



Adapter for Cisco ISC

1.1

USER'S GUIDE

P/N 300-002-534

REV A01

EMC Smarts

Corporate Headquarters:

Hopkinton, MA 01748-9103

1-508-435-1000

www.EMC.com

Copyright 1996-2005 by EMC Corporation ("EMC"). All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The Software and all intellectual property rights related thereto constitute trade secrets and proprietary data of EMC and any third party from whom EMC has received marketing rights, and nothing herein shall be construed to convey any title or ownership rights to you. Your right to copy the software and this documentation is limited by law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Use of the software is governed by its accompanying license agreement.

The information in this publication is provided "as is" without warranty of any kind. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties or merchantability or fitness for a particular purpose. In no event shall EMC Corporation be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, arising from any error in this publication.

The InCharge products mentioned in this publication are covered by one or more of the following U.S. Patent Nos. or pending patent applications: 5,528,516, 5,661,668, 6,249,755, 6,868,367 and 11/034,192.

"EMC," "InCharge," the InCharge logo, "SMARTS," the SMARTS logo, "Graphical Visualization," "Authentic Problem," "Codebook Correlation Technology," "Instant Results Technology," "InCharge Viewlet," and "Dashboard Viewlet" are trademarks or registered trademarks of EMC. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Additional copyright notices and license terms applicable to portions of the software are set forth in the Third-Party Copyright Read Me file.

Contents

Preface	v
Purpose	v
Intended Audience	v
Prerequisites	v
Document Organization	vi
InCharge MPLS Management Suite Installation Directory	vii
MPLS Management Suite Products	vii
Documentation Conventions	vii
Additional Resources	viii
InCharge Commands	ix
Documentation	ix
Technical Support	x
1 Introduction	1
ISC Adapter Communications Scenarios	3
2 Configuration Tasks	7
Configuring the Global Manager	8
Configuring ics.conf	8
Configuring serverConnect.conf	8
Configuring the ISC Adapter	9
Configuring the MPLS Manager	11
Configuring Cisco ISC to Communicate with the ISC Adapter	12
Configuring vpnsc.properties	12
Configuring Host Configuration Screen	13
Configuring clientReg	16
Restarting Cisco ISC	16

3	Administering the Adapter and the ProvisioningLink	17
	Starting the Adapter, ProvisioningLink and Servlet	17
	Stopping the Adapter, ProvisioningLink and Servlet	18
	Troubleshooting the Adapter	18
	Initiating Synchronization Manually	18
4	Viewing VPN Provisioning Information	19
	Business Services Map	20
	Topology Browser	22
	Notification Log	23
A	Event Notifications	25
B	Sample prov.conf File	27
C	Understanding the sm_edit Utility	31

Preface

The InCharge Adapter for Cisco ISC (ISC Adapter) collects virtual Private Network (VPN) provisioning information from the Cisco IP Solution Center (ISC) provisioning system, and sends it to the InCharge Service Assurance Manager. The adapter receives VPN discovery information from Global Manager, and synchronizes VPN information available in Cisco ISC and SMARTS MPLS Manager (MPLS Manager).

Purpose

This document provides the following:

- Overview of the ISC Adapter
- Configuration instructions
- Administration procedures
- Event notifications provided by the adapter

Intended Audience

This document is intended for administrators and integrators who set up and maintain the ISC Adapter.

Prerequisites

Before you perform the procedures in this document, the following SMARTS software must be installed:

- InCharge IP Availability Manager
- InCharge Service Assurance Manager (Global Manager)
- Global Console
- MPLS Manager

For information about installing these products, see the *InCharge IP Management Suite Installation Guide*, *InCharge Service Assurance Management Suite Installation Guide*, and the *InCharge MPLS Management Suite Installation Guide*.

Document Organization

This guide consists of the following chapters.

Table 1: Document Organization

1. INTRODUCTION	Provides an overview of the ISC Adapter, which transports VPN provisioning information from the Cisco IP Solution Center provisioning system, and receives VPN discovery information from the Global Manager.
2. CONFIGURATION TASKS	Describes the configuration tasks for the Global Manager, ISC Adapter, and Cisco ISC. These tasks are required to support communications and security.
3. ADMINISTERING THE ADAPTER AND THE PROVISIONINGLINK	Describes how to start and stop the adapter and ProvisioningLink, initiate synchronization manually, and interpret any errors.
4. VIEWING VPN PROVISIONING INFORMATION	Describes how the Global Console displays the VPN provisioning data that is provided by Cisco ISC via the ISC Adapter. In addition, this chapter provides an example of a Notification Log that shows VPNs for which provisioning information is not available.
A. EVENT NOTIFICATIONS	Lists the notifications generated by the ISC Adapter.
B. SAMPLE PROV.CONF FILE	Provides a sample configuration file used to communicate between InCharge and Cisco ISC.
C. UNDERSTANDING THE SM_EDIT UTILITY	Describes the sm_edit utility that is used when editing InCharge configuration files.

InCharge MPLS Management Suite Installation Directory

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

MPLS Management Suite Products

The MPLS Management Suite offers the following products:

- MPLS Manager
- InCharge Adapter for Cisco ISC
- Perl API

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.

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 Dynamic Modeling Tutorial*
- *InCharge MODEL Reference Guide*
- *InCharge ASL Reference Guide*
- *InCharge Perl Reference Guide*

MPLS Management Suite Documentation

The following SMARTS documents are relevant to users of the MPLS Management Suite product suite:

- *InCharge MPLS Management Suite Installation Guide*
- *InCharge MPLS Manager User's Guide*
- *InCharge MPLS Manager Configuration Guide*
- *InCharge IP Discovery Guide Supplement for MPLS*
- *InCharge MPLS Manager User's Guide for Cisco ISC Adapter*
- *InCharge MPLS Management Suite Release Notes*

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

Technical Support

For questions about technical support, call your local sales office or service provider. For service, call one of the following numbers:

United States: 800.782.4362 (SVC.4EMC)

Canada: 800.543.4782 (543.4SVC)

Worldwide: 508.497.7901

EMC Powerlink

EMC Powerlink is EMC's secure extranet for customers and partners. Powerlink is an essential tool for obtaining web-based support from EMC. Powerlink can be used to submit service or information requests (tickets) and monitor their progress, to review the knowledgebase for known problems and solutions, and to download patches and SmartPacks.

From training on EMC products and technologies, to online support, product announcements, software registration, technical white papers, interoperability information, and a range of configuration tools, Powerlink offers resources unavailable elsewhere.

