Service Inventory > Inventory and Connection Manager > Inventory Manager

This chapter describes how to use Inventory Manager to prepare service inventory for the IP Solution Center (ISC) provisioning process. It contains the following subsections:

Overview of Inventory Manager

Inventory Manager provides a method of managing mass changes to inventory and service model data in the ISC provisioning process. In this process, Inventory Manager enables an operator to import network specific data into the ISC Repository (Repository) in bulk mode.

Inventory Manager performs three primary functions:

- Imports devices and configures CPE and PE by associating devices with a Customer or Provider.
- Collects live configuration files from a variety of devices (for example, routers, firewalls, and switches) in a network.

Note IPsec, firewall, NAT: **These features are not supported in this release.**

- Discovers logical, physical, and service level connectivity in a network.

Auto Discovery is an important tool in this process and is invoked from Inventory Manager. It can also be invoked from a Unix command line interface although this method is not recommended (see UNIX Command Line Interface (UNIX CLI), page 4-107). For a detailed description of Auto Discovery, see Auto Discovery, page 4-105.

Prerequisites and Limitations

This document is intended for network engineers who have sufficient experience with MPLS VPN, L2VPN, and IPsec to provision these technologies using ISC.

Note IPsec: **This feature is not supported in this release.**

All of the network elements that you plan to provision should support the required hardware features and Cisco IOS versions.

Client Requirements

Java Runtime Environment (JRE) and Java Web Start must be installed to run Inventory Manager. If you are having trouble getting them to function properly, or need to update your local JRE, you can download and install the version appropriate for your operating system:

- Windows (all languages, including English): 1.4.2_04
- Solaris SPARC 32-bit self-extracting file: 1.4.2_04
- Linux self-extracting file: 1.4.2_04 (Not Supported)

Name Resolution

Inventory Manager requires name resolution. The ISC HTTP server host must be in the Domain Name System (DNS) that the web client is using or the name and address of the ISC server must be in the client host file.

SNMP

Prior to device discovery, SNMP must be enabled. All devices in the ISC provisioning environment must support SNMP. ISC supports SNMP versions 1, 2c, and 3.

CDP

CDP must be enabled to discover devices. Inventory Manager uses CDP to perform the service discovery task. CDP should be enabled globally and at the interface level for each device in the ISC provisioning environment.

NAT

This feature is not supported in this release.

Prior to device discovery, no Network Address Translation (NAT) mapping for router IP addresses is allowed.

Role Requirements

To run the Inventory Manager you need to use the predefined roles, CollectionRole and DeviceImportRole. This is the minimum requirement to successfully create physical or logical devices and to upload configuration files from the client to the ISC server.

Inventory Manager from End to End

This section describes how you use Inventory Manager to import and configure devices, collect configuration files, and perform service discovery.

These tasks should be carried out in the following order:

1. Launching Inventory Manager, page 4-3
2. Importing Devices, page 4-5
   - Importing Devices from Configuration Files, page 4-5
   - Importing Devices with Auto Discovery, page 4-6
3. Configuring Device Credentials and SNMP Parameters, page 4-7
4. Collecting Configuration Files, page 4-9
5. Marking Interfaces for IPsec, Firewall, NAT, or QoS, page 4-9
6. Creating a New Customer with Devices, page 4-10
7. Creating a New Provider with Devices, page 4-10
8. Importing Connections with NPC Auto Discovery, page 4-11
9. Importing Services with Service Discovery, page 4-11

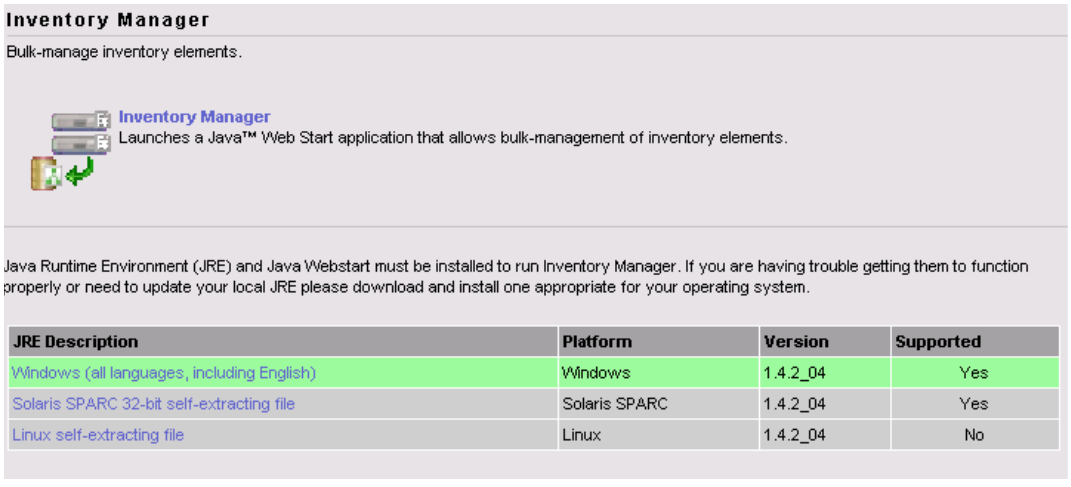
Launching Inventory Manager

To launch Inventory Manager, follow these steps:

Step 1 Log in to ISC.

Step 2 Navigate **Service Inventory** > **Inventory and Connection Manager** > **Inventory Manager** and you receive a window, as shown in Figure 4-1, "Inventory Manager." If you choose or need to click on an installation of Java Runtime Environment (JRE) for an operating system, follow that path, then quit the browser, log in again, and navigate the path in this step again.

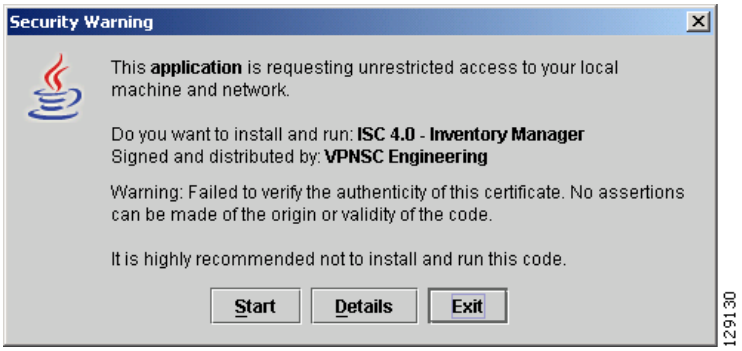
Figure 4-1 Inventory Manager



Step 3 Click **Inventory Manager** in Figure 4-1, "Inventory Manager" to launch Inventory Manager on the web client. The Java Web Start window appears.

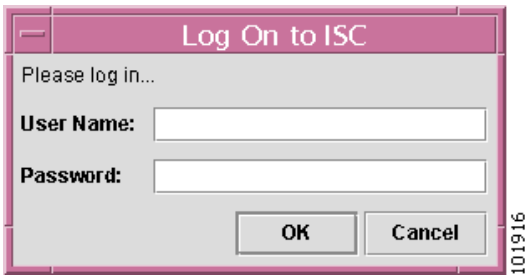
Step 4 From the Security Warning window, click **Start** to automatically complete the configuration, as shown in Figure 4-2.

Figure 4-2 Start Java Web Start



Step 5 You receive a login window, as shown in Figure 4-3, "Log On to ISC."

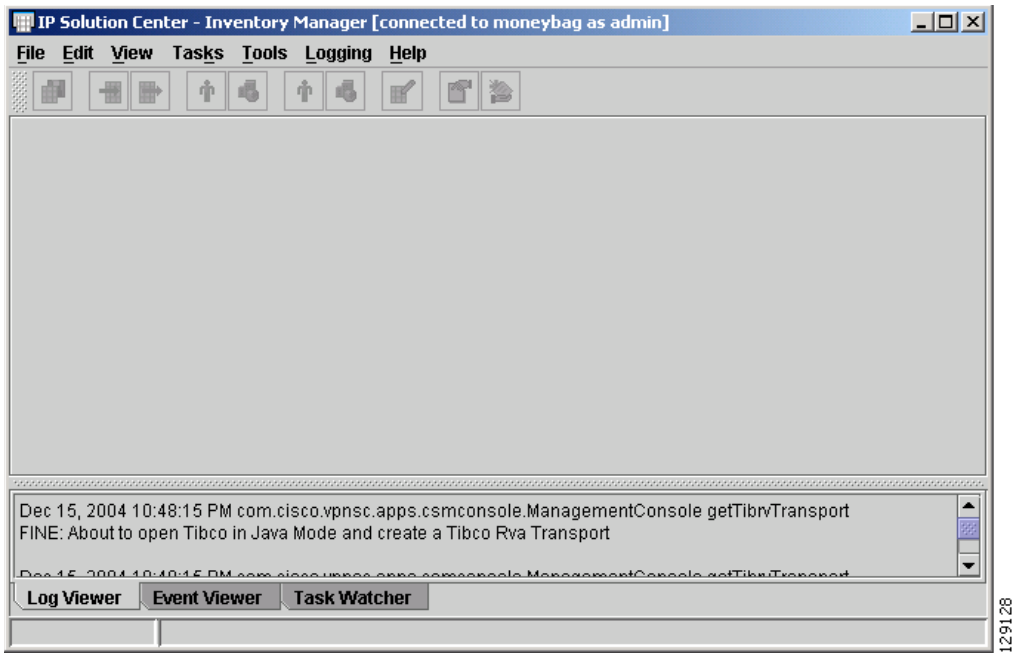
Figure 4-3 Log On to ISC



Step 6 Enter your **User Name** and **Password** and click **OK**.Inventory Manager launches and connects to the Master ISC server.

The Inventory Manager Opening Screen in Figure 4-4 appears.

Figure 4-4 Inventory Manager Opening Screen



Importing Devices

As described in the introduction to this chapter, devices can either be imported or created. The fastest way to bring device information into the Repository is to import devices using Inventory Manager.

Importing Devices from Configuration Files

If the configuration files are for a particular customer or provider, you can create a new customer or provider and associate the configuration files with CPEs or PEs. If the customer or provider currently exists in the Repository, you can open them and insert more CPEs or PEs to be associated with new or existing sites or regions.

To import devices with configuration files, follow these steps:

Step 1 From Inventory Manager, choose **File > New > New Device Group**.

This step creates a container for target devices that can be moved to a provider or customer during the initialization process.

Step 2 Enter a device group name and click **OK**.

You receive a prompt to import configuration files. You probably have a repository of configuration files on an existing network management device or TFTP server. Copy these files to the web client machine for import or make them available with a shared directory.

Step 3 At the **No Config Files Specified for Import** prompt, click **Yes**.

The configuration files on the web client can be located by normal file browsing with both Shift and Ctrl+Click selected for multiple selections. When creating a new device group, only one filtering option is available: All Files.

Note When creating new Providers, there are filters for files containing a specific BGP autonomous system number, or files that do not contain BGP configuration. The BGP filters can also be used to select PE devices that must have BGP configured or CE devices that do not require BGP.

Step 4 At the Open dialog box, browse to the location of the configuration files you want to import.

You may select multiple configuration files to import using SHIFT or CTRL + click. Please make sure that no more than X (250 or a number to be determined) configuration files are selected for import. There may be performance issues with Inventory Manager if more than X config files are selected for import at once.

Inventory Manager now imports a row in a spreadsheet workbook for each selected configuration file. By default, Inventory Manager inspects the configuration files and determines the device type, which includes Cisco IOS, CatOS, PIX, and VPN 3000 (IPsec, firewall, NAT, VPN 3000: **These features are not supported in this release)**. It also parses passwords, SNMP information, interfaces, and virtual circuits.

If cells in the resulting spreadsheet are empty, Inventory Manager was not able to determine the value and, if it is required, the operator must provide the data or choose the information from a defined set of choices before saving.

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

Step 5 Once the appropriate files are selected, click **Open**, then click **OK**.

Importing Devices with Auto Discovery

Note The Auto Discovery process can either be activated from Inventory Manager or from the command line on the ISC server using the Cisco Cornerstone Bridge Auto Discovery scripts.

To import devices with Auto Discovery, follow these steps:

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

This creates a spreadsheet where each row represents a potential seed device for discovery. For each seed device, the management interface must be provided. The management interface is the address on the device that the ISC host uses to reach the device.

After creating a new device list, a discovery starting point needs to be configured. This starting point is a device that can be reached from the ISC host. For each seed device, an accessible interface on the starting point is configured, because the management interface must be provided. The management interface is the address on the device that the ISC host uses to reach the device.

New dynamic device discovery requires the following manual tasks:

- Entering a seed IP address
- Entering a maximum hop count on the initialization of the task

A **policy.xml** file is created and a hop count is set automatically.

To choose the seed devices and hub, pick a seed device that can reach a large section of the network. Pick one or more of them until you think these devices will enable you to reach your entire managed network.

Point-of-presence (POP) routers are usually good choices. If you choose all the POPs in your network as the collection of seed devices and put in the appropriate number of hubs, you discover the entire managed network.

To pick the hub number, go to the CE that is the furthest from its associated POP, and count the number of devices between them. If this number is N, the hub number is N+1, assuming you are picking the POP as the seed.

Step 2 Click on the **Management Address** cell and enter the seed IP address for the new dynamic device list

Step 3 Choose **Tasks > Start Auto Discovery**.

A maximum hop count is specified for the Auto Discovery process. The Auto Discovery 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 are discovered.

Step 4 Specify the maximum hop count when you receive the prompt.

Note Only devices running the CDP process are discovered.

You are prompted to save two files. One file contains the list of the discovered devices and the other contains information related to connectivity between the devices. The discovered device information can be saved in XML to use as a starting point for future discovery efforts.

Step 5 Save the devices discovery.

Step 6 To view the Auto Discovery logs, go to **Administration > Control Center > Hosts >** *machine-name* **> cornerstone bridge**.

Configuring Device Credentials and SNMP Parameters

After the discovered devices are rendered in the spreadsheet, they must have several parameters set before the devices can be saved to the Repository and perform a successful live configuration collection. These parameters include:

- SNMP read and write community strings
- Telnet login password
- Device enable password

Note The reachable management address is usually Loopback 0.

First remove any devices that are not required in the provisioning process. These items include core network devices or non-PE, CPE, and CLE devices that are used within the operator's network.

To remove unwanted devices, follow these steps:

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

Shift-select and Control-select are useful for multiple devices.

Step 2 Choose **Edit > Remove Selected Devices**.

It is common in networks for devices to share many parameters. The Defaults option allows these common parameters to be entered for many devices at the same time; for example, login password, enable password, and SNMP strings.

To edit multiple devices, follow these steps:

Step 1 Choose **Edit > Edit Default Attributes**.

A row for default values can be edited for each tab of the device list. The next step of the configuration process collects live configurations that require login and enable passwords.

Step 2 Enter login and enable passwords into the defaults row.

After entering the default values, select all of the devices that share those common parameters. For devices that have values other than the default values, you can perform multiple editing techniques.

Step 3 Select multiple rows or columns using standard selection techniques and choose **Edit > Edit Selected Devices**.

A dialog box, similar to the defaults window appears, allowing you to enter values to be applied to the selection.

Note You can right click on the column name and a menu appears showing you choices for sorting and selecting or de-selecting of columns.

Step 4 To configure these devices, choose **Load Default Attributes to Selected Cells**.

The management IP address is the address that ISC uses 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. Verify the selected address for accessibility from the ISC host. ISC *must* be able to reach the network element for the configuration process to progress.

Step 5 Click on the Management Address cell and enter the IP address in the dialog box.

Collecting Configuration Files

Collecting configuration files serves two purposes. It loads the current configuration information for the device, which populates many of the cells. It also verifies reachability and passwords for the reachable devices.

This task is created in the Repository and starts immediately. Logs can be viewed as normal for a collection spawned using only the Web GUI.

The task name is Inventory_Manager_Collection_*xxxxxx_username*, where *xxxxxx* is a unique number and the *username* is admin, or whatever the logged in username is in ISC.

To collect configurations, follow these steps:

Step 1 Select all the devices that have valid passwords and could be reached.

Step 2 Choose **Tasks > Collect Latest Configuration Files**.

Marking Interfaces for IPsec, Firewall, NAT, or QoS

IPsec, firewall, NAT: **These features are not supported in this release**

The interface marking process is only required for provisioning IPsec, Firewall, NAT, or QoS services. Marking interfaces on a one-by-one basis can be a very time consuming and tedious task. Inventory Manager provides a helpful tool to create rules for marking interfaces based on predefined criteria. You can apply one or more rules to selected devices to mark the interfaces in a bulk fashion.

For IPsec, the public interfaces are the interfaces where the IPsec or GRE tunnels terminate and the private interfaces are the interfaces behind which the subnets to be protected reside.

For firewalls, the outside interfaces connect to the outside, typically unsecured, networks and the inside interfaces are for the subnets residing behind the firewall.

To mark interfaces with Inventory Manager, follow these steps:

Step 1 Choose **Tools > Interface Rule Marking Editor**.

A window appears allowing you to create, modify, or delete existing rules or folders. One simple rule can mark all Loopback0 interfaces as public for IPsec.

Step 2 To apply a rule to one or more devices, select the device(s) in the spreadsheet.

Step 3 Choose **Edit > Apply Interface Marking Rule**(s) to the selection. A rule chooser appears allowing you to select one or more rules to be applied.

Note After completing the device configuration process, all the red X marks on the Device List tabs should be converted to either yellow or green Check Marks. These marks indicate that you have completed the required configuration and can save the device list, provider, and/or customer. Save all the completed lists by selecting **Save** under the file menu. Now all the device preparation should be complete and provisioning setup can begin.

Creating a New Customer with Devices

The devices should now be assigned roles, either PE or CE. For customers, you can assign roles by highlighting each device group and adding it to a new or existing Customer. Routers can be moved in bulk to customers with Inventory Manager.

To move CE routers to a new customer, follow these steps:

Step 1 Select the desired routers and choose **Edit > Move to New Customer**.

Step 2 You are prompted to enter a customer name.

Step 3 Enter a customer name and click **OK**.

A new tab is created at the bottom of the device list and the routers are associated with the customer.

Each customer router must be put into a site. A site can have more than one router in it. All routers in a site should share routing information with the external provider network.

Step 4 Shift-select the **Site Name** cells for each customer router in the **CPE Attributes** tab.

Step 5 Choose **Edit Selected Devices**.

Step 6 Choose **CUSTOMER_ID+"SITE"+HOST_NAME**.

Repeat this process for all the CPEs.

All customer routers must have a **Management Type** selected. As with customer site, a range of router Management Type cells can be selected for bulk editing.

Step 7 Click the **Management Type** cell for all CEs.

Step 8 Choose **Edit Selected Devices.**

Step 9 Select the **Management Type**.

Creating a New Provider with Devices

A provider or provider administrative domain (PAD) is a group of Provider Edge (PE) devices that share a common BGP AS.

To move PE routers to a new provider and create a region, follow these steps:

Step 1 Highlight the devices with a common BGP AS to be added to a new provider.

Step 2 Choose **Edit > Move to New Provider**.

When 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 3 To place a PE into a region, click on the **Region** cell for the PE.

If the desired region has already been created, it can be selected.

Step 4 Choose **Create Region** to add a region.

You can also add multiple PEs to a single region in one step using standard multiple selection techniques and choosing the **Edit > Edit Selected Devices** menu. As with single PE editing, you are prompted to choose an existing region or create a new region.

This completes the assignment of roles to devices.

Note The tabs at the top of the device list pane of the Inventory Manager window corresponds to a grouping of information about the devices. The symbol to the left of the tab name indicates whether all 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 green or yellow.

Importing Connections with NPC Auto Discovery

To discover connections, referred to as Named Physical Circuits (NPC), run NPC Auto Discovery. This task defines the PE and CE link information, which is used by Common Discovery in the final stage of the Auto Discovery process. NPC Auto Discovery has one prerequisite, the **connection.xml** file. Ensure that this file has been uploaded from the ISC server to the client workstation before running this task.

To import connections with NPC Auto Discovery, follow these steps:

Step 1 Choose **Tasks > Start NPC Auto Discovery**.

You are prompted to provide the path to the correct **connection.xml file**.

Step 2 Select the correct **connection.xml** file and click **OK**.

A dialog box appears, indicating that the NPC discovery process has started.

Step 3 You are prompted if the task completes successfully. Select **OK** to finish this portion of the NPC Auto Discovery process.

To find the discovered NPCs, go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.

Importing Services with Service Discovery

At this point, you can choose to run the Common Discovery process. ISC manages Ethernet over MPLS (L2VPN) and MPLS networks with IPsec (IPsec: **This feature is not supported in this release)**. To detect free interfaces on each device for provisioning purposes, existing services either need to be discovered automatically or entered into the system manually.

For very large networks with many provisioned services, manual entry is time consuming and prone to human error. These issues are alleviated by the Common Discovery process. The Common Discovery process discovers:

- Layer 3 MPLS VPN services
- Layer 2 VPN (Metro) services
- Layer 2 VPN (L2TPv3) services.

To specifically import services with Auto Discovery, follow these steps:

Step 1 Choose **Tasks > Start Service Discovery**.

The Service Discovery window in Figure 4-112 appears (see Start Service Discovery, page 4-96, for the GUI description). You are prompted to select which type of Common Discovery to perform.

Step 2 Select one or more types of service discovery by checking the corresponding **Service Discovery** box.

If you select **L2VPN (L2TPv3)**, the bottom **L2TPv3 Options** section become available:

Step 3 Make the desired selections

You are notified when Service Discovery is finished.

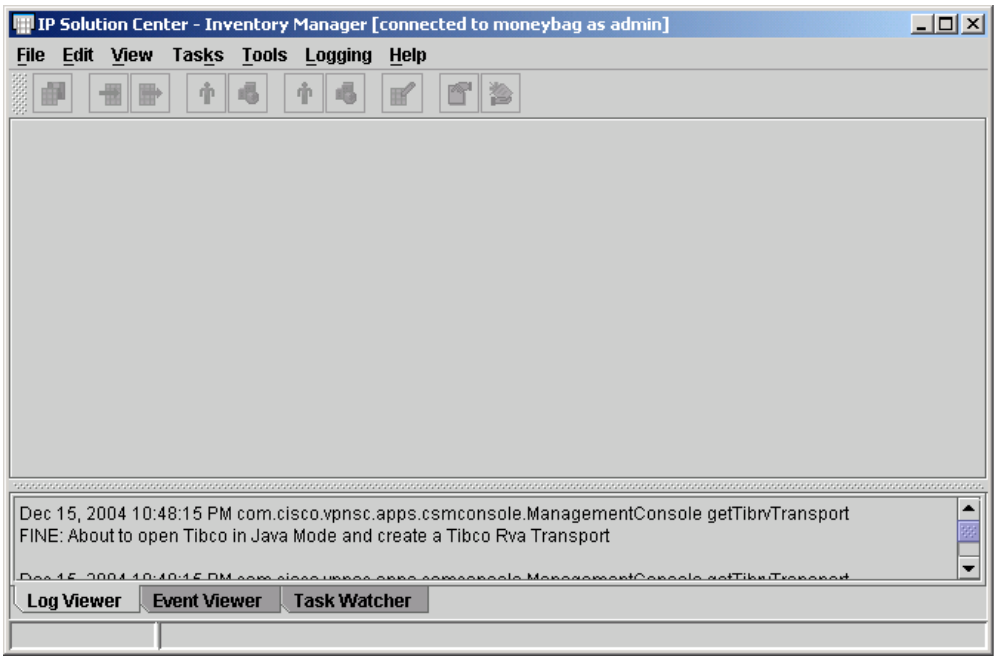
Step 4 To find the discovered service requests, go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

Introducing the Inventory Manager GUI

Although Inventory Manager has the physical look and feel of many windows applications, with File, Edit, View, Tasks, Tools, Logging, and Help menus, the application is designed to have the logical view of a spreadsheet. When you learn how to use one spreadsheet in Inventory Manager, you learn how to use them all.

After starting up Inventory Manager by following the steps outlined in Launching Inventory Manager, page 4-3, the main Inventory Manager window in Figure 4-4 appears.

Figure 4-5 Inventory Manager GUI



The various GUI elements are explained in the following sections and in Inventory Manager GUI Reference, page 4-34.

