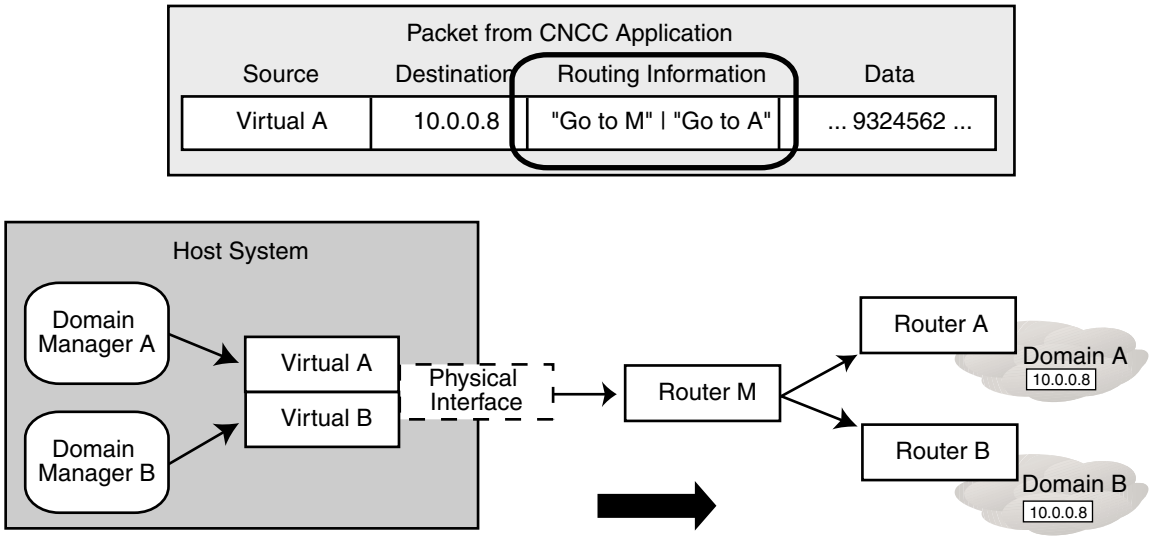


Figure 17: **Packets Containing Routing Instructions**

Configuring Devices to Send SNMP Traps

The final step to managing networks of overlapping IP addresses is to configure the devices in each network to forward SNMP traps to the appropriate NCM application. Devices should be configured to send SNMP traps to the IP address of the appropriate virtual interface used by the domain manager. In our example, devices in Domain A are configured to send SNMP traps to the virtual interface used by Domain Manager A.

The configuration of NCM's trap processing is described in *Designing Trap Processing* on page 53. NCM's trap processor runs automatically as a process within the domain manager. If the configuration for both trap processors is the same, they can share the same *trapd.conf* configuration file. Because each domain manager will listen for traps on different IP addresses, both domain managers can listen on the same port.

Consolidating Management Domain Information

Once the IP Management Domains have been defined, and the virtual IP interfaces and policy routes established, each NCM application separately monitors and correlates the information for each domain.

If you want to consolidate the topology and event information to a single point of reference, use CNCC NCM Service Assurance Manager. Service Assurance distinguishes between topology elements with the same IP address, providing separate notifications and a distinct topological representation for each element.

C

Design and Deployment Checklists

This Appendix gather the checklists that appear throughout this guide into a single, easily accessible location.

Before You Begin Checklist

Before you begin a NCM deployment, you must meet the requirements described in the following checklist.