For quickest access when you do not already have a Powerlink account, ask your EMC representative for the access code for your company and register at the Powerlink site. Visit the EMC Powerlink website at:

<http://powerlink.emc.com>

Introduction

This chapter provides a brief overview of the ISC Adapter. The ISC Adapter synchronizes Virtual Private Network (VPN) and customer information between the MPLS Manager and Cisco ISC.

Cisco ISC is a provisioning and management application for creating, discovering, managing, deploying, and decommissioning VPNs. When a Cisco ISC operator provisions or decommissions a VPN, Cisco ISC stores information about the VPN and the associated customer, devices, and interfaces. Cisco ISC provides the following information to Domain Manager via the ISC Adapter:

- Customer Name
- VPN Route Targets
- Interfaces that are associated with the Provider Edge Routers (PEs) of the VPN

The ISC Adapter includes two SMARTS applications: the ProvisioningLink and the Event Receiving Servlet. These components facilitate communication of VPN provisioning data and events between Cisco ISC and the adapter.

In addition, Domain Managers (via the Global Manager) provide the ISC Adapter with information on newly discovered VPNs. The adapter attempts to reconcile this information with what is contained in Cisco ISC, and reports on any discrepancies.

Figure 1 shows how the ISC Adapter fits into the MPLS architecture. In this architecture, InCharge Managers discover and manage MPLS and IP domains:

- The IP Availability Manager discovers and manages the underlying Layer 2 and Layer 3 transport domains.
- The MPLS Manager discovers and manages the MPLS and VPN domains, and performs cross-domain correlation.
- The Global Manager consolidates topology information and correlates notifications from the other InCharge Managers. It also provides end-to-end impact analysis.

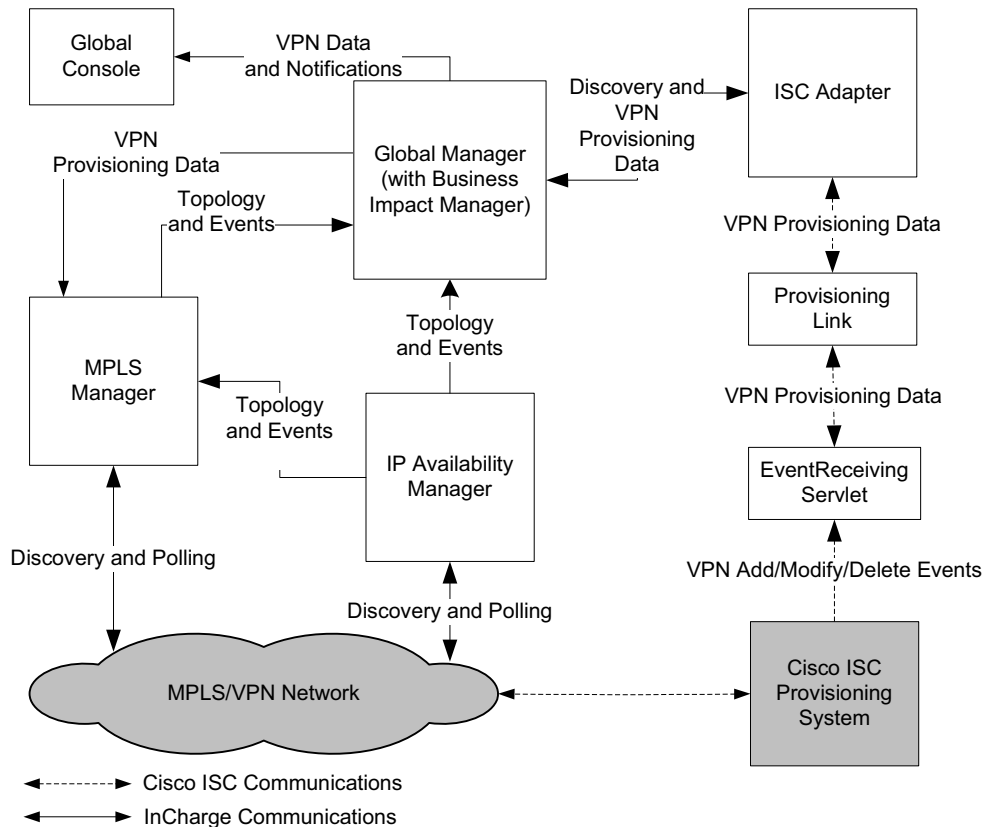


Figure 1: ISC Adapter in the MPLS Architecture

The ISC Adapter works with the Global Manager to communicate and synchronize VPN information. The ISC Adapter receives information from Cisco ISC, but does not write to Cisco ISC.

The Global Manager provides information about changes to VPNs to the ISC Adapter. The adapter receives changes from Cisco ISC and transfers them to the Global Manager.

VPN notifications are displayed on the Global Console with provisioned customer information. For a list of ISC Adapter notifications, see [Event Notifications](#) on page 25. The Global Console also provides comprehensive graphical displays of MPLS network elements and their relationships through the use of Business Impact Manager.

ISC Adapter Communications Scenarios

The basic scenarios for communicating VPN information are the following:

- An operator provisions or decommisions a VPN in Cisco ISC. (The flow is the same for either operation.)
- The MPLS Manager becomes aware of a new VPN in the network, or of the absence of a previously discovered VPN.

Scenario 1, An Operator Provisions a VPN

Figure 2 shows the flow of information from Cisco ISC through the ISC Adapter, Global Manager, and the MPLS Manager when a new VPN is provisioned.

In this flow, there are the following high-level steps:

- 1** An operator provisions a new VPN at the Cisco ISC console.
- 2** The ProvisioningLink, which listens to the EventReceivingServlet for events, receives the provisioning information for the VPN and communicates it to the ISC Adapter.
- 3** The ISC Adapter attempts to reconcile the new PE interface information with the data already available in the Global Manager, Availability Manager, and MPLS Manager repositories.
 - If it can reconcile the PE interface, the ISC Adapter communicates the information to the Global Manager.
 - If it cannot reconcile the information, the adapter (through the Global Manager) triggers a discovery by Availability Manager, which in turn triggers a discovery by the MPLS Manager.

