InCharge™

Network Protocol Manager Configuration Guide

Version 1.1

OL-7715-01

smarts®

CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED IN THE ABOVE-REFERENCED LICENSE BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARITES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. JfreeChart library (included herein as .jar files) is provided in accordance with, and its use is covered by the GNU Lesser General Public License Version 2.1, which is set forth at http://www.object-refinery.com/lgpl.html/.

BMC – product library

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

Crystal Decisions Products

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

GNU eTeks PJA Toolkit

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

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

IBM Runtime for AIX

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

HP-UX Runtime Environment for the Java™ 2 Platform

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

DataDirect Technologies

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

NetBSD

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

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

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

RSA Data Security, Inc.

AES

Contents

Preface

This document provides instructions for configuring InCharge Network Protocol Manager. Topics include updating control files and adapter files, and configuring InCharge Service Assurance Manager to work with Network Protocol Manager.

Intended Audience

This document is intended for administrators and integrators who need to configure and maintain InCharge Network Protocol Manager.

Prerequisites

It is assumed that readers of this document have the administrative privileges and the necessary experience to properly install and configure network management software.

Document Organization

This document consists of the following chapters.

Table 1: Document Organization

1. INTRODUCTION	Provides an architectural and functional overview of Network Protocol Manager, and highlights configuration tasks for Network Protocol Manager.
2. CONFIGURING NETWORK PROTOCOL MANAGER	Provides detailed information about configuring Network Protocol Manager.
3. CONFIGURING SERVICE ASSURANCE MANAGER	Provides detailed information about configuring Service Assurance Manager to work with Network Protocol Manager.

Documentation Conventions

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

Table 2: Documentation Conventions

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
▼▲	Indicates a command is wrapped over one or more lines. The command must be typed as one line.

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 InCharge Manager is used to refer to InCharge programs such as Domain Managers, Global Managers, and adapters.

InCharge Network Protocol Suite Installation Directory

In this document, the term ***BASEDIR*** represents the location where InCharge 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 InCharge software platform version number. The *<productsuite>* represents the InCharge product suite to which the product belongs. For example, on UNIX operating systems, InCharge Network Protocol Manager is, by default, installed to: */opt/InCharge6/NPM/smarts*. On Windows operating systems, this product is, by default, installed to: *C:\InCharge6\NPM\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 InCharge software, refer to the *InCharge System Administration Guide*.

InCharge Network Protocol Suite Products

The InCharge Network Protocol Management Suite includes the following products:

- Network Protocol Manager for BGP
- Network Protocol Manager for OSPF

Additional Resources

In addition to this document, SMARTS provides the following resources.

InCharge Commands

Descriptions of InCharge 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 document may find other SMARTS documentation (also available in the ***BASEDIR****/smarts/doc/pdf* directory) helpful.

InCharge Documentation

The following SMARTS documents are product independent and thus relevant to users of all InCharge products:

- *InCharge Release Notes*
- *InCharge Documentation Roadmap*
- *InCharge System Administration Guide*
- *InCharge ICIM Reference*
- *InCharge ASL Reference Guide*
- *InCharge Perl Reference Guide*

InCharge Network Protocol Management Documentation

The following SMARTS documents are relevant to users of the InCharge Network Protocol Management product suite:

- *InCharge Network Protocol Management Suite Installation Guide*
- *InCharge Network Protocol Manager for BGP User's Guide*
- *InCharge Network Protocol Manager for OSPF User's Guide*
- *InCharge Network Protocol Manager Configuration Guide*
- *InCharge IP Discovery Guide Supplement for Networking Protocols*

Refer to the *InCharge Documentation Roadmap* for documentation resources provided with other SMARTS InCharge product suites.

Technical Support

SMARTS provides technical support by e-mail or phone during normal business hours (8:00 A.M.—6:00 P.M. U.S. Eastern and Greenwich Mean Time). In addition, SMARTS offers the InCharge Express self-service web tool. The web tool allows customers to access a personalized web page and view, modify, or create help/trouble/support tickets. To access the self-service web tool, point your browser to:

https://websupport.smarts.com/SelfService/smarts/en-us

U.S.A Technical Support
E-Mail: *support@smarts.com*
Phone: +1.914.798.8600

EMEA Technical Support
E-Mail: *support-emea@smarts.com*
Phone: +44 (0) 1753.878140

Asia-Pac Technical Support
E-Mail: *support-asiapac@smarts.com*

You may also contact SMARTS at:

	U.S.A World Headquarters	United Kingdom
Address	SMARTS 44 South Broadway White Plains, New York 10601 U.S.A	SMARTS Gainsborough House 17-23 High Street Slough Berkshire SL1 1DY United Kingdom
Phone	+1.914.948.6200	+44 (0)1753.878110
Fax	+1.914.948.6270	+44 (0)1753.878111

For sales inquiries, contact SMARTS Sales at:
sales@smarts.com

SMARTS is on the World Wide Web at:
http://www.smarts.com

1

Introduction

This chapter provides a brief architectural and functional overview of InCharge Network Protocol Manager. It also highlights the configuration tasks that need to be performed to set up and maintain Network Protocol Manager.

Architectural and Functional Overview

InCharge Network Protocol Manager, working with InCharge IP Availability Manager, discovers and monitors network devices running Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF) services, diagnoses BGP- or OSPF-related failures, and reports the results of its analysis to InCharge Service Assurance Manager. Network Protocol Manager also detects common configuration problems that occur when deploying and maintaining the routing infrastructure.

Figure 1 illustrates the components and the flow of information. A single instance of Network Protocol Manager appears in the figure. Separate instances of Network Protocol Manager are required to manage each network protocol: one for BGP and another for OSPF.