BEFORE YOU BEGIN CHECKLIST		
COMPLETE	REQUIREMENT	DESCRIPTION
☐	Possess an understanding of the NCM architecture and capabilities.	At a minimum, you must understand the concepts and NCM architecture described in the following documents: • *Network Connectivity Monitor IP Availability Manager User's Guide* • *Network Connectivity Monitor IP Discovery Guide* • *InCharge IP Performance Manager User's Guide* • *Network Connectivity Monitor Service Assurance Manager Configuration Guide* • *An Introduction to Network Connectivity Monitor Service Assurance Manager* • *Network Connectivity Monitor Service Assurance Manager Adapter Platform User's Guide* • *Network Connectivity Monitor System Administration Guide* • *Installation Guide* that accompanied your software product suite
		To improve your understanding, attend NCM training courses offered by Cisco. Typically, deployment requires the knowledge equivalent to what is provided in the training courses on: • CNCC NCM for IP • CNCC NCM Service Assurance Manager • CNCC NCMService Assurance Manager Adapter Platform
☐	Obtain contact information for the deployment team.	The contact list should include titles, responsibilities, and contact methods for all team members.
☐	Get nondisclosure requirements and negotiate an agreement.	Be aware of the requirements of the non-disclosure agreements that are in place for the NCM deployment.
☐	Develop schedules and set milestones for early deliverable.	Scheduling a software deployment varies based on the size and scope of the deployment and the organization's requirements. Typical milestones might include: • Initial project meeting to define the deployment scope • Purchase of NCM software • Project development begins • Installation in test environment complete • Testing complete • Installation in production environment complete • NCM goes live Additional information on scheduling is beyond the scope of this guide.

Architectural Information Checklist

Use the following checklist to aid in gathering information for your architectural design.

ARCHITECTURAL INFORMATION CHECKLIST			
COMPLETE	TASK	DESCRIPITON	RELATED DOCUMENTATION
☐	Describe the organization's requirements and expectations.	Organization's vertical market: _____ (Reference to an organization's documentation) _____ _____ _____	*Determine the Organization's Requirements* on page 9
☐	Obtain network diagrams.	Ensure the diagrams include the locations of the following: • Network Operations Center (NOC) and LANs • Routing and switching devices • Firewalls • WAN links • High speed network technologies such as FDDI and Fast or Gigabit Ethernet In addition, important IP addresses and address ranges should be indicated.	*Obtaining Network Information* on page 10
☐	If possible, schedule and discover the network.	If you intend to use the Discovery Manager to inventory the organization's network, schedule a time to perform the process and then discover the network as scheduled.	*Obtaining Network Information* on page 10
☐	Describe the organization's network priorities.	Document these priorities in the Deployment Build Guide.	*Network Priorities* on page 12
☐	Get the organization's testing/acceptance requirements.	Your design may be required to meet test and acceptance requirements. Obtain any specifications that cover integration testing, user acceptance testing, and operational acceptance testing. You may be required to write an installation or deployment report that follows an organization's particular standards.	*Determine Requirements for Installing Software* on page 13
☐	Describe the organization's requirements for installing new software.	Lab installation and testing Staging (*strongly* recommended) Preproduction deployment Shadow operation period (existing MoM still used) Other _____ Document these requirements and how the design meets them in the Deployment Build Guide.	*Determine Requirements for Installing Software* on page 13

ARCHITECTURAL INFORMATION CHECKLIST			
COMPLETE	TASK	DESCRIPITON	RELATED DOCUMENTATION
☐	List the products that currently monitor the network and will be integrated with NCM.	CNCC NCM's open architecture allows easy integration with third-party software. Many networks have at least a rudimentary network availability monitoring or a legacy system such as HP OpenView or IBM NetView. Document the products (including version) in deployment Build Guide.	*Integrating Existing Software with NCM* on page 13
☐	List device types to manage.	To ensure devices are certified in NCM, obtain a list of the manufacturers and models for all devices in the network. Document the types of managed devices in the Deployment Build Guide.	*Identify the Types of Equipment in the Network* on page 12
☐	Determine the number of managed ports and interfaces in the network.	Document all quantities and calculations used to determine the number of managed ports and interfaces in the Deployment Build Guide.	*Determine Quantities of Network Devices* on page 13
☐	Estimate potential growth in quantity of managed devices.	The NCM deployment must support potential network growth. Estimate the growth over a specific time period. Document the calculations in the Deployment Build Guide.	*Accounting for Network Growth* on page 18
☐	Estimate number of managed systems and network adapters for licensing.	The NCM deployment can only discover and manage the quantity of systems and network adapters that are licensed. Document the quantities in the Deployment Build Guide.	*Determine Quantities of Devices for Licensing* on page 19
☐	Describe the network security.	Describe security features such as the firewalls that will be between parts of the NCM deployment and if access lists are used. Obtain SNMP security parameter values for each device where they are used: for SNMP V1 and V2C, obtain community strings; for SNMP V3, obtain the user name, SNMP engine ID (optional), authentication protocol and password, privacy protocol and password (currently NCM does not support the use of a privacy protocol), and context name, if used. Document the security features in the Deployment Build Guide.	*Gather Network Security Information* on page 20
☐	List any other network requirements or features that may affect NCM.	Document the features in the Deployment Build Guide.	*What Other Network Features Affect NCM?* on page 21