This section contains the following sections:

Spreadsheet Features

This section contains the following sections:

Understanding the Spreadsheet

Before using Inventory Manager, you need to know about these spreadsheet features:

- Spreadsheets
  - Contain Device Group and physical device information.
  - Contain PE and CPE logical device information.
  - Group information or attributes by tabs.
- Tabs
  - Contain a unique table of rows and columns within a spreadsheet.
  - Show the status of the entire spreadsheet with icons.
  - Signify with a Red X that the tab is missing required information.
  - Signify with a Yellow Arrow that the tab contains all required information, but not all optional information.
  - Signify with a Green Arrow that all required and optional information in the tab is provided.
- Rows
  - Contain information or attributes about a single device, module, or interface.
- Columns
  - Contain one type of information or attribute.
  - Have a unique description.
  - Have a Column Heading
  - Have referenced tabs. (For example, Domain Name is in every general tab for each spreadsheet.)
  - Sort up or down by clicking on the column header or clicking the column header and choosing a sort menu.
  - Sort a column in one tab of a spreadsheet to affect all other tables in the spreadsheet.

- Column Heading
  - Has a popup menu to click for selection, de-selection, and sorting.
  - Can have a color, depending on the column status (all cells combined for one column ordered together).
  - Indicates the status of the individual column with color. (As opposed to the Tab icon referenced above, which displays the status of the entire spreadsheet.)
- Host Name Column
  - Does not scroll and is always the first column on the left.
  - Selects or de-selects an entire row.
  - Available in every tab for a given logical or physical device.
  - Acts as a reference point when switching among tabs and scrolling to the right when columns exceed the window width (see menu **View > Fit Columns in Window**).

Note When debugging why a tab has a Red X, this can help to identify the column in error, or missing data, very quickly.

Editing the Spreadsheet

When you learn how to set defaults or edit columns in one spreadsheet, you can set defaults or edit columns for each type of spreadsheet in Inventory Manager.

Cell Editing

Cell editing has the following features:

- Provides dialog box when you click a cell.
- Provides choices for each attribute. (Device Role is either Cisco IOS, CATOS, PIX, or VPN 3000. (IPsec, firewall, NAT, VPN 3000: **These features are not supported in this release)**)
- Provides a simple input text dialog for some columns.
- Provides a password editor for some columns.
- Provides a choice dialog with a list of available options for some columns.

Cells

Cells have the following editing features:

- Can be edited by clicking. (Most individual cells can be edited, but not all columns.)
- Select or de-select multiple cells spanning multiple columns using standard selection techniques (Click, Shift-Click, or Ctrl-Click).
- Edit multiple cells in a single column at once using **Edit > Edit Selected Devices.**
- Edit multiple cells spanning multiple columns all at once using **Edit > Edit Selected Devices.**

Note Close a spreadsheet by choosing **File > Close** *filename.* Do not forget to save your edits.

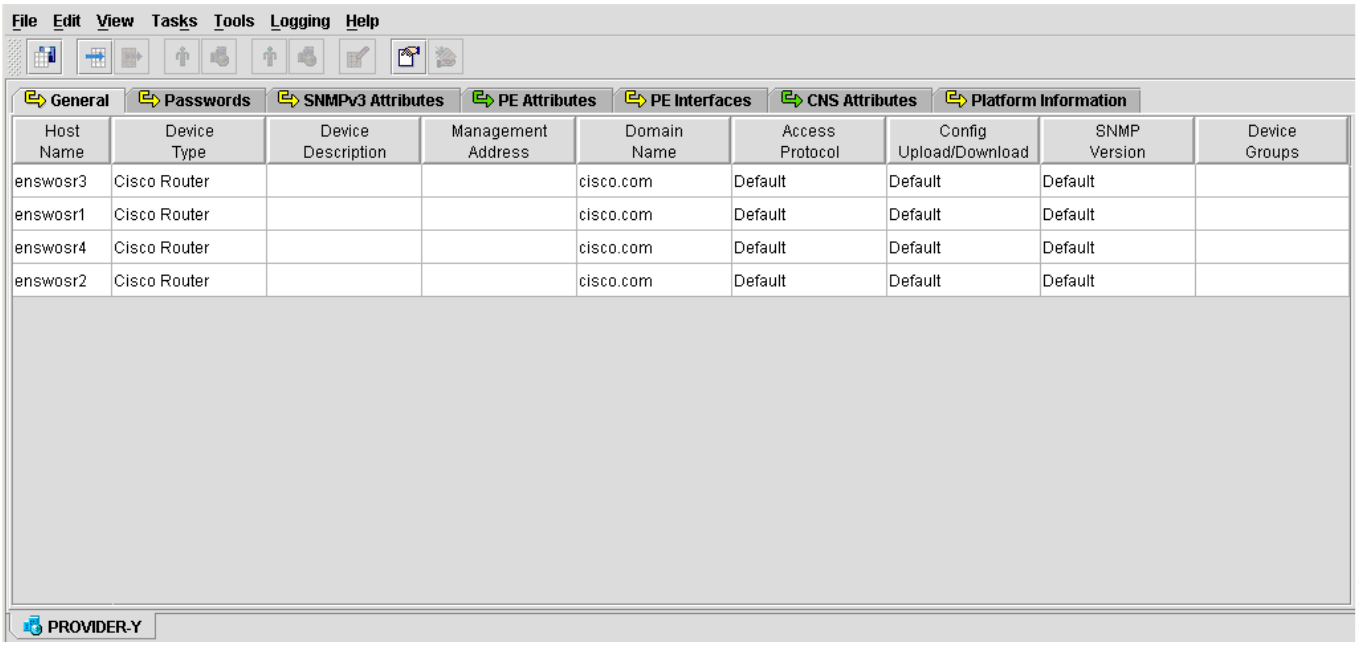
Provider Spreadsheet

The Provider spreadsheets contain the following tabs:

General

Figure 4-6 shows an example of the General tab:

Figure 4-6 Provider Spreadsheet - General Tab



The General tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
  - Cisco Router
  - Catalyst OS device
  - Terminal server

  - VPN 3000 (**This feature is not supported in this release)**
  - PIX firewall (**This feature is not supported in this release)**
  - IE2100 (Cisco CNS appliance)

- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.
- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Protocol for downloading configurations. Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-7 shows an example of the Passwords tab:

Figure 4-7 Provider Spreadsheet - Password Tab

General | Passwords | SNMPv3 Attributes | PE Attributes | PE Interfaces | CNS Attributes | Platform Information

Host Name	Login User	Login Password	Enable User	Enable Password	SNMP Read-Only	SNMP Read-Write
enswosr1		*****		*****	public	private
enswosr2		*****		*****	public	private
enswosr3		*****		*****	public	private
enswosr4		*****		*****	public	private

101023

The Passwords tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.

- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-8 shows an example of the SNMPv3 Attributes tab:

Figure 4-8 Provider Spreadsheet - SNMPv3 Attributes Tab

General | Passwords | SNMPv3 Attributes | PE Attributes | PE Interfaces | CNS Attributes | Platform Information

Host Name	Security Level	Authentication User	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
enswosr1	Default			NA		None
enswosr2	Default			NA		None
enswosr3	Default			NA		None
enswosr4	Default			NA		None

101024

The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, Authentication. Message Digest 5 (MD5), and the Secure Hash Algorithm (SHA). Default: None.

- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and IPsec Data Encryption Standard (DES 56). Default: None.

Note IPsec: **This feature is not supported in this release.**

PE Attributes

Figure 4-9 shows an example of the PE Attributes tab:

Figure 4-9 Provider Spreadsheet - PE Attributes Tab

General | Passwords | SNMPv3 Attributes | PE Attributes | PE Interfaces | CNS Attributes | Platform Information

Host Name	Provider Name	Region Name	Role	Loopback Interface	Is Managed
enswosr1	PROVIDER-Y	WEST-Y	PE POP	Loopback0 : 192.168.115.100/32	☑
enswosr2	PROVIDER-Y	SOUTH-Y	PE POP	Loopback0 : 192.168.115.101/32	☑
enswosr3	PROVIDER-Y	EAST-Y	PE POP	Loopback0 : 192.168.115.12/32	☑
enswosr4	PROVIDER-Y	NORTH-Y	PE POP	Loopback0 : 192.168.114.53/32	☑

101025

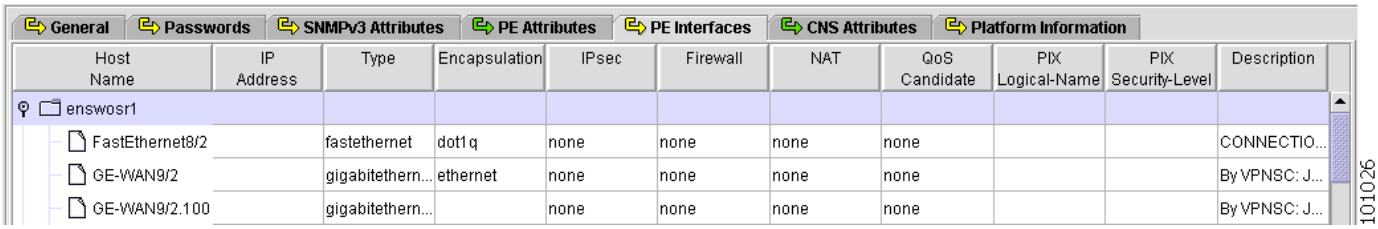
The PE Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Provider Name**—Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- **Region Name**—Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Role**—Choices include: PE POP, PE CLE, PE CORE, and PE MVRF.
- **Loopback Interface**—Loopback address is the IP address of any loopback interface on the device. You can select one of the loopback interfaces for this field and use the IP address on that loopback interface.
- **IS Managed**—Provisioned by ISC. Click the check box for yes. Default is no.

PE Interfaces

Figure 4-10 shows an example of the PE Interfaces tab:

Figure 4-10 Provider Spreadsheet - PE Interfaces Tab



The PE Interfaces tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IP Address**—IP address associated with this interface.
- **Type**—Specifies the type of interface. It is a display-only field. Types include:
  - VLAN
  - UNKNOWN
  - STATIC
  - UNNUMBERED
  - DHCP
  - PPP
  - DOCSIS
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
  - UNKNOWN
  - DEFAULT
  - DOT1Q
  - ETHERNET
  - ISL
  - FRAME_RELAY
  - FRAME_RELAY_IETF
  - HDLS
  - PPP
  - ATM
  - AAL5SNAP
  - AAL0
  - AAL5

  - AAL5MUX
  - AAL5NLPID
  - AAL2
  - ENCAP_QinQ
  - GRE

- **IPsec—This feature is not supported in this release.**
  View or edit (mark) interface settings for IPsec. Choices include:
  - None
  - Public

    Interface to the public network (internet). All traffic is encrypted.
  - Private

    Interface to the private network (internal LAN). All traffic is not encrypted.
- **Firewall—This feature is not supported in this release**
  View or edit (mark) interface settings for Firewall. If Device Type is VPN 3000, Firewall is not available. Choices include:
  - Inside

    Highest security interface.
  - Outside

    Lowest security interface.
  - DMZ 1, ..., DMZ N

    The Demilitarized Zone services to both inside and outside interfaces.
- **NAT—This feature is not supported in this release**
  View or edit (mark) interface settings for NAT. If Device Type is PIX firewall or VPN 3000, NAT is not available. Choices include:
  - None
  - Inside

    Highest security interface.
  - Outside

    Lowest security interface.
- **QoS Candidate**—View or edit (mark) interface settings for QoS. If Device Type is VPN 3000 (**This feature is not supported in this release)**, QoS is not available. Choices include:
  - None
  - Marking Rate Limit

    This setting marks the Customer LAN facing interface with the **set** and **police** commands.
  - Endpoint

    This setting marks the PE facing interface on the CE device and the CE facing interface on the PE device.

    On the PE side, all QoS commands go on this interface.

On the CE side, all QoS commands, including the **set** and **police** commands, go on this interface if no interface on the CE device is identified as the Marking Rate Limit interface.

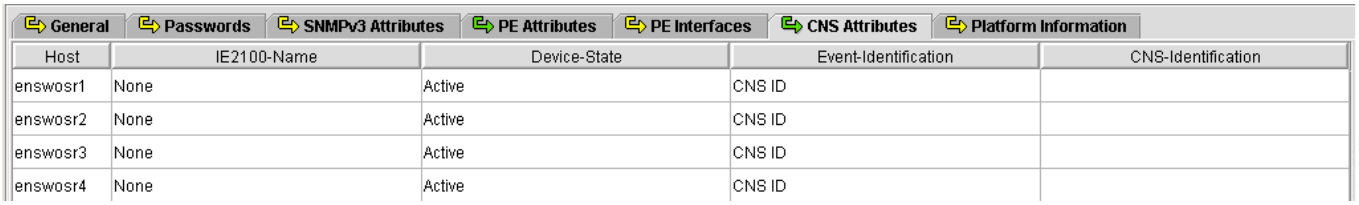
If one or more interfaces have been identified as Marking Rate Limit interfaces, then all QoS commands except the **set** and **police** commands go on this interface.

- **PIX Logical-Name**—Logical name of this interface. This field is displayed only. Field is populated by a collection/import of config file.
- **PIX Security-Level**—Security level of this interface. This field is display-only. Field is populated by importing a configuration file.
- **Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.

CNS Attributes

Figure 4-11 shows an example of the CNS Attributes tab:

Figure 4-11 Provider Spreadsheet - CNS Attributes Tab



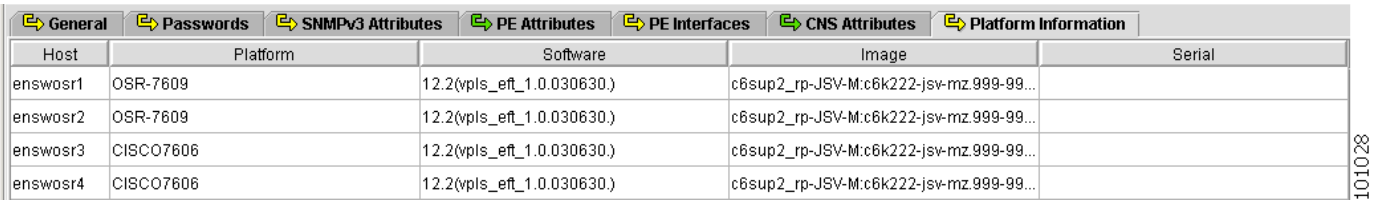
The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS appliance (CNS) must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing CNS names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-12 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-12 Provider Spreadsheet - Platform Information Tab



The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters

Customer Spreadsheet

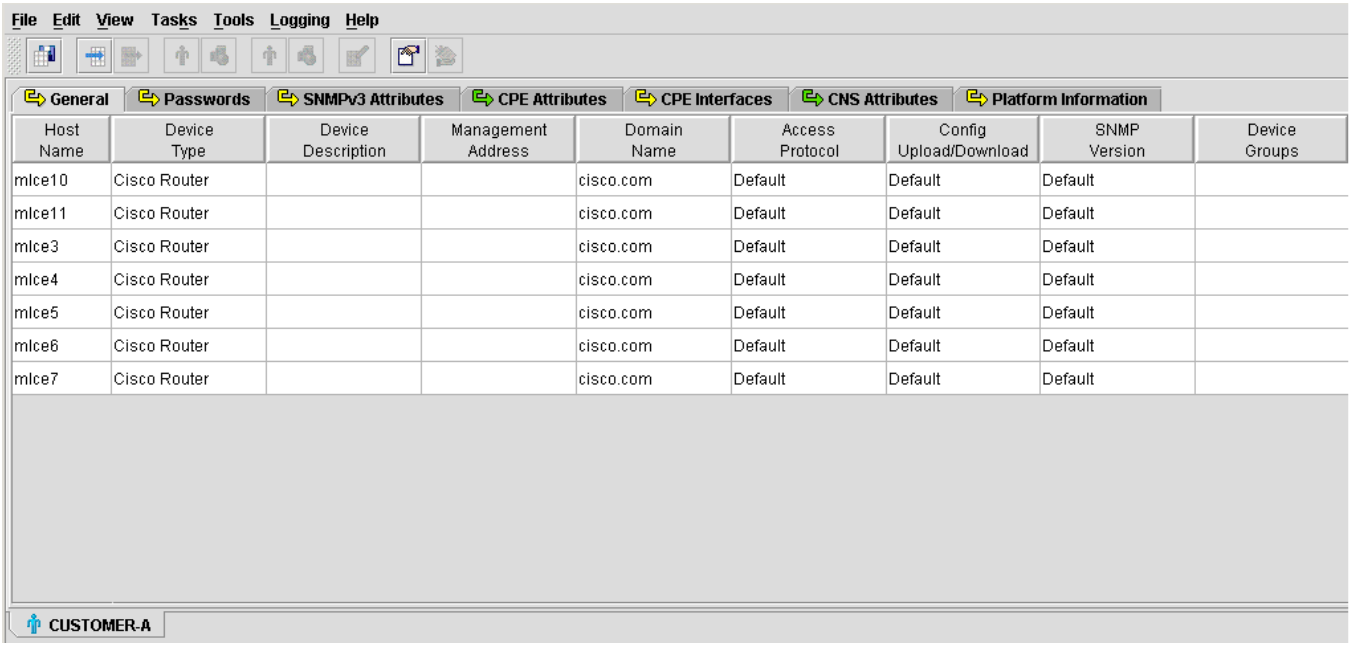
The Customer spreadsheets contain the following tabs:

- General, page 4-23
- Passwords, page 4-24
- SNMPv3 Attributes, page 4-25
- CPE Attributes, page 4-26
- CPE Interfaces, page 4-26
- CNS Attributes, page 4-28
- Platform Information, page 4-29

General

Figure 4-13 shows an example of the General tab:

Figure 4-13 Customer Spreadsheet - General Tab



The General tab contains the following columns:

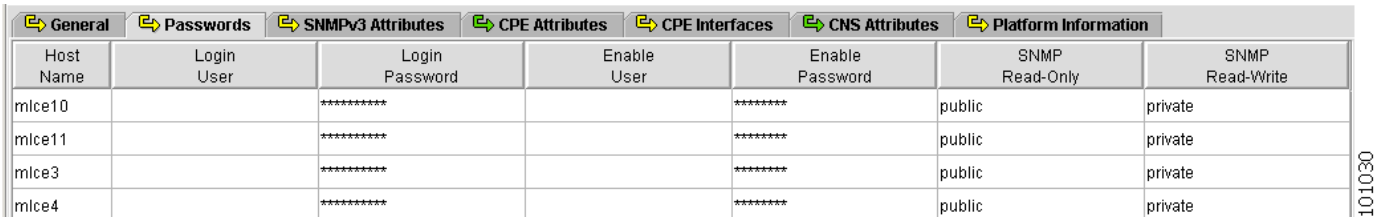
- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
  - Cisco Router
  - Catalyst OS device
  - Terminal server
  - VPN 3000 (**This feature is not supported in this release)**
  - PIX firewall (**This feature is not supported in this release)**
  - IE2100 (Cisco CNS appliance)
- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.
- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.

- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-14 shows an example of the Passwords tab:

Figure 4-14 Customer Spreadsheet - Passwords Tab



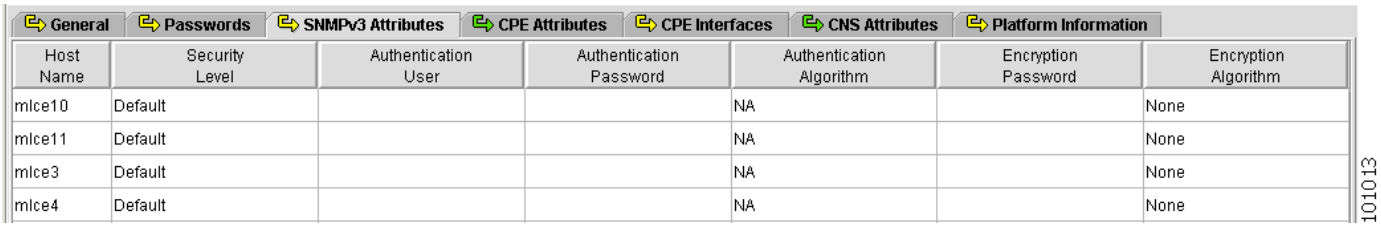
The Passwords tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-15 shows an example of the SNMPv3 Attributes tab:

Figure 4-15 Customer Spreadsheet - SNMPv3 Attributes Tab



Host Name	Security Level	Authentication User	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
mlce10	Default			NA		None
mlce11	Default			NA		None
mlce3	Default			NA		None
mlce4	Default			NA		None

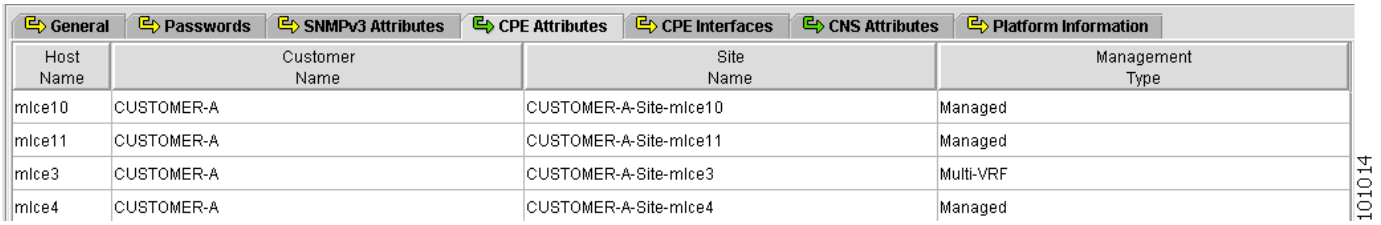
The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

CPE Attributes

Figure 4-16 shows an example of the CPE Attributes tab:

Figure 4-16 Customer Spreadsheet - CPE Attributes Tab



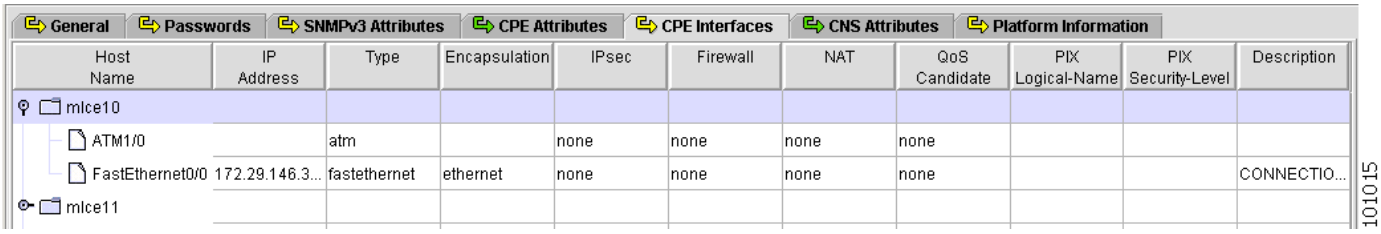
The CPE Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Customer Name** —Lists the names of the customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.
- **Site Name** —Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Management Type**—Choices include: Managed, Unmanaged, Managed - Management LAN, Unmanaged - Management LAN, Directly Connected, Directly Connected Management Host, and Multi-VRF.

CPE Interfaces

Figure 4-17 shows an example of the CPE Interfaces tab:

Figure 4-17 Customer Spreadsheet - CPE Interfaces Tab



The CPE Interfaces tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IP Address**—IP address associated with this interface.
- **Type**—Specifies the type of interface. It is a display-only field.

- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
  - UNKNOWN
  - DEFAULT
  - DOT1Q
  - ETHERNET
  - ISL
  - FRAME_RELAY
  - FRAME_RELAY_IETF
  - HDLS
  - PPP
  - ATM
  - AAL5SNAP
  - AAL0
  - AAL5
  - AAL5MUX
  - AAL5NLPID
  - AAL2
  - ENCAP_QinQ
  - GRE
- **IPsec—This feature is not supported in this release**
  View or edit (mark) interface settings for IPsec. Choices include:
  - None
  - Public

    Interface to the public network (internet). All traffic is encrypted.
  - Private

    Interface to the private network (internal LAN). All traffic is not encrypted.
- **Firewall—This feature is not supported in this release**
  View or edit (mark) interface settings for Firewall. If Device Type is VPN 3000, Firewall is not available. Choices include:
  - Inside

    Highest security interface.
  - Outside

    Lowest security interface.
  - DMZ 1, ..., DMZ N

    The Demilitarized Zone services to both inside and outside interfaces.

