



Discovering the Network

Overview

Service providers and Enterprise Customers need a way to efficiently manage a large number of physical and logical devices. They need to be able to quickly create as well as modify large numbers of devices in a timely manner in order to be competitive as well as profitable. The Inventory Manager application supplied with IP Solution Center (ISC) enables the operator to import network-specific data into the ISC database in a bulk fashion.

The Inventory Manager [IM] runs as a stand-alone Java Application on a client machine. Inventory Manager runs in its own Java Virtual Machine outside of the ISC servers. Tibco Rendezvous® (rvd) and the associated Tibco Gatekeeper® [rva] are used to communicate between the client and server appliances. These two applications can negotiate the use of firewalls by means of HTTP Tunneling between the Inventory Manager process and the ISC server

Inventory Manager enables the operator to import and administer required network specific data into the ISC database. It provides bidirectional functionality and changes made in the Inventory Manager will be reflected in the ISC Repository.

There are three primary activities performed by the Inventory Manager application:

- *Autodiscovery*: Bulk discovery of logical, physical, and service-level connectivity of the service provider's network.
- *Configuration collection*: Bulk collection of device configurations from the network.
- *Bulk administration*: Provides a method of managing bulk changes to network specific data required by ISC in the Provisioning process.

Assumptions

This chapter assumes that the network operator or service operator has a sufficient understanding of MPLS, Layer 2 VPN, and IPsec technology to support provisioning tasks as described throughout this chapter. This getting started guide includes a glossary of terms and acronyms. This chapter further assumes that all of the network elements configured support the proper features from both a hardware and IOS version standpoint.

- *Name Resolution*: Inventory Manager requires name resolution to work. Either the ISC HTTP server host must be in the DNS that the web client is using, or the name and address of the ISC server must be in the client's *hosts* file.
- *SNMP*: SNMP is used for initial device discovery and it is assumed that all devices that will partake in the ISC provisioning environment will be configured to support SNMP.

- *CDP*: The Cisco Discovery Protocol (CDP) is used to discover Network Physical Connectivity [NPC]. CDP is also required to perform the service discovery task. It is assumed that CDP will be enabled both globally and at the interface level of each device that is to partake in the ISC provisioning environment.
- *Supported Devices*: ISC Inventory Manager supports the following devices within the Provisioning environment:
 - PE: Cisco 7200 Series, Cisco 7500 Series, Cisco Gigabit Switch Router, Cisco 7600 Optical Services Router
 - PE-CLE: Cisco Catalyst® 2950 Switch, Cisco Catalyst Intelligent Ethernet 3550 Switch, Cisco Catalyst 4000 Switch, Cisco 10K series routers

Inventory Manager

This section describes the ISC Inventory Manager and how to use it.

Client Installation and Administration

The current release of the Inventory Manager application requires the client device to be running Java VM 1.4.0_03 and Java WebStart 1.0.1_02. The following describes the process for installing and configuring the Inventory Manager:

-
- Step 1 Remove existing Java VMs or JREs.
 - Step 2 Install Java SDK 1.4.0_03.
 - Step 3 Install Java WebStart 1.0.1_02.
 - Step 4 Launch Inventory Manager from ISC Web Browser.
-

Initial Client Configuration

For best results, it is recommended that the client machine run *only* the aforementioned versions of JRE and Java WebStart. The operator should remove all other versions from the client device.