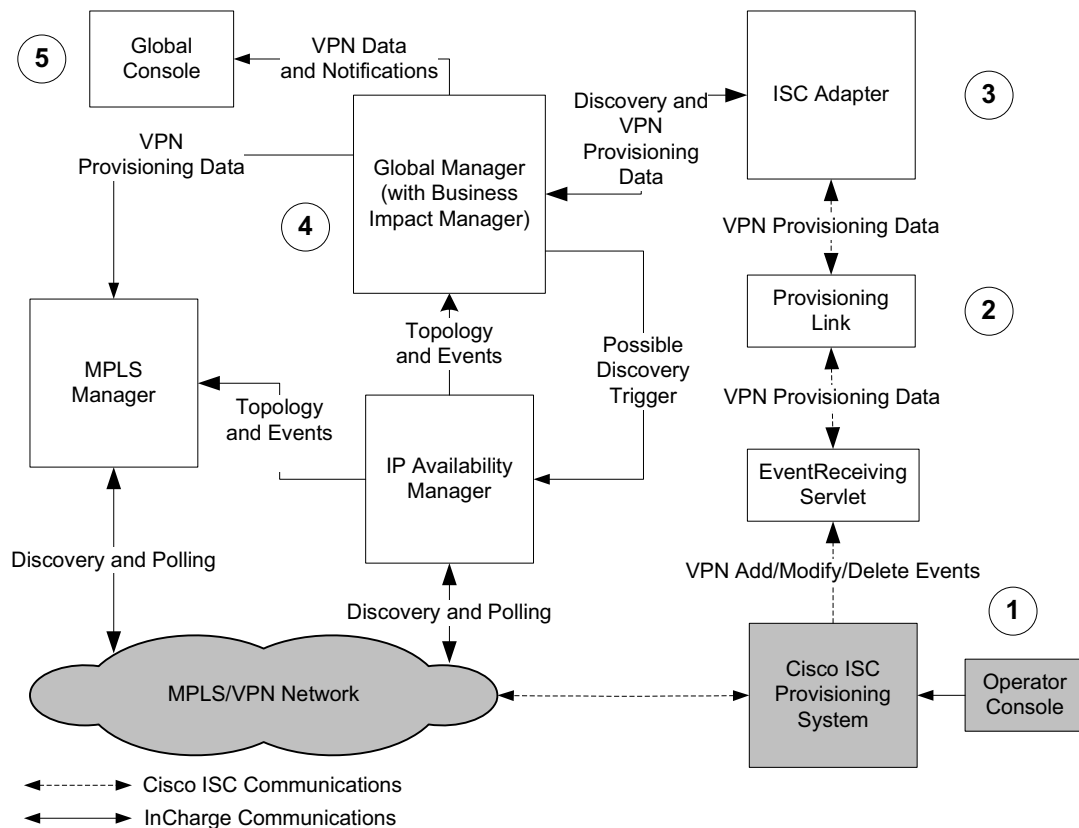


Figure 2: Information Flow When a New VPN is Provisioned

- 4 The Global Manager updates its repository and sends the information to the MPLS Manager.
- 5 The Global Console displays the provisioning information with any notifications for that VPN.

Scenario 2, MPLS Manager Discovers a New VPN

Figure 3 shows the flow of information from the MPLS Manager, through the Global Manager, ISC Adapter, and Cisco ISC when a new VPN is discovered. The flow is the same if a VPN formerly present in the network can no longer be discovered.

In this flow, there are the following high-level steps:

- 1 The MPLS Manager discovers a new VPN in the network.

- 2 The MPLS Manager communicates the information to the Global Manager.
- 3 The Global Manager updates its repository and sends the information to ISC Adapter.
- 4 The adapter queries Cisco ISC for customer name and PE interface information for the newly discovered VPN. The VPN's Route Target(s) are used as the key(s) for this query.
- 5 The ISC Adapter communicates the information to the Global Manager, which updates its repository.
- 6 The Global Manager sends the customer provisioning information to the MPLS Manager.

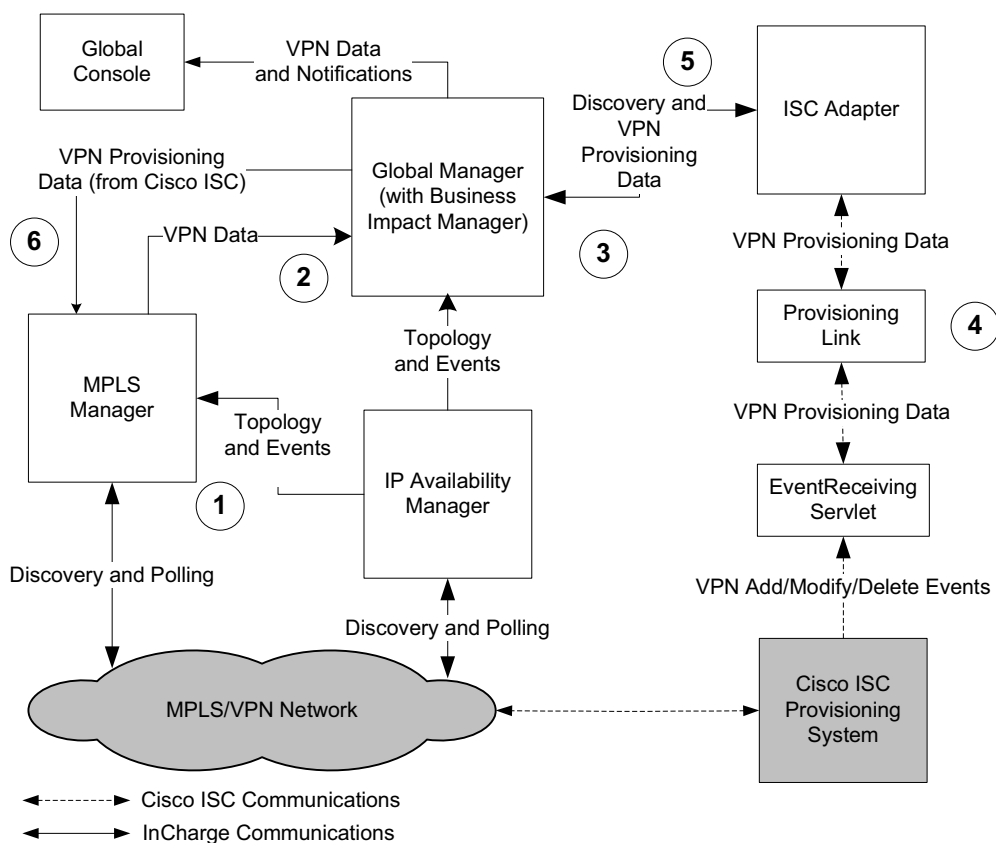


Figure 3: Information Flow When a New VPN is Discovered

Configuration Tasks

After installing the MPLS Management Suite, and before starting the ISC Adapter, configure the following SMARTS and Cisco ISC applications:

Table 3: Configure Applications to Operate with the ISC Adapter

APPLICATION	FILE/SCREEN	PURPOSE
InCharge Service Assurance Manager (Global Manager)	<i>ics.conf</i>	Set up communication with the ISC Adapter.
	<i>serverConnect.conf</i>	Configure SMARTS security to allow the ISC Adapter to communicate with the Global Manager.
ISC Adapter	<i>prov.conf</i>	Set up communication between the ISC Adapter and Cisco ISC. In addition, the ProvisioningLink component connects to SAM (using credentials from the prov.conf file) in order to check for the BIM license.
MPLS Manager	<i>client.Connect.conf</i>	Allow the ISC Adapter to connect to the Global Manager.
	<i>serverConnect.conf</i>	Allow the ISC Adapter to connect to the Message Server
Cisco ISC Note: After configuring Cisco ISC, you must restart it. You may wish to notify Cisco ISC operators before you restart the application.	<i>vpnsc.properties</i> (from the command line)	Set up communication with the ISC Adapter.
	Host Configuration screen of the Administration Console	Set up communication with the ISC Adapter.
	<i>clientReg.txt</i> (from the command line)	Specify the events to be sent from Cisco ISC to the ISC Adapter.

Configuring the Global Manager

This section explains how to configure the *ics.conf* and *serverConnect.conf* files to support communications between the Global Manager and the ISC adapter.

Configuring *ics.conf*

To allow the Global Manager to communicate with the ISC Adapter, use the *sm_edit* utility to edit the DomainType area of the DomainSection of the *ics.conf* file in the Global Manager. For more information, see [Understanding the sm_edit Utility](#) on page 31.

Create an entry as shown in the example below where the value for Name is INCHARGE-PROV, and the value for ConfFile is *dxa-prov-ics.conf*.

```
DomainSection
{
    DomainType
    {
        ConfFile           = "dxa-prov-ics.conf";
        MinimumCertainty   = 0.24;
        SmoothingInterval   = 65;
        Name                = "INCHARGE-PROV";
    }
}
```

INCHARGE-PROV is the default Name for the ISC adapter server.

To edit the file, issue the *sm_edit* command, as follows:

```
# ./sm_edit conf/ics/ics.conf
```

If you edit the *ics.conf* file when the Global Manager is running, you must reconfigure the Global Manager, by invoking the following command from the **BASEDIR**/*smarts/bin* directory, where **BASEDIR** refers to the directory where the Global Manager is installed:

```
# sm_adapter -s <global_manager> ics/ICS_RemoteConfig.asl
```

Configuring *serverConnect.conf*

To allow the ISC Adapter to connect to the Global Manager, you edit the *serverConnect.conf* file.

Use the *sm_edit* utility to edit the *serverConnect.conf* file, as follows:

- 1 Issue the *sm_edit* command:

```
# ./sm_edit SAM/smarts/local/conf/serverConnect.conf
```

2 Add the following line:

```
<SAM_SERVER>:<iscadapteruser>:<SYS>:All
```

Where

- **<SAM_SERVER>** is the domain name of the Service Assurance Manager server. By default, this name is `INCHARGE-SA`.
- A user with the name, **iscadapteruser**, was created in the operating system and also in InCharge using the Global Manager Administration Console.
- The value of the **<IC_USER>** parameter in the *prov.conf* file is set to **<iscadapteruser>**.

3 Save and close the file.

Configuring the ISC Adapter

To allow the ISC Adapter to communicate with Cisco ISC, configure the *prov.conf* file. The configuration parameters for the ISC Adapter are specified in the local copy of the *prov.conf* file, located in the **BASEDIR**/*smarts/local/conf/* directory, where **BASEDIR** refers to the directory where the ISC Adapter is installed. For reference, see [Sample prov.conf File](#) on page 27.

- 1** Open and modify the default *prov.conf* file, using *sm_edit* to ensure that the file is copied to **BASEDIR**/*smarts/local/conf/prov/* and that it retains the proper permissions. For example, to open and modify the default *prov.conf* file on UNIX, use the following command from **BASEDIR**/*smarts/bin*:

```
# ./sm_edit BASEDIR/smarts/local/conf/prov/prov.conf
```

Table 4 lists the configuration parameters of the *prov.conf* file. Modify these parameters to reflect your operating environment.

Table 4: Parameters in the prov.conf File

PARAMETER	DEFAULT VALUE	DESCRIPTION
EXTERNAL_SYSTEM	ISC	Name of the system in use. Valid value is: ISC (Cisco ISC provisioning system)
EXTERNAL_HOST	localhost	IP Address or host name where Cisco ISC is running.
EXTERNAL_PORT	8030	Port on which Cisco ISC is running.
EXTERNAL_USER	admin	Valid user login to Cisco ISC.
EXTERNAL_PASSWORD	cisco	Password for EXTERNAL_USER. Note: This password is not encrypted by InCharge, so it is not secure.
SM_BROKER	localhost:426	Relevant InCharge broker.
NAME	INCHARGE-PROV	Name of the ISC Adapter as it appears in the broker.
EVENT_HOST	localhost	Host on which the EventReceivingServlet is running; typically, this is the same host where the adapter is running.
EVENT_PORT	8080	Port that the ProvisioningLink uses to retrieve events of interest from the EventReceivingServlet.
SAM_SERVER	INCHARGE-SA	Name of the Global Manager.
IC_USER	admin	InCharge user name.
IC_PASSWORD	changeme	Password for IC_USER. Note: This password is not encrypted by SMARTS, so it is not secure.

- 2 Start the adapter, as described in [Starting the Adapter, ProvisioningLink and Servlet](#) on page 17.

Configuring the MPLS Manager

To support communications with the Global Manager and the Message Server, configure both the *clientConnect.conf* and the *serverConnect.conf* files.

Configuring the clientConnect File

To allow the ISC Adapter to connect to the Global Manager, use the *sm_edit* utility to edit the *clientConnect.conf* file in the MPLS Manager.

- 1 Issue the *sm_edit* command:

```
# ./sm_edit BASEDIR/smarts/local/conf/clientConnect.conf
```

- 2 Add the following line:

```
<SAM_SERVER>: iscadapteruser:iscadapteruser:<SYS>
```

Where

- <**SAM_SERVER**> is the domain name of the Service Assurance Manager server. By default, this name is **INCHARGE-SA**.
- A user with the name, **iscadapteruser**, was created in the operating system.
- <**iscadapteruser**> corresponds to <**iscadapteruser**> in the *prov.conf* file.