- **NAT—This feature is not supported in this release**
  View or edit (mark) interface settings for NAT. If Device Type is PIX firewall or VPN 3000, NAT is not available. Choices include:
  - None
  - Inside

    Highest security interface.
  - Outside

    Lowest security interface.
- **QoS Candidate**—View or edit (mark) interface settings for QoS. If Device Type is VPN 3000 (**This feature is not supported in this release)**, QoS is not available. Choices include:
  - None
  - Marking Rate Limit

    This setting marks the Customer LAN facing interface with the **set** and **police** commands.
  - Endpoint

    This setting marks the PE facing interface on the CE device and the CE facing interface on the PE device.

    On the PE side, all QoS commands go on this interface.

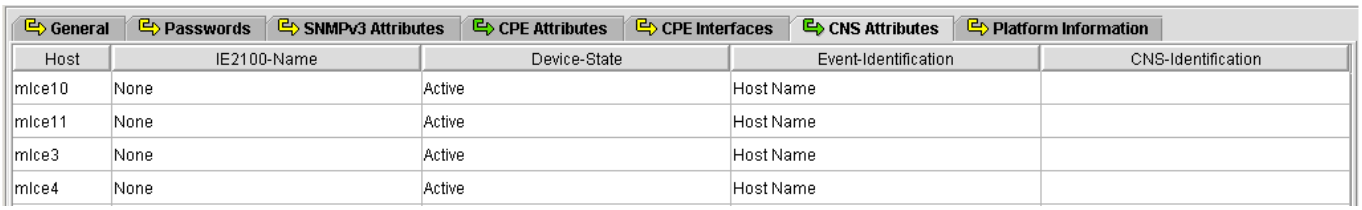
    On the CE side, all QoS commands, including the **set** and **police** commands, go on this interface if no interface on the CE device is identified as the Marking Rate Limit interface.

    If one or more interfaces have been identified as Marking Rate Limit interfaces, then all QoS commands except the **set** and **police** commands go on this interface.
- **PIX Logical-Name**—Logical name of this interface. This field is displayed only. Field is populated by a collection/import of config file.
- **PIX Security-Level**—Security level of this interface. This field is display-only. Field is populated by importing a configuration file.
- **Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.

CNS Attributes

Figure 4-18 shows an example of the CNS Attributes tab:

Figure 4-18 Customer Spreadsheet - CNS Attributes Tab



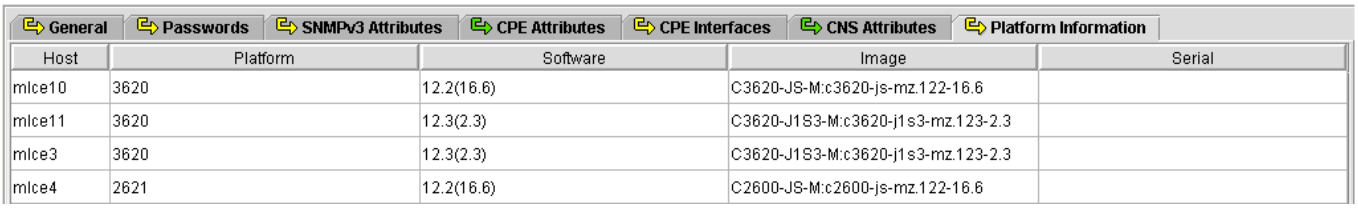
The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS IE2100 appliance must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing Cisco CNS IE2100 appliance names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-19 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-19 Customer Spreadsheet - Platform Information Tab



The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters.

Device Group Spreadsheet

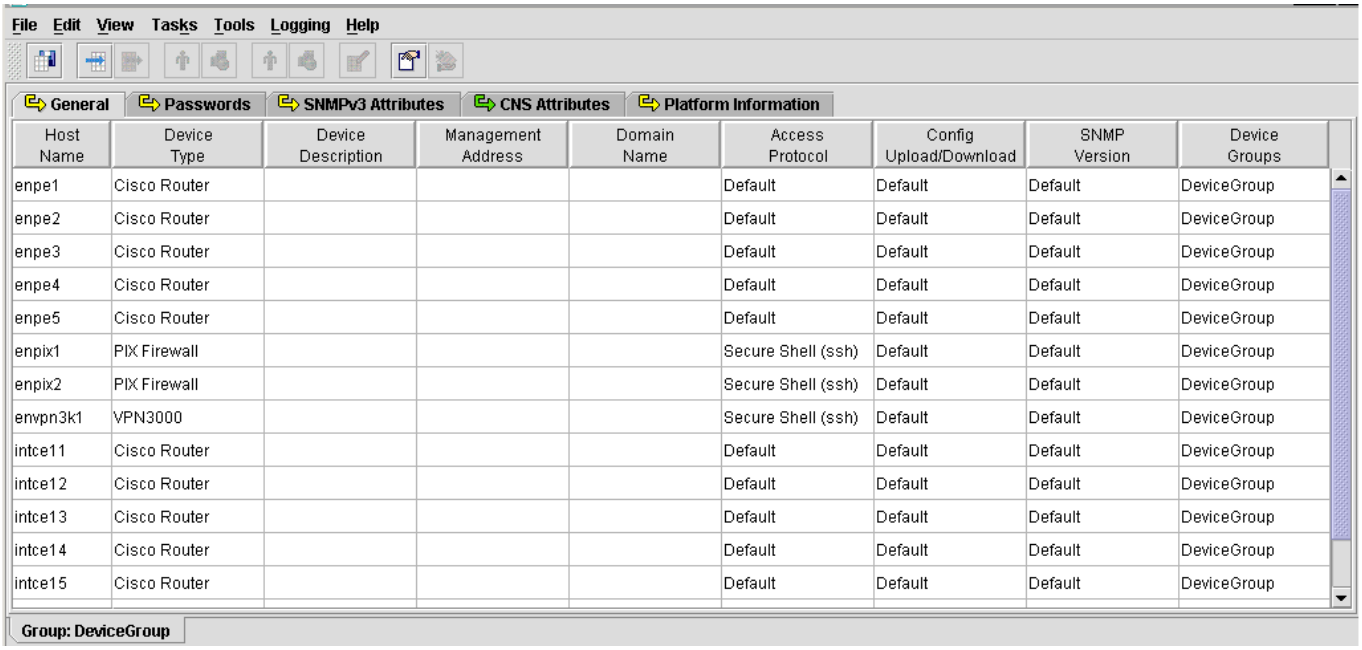
The Device Group spreadsheets contain the following tabs:

- General, page 4-30
- Passwords, page 4-31
- SNMPv3 Attributes, page 4-32

General

Figure 4-20 shows an example of the General tab:

Figure 4-20 Device Group Spreadsheet - General Tab



The General tab contains the following columns:

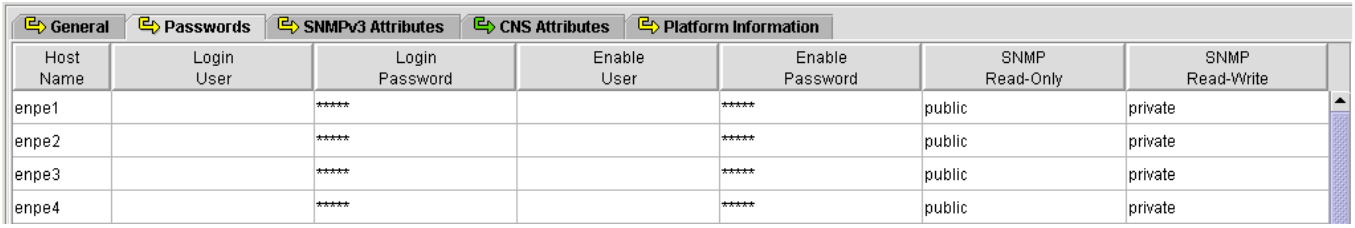
- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
  - Cisco IOS router
  - Catalyst OS device
  - Terminal server
  - VPN 3000 (**This feature is not supported in this release)**
  - PIX firewall (**This feature is not supported in this release)**
  - IE2100 (Cisco CNS appliance)
- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.

- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-21 shows an example of the Passwords tab:

Figure 4-21 Device Group Spreadsheet - Passwords Tab



The Passwords tab contains the following columns:

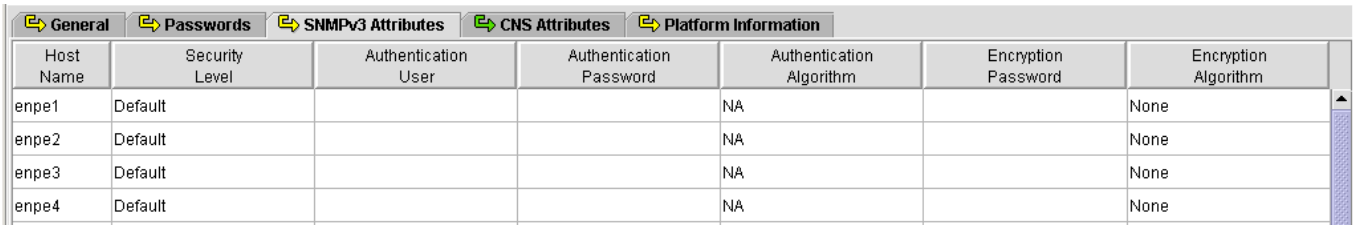
- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.

- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-22 shows an example of the SNMPv3 Attributes tab:

Figure 4-22 Device Group Spreadsheet - SNMPv3 Attributes Tab



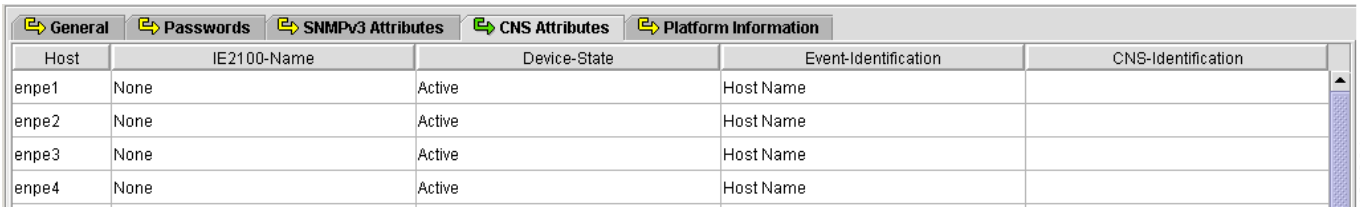
The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

CNS Attributes

Figure 4-23 shows an example of the CNS Attributes tab:

Figure 4-23 Device Group Spreadsheet - CNS Attributes Tab



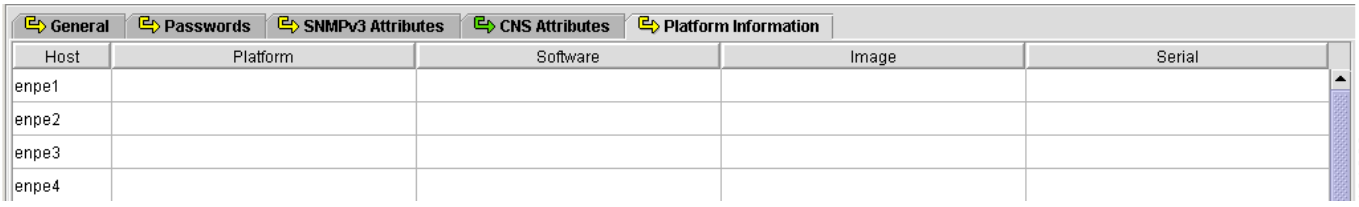
The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS IE2100 appliance must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing Cisco CNS IE2100 appliance names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-24 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-24 Device Group Spreadsheet - Platform Information Tab



The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.

- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters.

Inventory Manager GUI Reference

This section describes the Inventory Manager GUI. It is organized by the external design of the GUI: what you see when you look at the windows, menus, and options. It is intended for new users who want to get started with Inventory Manager, and for experienced users who need a reference for the GUI workflow.

To access the Inventory Manager GUI, follow these steps:

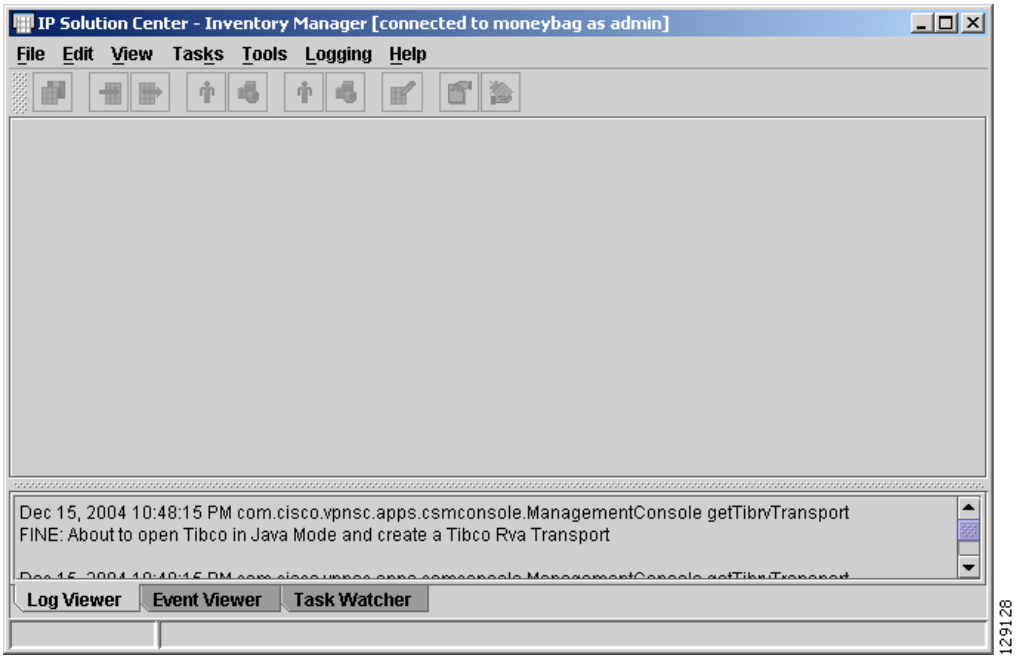
Step 1 Log in to ISC.

Step 2 Choose **Service Inventory** > **Inventory and Connection Manager** > **Inventory Manager**.

Step 3 Click the Inventory Manager icon.

After initializing Java Web Start, Inventory Manager appears, as shown in Figure 4-25.

Figure 4-25 Inventory Manager



You now have access to the Inventory Manager Task Bar.

This section contains a section for each Inventory Manager menu:

- Viewer and Task Watcher Tabs, page 4-35

Viewer and Task Watcher Tabs

The tabs at the bottom of the main Inventory Manager GUI in Figure 4-4 are used to monitor events and perform troubleshooting.

They serve the following purpose:

- Log Viewer—Displays Log messages.
- Event Viewer—Displays Inventory Manager and TIBCO events.
- Task Watcher—Can be used to monitor tasks used by Inventory Manager.

File Menu

The File menu has the following options:

New

From the Inventory Manager main menu, New is the first option under the File menu on the Task Bar. The New option has the following options:

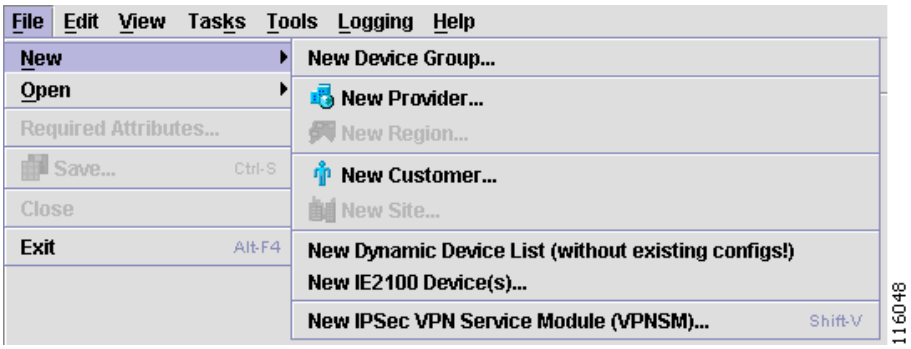
Additionally, Open, page 4-52, is an option from alternate tabs.

New Device Group

To create a new Device Group, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > New > New Device Group**, as shown in Figure 4-26.

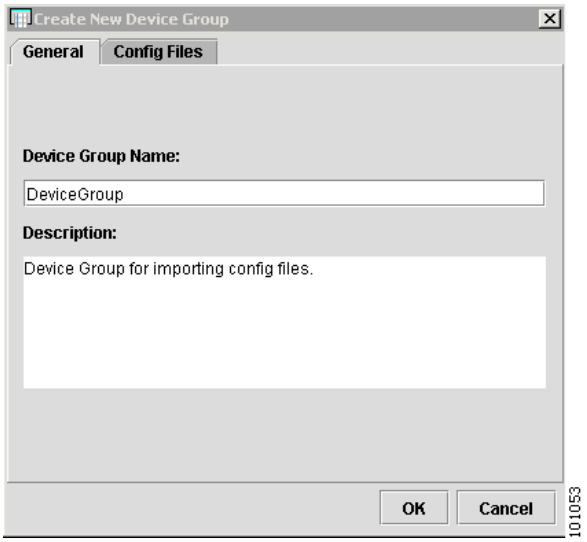
Figure 4-26 Choose New Device Group



The New Device Group window appears, as shown in Figure 4-27.

Note You have the option to add configuration files to a Device Group using the New Device Group window, by choosing the Config Files tab.

Figure 4-27 Create New Device Group



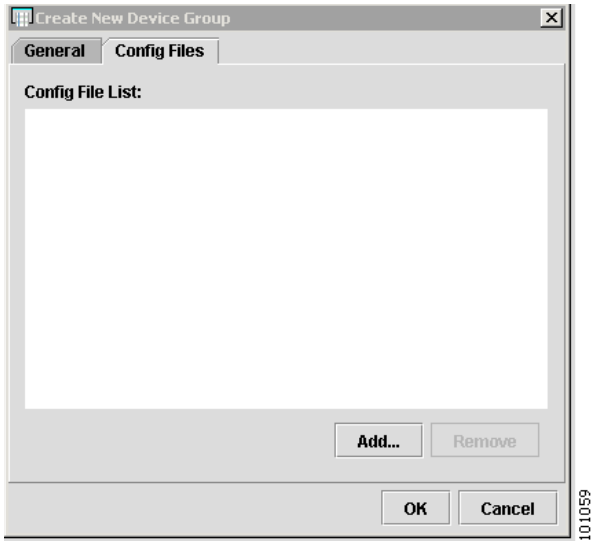
Step 2 **Device Group Name**: Enter the name of the device group.

Step 3 **Description**: Enter a description.

Step 4 Click the **Config Files** tab.

The **Config Files** tab appears, as shown in Figure 4-28.

Figure 4-28 Config Files Tab

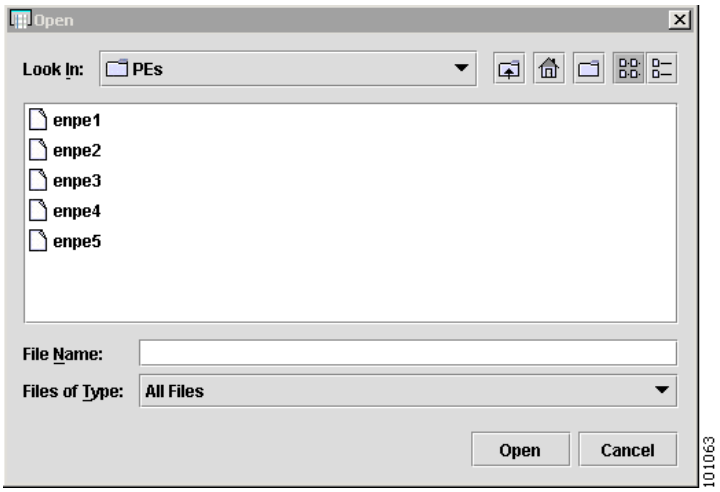


Step 5 Click **Add** to search for your configuration files.

Step 6 Navigate to your configuration file folder, select it, and click **OK**.

The Open Config Files window appears, as shown in Figure 4-29.

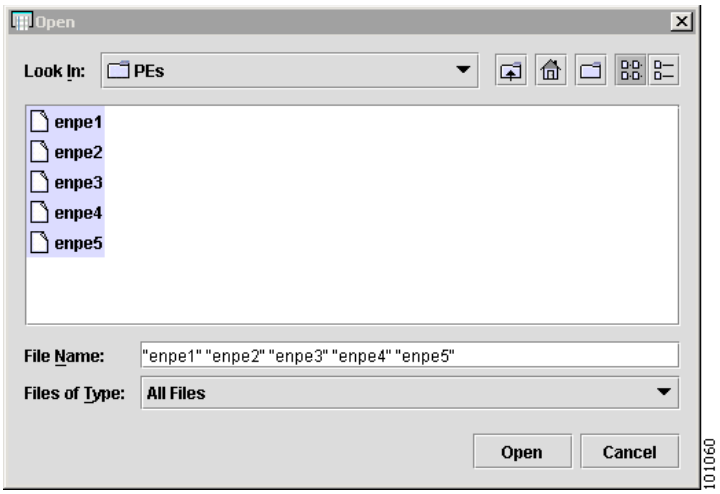
Figure 4-29 Open Config Files



Step 7 Use Ctrl+click to select the files.

The files appear highlighted, as shown in Figure 4-30.

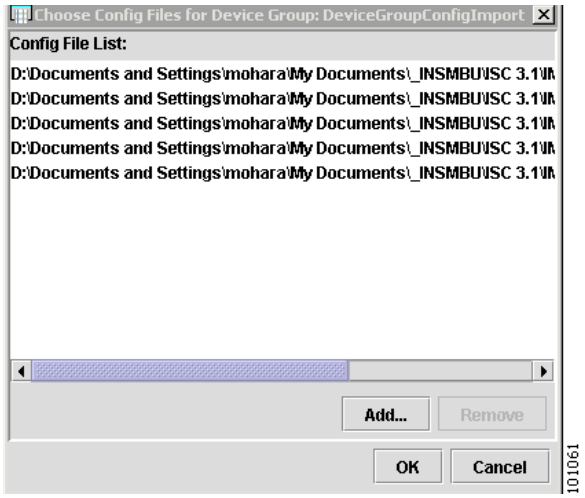
Figure 4-30 Highlighted Config Files



Step 8 Click **Open.**

The Config File List appears, as shown in Figure 4-31.

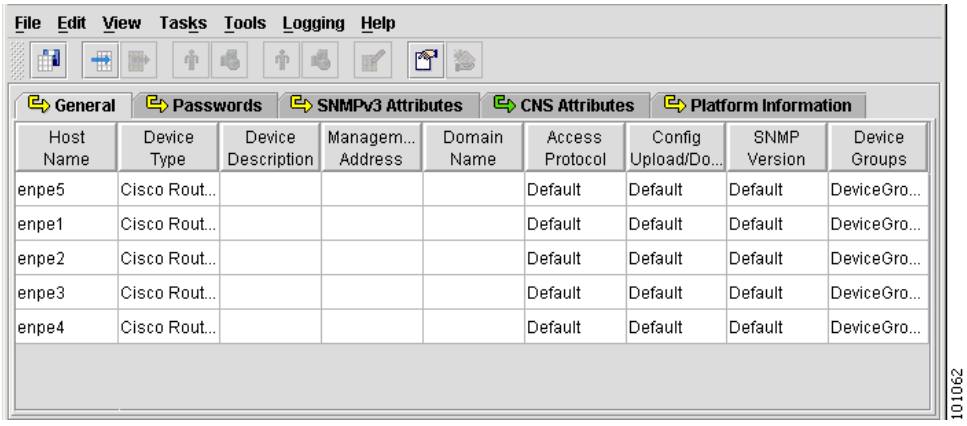
Figure 4-31 Config Files List



Step 9 Click **OK**.

The Device Group spreadsheet appears, as shown in Figure 4-32.