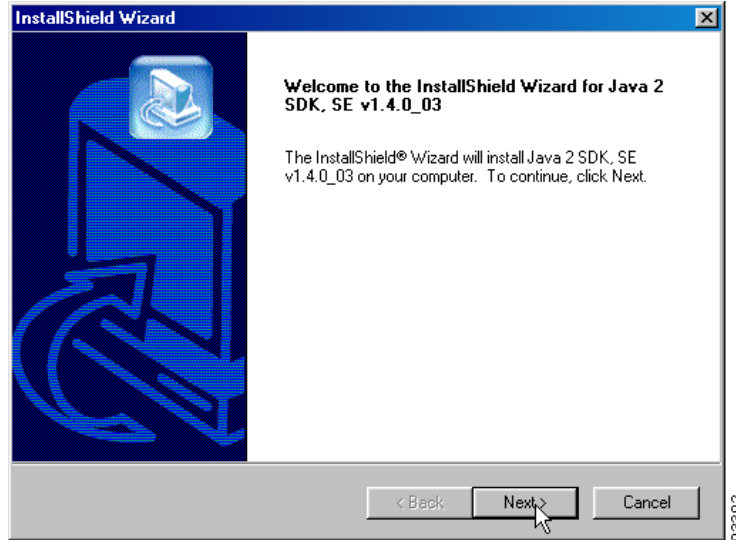
The following description assumes the operator is using a PC based system running Windows 2000 Professional Build 5.00.2195 with Service Pack 2 applied.

Installing the Client Java SDK

To install the Client Java SDK, follow these steps:

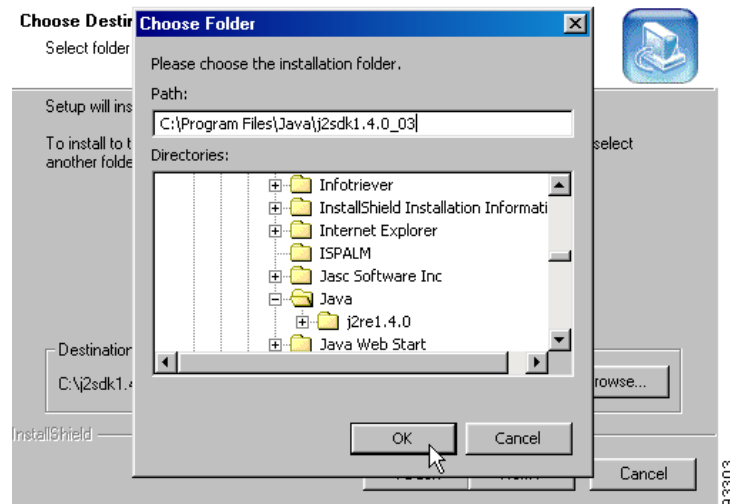
-
- Step 1 Remove any preexisting JREs or VMs.
 - Step 2 Run the `j2sdk-1_4_0_03-windows-i586.exe` program to install Java SDK 1.4.0_03 onto the client device. Follow the prompts and respond accordingly (see [Figure 3-1](#)).

Figure 3-1 Installing the Java SDK onto the Client Device



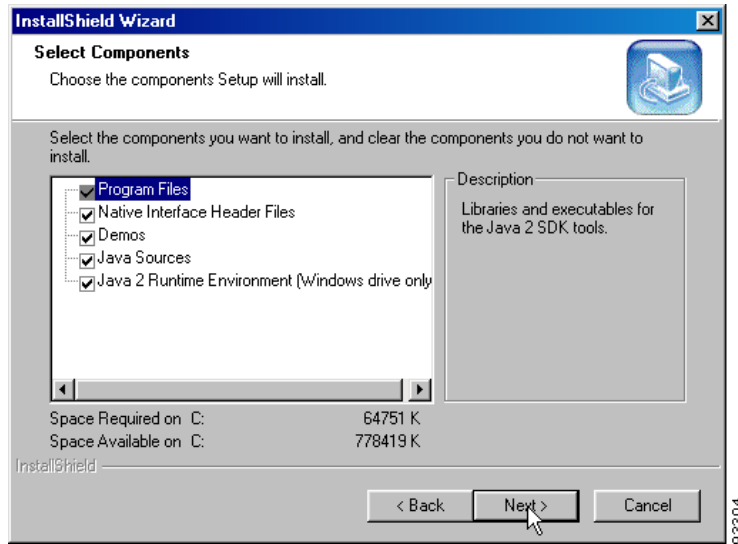
- Step 3** Click **Next**.
The License Agreement window appears.
- Step 4** Click **Yes** to accept the license agreement.
The Choose Folder dialog box appears (see [Figure 3-2](#)).