Solution Architecture Diagram Checklist

Use the Solution Architecture Diagram to document your initial overall design of the NCM deployment.

SOLUTION ARCHITECTURE DIAGRAM CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	List important device quantities on the Solution Architecture Diagram and in the Deployment Build Guide.	Start the Solution Architecture Diagram by listing the totals for Routers, Switches, Hubs, Bridges, Hosts, Ports and Interfaces. Include expected growth rate and estimates for managed ports and interfaces. Also document the quantities in the Deployment Build Guide.	*Documenting the Deployment* on page 25
☐	Choose a tier size for platforms supporting CNCC Managers.	☐ Small (P&I:10K/AM or 5K/AM PM) ☐ Medium (P&I:25K/AM or 15K/AM PM) ☐ Large:(P&I:50K/AM or 25K/AM PM) ☐ Very Large:(P&I:100K/AM or 50K /AM PM) Document the choice in the Deployment Build Guide.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Determine quantity of IP Managers required.	Include representations on the Solution Architecture Diagram.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Document equipment supporting NCM components.	Document the hardware and operating system supporting each of the NCM components. Start a chart for each host in the Deployment Build Guide and list the NCM components on the host.	*Determine the Required Size of the NCM Deployment* on page 26
☐	Locate the hosts supporting the NCM components.	Document choices on the Solution Architecture Diagram and in the Deployment Build Guide.	*Locating CNCC Managers and Platforms* on page 30
☐	Determine license server and licensing configuration requirements.	Document requirements on the Solution Architecture Diagram and in the Deployment Build Guide.	*Considering Volume Licensing Configurations* on page 32

SOLUTION ARCHITECTURE DIAGRAM CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine security requirements.	Document requirements in the Deployment Build Guide.	*Considering Security and Firewalls* on page 32
☐	Is Failover Capability Required for NCM?	☐No ☐Yes: Contact Cisco. Document choices on the Solution Architecture Diagram and in the Deployment Build Guide.	*Considering High Availability Configurations* on page 33
☐	Determine if overlapping IP networks are used.	Document needs in the Deployment Build Guide.	*Designing for Overlapping (Duplicate) IP Networks* on page 33
☐	Plan acceptance tests and completion criteria.	Document in the Deployment Build Guide as each portion of NCM functionality is designed. Use them in validation.	*Designing Acceptance Tests* on page 34

Discovery Design Checklist

Before discovering the network using NCM, the requirements in the following checklist must be completed.