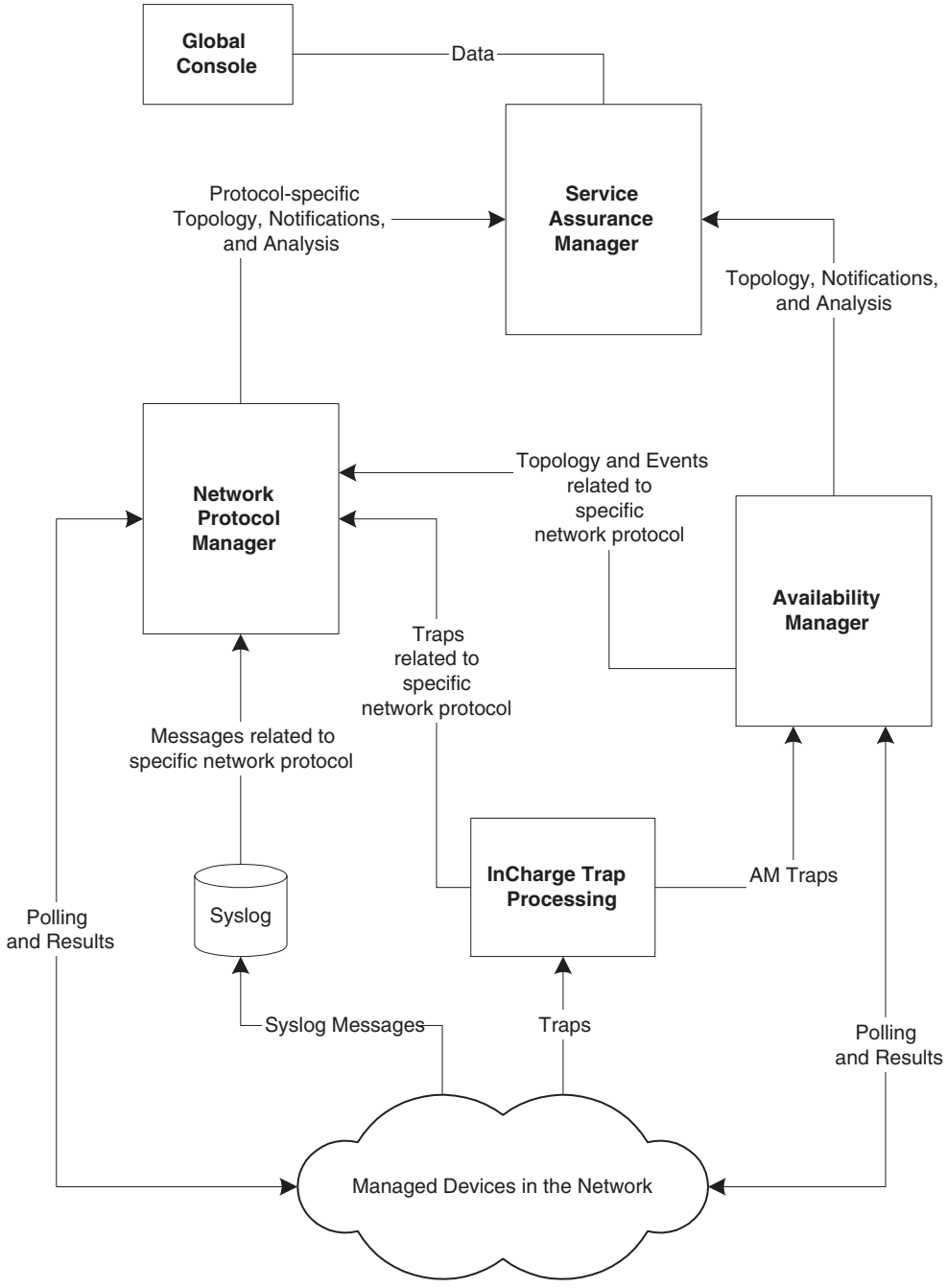

Figure 1: InCharge Network Protocol Manager Architecture

Availability Manager

Availability Manager discovers physical and logical Layer 2 and Layer 3 network elements in multi-vendor, switched, and routed networks. It monitors and analyzes network connectivity and sends network topology and event information to Service Assurance Manager, and sends BGP- or OSPF-relevant topology and event information to Network Protocol Manager.

Network Protocol Manager

Upon importing the initial topology from Availability Manager, Network Protocol Manager sends SNMP polls to the routing devices to discover the additional protocol information that it needs to build the routing protocol topology for the managed environment.

- For BGP, Network Protocol Manager discovers the BGP services running on the routing devices, the BGP sessions participating in the routing updates, and BGP configurations. The BGP configurations include autonomous system numbers.
- For OSPF, Network Protocol Manager discovers the OSPF services running on the routing devices, the OSPF adjacencies participating in the routing updates, and OSPF configurations. The OSPF configurations include OSPF areas, Hello intervals, Dead intervals, and authentication parameters.

Network Protocol Manager supports the BGP and OSPF routing protocols and any routing device—router, router switch module (RSM), router switch feature card (RSFC), or multi-layer switch feature card (MSFC)—that supports the following specifications:

- For BGP, the SNMP BGP-4 MIB defined in RFC 1657.
- For OSPF, the SNMP OSPF MIB defined in RFC 1253.

RSMs, RSFCs, and MSFCs are routing devices installed as cards in Layer 3 switches.

Network Protocol Manager for BGP discovers all BGP services running on a routing device and collectively represents the services as a single BGP service. Similarly, Network Protocol Manager for OSPF discovers all OSPF services running on a routing device and collectively represents the services as a single OSPF service. For detailed information about discovery, see the *InCharge IP Discovery Guide Supplement for Networking Protocols*.