Figure 4-32 Device Group Spreadsheet



When you create devices this way, no CPEs or PEs are created. To create CPEs or PEs, devices must be associated with a Customer, Site, Provider, or Region.

You have created a new Device Group and added the configuration files. The Spreadsheet Editor enables you to specify attributes for the devices. The following examples show how to edit or specify fields in the device workbook.

Cell Editing Examples

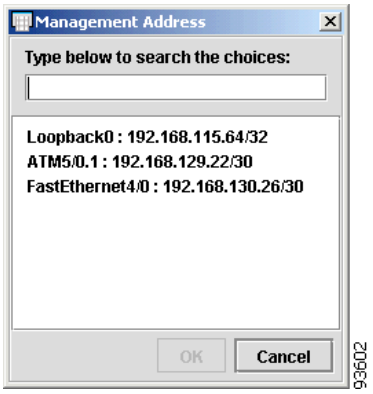
To enter the Domain Name, click the cell. The Domain Name dialog box appears, as shown in Figure 4-33.

Figure 4-33 Domain Name

Enter the Domain Name and click **OK**.

To enter the Management Address, click the cell. The Management Address dialog box appears, as shown in Figure 4-34.

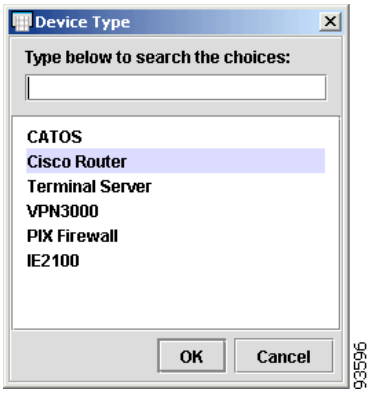
Figure 4-34 Management Address



Enter the Management Address, or select one from the list, and click **OK**.

To enter the Device Type, click the cell. The Device Type dialog box appears, as shown in Figure 4-35.

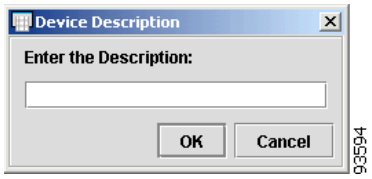
Figure 4-35 Device Type



Enter the Device Type, or select one from the list, and click **OK**.

To enter the Device Description, click the cell. The Device Description dialog box appears, as shown in Figure 4-36.

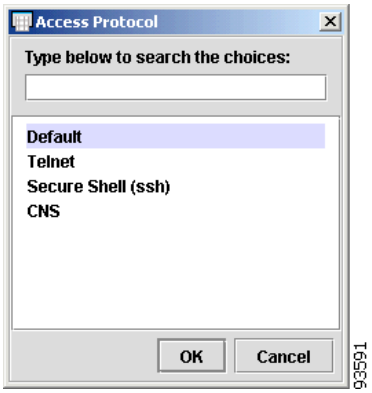
Figure 4-36 Device Description



Enter the Device Description and click **OK.**

To enter the Access Protocol, click the cell. The Access Protocol dialog box appears, as shown in Figure 4-37.

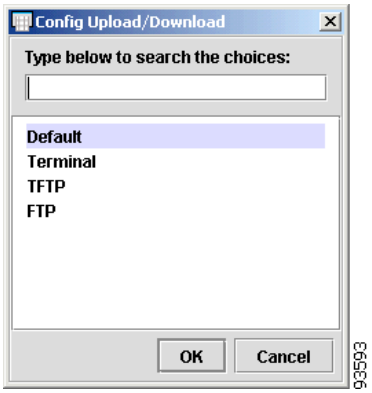
Figure 4-37 Access Protocol



Enter the Access Protocol, or select one from the list, and click **OK.**

To enter the Config Upload/Download, click the cell. The Config Upload/Download dialog box appears, as shown in Figure 4-38.

Figure 4-38 Config Upload/Download



Enter the Config Upload/Download, or select one from the list, and click **OK.**

To enter the Login User, click the cell. The Login User dialog box appears, as shown in Figure 4-39.

Figure 4-39 Login User

Enter the Login User and click **OK.**

To enter the Login Password, click the cell. The Login Password dialog box appears, as shown in Figure 4-40.

Figure 4-40 Login Password

Enter the Login Password in both dialog boxes and click **OK.**

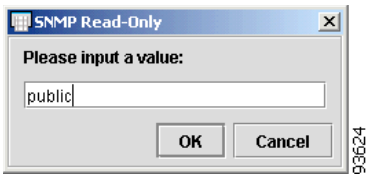
To enter the Enable Password, click the cell. The Enable Password dialog box appears, as shown in Figure 4-41.

Figure 4-41 Enable Password

Enter the Enable Password in both dialog boxes and click **OK.**

To enter the SNMP Read-Only, click the cell. The SNMP Read-Only dialog box appears, as shown in Figure 4-42.

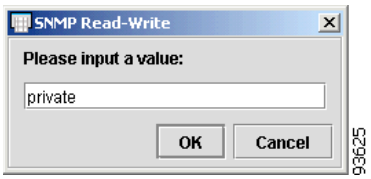
Figure 4-42 SNMP Read-Only



Enter the SNMP Read-Only value, or select one from the list, and click **OK.**

To enter the SNMP Read-Write value, click the cell. The SNMP Read-Write dialog box appears, as shown in Figure 4-43.

Figure 4-43 SNMP Read-Write



Enter the SNMP Read-Write value, or select one from the list, and click **OK.**

Step 10 To finish, choose **File > Save**.

New Provider

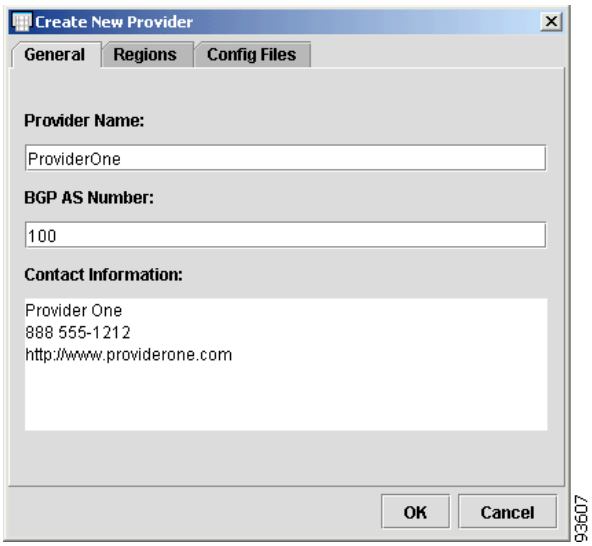
To create a new Provider, follow these steps:

Note You have the option to add regions or configuration files to a Provider using the **New Provider** window, by choosing the appropriate tab. For an example of how to add regions, see the "New Region" section on page 4-46.

Step 1 From the Inventory Manager menu, choose **File > New > New Provider**.

The New Provider window appears, as shown in Figure 4-44.

Figure 4-44 New Provider



Step 2 **Provider Name**: Enter the name of the Provider.

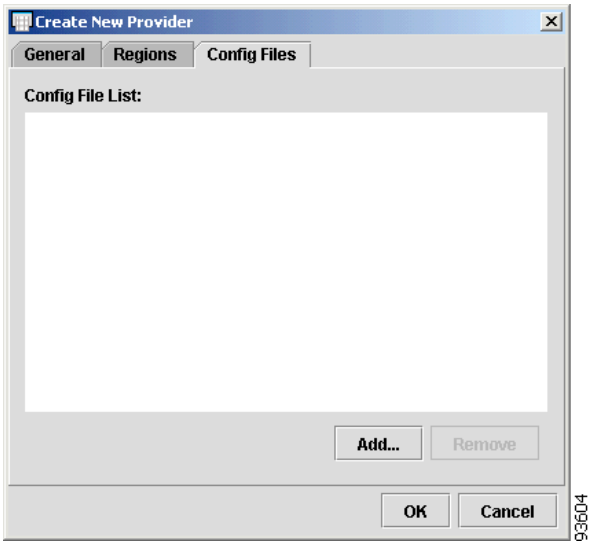
Step 3 **BGP AS Number**: Enter the BGP Autonomous System Number.

Step 4 **Contact Information**: Enter the contact information.

Step 5 Click the **Config Files** tab.

The **Config Files** tab appears, as shown in Figure 4-45.

Figure 4-45 Config Files Tab



Step 6 Click **Add** to search for configuration files.

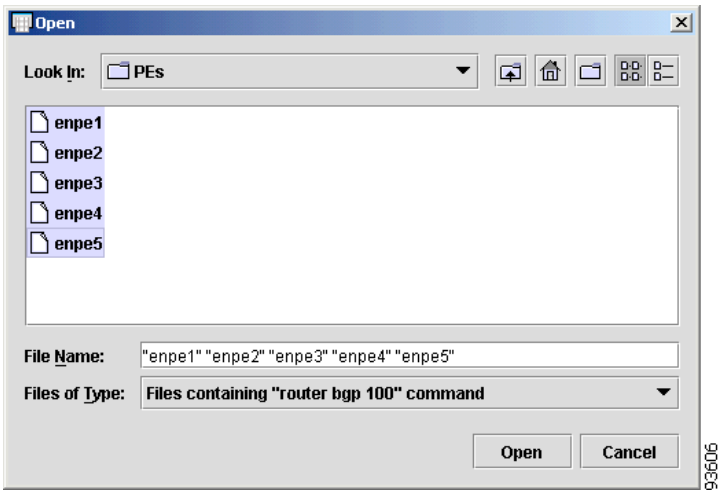
Step 7 Navigate to your configuration file folder, select it, and click **OK**.

The Open Config Files window appears.

Step 8 Use Ctrl+click to select the files.

The files appear highlighted, as shown in Figure 4-46.

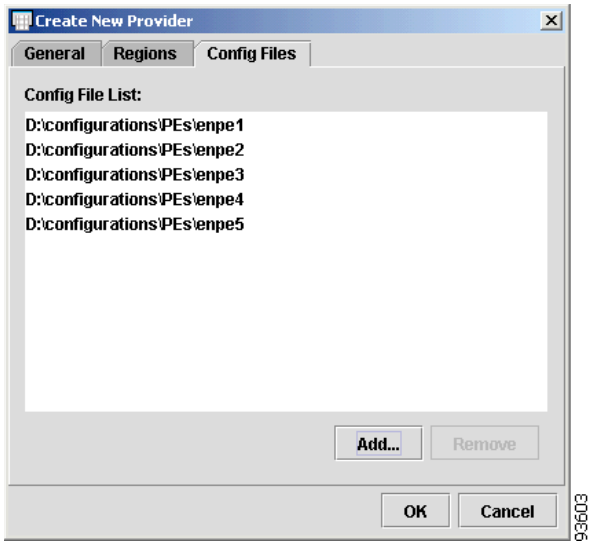
Figure 4-46 Highlighted Config Files



Step 9 Click **Open.**

The Config File List appears, as shown in Figure 4-47.

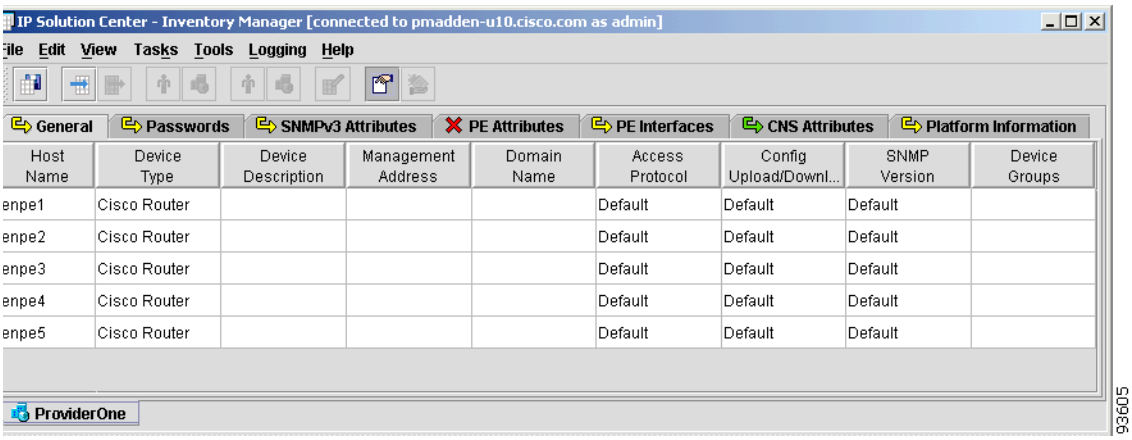
Figure 4-47 Config Files List



Step 10 Click **OK.**

The New Provider spreadsheet appears, as shown in Figure 4-48.

Figure 4-48 New Provider Spreadsheet



You have created a new Provider and added the configuration files. The Spreadsheet Editor enables you to specify attributes for the devices. When you create devices this way, PEs are created.

To finish, choose **File > Save**.

New Region

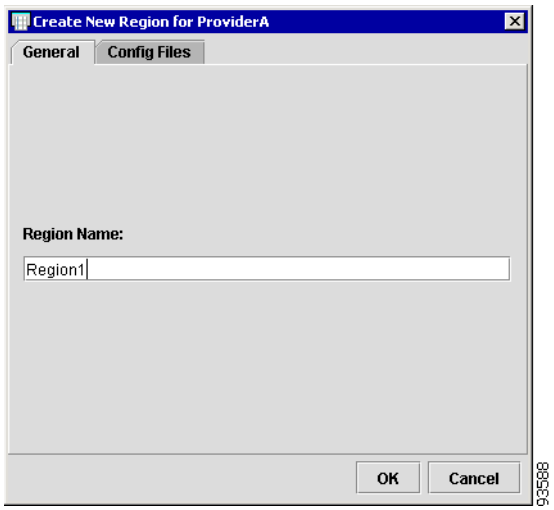
To create a new Region, follow these steps:

Note You have the option to add configuration files to a New Region using the New Region for Provider window, by choosing the Config Files tab.

Step 1 From the Inventory Manager menu, choose **File > New > New Region**.

The New Region for Provider window appears, as shown in Figure 4-49.

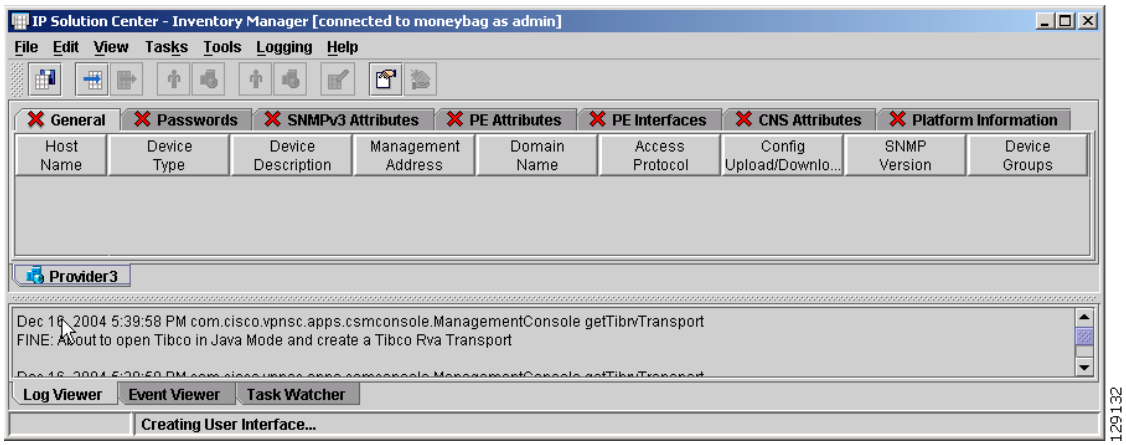
Figure 4-49 New Region for Provider



Step 2 **Region Name**: Enter the name of the Region and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Provider, as shown in Figure 4-50.

Figure 4-50 New Provider Spreadsheet



For a description of the tabs and definition of the fields in the Provider, Region, and PE spreadsheets, see the "Spreadsheet Features" section on page 4-13.

New Customer

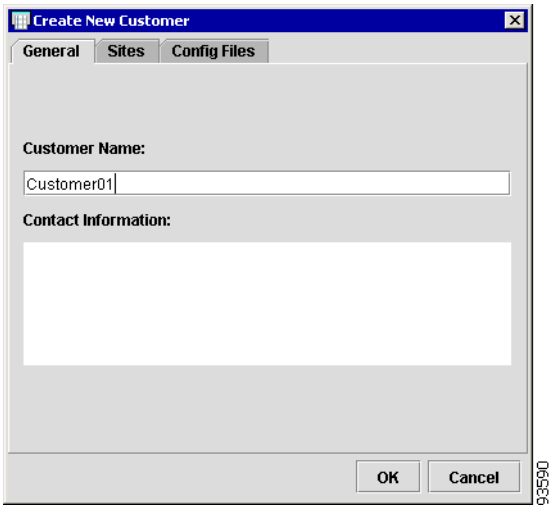
To create a new Customer, follow these steps:

Note You have the option to add sites or configuration files to a Customer using the New Customer window, by choosing the appropriate tab. For an example of how to add sites, see the "New Site" section on page 4-49.

Step 1 From the Inventory Manager menu, choose **File** > **New** > **Customer**.

The New Customer window appears, as shown in Figure 4-51.

Figure 4-51 New Customer

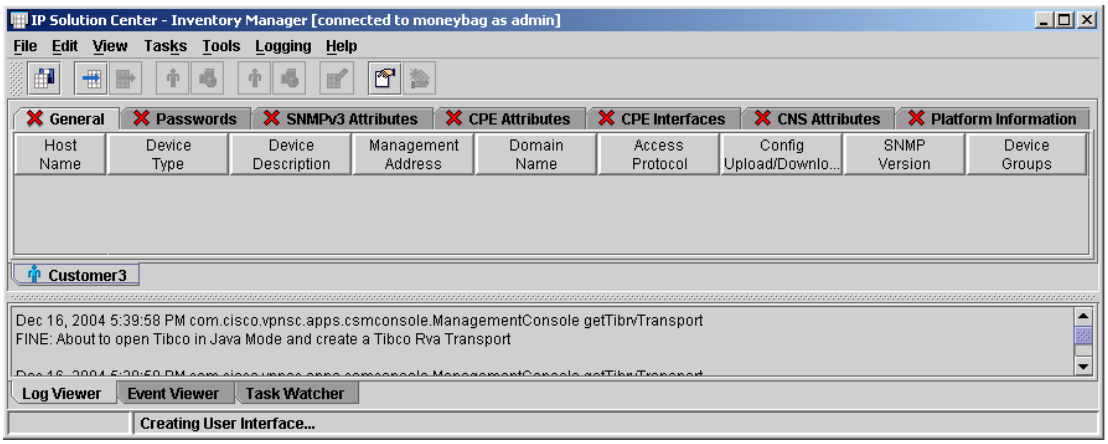


Step 2 **Customer Name**: Enter the name of the Customer.

Step 3 **Contact Information**: Enter contact information and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Customer, as shown in Figure 4-52.

Figure 4-52 New Customer Spreadsheet



You now have access to the Customer spreadsheet.

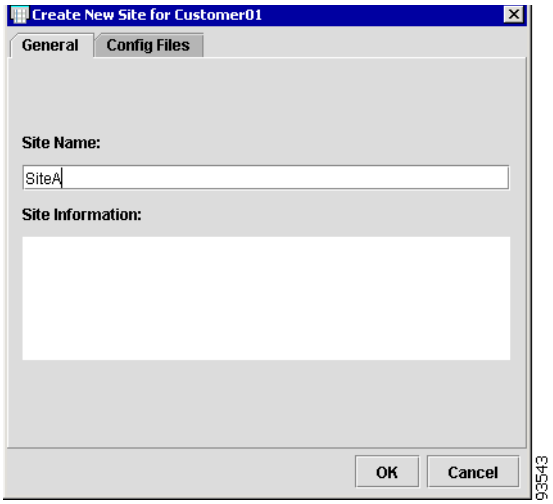
New Site

To create a new Site, follow these steps:

Note You have the option to add configuration files to a New Site using the New Site window, by choosing the Config Files tab.

Step 1 From the Inventory Manager menu, choose **File > New > Site**, as shown in Figure 4-53.

Figure 4-53 New Site

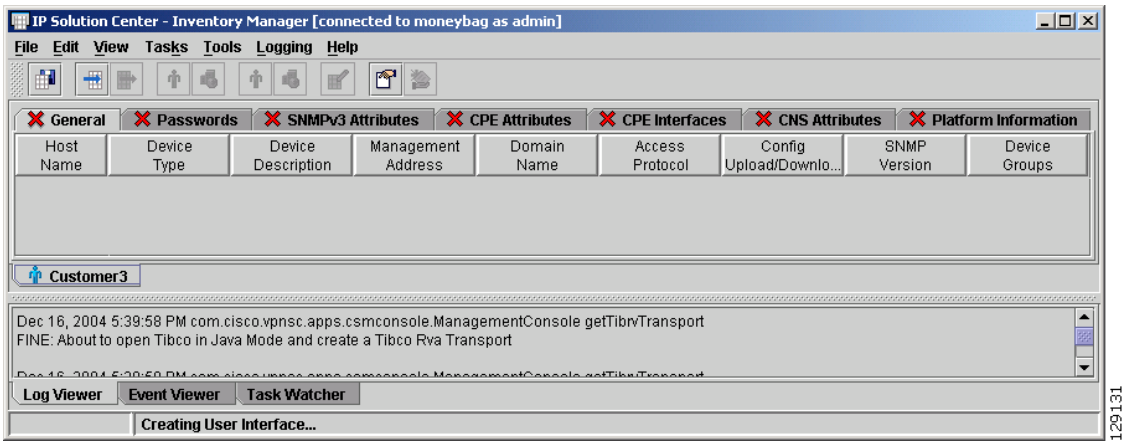


Step 2 **Site Name**: Enter the name of the Site.

Step 3 **Site Information**: Enter contact information and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Customer, as shown in Figure 4-54.

Figure 4-54 New Customer Spreadsheet



You now have access to the Customer spreadsheet.

New Dynamic Device List (without existing configs)

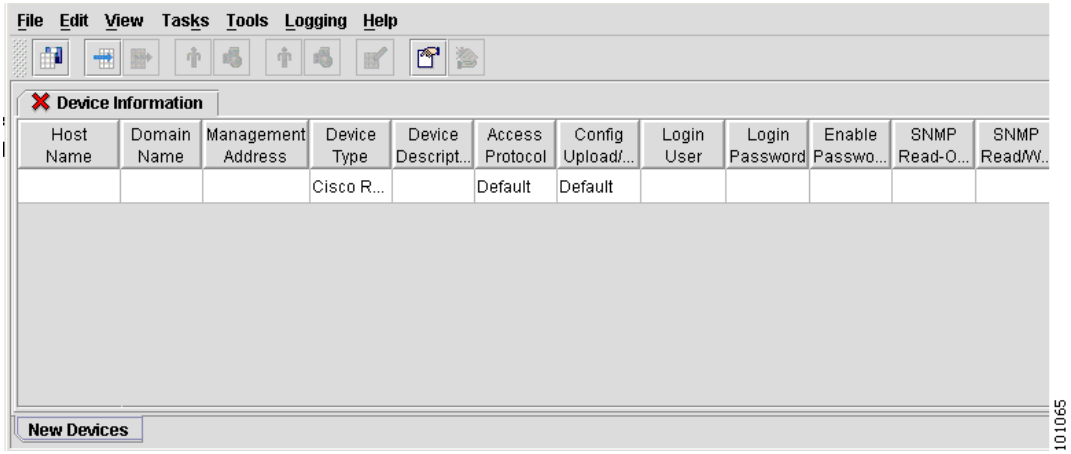
If you do not have existing configuration files, you can discover devices on your network, using the Dynamic Device List. The devices can be associated with logical CPE and PE devices at a later time.

To create a new Device List, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > New > New Dynamic Device List (without existing configs)**.

A new Device Spreadsheet appears, as shown in Figure 4-55.

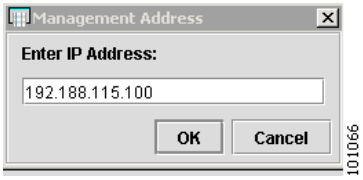
Figure 4-55 New Device Spreadsheet



Step 2 To discover devices on your network, click the **Management Address** cell.