Figure 3-2 Installing the Java SDK onto the Client Device



- Step 5** Set the correct path, then click **OK**.
The Choose Destination Location dialog box appears.
- Step 6** To accept the new path, click **Next**.
The Select Components dialog box appears (see [Figure 3-3](#)).

Figure 3-3 Installing the Java SDK onto the Client Device



- Step 7** To accept the default components, click **Next**.
The Select Browsers dialog box appears.
- Step 8** Select the appropriate browser, then click **Next**.
- Step 9** Click **Finish**.
The Client Java 2 SDK installation is complete.

Installing Client Java WebStart

After successfully installing the Client Java 2 SDK, the operator should now install Java WebStart 1.0.1_02.

To install Java WebStart, follow these steps:

- Step 1** Run `javaws-1_0_1_02-win-us-rt.exe`.
- Step 2** Accept the license agreement by clicking **Accept**.
The Installation Directory dialog box appears.
- Step 3** Set the correct path, then click **Next**.
- Step 4** Click **Finish**.
The Java WebStart installation begins. When it's completed, you will be asked whether you want to view the Readme.html file.
- Step 5** Click **No**.
The Java WebStart installation is complete.

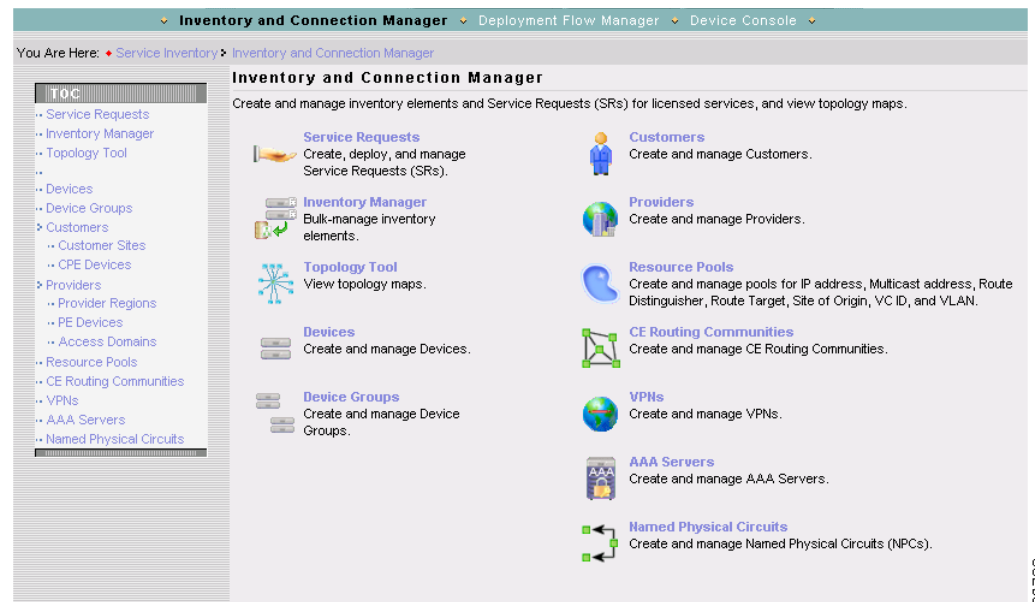
Launch the Inventory Manager

To launch the Inventory Manager:

- Step 1** Log into ISC.
- Step 2** From the Welcome to ISC screen, choose **Service Inventory**.
- Step 3** Choose **Inventory and Connection Manager**.

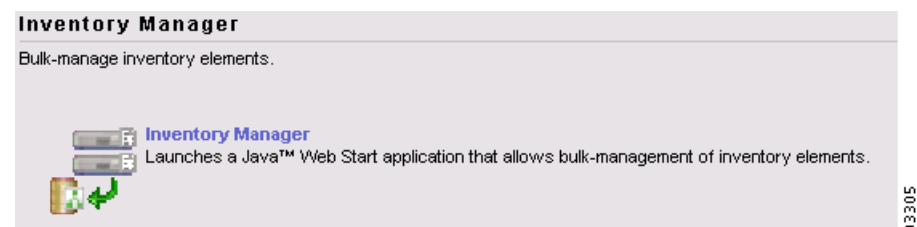
The Inventory and Connection Manager window appears (see [Figure 3-4](#)).