To determine the state of the managed OSPF or BGP devices in the network, Network Protocol Manager sends SNMP polls to the routing devices and combines the polling results with (1) the traps and syslog messages received from the managed network and (2) the events received from Availability Manager.

Network Protocol Manager correlates this data to diagnose and pinpoint the root cause of failures:

- For BGP, the failures include BGP service, session, and configuration failures.
- For OSPF, the failures include OSPF service, adjacency, and configuration failures.

Network Protocol Manager sends the analysis results along with topology and event information to Service Assurance Manager.

Service Assurance Manager

Service Assurance Manager integrates the topology and event information imported from Availability Manager and Network Protocol Manager and relates the information to services and customers. It also provides cross-domain, end-to-end impact analysis.

Service Assurance Manager displays the topology, event, and impact information through the Global Console.

Global Console

The Global Console enables users to browse the network protocol topology in various forms, including maps, and to view notifications about events that impact BGP or OSPF availability.

SNMP Trap and Syslog Processing

When SNMP trap and syslog processing is enabled, Network Protocol Manager obtains configuration, change, and BGP session or OSPF adjacency status information for the routing devices from SNMP trap messages and syslog messages sent by the routing devices. Network Protocol Manager extracts the information from the traps and syslog messages and updates the appropriate router attributes.

Processing of SNMP traps and syslog messages is recommended but not required because Network Protocol Manager polls the network for status information. However, if neither SNMP traps nor syslog messages are received by Network Protocol Manager, immediate asynchronous notification of status change is not available; instead, the response time is determined by the length of the SNMP polling interval (240 seconds by default).

By default, SNMP trap and syslog processing is disabled. For information about enabling trap and syslog processing, see *Configuring Network Protocol Manager* on page 7.

For information about the SNMP traps and the syslog messages processed by Network Protocol Manager, see the *InCharge Network Protocol Manager for BGP User's Guide* and the *InCharge Network Protocol Manager for OSPF User's Guide*.

Configuration Overview

The following sections highlight the configuration tasks associated with the setup and maintenance of a Network Protocol Manager deployment. These tasks involve configuring the Network Protocol Manager, Service Assurance Manager, and Availability Manager applications that are part of the deployment.

Network Protocol Manager Configuration Tasks

In addition to the configuration and administration tasks common to all InCharge Domain Managers, the following additional tasks need to be performed to set up Network Protocol Manager:

- Edit configuration files to enable the use of BGP and/or OSPF traps and syslog messages. Perform this task before starting Network Protocol Manager.
- Configure syslog message forwarding to forward syslog messages to Network Protocol Manager. Perform this task before starting Network Protocol Manager.
- Add Availability Manager as a source to Network Protocol Manager. Perform this task after starting Network Protocol Manager.

For detailed information about these configuration tasks, see *Configuring Network Protocol Manager* on page 7.

Service Assurance Manager Configuration Tasks

In addition to the configuration and administration tasks common to all Service Assurance Global Managers, the following additional tasks need to be performed to set up Service Assurance Manager in a Network Protocol Manager deployment:

- Edit the Service Assurance *ics.conf* file so that Availability Manager and Network Protocol Manager data can be imported into Service Assurance Manager.
- Edit the Service Assurance *trapd.conf* file for the SNMP Trap Adapter (Receiver) so that BGP and OSPF traps can be forwarded to Network Protocol Manager.
- Use the Global Manager Administration Console to enable the display of the BGP and OSPF Connectivity Maps for users who require access to these maps.

For detailed information about these configuration tasks, see *Configuring Service Assurance Manager* on page 15.

Availability Manager Configuration Tasks

No special Network Protocol Manager-related configuration tasks are required at Availability Manager to support the Network Protocol Manager deployment. For general information about configuring Availability Manager, see the *InCharge IP Deployment Guide*. Also, see the *InCharge IP Discovery Guide Supplement for Networking Protocols*.

2

Configuring Network Protocol Manager

This chapter provides detailed information about configuring Network Protocol Manager. It includes the following topics:

- Editing the Network Protocol Manager *.conf* files (Optional)
- Configuring syslog message forwarding (Optional)
- Adding Availability Manager as a Source for Network Protocol Manager (Required)

Network Protocol Manager is installed as either a BGP service or an OSPF service: if you intend to manage both BGP and OSPF protocols, you must deploy separate Network Protocol Managers, one for each protocol. Separate Network Protocol Managers may run on the same computer system.

Using the sm_edit Utility to Modify Network Protocol Manager Files

As part of the InCharge deployment and configuration process, you will need to modify certain files. User modifiable files include InCharge configuration files, rule set files, templates, and files (such as seed files, and security configuration files) containing encrypted passwords. Original versions of these files are installed into appropriate subdirectories under the ***BASEDIR****/smarts/* hierarchy. For example, on UNIX operating systems the original versions of Global Manager configuration files are installed to */opt/InCharge6/SAM/smarts/conf/ics.*

Original versions of files should not be altered. If a file requires modification, it must be stored as a local copy of the file in ***BASEDIR****/smarts/local* or one of its subdirectories. For example, a modified *ics.conf* file should be saved to */opt/InCharge6/SAM/smarts/local/conf/ics.* InCharge software is designed to first search for user modifiable files in ***BASEDIR****/smarts/local* or one of its subdirectories. If a modified version of a file is not found in the local area, InCharge software then searches appropriate nonlocal directories.

Note: Original versions of files may be changed or updated as part of an InCharge software upgrade. However, files located in ***BASEDIR****/smarts/local* are always retained during an upgrade.