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
Initial Discovery			
☐	Define a method for the initial topology discovery.	☐Use a comprehensive seed file without autodiscovery. ☐Use autodiscovery with an agent or seedfile. Document the method in the Deployment Build Guide.	*Initial Discovery* on page 38
Topology Maintenance and Subsequent Discovery			
☐	Define a schedule for Full Discovery.	Define a regular schedule for full discovery. Choose a time of relative inactivity. Document the schedule in the Deployment Build Guide. Include *crontab* or *sm_sched* control file entries if used.	*Topology Maintenance and Subsequent Discovery* on page 40

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Define a schedule for Pending Discovery.	Define a regular schedule for pending discovery. Choose a time of relative inactivity. Document the schedule in the Deployment Build Guide. Include *crontab* or *sm_sched* control file entries if these utilities are used.	*Topology Maintenance and Subsequent Discovery* on page 40
☐	Determine if Autodiscovery is appropriate.	Document choice in the Deployment Build Guide.	*Topology Maintenance and Subsequent Discovery* on page 40
☐	Choose a method for adding devices to the topology.	☐ Agent without autodiscovery. ☐ Seed file without autodiscovery. ☐ Use autodiscovery with an agent or seedfile. Document choice in the Deployment Build Guide.	*Adding New Systems to an Existing Topology* on page 41
☐	Prepare Seed File or Choose Agent.	If a seed file will be used to add devices to the topology, obtain a list of devices with names or IP addresses. Document how to obtain the list or the location of the list in the Deployment Build Guide. If an agent will be used instead, document the IP address or name of the agent.	*Adding New Systems to an Existing Topology* on page 41
☐	Define Autodiscovery Filters.	If autodiscovery is enabled, configure autodiscovery filters. These are inclusive filters that add devices to the topology. Document the autodiscovery filter criteria in the Deployment Build Guide.	*Controlling Autodiscovery with Filters* on page 41
☐	Define an Exclude Filter.	To exclude specific devices, use the exclude filter in the *discovery.conf* file. This simplifies creation of the autodiscovery filters. Document exclude filter entries in the Deployment Build Guide.	*Controlling Autodiscovery with Filters* on page 41
☐	Obtain SNMP security parameters per device.	NCM Domain Managers use SNMP to poll the device agents. In order to do this, the Domain Manager needs the appropriate security information for the SNMP version: V1 and V2C use READ community strings for every device that will be managed; V3 uses the user name, SNMP engine ID, authentication protocol and password, privacy protocol and password and the context name. These parameters will be needed during discovery. Document in the Deployment Build Guide if permitted.	*Discovery and Security* on page 43

DISCOVERY CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Open necessary firewall ports.	If there is a firewall between any portions of the management infrastructure, certain TCP and UDP ports in the firewall must be opened for proper communications: • SNMP polls: 161 • SNMP traps: 162 • NCM Broker: 426 • NCM License Manager: 1744 • CNCC Managers (1 per manager): configurable • NCM adapters, including SNMP Trap Adapter (Receiver) and Syslog Adapter: configurable Document the ports that are opened in the Deployment Build Guide.	*Discovery and Security* on page 43
☐	Provide access to network devices to manage.	For each device that NCM will monitor, the device's access list must include the IP address of the hosts where CNCC Managers are installed. NCM must have full access to browse the MIBs of the devices. Document in the Deployment Build Guide.	*Discovery and Security* on page 43
☐	Ensure DNS is properly configured.	For NCM to correctly name devices in its topology, the DNS needs to be clean (proper forward and reverse lookup). If DNS is not used, use of an */etc/hosts* file or not doing any name resolution at all can be considered.	*Discovery and the Domain Name System* on page 44
☐	Determine if Discovery post processing is required.	Determine if discovery post processing using ASL rulesets will be used. Document in the Deployment Build Guide.	*Advanced Discovery Post-Processing* on page 44
☐	List unreachable IP Addresses	If there are groups of IP addresses that are NOT normally reachable, assemble a list of IP ranges or some matching criteria so NCM will not unnecessarily ping these addresses. Document these addresses in the Deployment Build Guide.	*Advanced Discovery Post-Processing* on page 44