A Management Address window appears, as shown in Figure 4-56.

Figure 4-56 Enter IP Address



Step 3 Enter the IP address and click **OK**.

A new Device Spreadsheet appears.

Step 4 Start the Device Discovery process.

For an example of how to start the device discovery process, see the "Start Auto Discovery" section on page 4-91.

New IE2100 Device List

ISC supports the Cisco CNS IE2100 appliance Device Access Protocol for communication with any Cisco IOS device. Inventory Manager supports the same functionality for the Cisco CNS IE2100 appliance as the other devices described in the chapter.

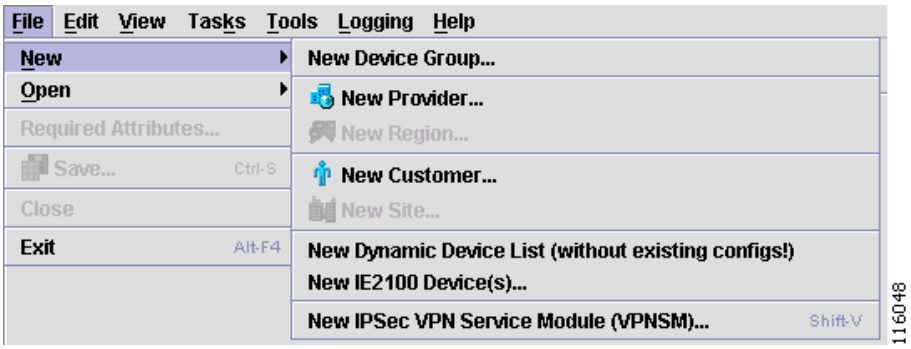
New IPsec VPN Service Module (VPNSM)

This feature is not supported in this release

To create a new VPNSM Device, follow these steps:

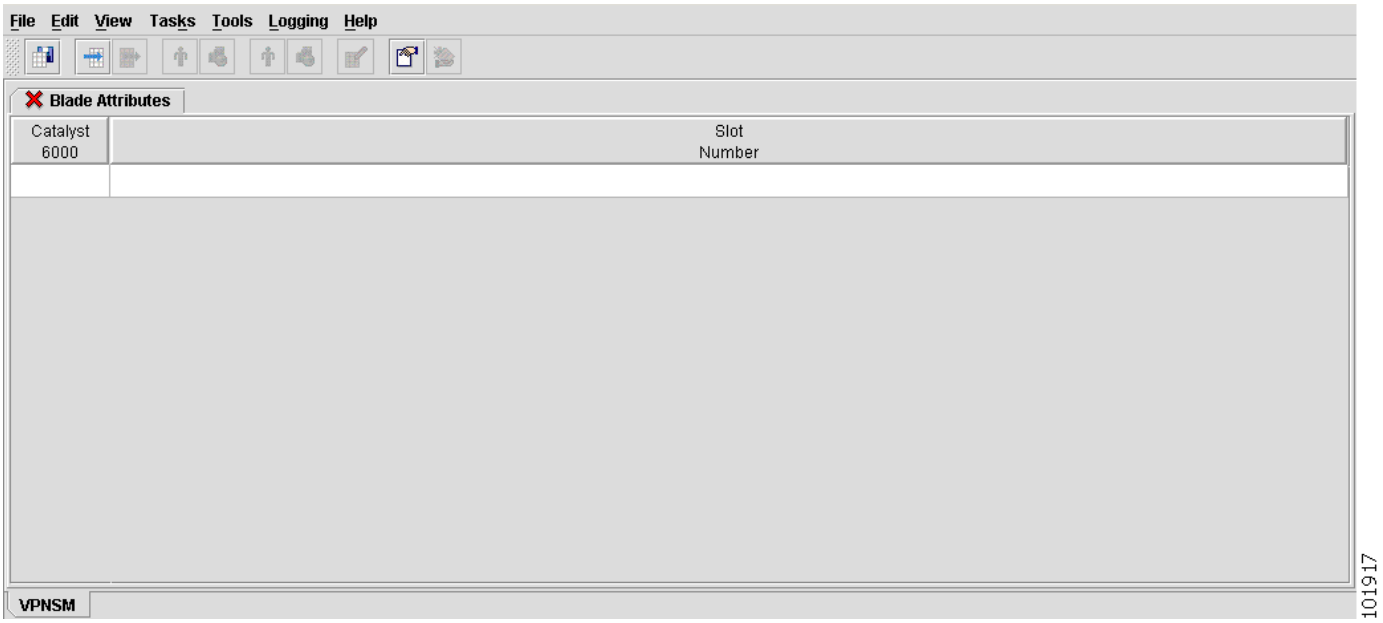
Step 1 From the Inventory Manager menu, choose **File > New > New IPsec VPN Service Module (VPNSM)**, as shown in Figure 4-57.

Figure 4-57 Choose New IPsec VPN Service Module



The New IPsec VPN Service Module spreadsheet appears, as shown in Figure 4-58.

Figure 4-58 Create New IPsec VPN Service Module



Step 2 Click the **Catalyst 6500** cell.

The **Catalyst 6500** window appears (not shown).

Step 3 Choose a Catalyst 6500 Device.

Step 4 Click the **Slot Number** cell and then enter a *slot number*.

Step 5 Choose **File** > **Save** to create a VPNSM in the Repository.

Open

From the Inventory Manager main menu, shown in Figure 4-26 on page 4-36, Open is the second option under the File menu on the Task Bar. The Open option has the following options:

- Open Devices, page 4-53
- Open Discovery Seed File, page 4-54
- Open Device Group, page 4-56
- Open Provider, page 4-57
- Open Region, page 4-58
- Open Customer, page 4-59
- Open Site, page 4-60
- Open IPsec VPN Service Modules, page 4-61

Open Devices

This section describes how to open a Device with Inventory Manager. To open a Device, follow these steps:

Step 1 From the **Inventory Manager** task bar (not shown), choose **File > Open > Open Devices.**

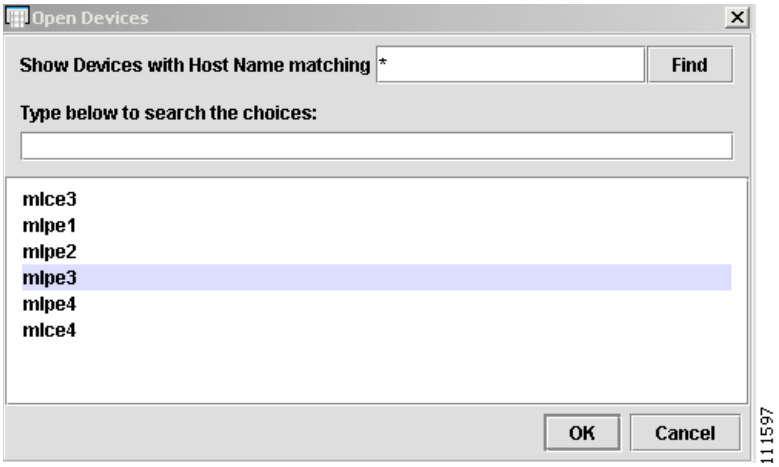
The **Open Devices** window appears, as shown in Figure 4-59.

Figure 4-59 Open Devices

Step 2 Click **Find**.

The **Open Devices** window now displays available devices, as shown in Figure 4-60.

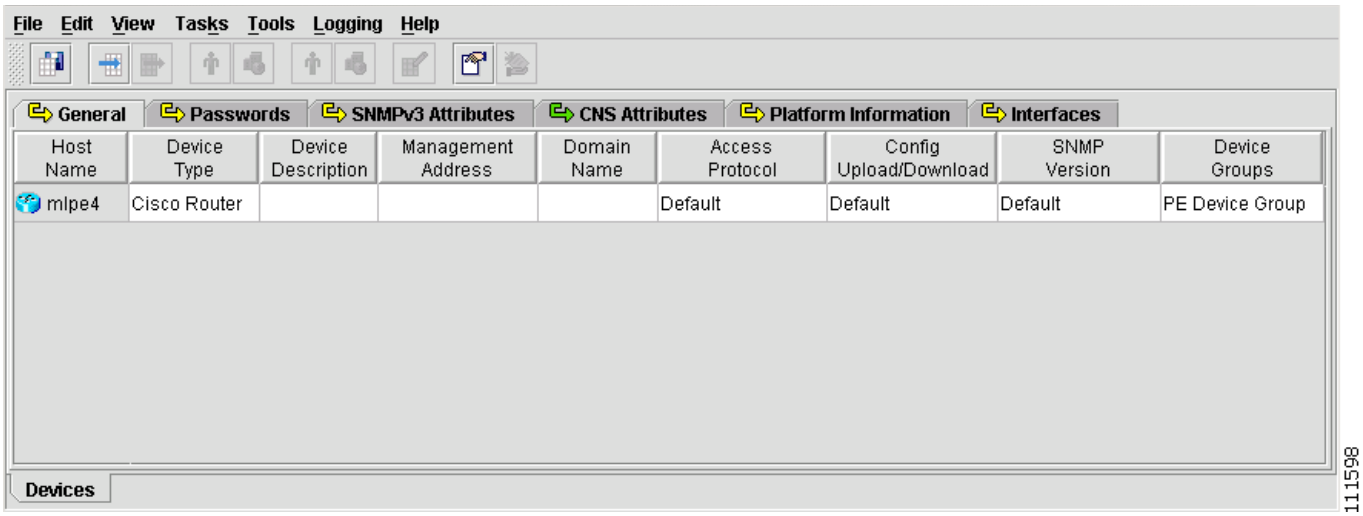
Figure 4-60 Open Devices Found



Step 3 Choose a Device and click **OK**. (**mlpe3**)

The **Devices** spreadsheet appears, as shown in Figure 4-61.

Figure 4-61 Devices Spreadsheet



Open Discovery Seed File

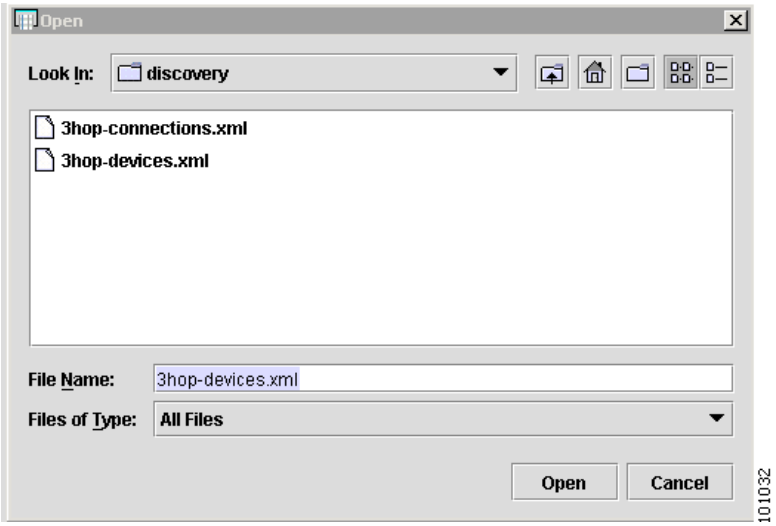
Note A discovery seed file is an XML representation of the devices found during Auto Discovery.

To open a discovery seed file, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Discovery Seed File**.

The Open window appears, as shown in Figure 4-62.

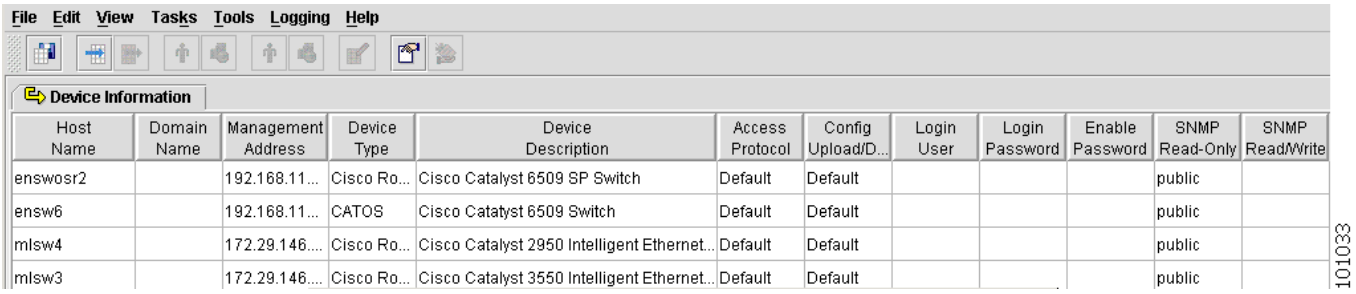
Figure 4-62 Open Discovery Seed File



Step 2 Select the devices file, which you saved after discovering your devices, and choose **Open**.

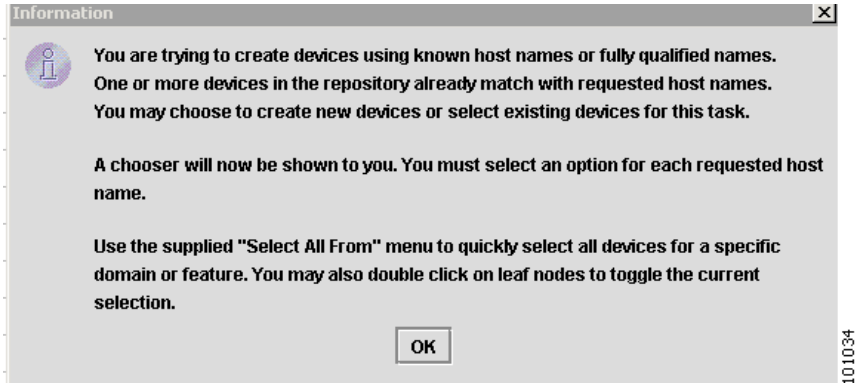
The Device Information spreadsheet appears, as shown in Figure 4-63.

Figure 4-63 Device Information



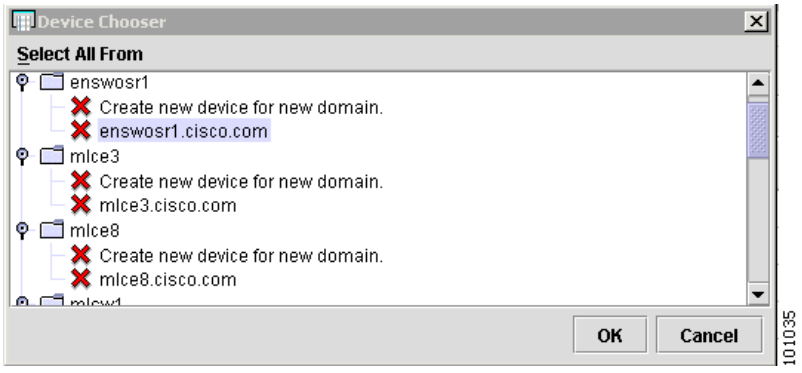
If a device has already been created in the Repository, a message window appears, as shown in Figure 4-64.

Figure 4-64 Device in the Repository



Step 3 Click **OK** and the Device Chooser window appears, as shown in Figure 4-65.

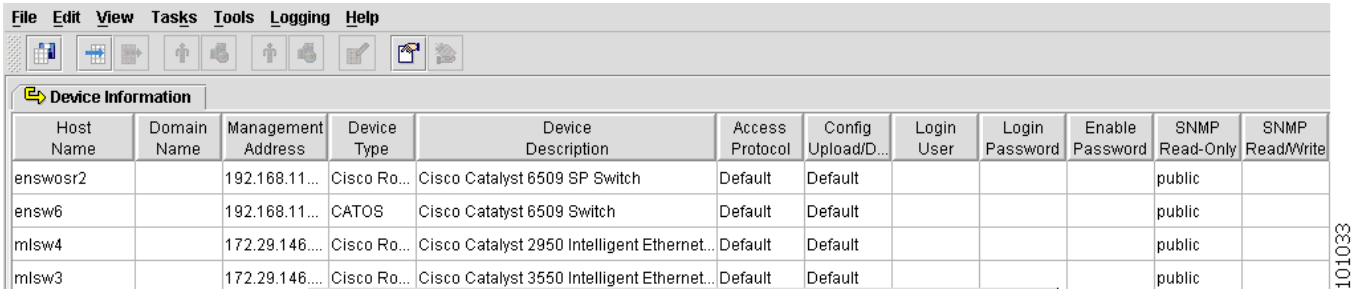
Figure 4-65 Device Chooser



Step 4 Click the device name and domain to save the device as is. To create a new domain for the device and save it, **click Create new device for new domain**.

The Device Information spreadsheet appears, as shown in Figure 4-66.

Figure 4-66 Device Information



Now you can edit your devices and collect the latest configuration files.

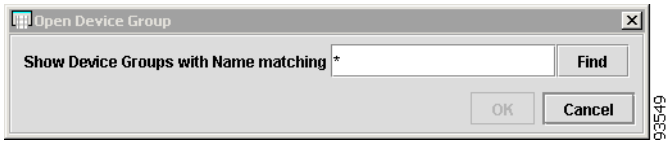
Open Device Group

To open an existing Device Group, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Device Group**.

A search dialog appears, as shown in Figure 4-67.

Figure 4-67 Open Device Group

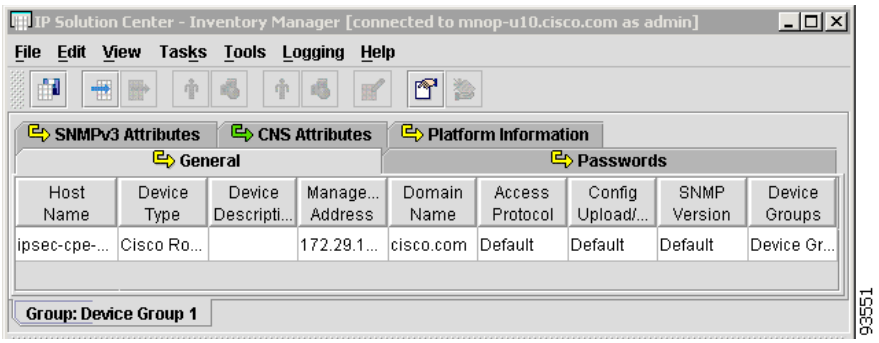


Step 2 Click the **Find** button to download all Device Groups, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available device names.

Step 3 Select the Device Group and click **OK**.

A Device Spreadsheet Editor appears, where you can edit device parameters such as passwords and SNMP information, as shown in Figure 4-68.

Figure 4-68 Device Spreadsheet Editor



You now have access to the Device spreadsheet.

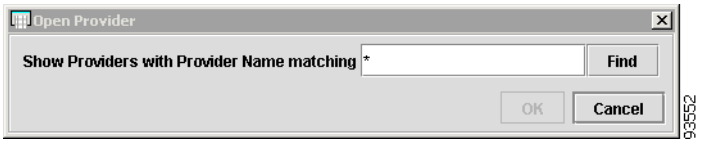
Open Provider

To open an existing Provider, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Provider**.

A search dialog appears, as shown in Figure 4-69.

Figure 4-69 Open Provider



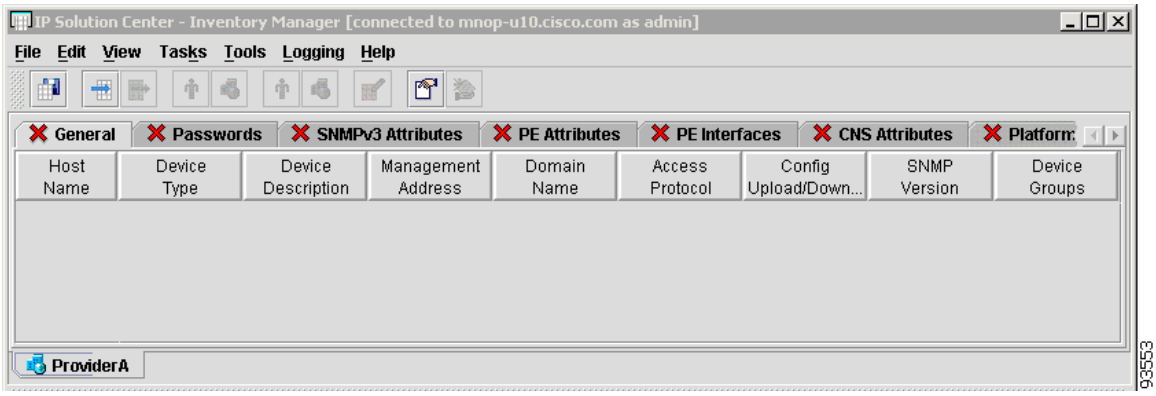
Step 2 Click the **Find** button to download all Providers, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available Providers.

Step 3 Select the Provider and choose **OK**.

A PE Spreadsheet Editor appears with all Regions and PEs for that Provider listed in the Spreadsheet Editor, as shown in Figure 4-70.

Note In the following example, the Spreadsheet Editor is empty.

Figure 4-70 Provider Spreadsheet Editor



You now have access to the Provider spreadsheet.

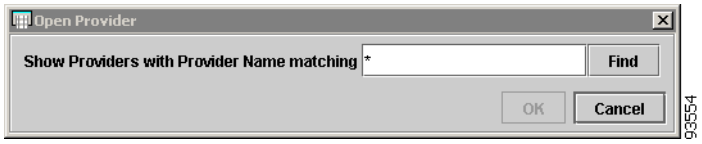
Open Region

To open an existing Region, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Region**.

A search dialog appears, as shown in Figure 4-71.

Figure 4-71 Open Provider



Step 2 Click the **Find** button to download all Providers, enter the name of the provider to search for the one you want, or enter a partial name with an asterisk to get a list of available Providers.

Step 3 Select the Provider and choose **OK**.

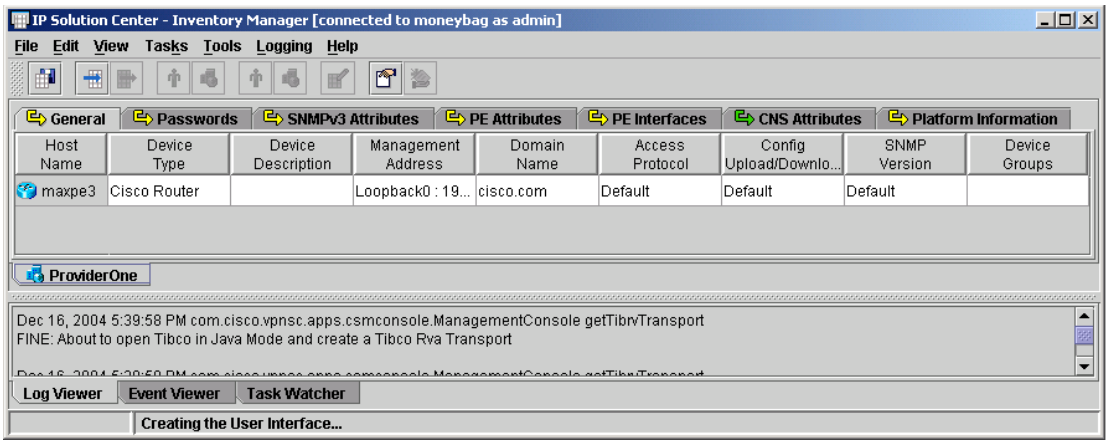
Step 4 Choose from the list of existing Regions, as shown in Figure 4-72.

You can also create a Region for the Provider by choosing **Create Region**.

Figure 4-72 Open Region

A PE Spreadsheet Editor appears with all PEs for the Region listed in the Spreadsheet Editor, as shown in Figure 4-73.

Figure 4-73 PE Spreadsheet Editor



You now have access to the Provider spreadsheet.

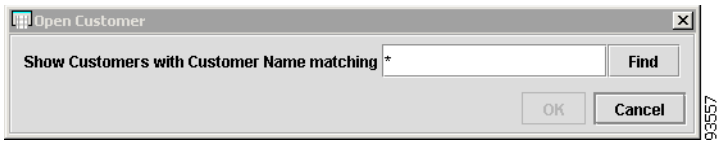
Open Customer

To open an existing Customer, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Customer**.

A search dialog appears, as shown in Figure 4-74.