To facilitate proper file editing, SMARTS provides the *sm_edit* utility with every InCharge product suite. When used to modify an original version of a file, this utility automatically creates a local copy of the file and places it in the appropriate location under ***BASEDIR****/smarts/local*. This ensures that the original version of the file remains unchanged. In both UNIX and Windows environments, you can invoke *sm_edit* from the command line. Optionally, you can configure Windows so that *sm_edit* is automatically invoked when user-modifiable files are double-clicked in Windows Explorer.

To invoke the *sm_edit* utility from the command line, specify the path and the name of the file you want to edit under ***BASEDIR****/smarts*. If multiple InCharge products are running on the same host, you should ensure that you invoke *sm_edit* from the *bin* directory of the product suite whose files you wish to edit. For example, to edit the configuration file for the Global Manager, you invoke the *sm_edit* utility as follows:

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

The *sm_edit* utility automatically creates a local copy of the *ics.conf* file in the ***BASEDIR****/smarts/local/conf/ics* directory, if necessary, and opens the file in a text editor. If a local version of the file already exists, the *sm_edit* utility opens the local version in a text editor. In addition, *sm_edit* creates any necessary directories.

For more information about how to properly edit user modifiable InCharge files and how to use the *sm_edit* utility, refer to the *InCharge System Administration Guide*.

Editing the Network Protocol Manager .conf Files

Two configuration files are supplied with Network Protocol Manager:

- The *bgp.conf* file is located in the ***BASEDIR****/smarts/conf/bgp* directory
- The *ospf.conf* file is located in the ***BASEDIR****/smarts/conf/ospf* directory.

If your implementation of Network Protocol Manager requires trap processing and/or syslog message processing, enable the processing by editing one or both of these configuration files. You must make these edits before Network Protocol Manager is started.

The following illustrates the content of the *bgp.conf* file as supplied with Network Protocol Manager.

```
#
# Copyright (C) 2004 System Management ARTS (SMARTS)
# All Rights Reserved
#
# RCS $Id: bgp.conf,v 1.1.2.1 2004/08/19 18:48:00 sv1 Exp $
#
#
# The purpose of this file is to set up local environment
# for NPM for BGP.
#
MSI_AdapterManager::BGP-Adapter-Manager {
    Config      = "bgp"
    TrapPort    = 0
    TraceTraps  = FALSE
    SyslogName  = ""
    TraceSyslog = FALSE
    AdminDownFlag = FALSE
}
```

The following illustrates the content of the *ospf.conf* file as supplied with Network Protocol Manager.

```
#
# Copyright (C) 2004 System Management ARTS (SMARTS)
# All Rights Reserved
#
# RCS $Id: ospf.conf,v 1.1.2.1 2004/08/19 18:48:50 sv1 Exp $
#
#
# The purpose of this file is to set up local environment
# for NPM for OSPF.
#
MSI_AdapterManager::OSPF-Adapter-Manager {
    Config      = "ospf"
    TrapPort    = 0
    TraceTraps  = FALSE
    SyslogName  = ""
    TraceSyslog = FALSE
    AdminDownFlag = FALSE
}
```

Network Protocol Manager for BGP reads the *bgp.conf* file at startup and saves the configuration information for BGP in its repository. Similarly, Network Protocol Manager for OSPF reads the *ospf.conf* file at startup and saves the configuration information for OSPF in its repository.

Table 3 describes the parameters in the *bgp.conf* and *ospf.conf* files.Use the *sm_edit* utility to change the parameter settings as needed.

Table 3: Network Protocol Manager .conf File Parameters

PARAMETER	PURPOSE	COMMENT OR EXAMPLE SETTINGS
Config	Determines whether Network Protocol Manager is a BGP or OSPF Manager.	Do not change this parameter.
TrapPort	Enables Network Protocol Manager trap processing and determines which port Network Protocol Manager will use to listen for trap messages. Default: TrapPort = 0	To enable Network Protocol Manager trap processing and set the trap port to 162: TrapPort = 162 To disable Network Protocol Manager trap processing: TrapPort = 0
TraceTraps	Activates tracing for Network Protocol Manager trap processing. Default: TraceTraps = False	Do not change this parameter.

Table 3: Network Protocol Manager .conf File Parameters*(continued)*

PARAMETER	PURPOSE	COMMENT OR EXAMPLE SETTINGS
SyslogName	Enables Network Protocol Manager syslog message processing and Identifies the local syslog file to be tailed. Default: SyslogName = ""	To enable local Network Protocol Manager syslog message processing and to tail the /var/adm/messages file: SyslogName = "/var/adm/messages" To disable local Network Protocol Manager syslog message processing: SyslogName = "" Note that when the syslog file is on a remote system, always disable local syslog message processing (SyslogName = "").
TraceSyslog	Activates tracing for Network Protocol Manager syslog message processing. Default: TraceSyslog = False	Do not change this parameter.
AdminDownFlag	In the bgp.conf file: For BGP protocol endpoints or physical interfaces that are administratively down (manually disabled), disables all alarms on their BGP sessions. Default: AdminDownFlag = False	To disable alarms for administratively down BGP endpoints or physical interfaces on their BGP sessions: AdminDownFlag = True To enable alarms for administratively down BGP endpoints or physical interfaces on their BGP sessions: AdminDownFlag = False
	In the ospf.conf file: For OSPF interfaces or physical interfaces that are administratively down (manually disabled), disables all alarms on their OSPF neighbor relationships. Default: AdminDownFlag = False	To disable alarms for administratively down OSPF interfaces or physical interfaces on their OSPF neighbor relationships: AdminDownFlag = True To enable alarms for administratively down OSPF interfaces or physical interfaces on their OSPF neighbor relationships: AdminDownFlag = False

Configuring Syslog Message Forwarding

Managed devices running the BGP or OSPF protocols typically send syslog messages to a remote system that is running a syslog daemon. The syslog daemon writes all of the messages to a single syslog file. If needed, the appropriate messages in this file can be forwarded to Network Protocol Manager for analysis.