- 3 Save and close the file.

Configuring the serverConnect File

To allow the ISC Adapter to connect to the Message Server, use the *sm_edit* utility to edit the *serverConnect.conf* file in the MPLS Manager, as follows:

- 1 Issue the *sm_edit* command:

```
# ./sm_edit BASEDIR/smarts/local/conf/serverConnect.conf
```

- 2 Add the following line:

```
MSERV:<iscadapteruser>:<SYS>:All
```

Where

- A user with the name, **iscadapteruser**, was created in the operating system and also in InCharge using the Global Manager Administration Console.
- The value of the <**IC_USER**> parameter in the *prov.conf* file is set to <**iscadapteruser**>

Note: Do not change `MSERV`. Ensure that the All permission is set for this entry.

- 3 Save and close the file.

Configuring Cisco ISC to Communicate with the ISC Adapter

To enable communications with the ISC Adapter, and to specify the types of events that Cisco ISC will send to the adapter, modify the files and screen listed in Table 5.

Table 5: Cisco ISC Files/Screen for Configuration

FILE/SCREEN	PURPOSE
<i>vpncsc.properties</i>	Set up communication with the ISC Adapter.
Host Configuration screen of the Administration Console	Continue to set up communication with the ISC Adapter.
<i>clientReg.txt</i>	Specify events that Cisco ISC sends to the ISC Adapter.

Configuring *vpncsc.properties*

Follow these steps to configure Cisco ISC to send VPN-related provisioning events to the ISC Adapter.

- 1 On the host where Cisco ISC is installed, log in as ISC admin user.
- 2 At a command line, open the file, *\$ISC_HOME/etc/vpncsc.properties*, and edit the parameters to the values shown in Table 6.

Table 6: Required Values for the *vpncsc.properties* File

PARAMETER	VALUE
<i>notification.clientEnabled</i>	true
<i>notification.clientHost</i>	The name of host on which Cisco ISC resides.
<i>notification.clientMethod</i>	<i>/ISCEvents/EventReceivingServlet</i>
<i>notification.clientPort</i>	The same value as <i>EVENT_PORT</i> in <i>prov.conf</i> .
<i>notification.clientRegFile</i>	<ISC_HOME> /resources/nbi/notification/clientReg.txt

- 3 Save the file.

Configuring Host Configuration Screen

Follow these steps to add the same information to the Host Configuration screen in the Administration console.

- 1 On the host where Cisco ISC is installed, log in to the Cisco ISC application as administrator.
- 2 At the welcome screen, select *Administration*.
- 3 On the Administration screen, select *Control Center*, as shown in Figure 4.



Figure 4: Cisco ISC Application Administration Screen

- At the Hosts screen, select the checkbox for the host you are configuring, as shown in Figure 5, and then click **Config**.



Figure 5: Cisco IPS Hosts Configuration Screen

- At the Host configuration screen, scroll down to the *notification* directory, as shown in Figure 6, click the **+**, and then select *clientEnabled*.

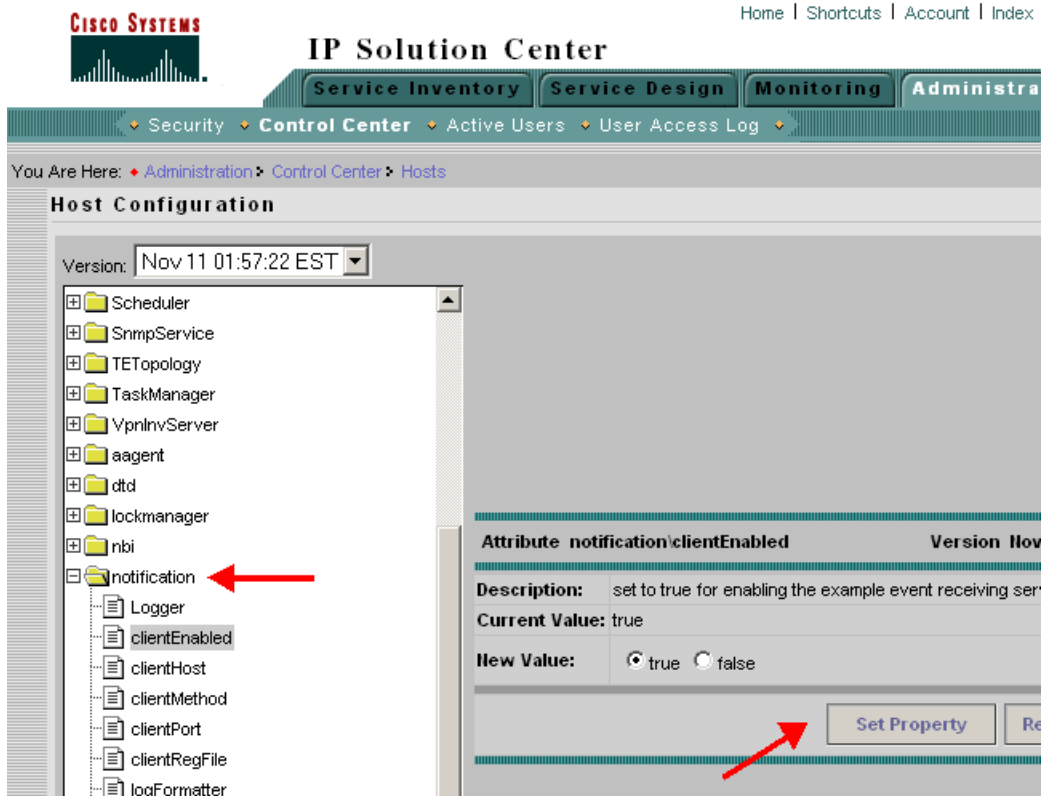


Figure 6: Notification Menu

- 6 At the *Attribute notification\clientEnabled* screen, set the value to **true**, and then click **Set Property**.
- 7 Return to the scrolling menu, scroll down to the *notification* directory, and then select *clientHost*.
- 8 At the *Attribute notification\clientHost* screen, type the hostname for Cisco ISC in the *New Value* field, and then click **Set Property**.
- 9 Return to the scrolling menu, scroll down to the *notification* directory, and then select *clientMethod*.
- 10 At the *Attribute notification\clientMethod* screen, type `/ISCEvents/EventReceivingServlet`, and then click **Set Property**.
- 11 Return to the scrolling menu, scroll down to the *notification* directory, and then select *clientPort*.