Figure 3-4 Creating an MPLS VPN in ISC



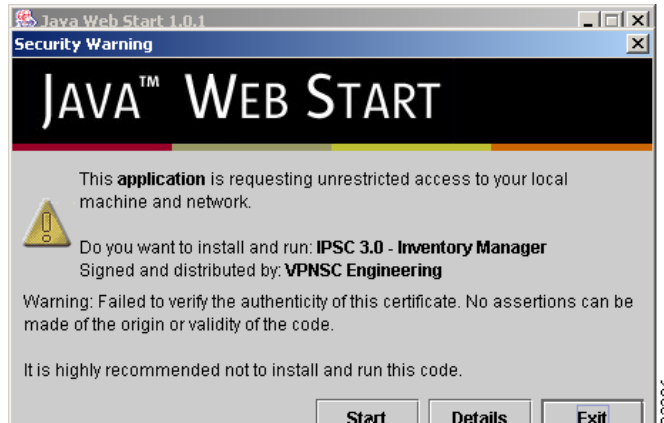
- Step 4** From the Inventory and Connection Manager, choose **Inventory Manager**.
The Inventory Manager option appears (see [Figure 3-5](#)).

Figure 3-5 Choosing the Inventory Manager



- Step 5** Choose **Inventory Manager**.
This starts the Java WebStart process (see [Figure 3-6](#)).

Figure 3-6 Starting Java WebStart



Step 6 Click **Start**.

Java WebStart installs. You then receive a splash image indicating that the installation was successful. The Inventory Manager now launches automatically and is connected to the ISC Master server.

Using the Inventory Manager

This section describes how to use the Inventory Manager to import devices in ISC.

There are two different ways of getting started deploying services with ISC:

- The quickest method is to import the configuration files all of the targets (routers, firewalls, and so forth) from a directory.

These configuration files do not need to be the most current version of the device configuration, but the files should be from the current hardware configuration. This is not a hard requirement, but doing so does ease the set-up process.

- The second method for initializing the targets is *autodiscovery*.

From a single address and some parameters, the autodiscovery process leverages CDP (Cisco Discovery Protocol) to discover devices within a specified number of hops from the starting point. Enabling CDP for the desired devices is a requirement for autodiscovery.

Importing Configuration Files

You should have a repository of configuration files accessible on the client machine where Inventory Manager is running. If you have not already done so, copy these configuration files to the Web Client machine for import.

Step 1 Log in to the Inventory Manager application using your username and password controlled by the ISC Administrator.

The default user is **admin**; the default password is **cisco**.

Step 2 From the Inventory Manager, choose **File >New > New Device Group**.

This creates a container for targets that can be later moved to a provider or customer as initialization continues.

Step 3 Enter the Device Group name.

You are asked if you want to import configuration files.

Step 4 At the No Config Files Specified for Import prompt, click **Yes**.

Step 5 At the Open dialog box, browse to the location of the configuration files you want to import.

The configuration files on the Web Client can be located by normal file browsing with both **Shift** and **Control+Click** available for selecting multiple files. There are filters to display all the files in a directory, just files containing BGP autonomous systems, and files that do not contain BGP configurations. You can use the BGP filters to select the PE devices that must have BGP configured or CE devices that do not require BGP.

Step 6 Once the appropriate files are selected, click **Open**, then click **OK**.

The Inventory Manager now imports these devices based upon the selected configuration files. The operator should now assign the correct roles to these devices and fill out other information required for the Provisioning process.

These operations are described in more detail in the following sections, as they are common to both methods of importing device information and administration.

Device Autodiscovery

ISC provides a mechanism that automatically discovers the state of the service provider's network. The ISC Autodiscovery feature delivers two significant advantages to the service provider:

- The service operator needs to enter only minimal information to create service requests, even services that include many physically connected network devices.
- Services that were originally provisioned by applications other than ISC (or its predecessor, VPN Solutions Center) can be managed by ISC.