Figure 4-74 Open Customer

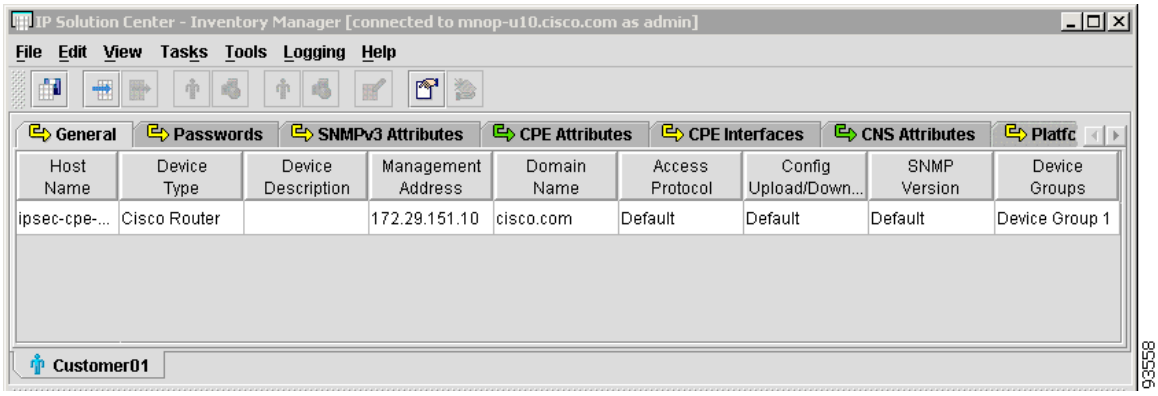


Step 2 Click the **Find** button to download all Customers, enter the name of the Customer to search for the one you want, or enter a partial name with an asterisk to get a list of available Customers.

Step 3 Select the Customer and choose **OK**.

A CPE Spreadsheet Editor appears with all Sites and CPE for the Customer listed in the Spreadsheet Editor, as shown in Figure 4-75.

Figure 4-75 CPE Spreadsheet Editor



You now have access to the Customer spreadsheet.

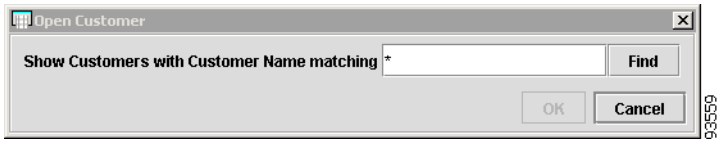
Open Site

To open an existing Site, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Site**.

A search dialog appears, as shown in Figure 4-76.

Figure 4-76 Open Customer

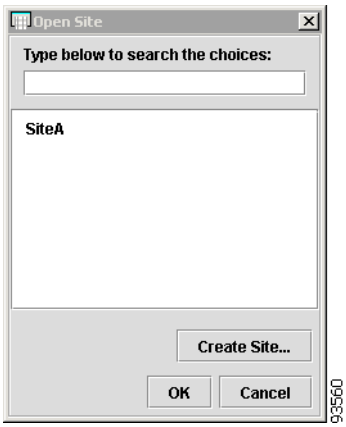


Step 2 Click the **Find** button to download all Customers, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available Customers. You must specify a Customer first.

Step 3 Select the Customer and choose **OK**.

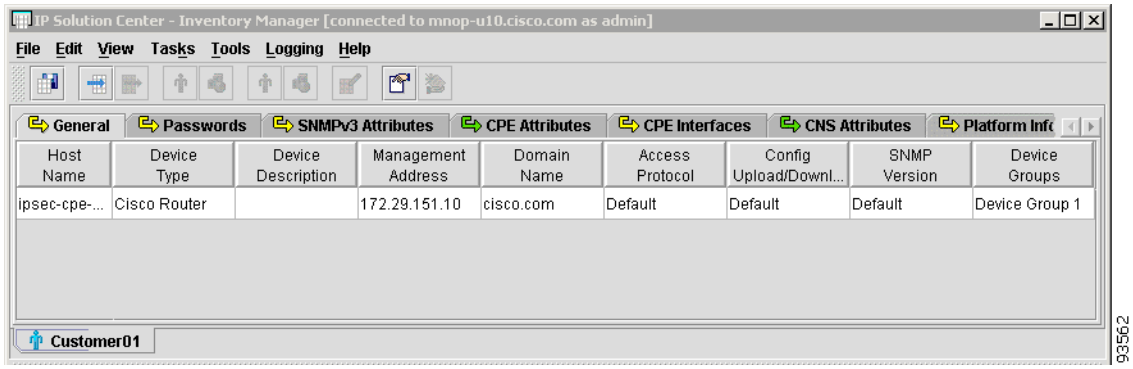
Choose from the list of existing Sites, as shown in Figure 4-77. You can also create a Site for the Customer by choosing **Create Site**.

Figure 4-77 Open Site



A CPE Spreadsheet Editor appears with all the CPEs for that Site listed in the Spreadsheet Editor, as shown in Figure 4-78.

Figure 4-78 CPE Spreadsheet Editor



You now have access to the Customer spreadsheet.

Open IPsec VPN Service Modules

This feature is not supported in this release

To open an existing VPNSM, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open IPsec VPN Service Modules**.

Open Device Blades window appears (not shown).

Step 2 Choose a De‘vice Blade.

Step 3 Choose **File** > **Save** to save your changes to the VPNSM in the Repository.

Required Attributes

From the Inventory Manager main menu, shown in Figure 4-26 on page 4-36, Required Attributes is the third option under the File menu on the Task Bar. To specify required attributes, you must open a Spreadsheet Editor for one of the following options:

- Discovery Seed File (No example is provided)
- Device Groups
- Providers
- Regions
- PEs
- Customers
- Sites
- CEs

The Spreadsheet Editors work the same for each inventory group. They default to the General tab and display a list of attributes. Some attributes in each Spreadsheet Editor are required and others are not. You can make some of the non-system required attributes required by clicking a checkbox for that attribute.

If an attribute is required, the spreadsheet tab will have a red X indicating that more information is required by the system for all later processing to proceed without errors. For example, errors can occur when processing service requests or creating a VPN. When all required information is filled out, the red X changes to either a yellow or green Continue Image. When you see a red X on a tab, it means you need to fill out more information for the tab.

From the Required Attributes option, you can specify required attributes for the following inventory groups:

- Device Groups, page 4-62
- Providers, Regions, and PE, page 4-68
- Customers, Sites, and CE, page 4-76

Device Groups

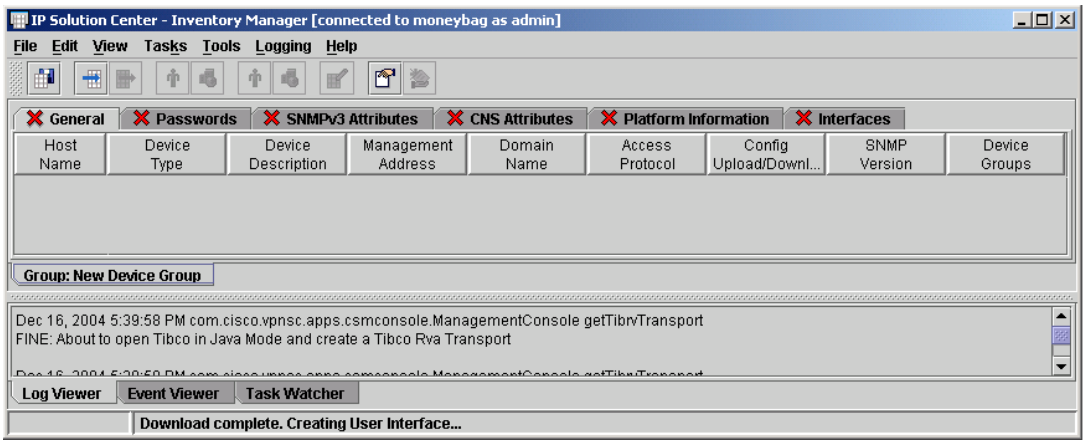
To specify required attributes for a Device Group, follow these steps:

Step 1 From the Inventory Manager menu, choose **File** > **Open** > **Open Device Group**.

A search dialog appears.

Step 2 Select the Device Group and a Spreadsheet Editor appears, as shown in Figure 4-79.

Figure 4-79 Open Device Group

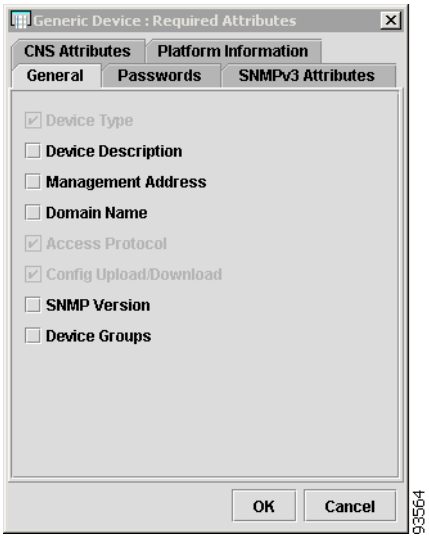


Step 3 Choose **File > Required Attributes**.

The **General** tab on the Required Attributes window for a Device Group appears, as shown in Figure 4-80.

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-80 Generic Device - General Attributes



The General tab contains the following attributes:

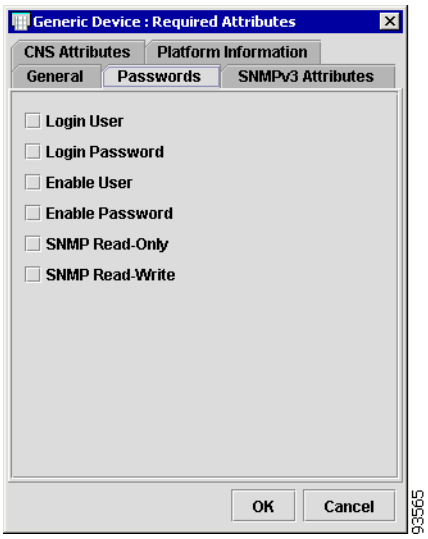
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in Figure 4-81.

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-81 Generic Device - Password Attributes



The Passwords tab contains the following attributes:

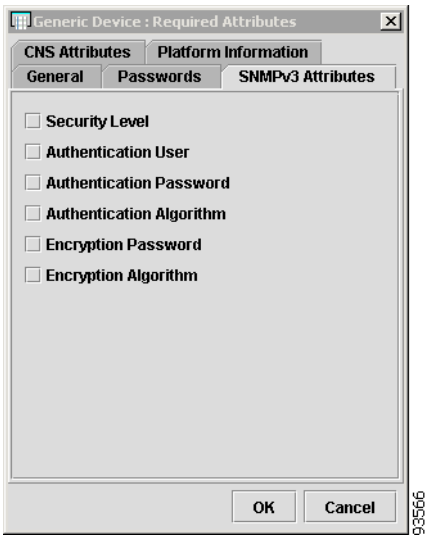
- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMPv3, choose the **SNMPv3 Attributes** tab.

The SNMPv3 tab on the Required Attributes window appears, as shown in Figure 4-82.

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-82 Generic Device - SNMPv3 Attributes



The SNMPv3 Attributes tab contains the following attributes:

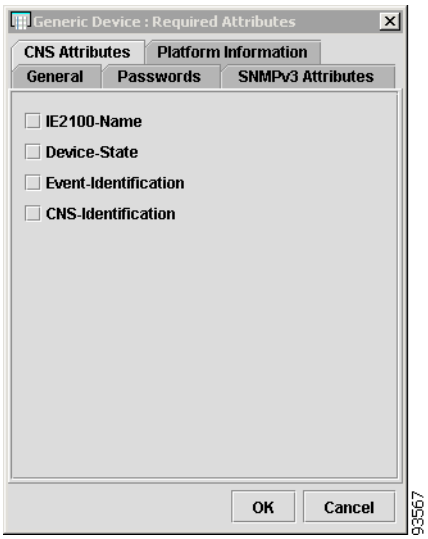
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for CNS, choose the **CNS Attributes** tab.

The **CNS** tab on the Required Attributes window appears, as shown in Figure 4-83.

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-83 Generic Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

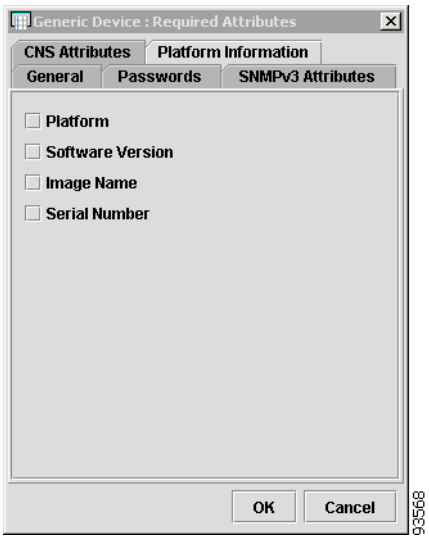
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 11 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in Figure 4-84.

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-84 Generic Device - Platform Information Attributes



The Platform Information tab contains the following attributes:

- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Providers, Regions, and PE

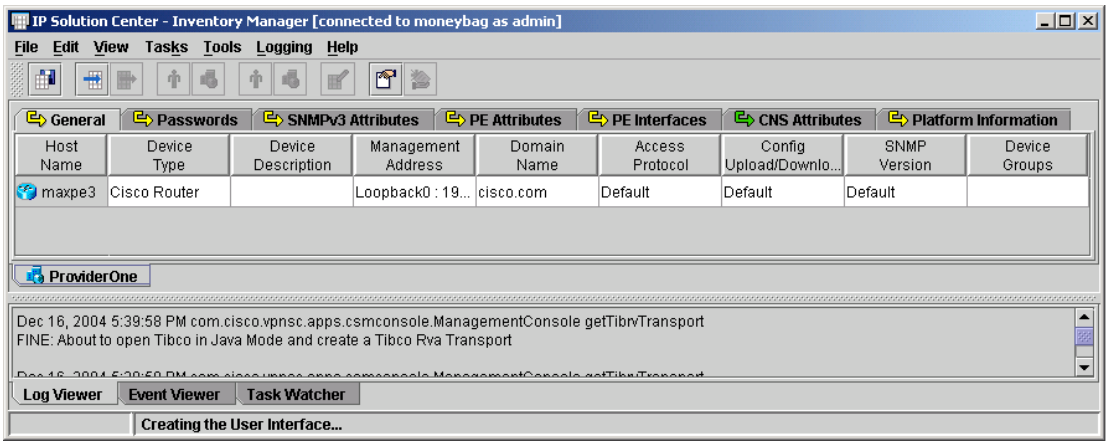
To specify required attributes for a Provider, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Provider**.

A search dialog appears.

Step 2 Select the Provider and a Spreadsheet Editor appears, as shown in Figure 4-85.

Figure 4-85 Open Provider

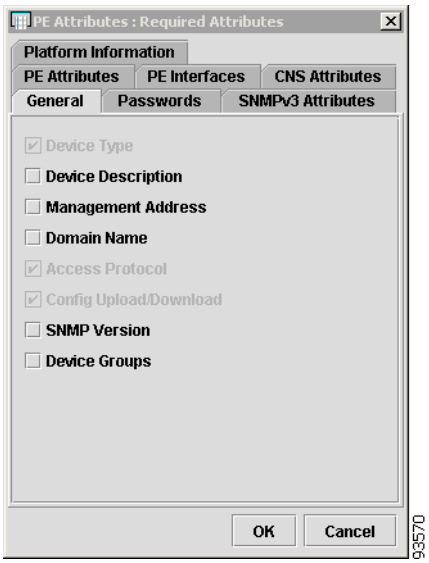


Step 3 Choose **File > Required Attributes**.

The General tab on the Required Attributes window for the provider appears, as shown in Figure 4-86.

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-86 PE Device - General Attributes



The General tab contains the following attributes:

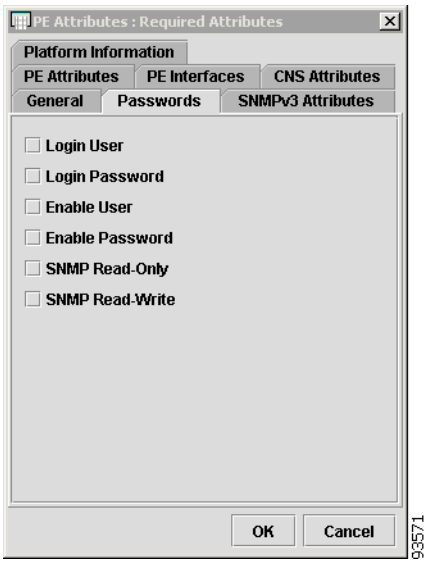
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in Figure 4-87.

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-87 PE Device - Password Attributes



The Passwords tab contains the following attributes:

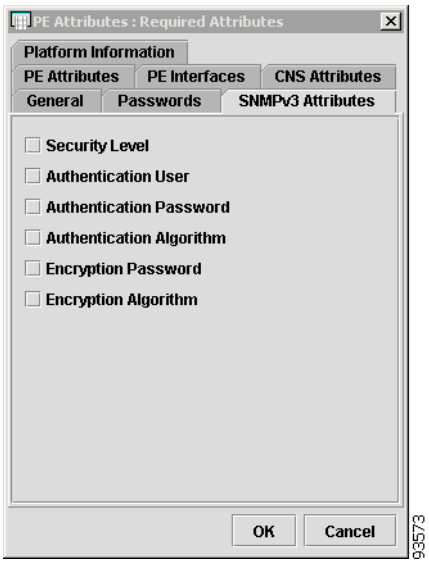
- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMP attributes, choose the **SNMPv3 Attributes** tab.

The SNMPv3 Attributes tab on the Required Attributes window appears, as shown in Figure 4-88.

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-88 PE Device - SNMPv3 Attributes



The SNMPv3 Attributes contains the following attributes:

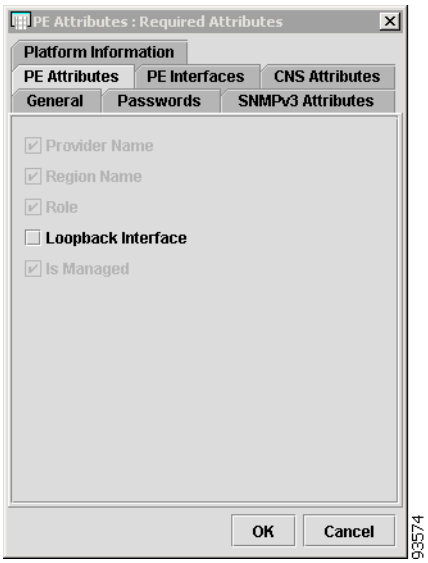
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for PE attributes, choose the **PE Attributes** tab.

The PE Attributes tab on the Required Attributes window appears, as shown in Figure 4-89.

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-89 PE Device - PE Attributes



The PE Attributes tab contains the following attributes:

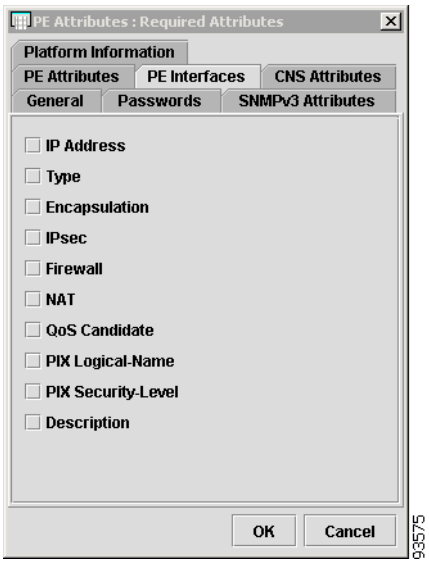
- **Provider Name**
- **Region Name**
- **Role**
- **Loopback Interface**
- **IS Managed**

Step 11 To modify attributes for PE interfaces, choose the **PE Interfaces** tab.

The PE Interfaces tab on the Required Attributes window appears, as shown in Figure 4-90.

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-90 PE Device - PE Interfaces



The PE Interfaces tab contains the following attributes:

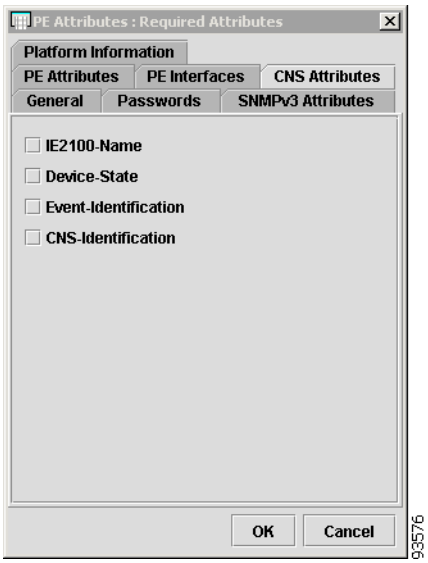
- **IP Address**
- **Type**
- **Encapsulation**
- **IPsec (This feature is not supported in this release)**
- **Firewall (This feature is not supported in this release)**
- **NAT (This feature is not supported in this release)**
- **QoS Candidate**
- **PIX Logical Name**
- **PIX Security-Level**
- **Description**

Step 13 To modify attributes for CNS attributes, choose the **CNS Attributes** tab.

The CNS Attributes tab on the Required Attributes window appears, as shown in Figure 4-91.

Step 14 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-91 PE Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

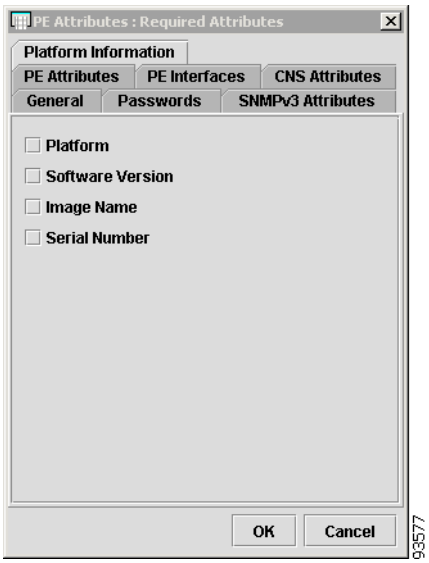
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 15 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in Figure 4-92.

Step 16 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-92 PE Device - Platform Information



The Platform Information tab contains the following attributes:

- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Customers, Sites, and CE

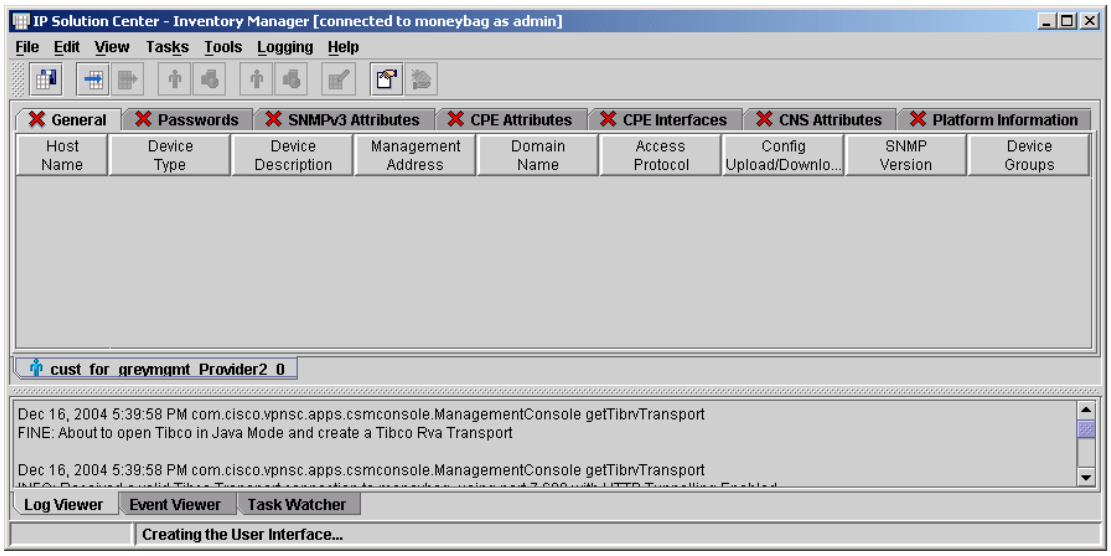
To specify required attributes for a Customer, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > Open > Open Customer**.