Polling and Threshold Checklist

POLLING AND THRESHOLD CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine if polling changes are needed.	Design polling groups based on importance of network device performance both to the network and to the various parts of the organization. Also consider network latency to determine if changes are needed. Document choices in the Deployment Build Guide.	*Modifying Polling and Polling Groups* on page 50
☐	List all polling changes by polling group.	Modify polling parameters based on importance of network device performance. Additional modifications may be necessary if polling does not present an accurate picture of network availability during validation. Document new polling parameters in the Deployment Build Guide.	*Modifying Polling and Polling Groups* on page 50
☐	Determine if threshold changes are needed.	Design threshold groups based on importance of network device performance both to the network and to the various parts of the organization. Document choices in the Deployment Build Guide.	*Modifying Threshold Values and Threshold Groups* on page 51
☐	List all threshold changes by threshold group.	Modify threshold parameters based on the expected effect of degraded performance on network operations. Additional modifications may be necessary during validation and as the organization gains experience with the performance indicators. Document new threshold parameters in the Deployment Build Guide.	*Modifying Threshold Values and Threshold Groups* on page 51

Trap Processing Checklist

TRAP PROCESSING CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Adapt the recommended trap processing design to the NCM deployment.	Use the recommended trap processing design whenever possible. If you must use a different design, ensure that Cisco approves of the design. Add the trap processing design to the Solution Architecture Diagram.	*Recommended Trap Processing Design* on page 53
☐	Determine IP address:port locations to forward Availability Manager and Performance Manager traps.	For the trap exploder instance of theCNCC NCM SNMP Trap Adapter, the *trapd.conf* file must be modified to specify destinations for the Availability Manager and Performance Manager traps. Document in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Determine where network devices send traps.	In most cases, the trap exploder should be configured to listen for traps at the location where network devices already send traps. Document port locations in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Determine which traps will be discarded.	The design will use the trap exploder instance of the CNCC NCM SNMP Trap Adapter to forward useless traps to a nonexistent IP address:port. Document these traps in the Deployment Build Guide.	*Trap Forwarding* on page 58
☐	Choose traps to process into notifications and define notification properties.	Use parameters in the *trap_mgr.conf* configuration file to choose the appropriate traps to process into notifications and to define the characteristics of the corresponding notifications. Document the traps and notifications properties in the Deployment Build Guide.	*Traps and Notifications* on page 58
☐	Choose traps to aggregate into a common notification.	Use aggregate notifications to combine related traps and reduce the workload of NCM operators. Document the aggregated notifications in the Deployment Build Guide.	*Traps and Notifications* on page 58
☐	If needed, plan for advanced processing of traps using ASL scripts.	Define the desired trap processing that requires ASL scripts. Document the purpose of this processing purpose and explain the code in the Deployment Build Guide.	*Advanced Trap Processing Using ASL Scripts* on page 59

Syslog Processing Checklist (Optional)

SYSLOG PROCESSING CHECKLIST			
COMPLETE	TASK	DESCRIPTION	RELATED DOCUMENTATION
☐	Determine how to create the file for processing by the CNCC NCM Syslog Adapter.	A file must be created that the CNCC NCM Syslog Adapter can parse. Determine which devices will contribute messages to the file. Consistent layout of the messages in the file is required for CNCC NCM Syslog Adapter processing. Include all details in the Deployment Build Guide.	*Creating the Syslog File* on page 62
☐	Determine the location of the file that the Syslog Adapter will process.	The process that is creating the file must be able to receive messages from source applications and the created file must be accessible by the CNCC NCM Syslog Adapter. Include all details in the Deployment Build Guide, including location, host and path.	*Processing the Syslog File* on page 62
☐	Choose the messages that are most important for processing.	Choose the messages that are most important for processing. Include all details in the Deployment Build Guide.	*Processing the Syslog File* on page 62
☐	Determine the characteristics of the notifications that are generated.	For each message that generates a notification, determine the notification format. These characteristics will be used to develop the hook script for the CNCC NCM syslog processing deployment. Include all details in the Deployment Build Guide.	*Processing the Syslog File* on page 62
☐	Add Syslog Processing to the Solution Architecture Diagram.	Add Syslog Processing to the Solution Architecture Diagram.	*Processing the Syslog File* on page 62

Index