- 12 Verify that the value in the *Port* field is the same as that in `EVENT_PORT` in `prov.conf`. Type a new value, if necessary, and then click **Set Property**.
- 13 Return to the scrolling menu, scroll down to the *notification* directory, and then select *clientRegFile*.
- 14 At the *Attribute notification\clientRegFile* screen, type
`<home directory>/resources/nbi/notification/clientReg.txt`,
and then click **Set Property**.

Configuring clientReg

Follow these steps to specify which events Cisco ISC sends to the ISC Adapter.

- 1 At a command line, open the file,
`$ISC_HOME/resources/nbi/notification/clientReg.txt`
- 2 Copy the following settings and paste them into the file, replacing any current entries with these exact settings:

```
com.cisco.vpnsc.repository.task.PersistentTask.>  
com.cisco.vpnsc.repository.devices.PIX.>  
com.cisco.vpnsc.repository.common.Interface.>  
com.cisco.vpnsc.repository.common.Customer.>  
com.cisco.vpnsc.repository.devices.CiscoRouter.>  
com.cisco.vpnsc.repository.common.VPN.>  
com.cisco.vpnsc.repository.common.PEDevice.>  
com.cisco.vpnsc.repository.mpls.MplsSR.>  
com.cisco.vpnsc.repository.common.Site.>
```

- 3 Save the file.

Restarting Cisco ISC

After configuration is complete, restart Cisco ISC by issuing the following commands from the same command line, in this sequence:

- 1 **% stopall**
- 2 **% startwd**

Administering the Adapter and the ProvisioningLink

This chapter describes how to do the following:

- Start and stop the ISC Adapter, the ProvisioningLink, and the Event Receiving Servlet.
- Initiate data synchronization through the Global Manager manually.

Starting the Adapter, ProvisioningLink and Servlet

The ISC Adapter, ProvisioningLink and Event Receiving Servlet are all started and stopped together. To start the adapter, ProvisioningLink and Servlet, issue the following command from the **BASEDIR**/*smarts/bin* directory:

```
sm_service start ic-INCHARGE-PROV
```

Stopping the Adapter, ProvisioningLink and Servlet

To stop the adapter, ProvisioningLink and Servlet, issue the following command from the **BASEDIR**/smarts/bin directory:

```
sm_service stop ic-INCHARGE-PROV
```

Troubleshooting the Adapter

To determine if the Event Receiving Servlet is running, you can connect to the following URL:

http://<EVENT_HOST>:<EVENT_PORT>/ISCEvents/EventReceivingServlet

For example:

<http://localhost:8030/ISCEvents/EventReceivingServlet>

Depending on whether the adapter is running, you will see one of the following:

- Is running—blank page
- Is not running—http failure message

Initiating Synchronization Manually

When the ISC Adapter is started or restarted after losing a connection, it synchronizes topology data and event information with the Global Manager. You can also synchronize this data manually. Issue the following command for manual synchronization from the **BASEDIR**/smarts/bin directory:

```
sm_adapter -s MSERV prov/prov-sync.asl
```

Viewing VPN Provisioning Information

This chapter describes how the Global Console displays the VPN provisioning data that is provided by Cisco ISC via the ISC Adapter. In addition, this chapter provides an example of a Notification Log that shows VPNs for which provisioning information is not available.

In conjunction with InCharge Business Impact Manager, Global Manager uses the VPN provisioning data to create instances of the ServiceOffering and ServiceSubscriber classes. The classes can then be displayed by the Global Console in maps and in the topology browser. These classes represent the following:

- **ServiceOffering**—A business service delivered to a set of subscribers (consumers). A ServiceOffering is mapped to an SMARTS-defined VPN that is associated with a Cisco ISC VPN. The ServiceOffering is related to its subscribers through the Subscribers relationship. It is also related to the infrastructure elements that implement the offering through the ConsistsOf relationship.
- **ServiceSubscriber**—A consumer of services provided through a ServiceOffering. A ServiceSubscriber is mapped to a Cisco ISC-defined Customer “object.”

Note: To display the maps, the ISC Adapter requires a license for the Business Impact Manager, which is installed as part of the Service Assurance Management Suite. For more information, see *InCharge Service Assurance Manager User’s Guide for Business Impact Manager*.

For information on Global Console, see *InCharge Operator's Guide*.

Business Services Map

Figure 7 shows an example of a Business Services map representing the ServiceOffering named VPN-VPN-1 in Cisco ISC. In this example, the MPLS Manager received the VPN name from Cisco ISC through the ISC Adapter.

Note: If the Global Manager did not have access to the VPN provisioning data from Cisco ISC, the VPN name would be the route target.