If Syslog File Is on Local System

If the syslog file is on the same computer system as Network Protocol Manager, set the value of the *SyslogName* parameter in the *bgp.conf* and/or *ospf.conf* files to the full path and name of the syslog file to forward messages to Network Protocol Manager.

If Syslog File Is on Remote System

If the syslog file is on a different computer system than Network Protocol Manager, follow these steps to forward messages to the Network Protocol Manager:

1. On the local system, where the Network Protocol Manager for BGP and/or Network Protocol Manager for OSPF reside, set the value of the *SyslogName* parameter in the *bgp.conf* and/or *ospf.conf* files to "".
2. On the remote system, where the syslog file resides, install a second instance of the Network Protocol Management Suite.

   During the installation, do not select *NPM for BGP* or *NPM for OSPF* in the Services screen because you will manually start the Network Protocol Manager executable as a *syslog adapter*. One syslog adapter instance is required to forward syslog messages to Network Protocol Manager for BGP, and another syslog adapter instance is required to forward syslog messages to Network Protocol Manager for OSPF.
3. On the remote system, start the syslog adapters.

   A sample command line for a target Network Protocol Manager for BGP named INCHARGE-BGP is:

   ▼
   ```
   sm_adapter --name=INCHARGE-BGP-SYSLOG -s INCHARGE-BGP
   --output=BGP-SYSLOG --daemon --tail=[full path to log
   file]bgp/bgp-syslog.asl
   ```
   ▲

   A sample command line for a target Network Protocol Manager for OSPF named INCHARGE-OSPF is:

   ▼
   ```
   sm_adapter --name=INCHARGE-OSPF-SYSLOG -s INCHARGE-OSPF
   --output=OSPF-SYSLOG --daemon --tail=[full path to log
   file]ospf/ospf-syslog.asl
   ```
   ▲

▼▲ Indicates the command must be typed as one line.

Figure 2 shows the forwarding of syslog messages from a remote system.