A search dialog appears.

Step 2 Select the Customer and a Spreadsheet Editor appears, as shown in Figure 4-93.

Figure 4-93 Open Customer

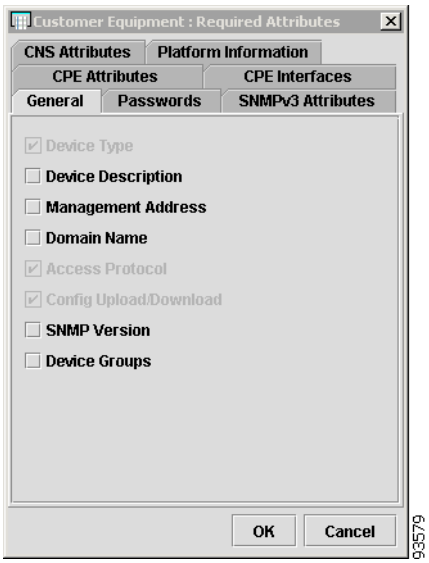


Step 3 Choose **File > Required Attributes**.

The General tab on the Required Attributes window appears, as shown in Figure 4-94.

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-94 CPE Device - General Attributes



The General tab contains the following attributes:

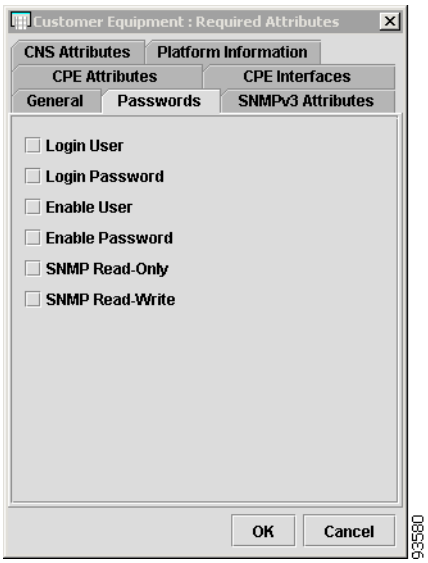
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in Figure 4-95.

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-95 CPE Device - Password Attributes



The Passwords tab contains the following attributes:

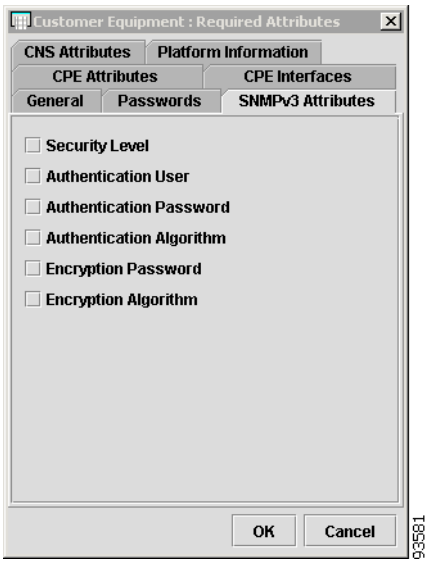
- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMPv3, choose the **SNMPv3 Attributes** tab.

The SNMPv3 Attributes tab on the Required Attributes window appears, as shown in Figure 4-96.

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-96 CPE Device - SNMPv3 Attributes



The SNMPv3 Attributes contains the following attributes:

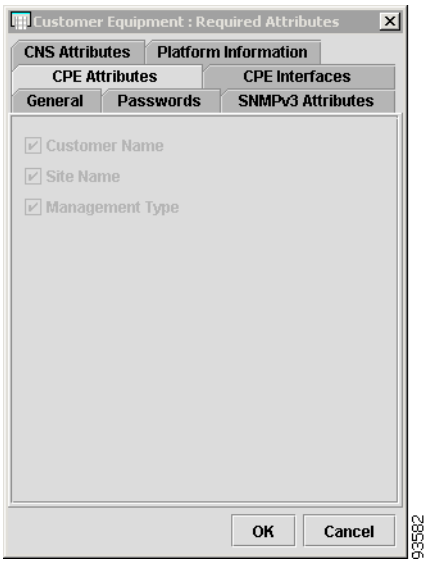
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for CPE, choose the **CPE Attributes** tab.

The CPE Attributes tab on the Required Attributes window appears, as shown in Figure 4-97.

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-97 CPE Device - CPE Attributes



The CPE Attributes tab contains the following attributes:

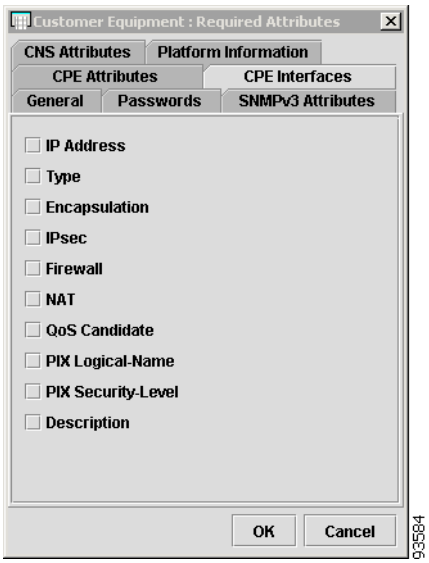
- **Customer Name**
- **Site Name**
- **Management Type**

Step 11 To modify attributes for CPE interfaces, choose the **CPE Interfaces** tab.

The CPE Interfaces tab on the Required Attributes window appears, as shown in Figure 4-98.

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-98 CPE Device - CPE Interfaces



The CPE Interfaces tab contains the following attributes:

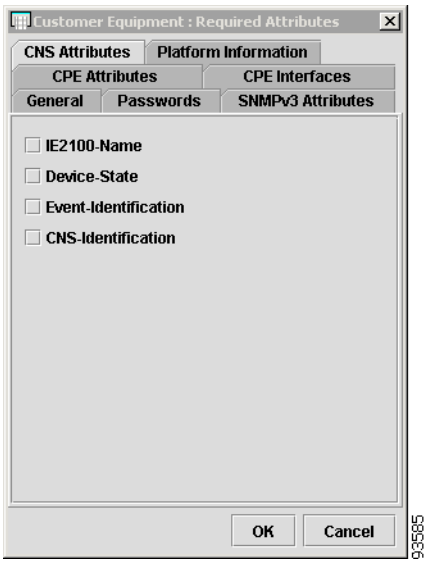
- **IP Address**
- **Type**
- **Encapsulation**
- **IPsec (This feature is not supported in this release)**
- **Firewall (This feature is not supported in this release)**
- **NAT (This feature is not supported in this release)**
- **QoS Candidate**
- **PIX Logical-Name**
- **PIX Security-Level**
- **Description**

Step 13 To modify attributes for CNS, choose the **CNS Attributes** tab.

The CNS Attributes tab on the Required Attributes window appears, as shown in Figure 4-99.

Step 14 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-99 CPE Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

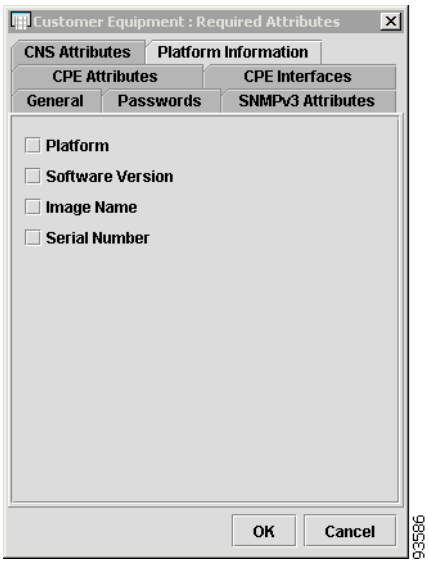
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 15 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in Figure 4-100.

Step 16 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-100 CPE Device - Platform Information Attributes



The Platform Information tab contains the following attributes:

- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Save

From the Inventory Manager main menu, shown in Figure 4-26 on page 4-36, Save is the fourth option under the File menu on the Task Bar.

This option saves your work.

Close

From the Inventory Manager main menu, shown in Figure 4-26 on page 4-36, Close is the fifth option under the File menu on the Task Bar.

This option name changes depending on which Spreadsheet Editor you choose. For example, if you are editing a Customer named CustomerA, the menu would show File Close CustomerA.

If there are changes to be saved, the system prompts you to save, and then the Spreadsheet Editor closes. You have an opportunity to cancel the operation if saving is required.

Exit

From the Inventory Manager main menu, shown in Figure 4-26 on page 4-36, Exit is the sixth option under the File menu on the Task Bar.

This option shuts down the Inventory Manager. If there are changes to be made, the system prompts you to save changes before exiting.

Edit Menu

From the Inventory Manager main menu, shown in Figure 4-25 on page 4-34, Edit is the second menu on the Task Bar. The Edit menu has the following options:

Insert More Devices

When editing a Device Group, Provider, or Customer, choosing this option causes a File Open Dialog to appear, where you can select more configuration files to be inserted. A new row is created for each new configuration file that is added:

- If you are editing a Provider or a Region, a physical device and a logical PE are created in the Repository.
- If you are editing a Customer or a Site, a physical device and a logical CPE are created in the Repository.
- If you are editing a Device Group, only a physical device is created and you *must* associate it with a PE or CPE using the **Edit > Move To** menu options.
- If you are editing in a Dynamic Device List spreadsheet, choosing this option adds one more empty row into the spreadsheet for editing.

To insert more devices in a Spreadsheet Editor, choose **Edit > Insert More Devices** from the Inventory Manager Task Bar.

Remove Selected Devices

When editing a Device Group, Provider, or Customer, choosing this option allows selected rows to be removed from the spreadsheet.

To delete rows in a Spreadsheet Editor, choose **Remove Selected Devices** from the Inventory Manager Task Bar.

Use the Host Name Column to select rows of device information. A confirmation dialog appears. If you choose **Yes**, the selected rows are removed from the Spreadsheet Editor.

Note These objects are not removed from the Repository.

Move to New Customer

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List options. You must select rows using the Host Name Column or the Select All option. The selected rows in the spreadsheet are moved to a new tab for a Customer in a CPE Spreadsheet Editor.

To create a new Customer and move the selected rows to a new CPE Spreadsheet Editor, follow these steps:

Step 1 Select the desired rows using the host name column of a device spreadsheet.

Step 2 From the Inventory Manager Task Bar, choose **Edit > Move to New Customer** to create a new Customer and move the selected rows to a new CPE Spreadsheet Editor.

Step 3 A dialog box prompts you to enter the new Customer information such as Name and Contact information.

Step 4 Click OK and the selected rows are removed from the current spreadsheet and moved into a new Customer CPE spreadsheet. In the process, each moved physical device is associated with a new CPE logical device in the Repository.

Step 5 Proceed to edit the CPE as you would for any Customer, by associating it with new Site objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Move to New Provider

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List options. You must select rows using the Host Name Column or the Select All option. The selected rows in the spreadsheet are moved to a new tab for a Provider in a PE Spreadsheet Editor.

To create a new Provider and move the selected rows to a new PE Spreadsheet Editor, follow these steps:

Step 1 Select the desired rows using the host name column of a device spreadsheet.

Step 2 From the Inventory Manager Task Bar, choose **Edit > Move to New Provider** to create a new Provider and move the selected rows to a new PE Spreadsheet Editor.

Step 3 A dialog box prompts you to enter the new Provider information such as Name, BGP AS number, and Contact information.

Step 4 Click OK and the selected rows are removed from the current spreadsheet and moved into a new Customer PE spreadsheet. In the process, each moved physical device is associated with a new PE logical device in the Repository.

Step 5 Proceed to edit the PE as you would for any Provider, by associating it with new Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Move to Customer

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List. You must use the Host Name Column or the Select All options to select rows. The selected rows in the spreadsheet are moved to a new tab for the customer in a CPE Spreadsheet Editor.

To select rows in a table, open an existing customer, and move the rows to a new CPE Spreadsheet Editor, and follow these steps:

Step 1 Select the desired rows using the host name column.

Step 2 From the Inventory Manager Task Bar, choose **Edit > Move to Customer**.

A dialog box appears asking you to enter the existing Customer name.

Step 3 Click the Find button and a list of customers appears.

Step 4 Choose a customer.

If you click OK, the selected rows are removed from the current spreadsheet into an existing customer CPE spreadsheet.

Note In the process, each moved physical device is associated with a new CPE logical device in the Repository.

Edit the CPEs as you would for any customer by associating them with new or existing Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Move to Provider

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List. You must use the Host Name Column or the Select All options to select rows. The selected rows in the spreadsheet are moved to a new tab for the Provider in a PE Spreadsheet Editor.

To select rows in a table, open an existing provider, and move the rows to a new PE Spreadsheet Editor, and follow these steps:

Step 1 Select the desired rows using the host name column.

Step 2 From the Inventory Manager Task Bar, choose **Edit > Move to Provider**.

A dialog box appears asking you to enter the existing Provider name.

Step 3 Click the Find button and a list of providers appears.

Step 4 Choose a provider.

If you click OK, the selected rows are removed from the current spreadsheet into an existing Provider PE spreadsheet.

Note In the process, each moved physical device is associated with a new PE logical device in the Repository.

Step 5 Edit the PEs as you would for any provider by associating them with new or existing Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Edit Selected Devices

To edit selected devices from rows in a spreadsheet, follow these steps:

Step 1 Choose **Edit > Edit Selected Devices** from the Inventory Manager Task Bar.

A Multi-Attribute Cell Editor appears where you can set a value that is applied to all selected cells for each respective column in the selection.

Step 2 Click the Multi-Attribute Editor cell to set the value.

Step 3 To edit an individual cell in a column, click the cell.

A column-specific editor appears.

Step 4 Use the column-specific editor to specify a value for the cell.

A new dialog appears showing a table with one row. Each column containing selected cells in the originating spreadsheet is represented in the dialog.

Step 5 Click each cell in the new dialog and a column specific editor appears allowing you to enter a value or select from a list of existing values.

Step 6 When you are finished filling in the one row spreadsheet, click OK and the values are applied to each selected cell in the original spreadsheet respectively.

Step 7 To edit a single value in a cell, click the cell.

You are prompted with a search dialog to specify the value. The type of search dialog depends on the column you are editing. For example, if you edit a username you are prompted with a single input editor. If you are editing a password column, you get a password editor.

To edit multiple attributes at one time, select the cells using the following standard techniques for multiple selections:

- Select a single cell that represents the upper boundary. Press the Shift Key and select the lower boundary of the selection.
- Click and drag to and from a boundary.
- To toggle your selection, press the Ctrl Key and click on a cell.
- To select entire rows, use the Host Name Column as your main point of selection.

Edit Default Attributes

Each spreadsheet editor (Device Group, CPE, PE, and Dynamic Device List) has the ability to store separate default attributes. Defaults for passwords and other parameters for PEs can be different from those of CPEs.

For example, all PEs in a provider network can share the same passwords, SNMP attributes, and so on. Using Inventory Manager, you can store default attributes for most of the attributes in each spreadsheet. These default attributes can then be applied to selected cells using the **Edit > Load Default Attributes to Selected Cells** menu.

To edit default attributes, follow these steps:

Step 1 Choose **Edit > Edit Default Attributes** from the Inventory Manager Task Bar.

A new dialog appears containing a table with one row.

Step 2 To specify the default attribute for a particular column, click it and specify the value in the column-specific editor.

Step 3 When you are finished editing the desired defaults, click the OK button and the default attributes are stored.

Each specific Spreadsheet Editor has its own unique set of columns. Each editor allows the specification for default values to be stored and retrieved at a later time. It is the standard spreadsheet format, and to specify the values you must click on each cell. These values are automatically saved between sessions and are stored per user on the client machine running the Inventory Manager.

When specifying default values for the Management Address or PE Loopback Interface columns, you may enter more than one interface name.

For example, **Loopback0;FastEthernet0;Ethernet0**, where the separator between names must be a semicolon. When attempting to set the Management Interface using the default supplied for any given device, the interfaces stored on the device must be checked against the value provided. If the value provided is Loopback0 and the interface does not exist on the device, it can not be set. The interface must actually exist on the device before Inventory Manager allows it as a valid value.

In the example of **Loopback0;FastEthernet0;Ethernet0**, Inventory Manager uses a left to right precedence rule. For each selected device it first checks to see whether Loopback0 exists. If it is found on the device, it is used as the correct value, otherwise it looks for FastEthernet0 and continues down the list until it finds an acceptable result. If no interfaces on the device match the request string, the value remains unchanged.

Load Default Values to Selected Cells

To load default values to selected cells, follow these steps:

Step 1 From the Inventory Manager Task Bar, choose **Edit > Edit Default Attributes.**

Step 2 Select the desired cells in the spreadsheet.

Step 3 Choose **Edit > Load Default Attributes to Selected Cells** option.

Step 4 Specify the default attributes for desired columns.

Step 5 Modify the selected cell values with the default attribute, if possible.

Step 6 Select the cells you want to edit.

Step 7 Choose **Edit > Load Default Values to Selected Cells**.

The values that you stored using the Edit > Edit Default Attributes menu are applied to each selected cell.

For example, if all the devices you are editing belong to the same provider and share the same passwords, you can specify the default password and apply it to the entire spreadsheet without having to remember it.

Apply Interface Marking Rules to Selection

This option is only enabled when you are editing CPE and PE devices in a spreadsheet. To apply the rules, select the desired cells in the spreadsheet and, from the Inventory Manager Task Bar, choose **Tools > Apply Interface Marking Rules to Selection**.

A Rule chooser dialog appears. Select one or more rules to apply on interfaces.

If you select one or more devices, the rules are applied to each interface on the selected devices.

If you select one or more interfaces in the Interface tab, the rules are only applied to the selected interfaces.

For each interface encountered, marking will only occur if the interface and/or parent device properties meet those specified in the rule.

Before you apply interface marking rules to selected devices, you must first create a set of rules for your organization. For an example of how to create interface marking rules, see the "New Rule" section on page 4-98.

Select All

From the Inventory Manager Task Bar, choose **Edit > Select All** to use this option.

This option selects all the cells in a spreadsheet, except the host name column. Typically, the host name column is not editable and does not participate in typical edit operations.

If you want to select all rows in the spreadsheet, first click on the Host Name column and press the Ctrl+A accelerator key. This operation selects all the cells in a Spreadsheet Editor that are currently open.

View Menu

From the Inventory Manager Task Bar, shown in Figure 4-25 on page 4-34, View is the third menu on the Task Bar. The View menu has the following options:

- Fit Columns in Window, page 4-90
- Show Color Coded Column Headers, page 4-90

Fit Columns in Window

From the Inventory Manager Task Bar, choose **View > Fit Columns in Window** to expand or contract the cells in the Spreadsheet Editor to fit the window.

Show Color Coded Column Headers

From the Inventory Manager Task Bar, choose **View > Show Color Coded Column Headers** to show the colors of the column headers.

If you choose **View > Show Color Coded Column Headers**, you could see three colors:

- Red—some required data is missing in this column.
- Yellow—all required data is in this column, but not all optional data.
- Green—all data is provided.

Tasks Menu

From the Inventory Manager Task Bar, shown in Figure 4-25 on page 4-34, Tasks is the fourth menu on the Task Bar. The Task menu has the following options:

- Collect Latest Configuration Files, page 4-90
- Start Auto Discovery, page 4-91
- Start NPC Auto Discovery, page 4-95
- Start Service Discovery, page 4-96

Collect Latest Configuration Files

This option is applied to selected rows in a spreadsheet, if rows are selected. If no rows are selected, all devices contained in the spreadsheet are visited and their configurations are downloaded to the ISC server. It is important for the login and enable passwords to be specified correctly, together with the management address, for each device to be reached and files to be successfully collected.

A persistent task is created on the Master server and Inventory Manager waits for the collection process to complete. When the task completes, you are notified of success or failure. You can use the Web GUI to view the task logs on the Master server to see why a task has failed. If successful, you are prompted to refresh from the Repository. This is recommended, because it is possible that the configuration has changed since the last time the configuration was retrieved.

From the Inventory Manager Task Bar, choose **Tasks > Collect Latest Configuration Files** to collect the latest configuration files.

Start Auto Discovery

Note This option is designed to work in conjunction with the **New Dynamic Device List** option.

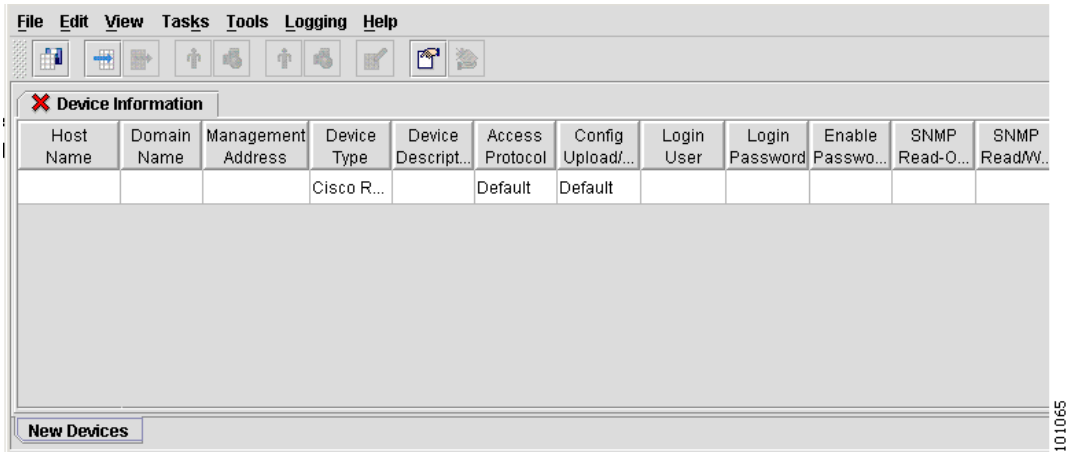
If you do not have existing configuration files, you can discover devices on your network, using the Dynamic Device List.

To create a new Device List and start Auto Discovery, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > New > New Dynamic Device List (without existing configs)**.

A new Device Spreadsheet appears, as shown in Figure 4-101.

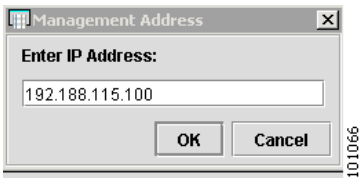
Figure 4-101 New Device Spreadsheet



Step 2 Click the **Management Address** cell.

A Management Address window appears, as shown in Figure 4-56.

Figure 4-102 Enter IP Address

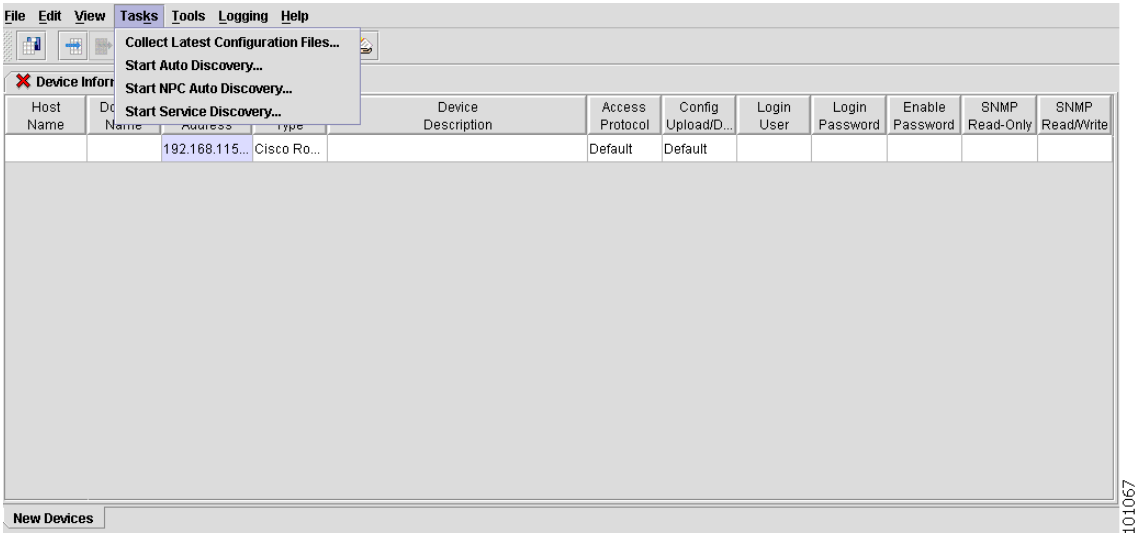


Step 3 Enter the IP address of the device from which you want to start the device discovery process and click **OK**.