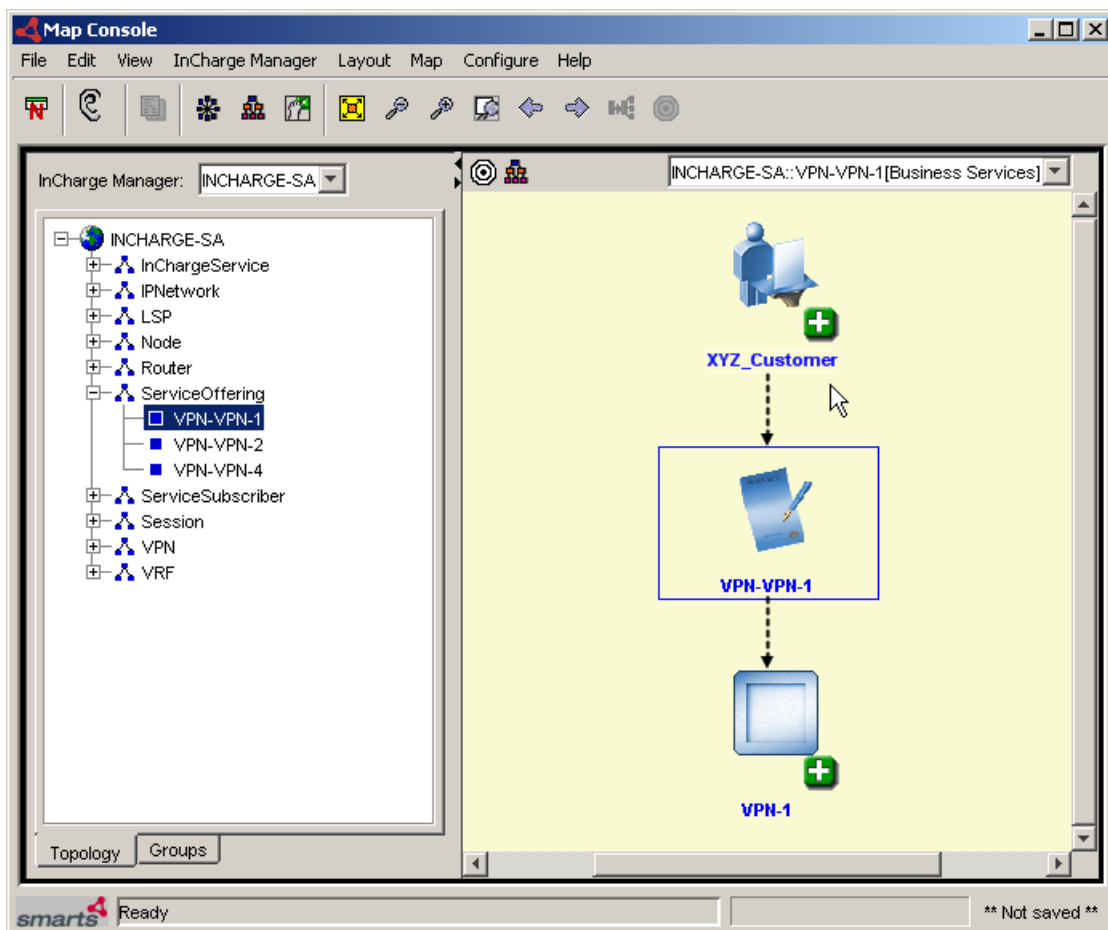


Figure 7: Business Services Map Showing a ServiceOffering

Figure 8 shows a Business Services map representing a ServiceSubscriber relationship, with XYZ_Customer subscribing to the VPN-VPN-1 and VPN-VPN-4 ServiceOfferings.

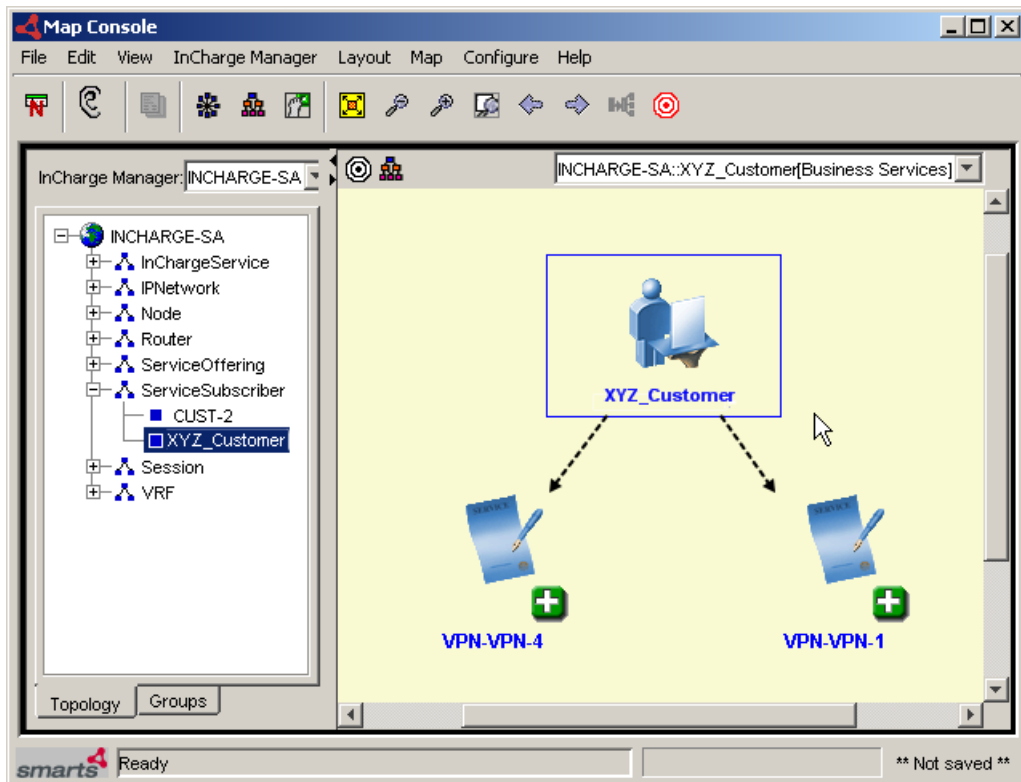


Figure 8: Business Services Map Showing a ServiceSubscriber

Topology Browser

Figure 9 shows a Topology Browser for an MPLS network. In this figure, the attributes for a VPN are shown. The Global Manager populates the Name and DisplayName attributes with data from Cisco ISC via the ISC Adapter.

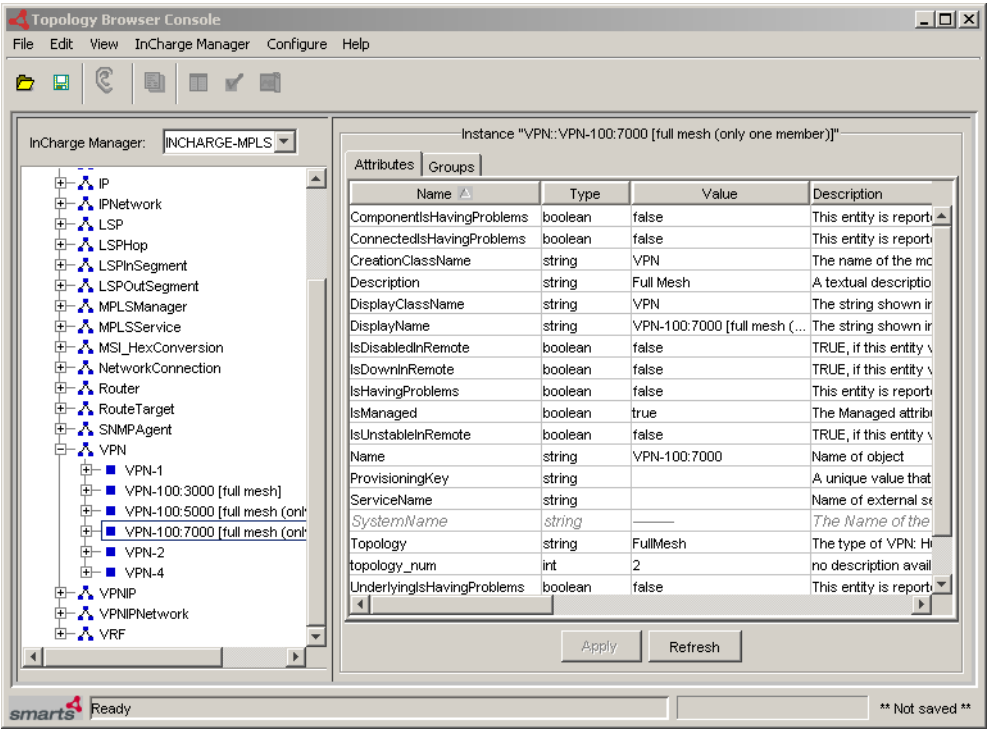


Figure 9: Topology Browser Showing a VPN with Customer Provisioning Information

Notification Log

Figure 10 shows a Notification List with three VPNs that are not known to the provisioning system. The source for this information is the INCHARGE-PROV domain or customer provisioning system (Cisco ISC via the ISC Adapter).