The Autodiscovery tool provides the following functions:

- Detects the physical connection between Cisco network devices that have the Cisco Discovery Protocol (CDP) and the Simple Network Management Protocol (SNMP) enabled.
- Discovers a set of interconnected Cisco network devices and the device type.
- Discovers the encapsulation types of each Cisco router interface.
- Discovers routing information for the MPLS-VPN link, as well as VRF and CE Routing Community information (this is the Service Discovery feature).

The Autodiscovery process allows devices to be added to the Repository without existing configuration files.

Start the Dynamic Autodiscovery Process

To use the Autodiscovery tool, follow these steps:

Step 1 From the Inventory Manager, choose **File > New > New Dynamic Device List**.

The Device Information dialog box appears.

This creates a container for targets that can be moved to a Provider or Customer as initialization continues. After creating a new Device List, a discovery starting point must be configured. This starting point is a device that can be reached from the ISC host.

A reachable interface on the starting point is configured as the *management interface*. The management interface is the address on the device that the ISC host will use to reach the device.

Prerequisites for New Dynamic Device discovery include the following:

- *Policy.xml*: Created by entering a seed IP address.
- Maximum Hop count: Entered when initializing the task.

Step 2 To start the Autodiscovery process, choose **Tasks > Start Auto-Discovery**.

The Discovery Policy dialog box appears.

Step 3 Enter the number of hops.

You must specify a maximum hop count for the Autodiscovery process. The Autodiscovery process queries the starting point device for its CDP table. From this table, all of those devices are queried for their CDP information. This CDP query process continues until the maximum hop count from the starting point is reached. Please note that only devices running the CDP process will be discovered.

The Save Connection Information prompt box appears:

Do you want to save the device connection information for use at a later time to perform an NPC Discovery task?

After completing the discovery process, you can save the discovered device information in XML format to use as a starting point for future discovery efforts.

Step 4 Click **Yes**.



Tip

The two output files created by the autodiscovery process—*connection.xml* and *seed.xml*—must now be sent via FTP to the client workstation. These files will be utilized in the coming tasks.

Step 5 Using FTP, send the *connection.xml* and *seed.xml* files to the client workstation.

Assign Device Roles and Passwords

After raw devices are imported to the Repository, you must set several parameters before the devices can be saved to the Repository. These include:

- SNMP R/W Community Strings
- Telnet login password
- Device enable password
- Correct management address (usually that of Loopback 0)

The first stage is to remove from the discovered device list any superfluous devices not required by the ISC Provisioning process. These include core network devices or non-PE/CPE/CLE devices used within the operator's network.

Step 1 Select the rows for the devices to be deleted.

- Step 2** Once the superfluous devices are selected, from the Edit menu, choose **Remove Selected Devices**.
It is common in networks for devices to share many parameters. The Defaults mechanism allows these common parameters to be entered into many elements at the same time, such as login password, enable password, and SNMP strings.
- Step 3** From the Edit menu, choose **Edit Default Attributes**.
You can then edit a row for default values for each tab of the device list.
The next step of the configuration process will be to collect live configurations that will require login and enable passwords.
- Step 4** Enter these attributes into the Defaults row.
After entering the default values, select all of the devices that share those common parameters.
- Step 5** From the Edit menu, choose **Load Default Attributes to Selected Cells**.
- Step 6** If different groups of devices share different common values, repeat the edit and load defaults process for each group
The management address is the IP address that ISC will use to communicate with the element. This address must be reachable from the ISC host. When the devices were imported or discovered, ISC attempts to select the proper address as a management address, starting with a loopback address. The selected address should be verified for reachability from the ISC host. ISC must be able to reach the network element for the configuration process to progress.
- Step 7** **Double-click** the *Management Address* cell.
The Management Address dialog box appears.
- Step 8** Enter the management address for each device, then click **OK**.
You should now assign roles to these devices—either *PE* or *CE*.
- Step 9** Highlight each device group and add them to an existing or new Provider or Customer.
You must create and populate a Provider Administrative Domain (PAD). A PAD is a group of Provider Edge devices that share a common BGP autonomous system (AS) number.
- Step 10** Highlight the devices sharing the common BGP AS to be added to a new PAD.
- Step 11** From the Edit menu, choose **Move to New Provider**.
Now you must configure the PAD. Once the devices are assigned a PAD, they become Provider Edge (PE) routers. PEs must be placed into Regions. Each PAD must have one or more Regions. A Region is a collection of PEs that may share an address pool.
- Step 12** To place a PE into a Region, double click on the *Region* cell for the PE.
If the desired Region has already been created, it can be selected, or you can choose **Create Region** to add a Region.
Create and populate the Customer. Routers can be moved in bulk to customers through the Inventory Manager.
- Step 13** To move routers to a new Customer, highlight the desired routers, then choose **Edit > Move to New Customer**.
You are prompted for a Customer name.
- Step 14** Enter the Customer name.
A new tab is created at the bottom of the device list, and the selected routers are moved to the Customer.
- Step 15** Repeat this process for all the desired Customers.
This completes the assignment of roles to devices.