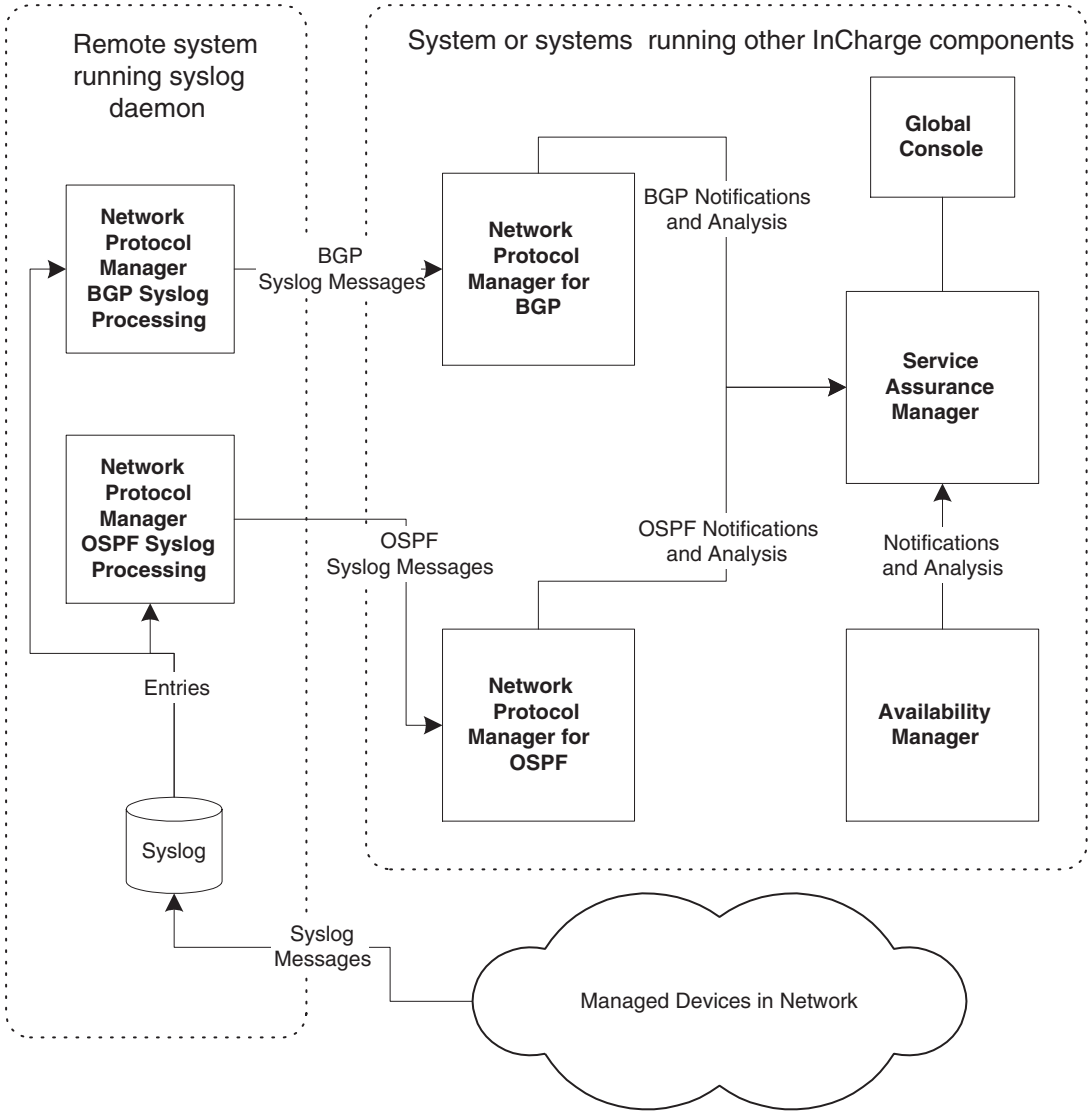

Figure 2: Syslog Forwarding from a Remote System to Network Protocol Manager

Adding Availability Manager as a Source to Network Protocol Manager

To allow Network Protocol Manager to import a BGP- or OSPF-related topology that is discovered by an Availability Manager, the Availability Manager is added as a source to Network Protocol Manager. Perform this after starting Network Protocol Manager. Multiple instances of Availability Manager can be sources to Network Protocol Manager.

To add an Availability Manager as a source to Network Protocol Manager, follow these steps:

1. In the Domain Manager Administration Console, after attaching to the appropriate Network Protocol Manager, choose *Topology > Add Source* to launch the Add Source dialog.
2. In the Add Source dialog, select the AM element type, enter the name of the Availability Manager, and then click **OK**.

   In response, Network Protocol Manager probes the selected Availability Manager for BGP- or OSPF-related topology information. A Discovery Progress window opens and displays progress messages. When "Last discovery completed" appears near the end of the progress report in the Discovery Status section, the probing of topology information has completed.
3. Repeat Steps 1 and 2 until each Availability Manager in the deployment has been added as a source to Network Protocol Manager.

When an Availability Manager is added as a source to Network Protocol Manager, Network Protocol Manager immediately imports the BGP or OSPF object collection set from Availability Manager. Thereafter, Network Protocol Manager imports the BGP or OSPF object collection set from Availability Manager whenever Availability Manager saves its topology.

3

Configuring Service Assurance Manager

This chapter provides detailed information about configuring Service Assurance Manager, also referred to as the Global Manager, to work with Network Protocol Manager. It includes the following topics:

- Editing the Service Assurance Manager's *ics.conf* file (Required)
- Editing the SNMP Trap Adapter's *trapd.conf* file (Optional)
- Enabling BGP and OSPF maps (Required)

For general information about configuring Service Assurance Manager, see the *InCharge Service Assurance Manager Configuration Guide*. For general information about configuring Service Assurance adapters, see the *InCharge Service Assurance Manager Adapter User's Guide*.

Editing the Service Assurance Manager's ics.conf File

For Service Assurance Manager to import Network Protocol Manager topology and events, you need to uncomment DomainType entries for Network Protocol Manager for BGP or Network Protocol Manager for OSPF in the Service Assurance *ics.conf* file. (The DomainType entry for Availability Manager is uncommented by default.) This file is located in the ***BASEDIR****/smarts/conf/ics* directory of the Service Assurance Manager install area.

Use the *sm_edit* utility to uncomment the DomainType entries. The minimum certainties and smoothing intervals for Network Protocol Manager for BGP and Network Protocol Manager for OSPF are set to the same value as set for Availability Manager.

The following illustrates the uncommented DomainType entries for Network Protocol Manager in the *ics.conf* file.

```
DomainSection
{
.
.
.
#   DomainType definition for BGP.
     DomainType
     {
          ConfFile          = "dxa-bgp.conf";
          MinimumCertainty  = 0.24;
          SmoothingInterval = 65;
##         HookScript        = "ics/dxa-sample-hook.asl";
          Name              = "INCHARGE-BGP";
     }

#   DomainType definition for OSPF.
     DomainType
     {
          ConfFile          = "dxa-ospf.conf";
          MinimumCertainty  = 0.24;
          SmoothingInterval = 65;
##         HookScript        = "ics/dxa-sample-hook.asl";
          Name              = "INCHARGE-OSPF";
     }

}
```

Note: Do not uncomment the HookScript fields unless you customize the associated ASL hookscript files.

Editing the SNMP Trap Adapter's trapd.conf File

For Network Protocol Manager to receive BGP or OSPF traps that are sent to a remote system, the traps must be forwarded to the port that the Network Protocol Manager is using to listen for traps. Typically, on the system where the managed network devices send their traps, an instance of the Service Assurance SNMP Trap Adapter (Receiver) is configured as a "trap exploder" and forwards the appropriate traps to the appropriate destinations.

Figure 3 details the flow of information during trap processing with Network Protocol Manager.