Sev...	Ack...	Class	Name	Event	Source	Impact
✖	No	Session	INCHARGE-SA->INC...	Disconnected	INCHARGE-SA	
!	No	Interface	IF-qa-gw6.smarts.c...	Down	INCHARGE-AM, INCHAR...	
⚠	No	VPN	VPN-100:5000	VpnNotKnownToProvisioningSystem	INCHARGE-PROV	
⚠	No	VPN	VPN-100:3000	VpnNotKnownToProvisioningSystem	INCHARGE-PROV	
⚠	No	VPN	VPN-100:7000	VpnNotKnownToProvisioningSystem	INCHARGE-PROV	
⚠	No	VRF	VRF-TEST/qa-gw6.s...	Down	INCHARGE-MPLS	
⚠	No	VRF	VRF-CE100/qa-gw6....	Down	INCHARGE-MPLS	
⚠	No	VRF	VRF-VRF-DEV/qa-gw...	Down	INCHARGE-MPLS	
⚠	No	VRF	VRF-VRF/qa-gw6.sm...	Down	INCHARGE-MPLS	
?	No	VRF	VRF-Dev/qa-mplspe...	NoRoutes	INCHARGE-MPLS	
?	No	VRF	VRF-TEST/qa-mplsp...	NoRoutes	INCHARGE-MPLS	

Figure 10: Notification Log Showing an Unprovisioned VPN



Event Notifications

Table 7 lists the event notifications generated by the ISC Adapter, and sent to the Global Manager for display in the Global Console.

For information about MPLS managed elements, notifications, root cause and impact analysis, see the *InCharge MPLS Manager User's Guide*.

Table 7: Notifications from the ISC Adapter

MANAGED ELEMENT	EVENT	DESCRIPTION
VPN	VpnNotFound	A VPN that is provisioned in Cisco ISC was not found during discovery by the MPLS Manager.
	InterfaceNotFound	A PE interface that is provisioned in Cisco ISC was not found during discovery by the MPLS Manager.
	VpnNotKnownToProvisioningSystem	A VPN recognized by the InCharge discovery process has not been provisioned in Cisco ISC.
	VpnInterfaceMismatch	Cisco ISC erroneously reports that a provisioned interface is associated with a particular VPN.

B

Sample prov.conf File

The following is a sample prov.conf file:

```
#####
# Configuration file for Provisioning Adapter
# All values must be placed in quotes
#####

PROV_Parameters::ICF-ProvisioningAdapter-CiscoISC {
    params = {
        #####
        # Provisioning System Configuration
        #####
        # The name of the provisioning system being interfaced
        # with
        {"EXTERNAL_SYSTEM", "ISC"},

        # The host of the provisioning system
        {"EXTERNAL_HOST", "flagman"},

        # The port on EXTERNAL_HOST where the provisioning system
        # can be reached
        {"EXTERNAL_PORT", "8030"},
```

```
# Enable/Disable verbose logging.
{"DEBUG", "FALSE"},

# Login information for ProvisioningLink's access to
# provisioning system.
{"EXTERNAL_USER", "admin"},
{"EXTERNAL_PASSWORD", "changeme"},

#####
#The following are configuration elements for Cisco ISC
#####

{"EVENT_HOST", "localhost"},
{"EVENT_PORT", "8080"},

#####
# The following are configuration elements for InCharge
#####
# Name of this server
{"NAME", "INCHARGE-PROV"},

# InCharge BROKER Location.
{"SM_BROKER", "localhost:426"},

# Name of the SAM server to be used.
{"SAM_SERVER", "INCHARGE-SA"},

# InCharge user name and password - used to allow the
# Adapter
# contact SAM (The ProvisioningLink does not consult
# clientConnect.conf)
{"IC_USER", "admin"},
{"IC_PASSWORD", "changeme"},
```

```
    { "MESSAGE_SERVER" , "MSERV" } ,  
    { "MESSAGE_SERVER_PORT" , "0 " }  
  
    }  
}
```




Understanding the sm_edit Utility

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*.

Index

A

Availability Manager 2

B

BASEDIR vii

BROKER parameter 10

Business Impact Manager 19

C

Cisco ISC 1

 configuring 12

clientConnect.conf

 Configuring 11

Configuring

 Cisco ISC 12

 clientConnect.conf 11

 ics.conf 8

 ISC Adapter 9

 MPLS Manager 11

 prov.conf 9

 serverConnect.conf 8

E

Event Receiving Servlet 1

EVENT_HOST parameter 10

EVENT_PORT parameter 10

EXTERNAL_HOST parameter 10

EXTERNAL_PASSWORD parameter 10

EXTERNAL_PORT parameter 10

EXTERNAL_SYSTEM parameter 10

EXTERNAL_USER parameter 10

G

Global Console 3

Global Manager 2

 Reconfigure 8

I

IC_PASSWORD parameter 10

IC_USER parameter 10

ISC Adapter

 Architecture 2

 Configuring 9

 Starting 17

 Stopping 18

isc.conf

 Configuring 8

M

Map

 ServiceOffering 20

 ServiceSubscriber 21

N

New VPN is Discovered 5

Notification List 23

Notification Log 23

O

Operator provisions a VPN 3

P

prov.conf

 Configuring 9

Provisioning information 1

Provisioning Link 1

R

Reconfiguring the Global Manager 8

S

SAM_SERVER parameter 10

serverConnect.conf

 Configuring 8

ServiceOffering 19

ServiceOffering Map 20

ServiceSubscriber 19

ServiceSubscriber Map 21

Starting the adapter 17

Stopping the adapter 18

T

Technical Support x
Topology Browser 22

V

VPN Provisioning Data
Viewing 19