The tabs at the top of the device list pane of the Inventory Manager window correspond to a grouping of information about the devices. The symbol to the left of the tab name indicates if all of the information required on that tab has been configured.

- A red **X** means that additional information is required.
- A yellow check mark indicates that all required information has been entered, but not all possible information.
- A green check mark shows that all information for that tab has been entered.

To save the devices to the Repository, each tab must show a check mark of either color.

Collect Latest Device Configurations

Collecting configurations serves two main purposes:

- It loads the current configuration information for the devices that populates many of the configuration cells.
- It also verifies reachability and passwords for the devices that it succeeds in collecting configuration files from.

Reachability and password problems are the most common cause of difficulty in the provisioning process, so resolving those issues as soon as possible is important.

- Step 1** From the Tasks menu, choose **Collect Latest Configuration Files**.
- Step 2** To collect configuration files, select all of the devices which you have reachability to and passwords for. When the collection is complete, you will be notified of the success or failure of the process and given the option of refreshing the information in the Repository.
- Step 3** Save the updated information to the Repository.
- If the collection fails, test the reachability of the selected management addresses and the configured passwords for the devices.
-

Perform Network Physical Discovery

Now the operator is free to run the Network Physical Discovery task that defines the PE-CE link information. This interface-specific device information is used by the Common Discovery process, which is the final stage of the Autodiscovery mechanism.

Discover NPC has one prerequisite—*Connection.xml*.

Ensure that this file has been uploaded from the ISC server to the client workstation before running this task.

- Step 1** To begin the process, from the Tasks menu, choose Start NPC **AutoDiscovery**. You are prompted to provide the path to the correct connection.xml file.
- Step 2** Browse to the appropriate directory, select the **connection.xml** file, then click **OK**.

A dialog box appears indicating that the NPC Discovery Process has started.

Finally, you are prompted to confirm that the task completed successfully.

Step 3 Click **OK**.

This finishes this portion of the device Autodiscovery process.

Common or Service Discovery

You may choose to run the Common Discovery process. ISC can manage Ethernet over MPLS (for Layer 2 VPN), MPLS, and IPsec networks. However, in order to detect free interfaces on each device for provisioning purposes, existing service(s) will either need to be discovered automatically, or be entered into the system by the operator.

Until the release of ISC, this process could only be achieved manually. For very large networks with many provisioned services, this is both time consuming and open to human error. This problem is alleviated by means of the Common Discovery process, which enables discovery of the following services:

- Layer 3 VPN MPLS service(s)
 - Layer 2 VPN ERS/EWS service(s)
-

Step 1 To start the Common Service discovery process, choose **Tasks > Start Service Discovery**.

The Service Discovery dialog box appears. The options are:

- **L2VPN**
- **MPLS Only**
- **Both MPLS and L2VPN**

Step 2 Choose the type of service discovery you desire.

You are informed that the service discovery process has started. Finally, you are informed that the process is complete.

Step 3 Click **OK**.