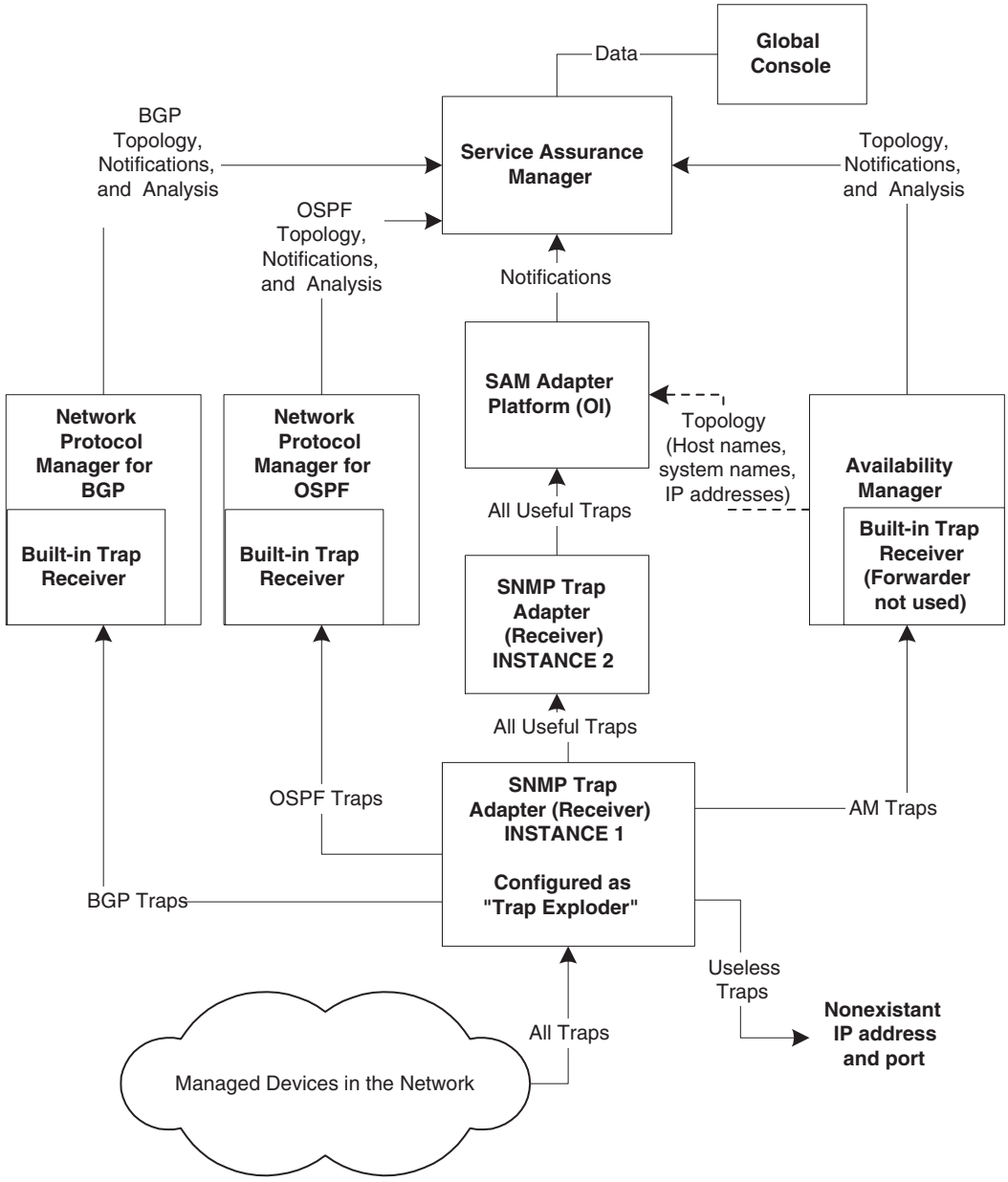

Figure 3: InCharge Trap Processing with Network Protocol Manager

The configuration of the trap exploder is controlled by FORWARD entries in the Service Assurance *trapd.conf* file, which is located in the ***BASEDIR****/smarts/conf/trapd* directory of a Service Assurance Manager install area. Use the *sm_edit* utility to configure the *trapd.conf* file to forward traps to the BGP and/or OSPF trap ports designated in the *bgp.conf* and/or *ospf.conf* files of the target Network Protocol Manager.

To forward BGP traps, add the following FORWARD entries (and comments for usability purposes) to the *trapd.conf* file. Replace ***host:port*** with the Network Protocol Manager destination (host name and port number) that is to receive the BGP trap messages.

```
#       BGP Snmp v2 traps
FORWARD: *.*.*.* .1.3.6.1.2.1.15.7 * * host:port
#       BGP Snmp v1 traps
FORWARD: *.*.*.* .1.3.6.1.2.1.15 * * host:port
#       CiscoMgmt trap for reconfiguration
FORWARD: *.*.*.* .1.3.6.1.4.1.9.9.43.2 * * host:port
```

To forward OSPF traps, add the following FORWARD entries (and comments for usability purposes) to the *trapd.conf* file. Replace ***host:port*** with the Network Protocol Manager destination (host name and port number) that is to receive the OSPF trap messages.

```
#       OSPF traps for non-cisco devices
FORWARD: *.*.*.* .1.3.6.1.2.1.14.16.2 * * host:port
#       CiscoMgmt trap for reconfiguration
FORWARD: *.*.*.* .1.3.6.1.4.1.9.9.43.2 * * host:port
```

The *trapd.conf* file used for forwarding has the entry ENABLE_FWD: TRUE.

For complete details about configuring InCharge trap processing, including the use of the trap exploder to forward traps to other InCharge Domain Managers, see the *InCharge IP Deployment Guide*.

Enabling BGP and OSPF Maps

View BGP and OSPF topology maps by attaching the Global Console to Service Assurance Manager. For detailed information about these maps, see the *InCharge Network Protocol Manager for BGP User's Guide* and the *InCharge Network Protocol Manager for OSPF User's Guide*.

By default, the display of the BGP and OSPF maps is disabled. To enable the display of these maps, follow these steps:

1. Attach a Global Console to the Service Assurance Manager (Global Manager).
2. In the Notification Log Console, select *Configure > Global Manager Administration Console*.
3. In the Global Manager Administration Console, click the plus sign (+) next to User Profiles to display the available user profiles.
4. Select the user profile for which you want to enable the viewing of BGP and OSPF maps. For example, select admin-profile. The Configure User Profile "admin-profile" panel appears on the right side of the Global Manager Administration Console as shown in Figure 4.

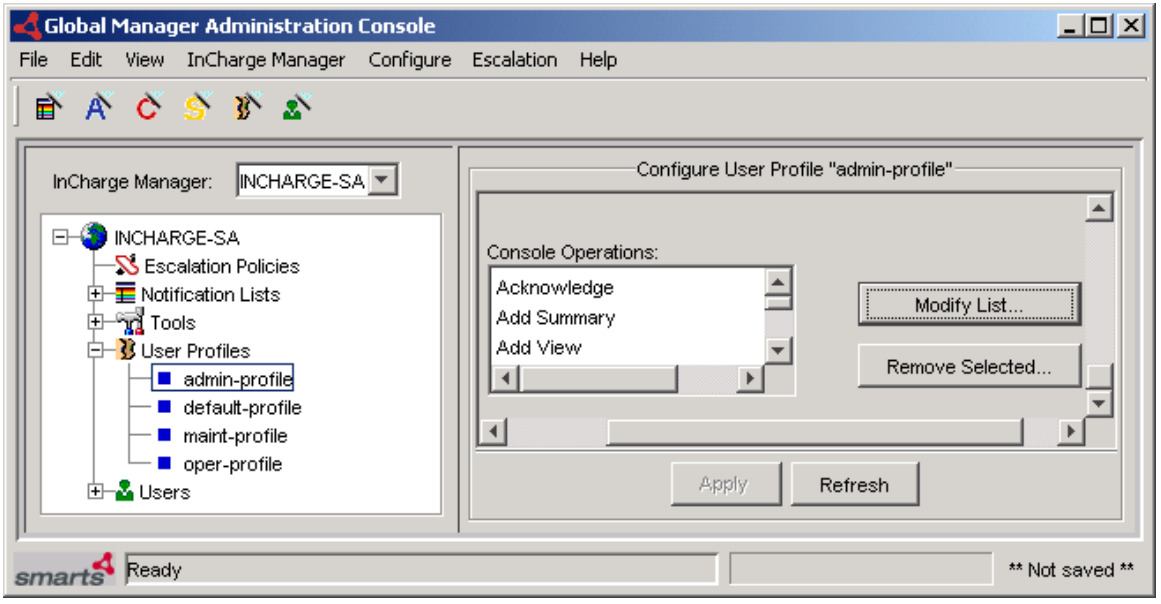

Figure 4: Configure User Profile Example

5. In the Configure User Profile panel, scroll down to the Console Operations drop-down menu.
6. Click the **Modify List** button to the immediate right of the Console Operations drop-down menu to display the Console Operations dialog.
7. In the dialog, click the plus sign (+) next to the Map checkbox to display a list of map types.

8 In the list of map types, click the BGP Connectivity and OSPF Connectivity checkboxes to enable the viewing of the BGP and OSPF maps as shown in Figure 5.

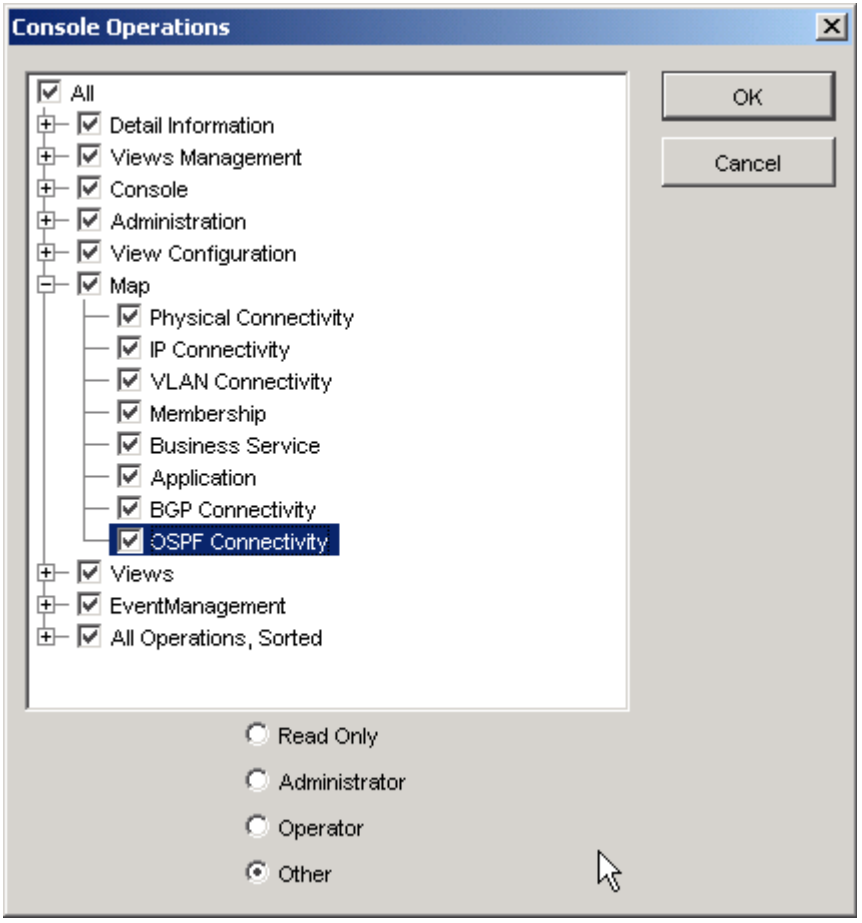

Figure 5: Selecting BGP Connectivity

9 Click **OK** and then **Apply**.

10 Close the Global Console and open it again to view the BGP and/or OSPF maps.

Security

A Network Protocol Manager deployment can employ encrypted connections between InCharge applications.

For detailed information about InCharge secure communications, see the *InCharge System Administration Guide*.

Index

T

U