A Device Information spreadsheet appears, as shown in Figure 4-103.

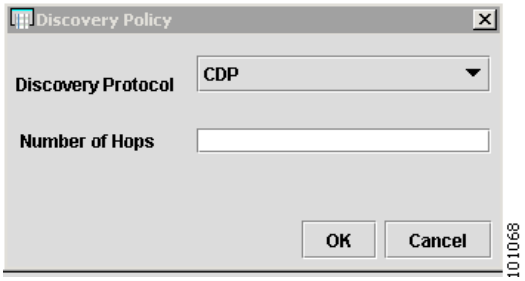
Step 4 From the Inventory Manager Task Bar, choose **Tasks** > **Start Auto Discovery** to start the device discovery process.

Figure 4-103 Start Device Discovery



The Discovery Policy window appears, as shown in Figure 4-104.

Figure 4-104 Discovery Policy

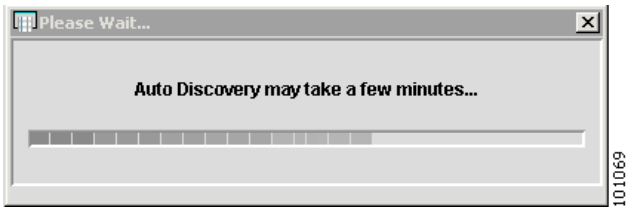


Step 5 Enter the Number of Hops.

This number represents the number of hops from the device with the IP address. For example, the number **1**.

The Please Wait window appears, as shown in Figure 4-105.

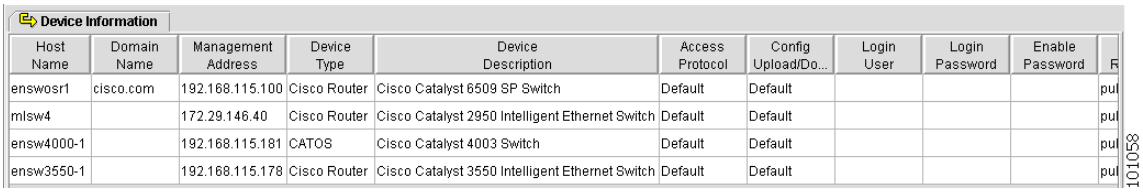
Figure 4-105 Please Wait



Note This waiting period depends on the number of hops and number of devices in the network.

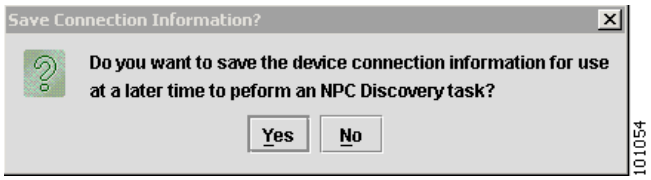
When the waiting period ends, the Device Information spreadsheet appears with the discovered devices, as shown in Figure 4-106.

Figure 4-106 Discovered Devices



The Save Connection Information window also appears, as shown in Figure 4-107.

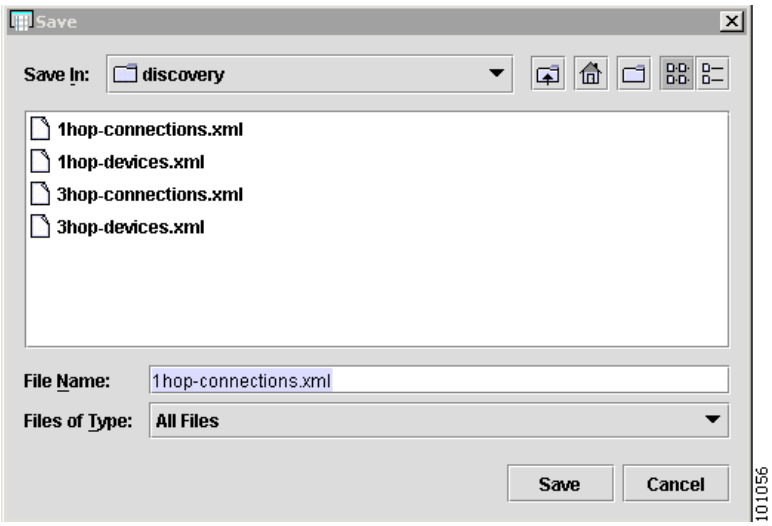
Figure 4-107 Save Connection Information



Step 6 To save the connection information, click **Yes**. This information will be used in the **Start NPC Auto Discovery** process.

A Save Connection Information Confirmation window appears, as shown in Figure 4-108.

Figure 4-108 Save Connection Information Confirmation



Step 7 To save the connection information, give the file a name and click **Save**.

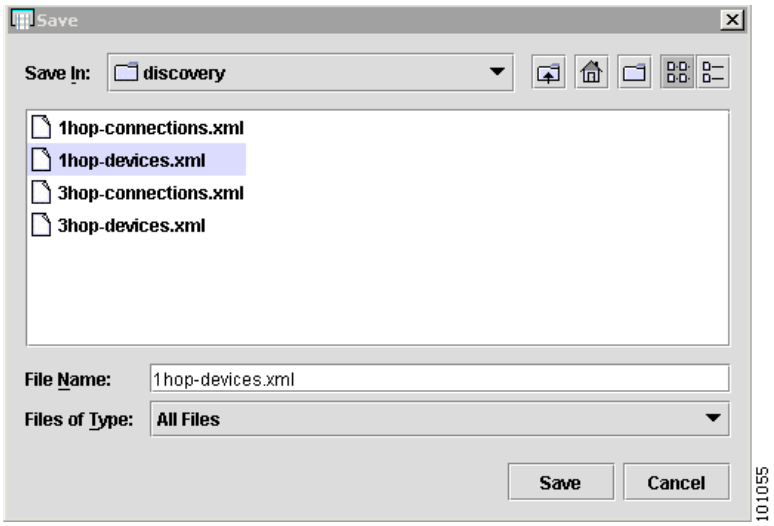
Another Save Device Information window appears, as shown in Figure 4-109.

Figure 4-109 Save Device Information

Step 8 To save the device information, click **Save**.

The Save Device Information Confirmation window appears, as shown in Figure 4-110.

Figure 4-110 Save Device Information Confirmation



Step 9 To save the device information, give the file a name and click **Save**.

The Device Information spreadsheet appears, as shown in Figure 4-111.

Figure 4-111 Device Information

Device Information

Host Name	Domain Name	Management Address	Device Type	Device Description	Access Protocol	Config Upload/Do...	Login User	Login Password	Enable Password	R
enswosr1	cisco.com	192.168.115.100	Cisco Router	Cisco Catalyst 6509 SP Switch	Default	Default				pul
mlsw4		172.29.146.40	Cisco Router	Cisco Catalyst 2950 Intelligent Ethernet Switch	Default	Default				pul
ensw4000-1		192.168.115.181	CATOS	Cisco Catalyst 4003 Switch	Default	Default				pul
ensw3550-1		192.168.115.178	Cisco Router	Cisco Catalyst 3550 Intelligent Ethernet Switch	Default	Default				pul

101058

Now you can edit your devices and collect the latest configuration files.

Start NPC Auto Discovery

From the Inventory Manager Task Bar, choose **Tasks > Start NPC Auto Discovery** to start the connection discovery process.

To import connections with NPC Auto Discovery, follow these steps:

Step 1 Choose **Tasks > Start NPC Auto Discovery**.

You are prompted to provide the path to the correct **connection.xml file**.

Step 2 Select the correct **connection.xml** file and click **OK**.

A dialog box appears, indicating that the NPC discovery process has started.

Step 3 You are prompted if the task completes successfully. Select **OK** to finish this portion of the NPC Auto Discovery process.

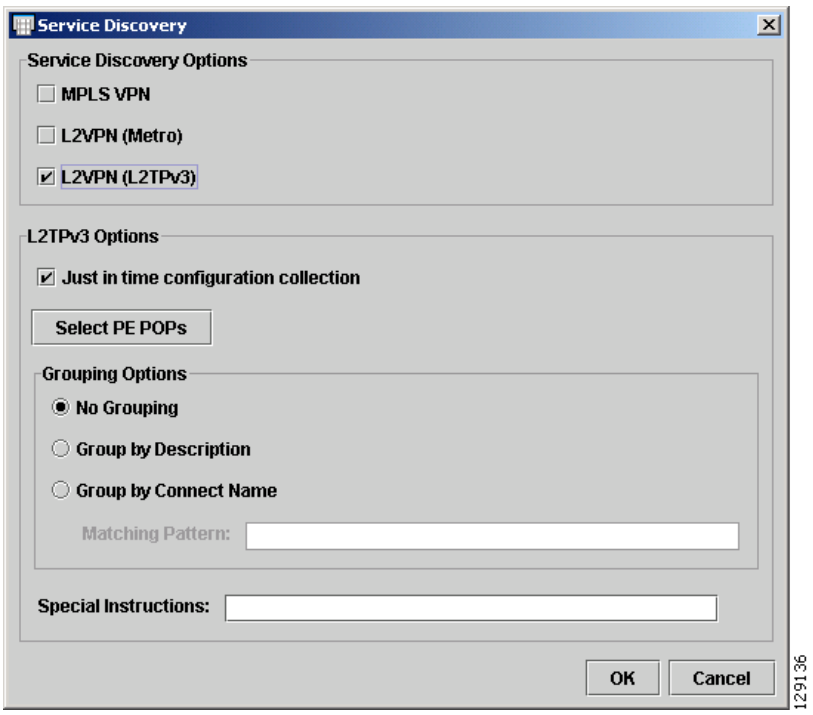
To find the discovered NPCs, go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.

Start Service Discovery

To import services with Auto Discovery from Inventory Manager, in the Task Bar choose **Tasks > Start Service Discovery** to start the service discovery process.

The Service Discovery window in Figure 4-112 appears.

Figure 4-112 Service Discovery



You can choose between the following Service Discovery options:

- **MPLS VPN**—Create a MPLS VPN Service Request for each VRF-enabled interface.
- **L2VPN (Metro)**—Create a L2VPN (Metro) Service Request.
- **L2VPN (L2TPv3)**—Create a L2VPN (L2TPv3) Service Request

Note L2TPv3 auto discovery is limited to L2TPv3 L2VPN service requests.

Checking the **L2VPN (L2TPv3)** box enables the bottom L2TPv3 Options (see Figure 4-112):

Just in time configuration collection—Upload the PE configurations from the routers before auto discovery.

Select PEs—Opens the Select PE POPs window, where you can select one or more PE POPs

- Grouping Options:
  - **No Grouping**—One auto-discovered L2TPv3 session (link) will become one SR.
  - **Group by Description**—(Currently not implemented)
  - **Group by Connect Name**—More than one auto-discovered L2TPv3 session will be grouped into one SR if they share the same connect name.
- **Special Instructions**—(Currently not implemented)

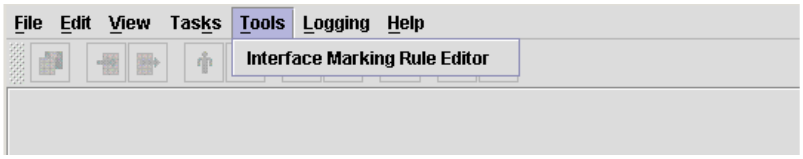
You are notified when service discovery is finished.

Tools Menu

Note IPsec, firewall, NAT: **These features are not supported in this release.**

To open a rule editor where you can create and modify rules for marking interfaces, import and export rule files, and specify values for IPsec, NAT, QoS, and Firewall, choose **Tools > Interface Marking Rule Editor** from the Inventory Manager Task Bar, as shown in Figure 4-113.

Figure 4-113 Interface Marking Rule Editor



The Interface Rule Editor Task Bar appears with an **interface-rules** dialog box, as shown in Figure 4-114.

Figure 4-114 Interface Rule Editor Task Bar

The Task Bar has the following options:

- File, page 4-98
- Edit, page 4-104
- Help, page 4-104

File

The File option has the following options:

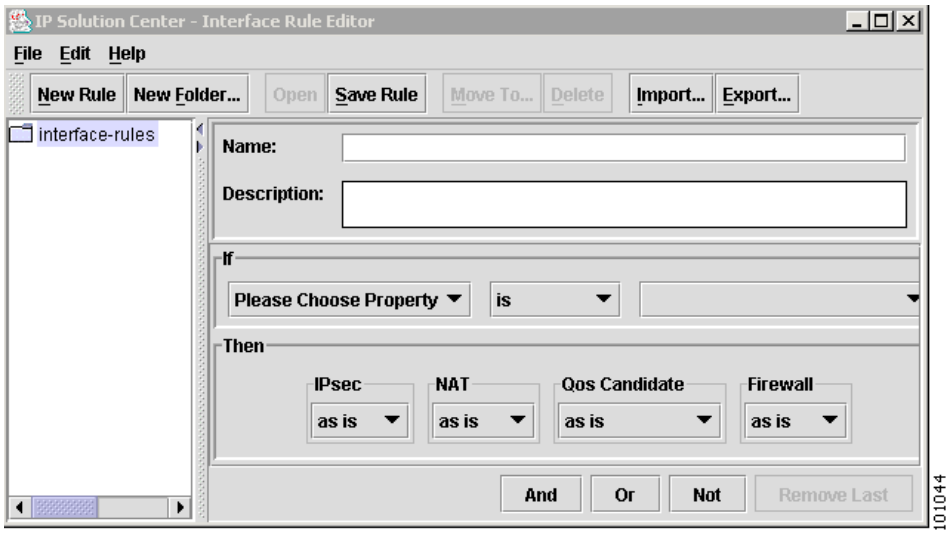
- New Rule, page 4-98
- New Folder, page 4-103
- Open, page 4-103
- Close, page 4-103
- Import, page 4-103
- Export, page 4-103
- Save Rule, page 4-104

New Rule

To create a new rule, follow these steps:

Step 1 Click the **interface-rules** folder and choose **New Rule** from the File option or New Rule icon. A dialog box appears, as shown in Figure 4-115.

Figure 4-115 Interface Rule Editor Dialog Box

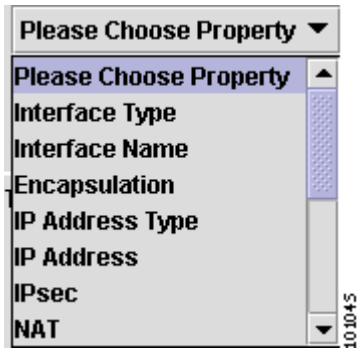


Step 2 Enter the following information:

- **Name—**Name of the rule (required).
- **Description—**Description of the rule (optional).

Step 3 From the If clause drop-down buttons, click **Please Choose Property** and a Property drop-down list appears, as shown in Figure 4-116.

Figure 4-116 Property Drop-Down List

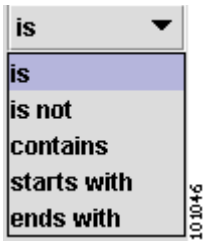


Step 4 Select a Property.

Note The Property that you select determines the content of subsequent drop-down lists.

Step 5 Click **is** and a Relationship drop-down list appears, as shown in Figure 4-117.

Figure 4-117 Relationship Drop-Down List



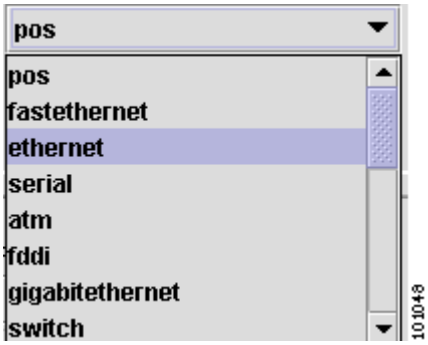
Step 6 Select a Relationship.

Step 7 If you had chosen **Interface Type** for the Property and **is** for the Relationship, the drop-down button would show **pos**, as shown in Figure 4-118.

Figure 4-118 Pos Drop-Down Button

Step 8 Click **pos** and a Type drop-down list appears, as shown in Figure 4-119.

Figure 4-119 Type Drop-Down List



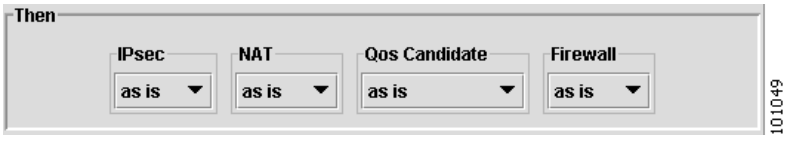
Step 9 Select a Type.

If you chose **ethernet**, for example, you would have defined the following interface type If clause in the new rule:

- If the interface type is Ethernet

You can define how to mark the interface with the Then clause drop-down buttons, as shown in Figure 4-120.

Figure 4-120 Then Clause Drop-Down List



You can create a new rule to mark interfaces for the following security and quality features:

- IPsec
- NAT
- QoS
- Firewall

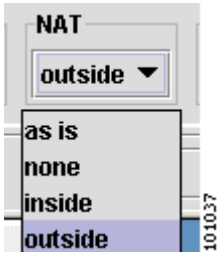
Step 10 To change the interface marking for IPsec, click the IPsec drop-down list, and make the appropriate selection. An IPsec drop-down list appears, as shown in Figure 4-121.

Figure 4-121 IPsec Drop-Down List

Step 11 Select a setting.

Step 12 To change the interface marking for NAT, click the NAT drop-down list, and make the appropriate selection. A NAT drop-down list appears, as shown in Figure 4-122.

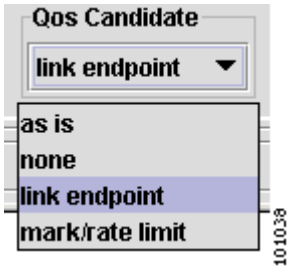
Figure 4-122 NAT Drop-Down List



Step 13 Select a setting.

Step 14 To change the interface marking for QoS, click the QoS drop-down list, and make the appropriate selection. A QoS drop-down list appears, as shown in Figure 4-123.

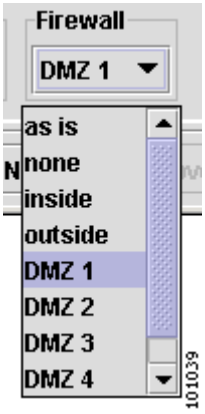
Figure 4-123 QoS Drop-Down List



Step 15 Select a setting.

Step 16 To change the interface marking for Firewall, click the Firewall drop-down list, and make the appropriate selection. A Firewall drop-down list appears, as shown in Figure 4-124.

Figure 4-124 Firewall Drop-Down List



Step 17 Select a setting.

If you selected the security and quality features above, you would have formulated the following Then clause in the new rule:

- Set:
  - IPsec to **private**
  - NAT to **outside**
  - QoS to **Link Endpoint**
  - Firewall to **DMZ1**

The **as is** for each service shows the changed value in the Then clause drop-down buttons, as shown in Figure 4-125.

Figure 4-125 Then Clause Drop-Down List

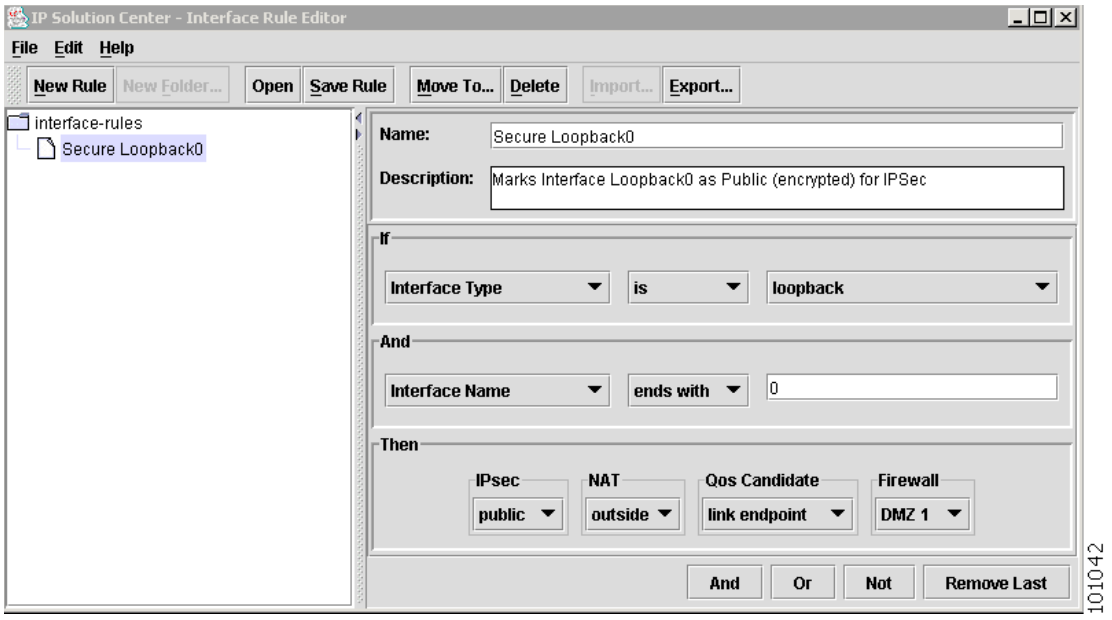
You can create additional If clause statements with more complicated logic, by using the And, Or, and Not drop-down buttons, as shown in Figure 4-126.

Figure 4-126 Additional If Clause Drop-Down List

You can remove the additional statements by using the Remove Last button.

Figure 4-127 show an example of a rule with an additional If clause.

Figure 4-127 Example of a Rule



Note One rule can mark all Loopback0 interfaces as public for IPsec, outside for NAT, link endpoint for QoS, and DMZ1 for Firewall.

New Folder

Creates a new folder under the selected folder.

Open

Opens the selected rule.

Close

Closes the selected rule.

Import

Imports external rules to an existing folder. Each rule and folder contained in the file is created under the selected folder in the tree.

Export

If you select one or more rules without a folder, the rules are exported to a file of your choice. You can then share this file with other users of Inventory Manager.

If you select a folder, all child folders and contained rules can be exported to a file of your choice. You can then share this file with other users of Inventory Manager.

If used with a single rule, it exports that rule, to a single file.

If used on a folder, it will export all the rules from that folder, to a single file.

Save Rule

Saves the modified rule.

Edit

Delete

Deletes the selected rule or folder.

Moves To

Moves a rule or folder to an existing folder.

Help

About

Contains information on Cisco Systems and the ISC software version.

License

Contains the ISC software license agreement.

Logging Menu

From the Inventory Manager Task Bar, shown in Figure 4-25 on page 4-34, Logging is the sixth menu on the Task Bar. The Logging menu allows you to specify the following log output levels to the Logging UI:

- All

  All log messages are sent to the Log Viewer located near the bottom of Inventory Manager

- Severe

  Only severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Warning

  Only warning and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Info

  Only informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Fine

  Only fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Finer

  Only finer, fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Finest

  Only finest, finer, fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- Off

  No log messages are sent to the Log Viewer located near the bottom of the Inventory Manager.

Help

From the Inventory Manager Task Bar, shown in Figure 4-25 on page 4-34, Help is the seventh menu on the Task Bar. The Help menu has the following option:

- About, page 4-105

About

Loads the About dialog showing version information and some web URLs for Cisco Systems Inc.

Auto Discovery

This section describes the Auto Discovery features. It contains the following sections:

Auto Discovery Overview

With Auto Discovery, ISC can automatically perform the following operations:

- Discover all the devices and the physical links between the devices.
- Discover Ether channels, loopback addresses, interfaces, and encapsulation types for interfaces on each device.
- Discover all L2VPN/VPLS and L3VPN services.

To understand the benefits of Auto Discovery, consider the following business scenario. ISC is connected to a network that contains more than 50 devices with some L2VPN and L3VPN services already provisioned.

Without Auto Discovery, the operator would need to manually enter the following information in ISC:

- Information about all the devices and the physical links between these devices.
- Information about all the existing L2VPN services and L3VPN services.

Auto Discovery Prerequisites

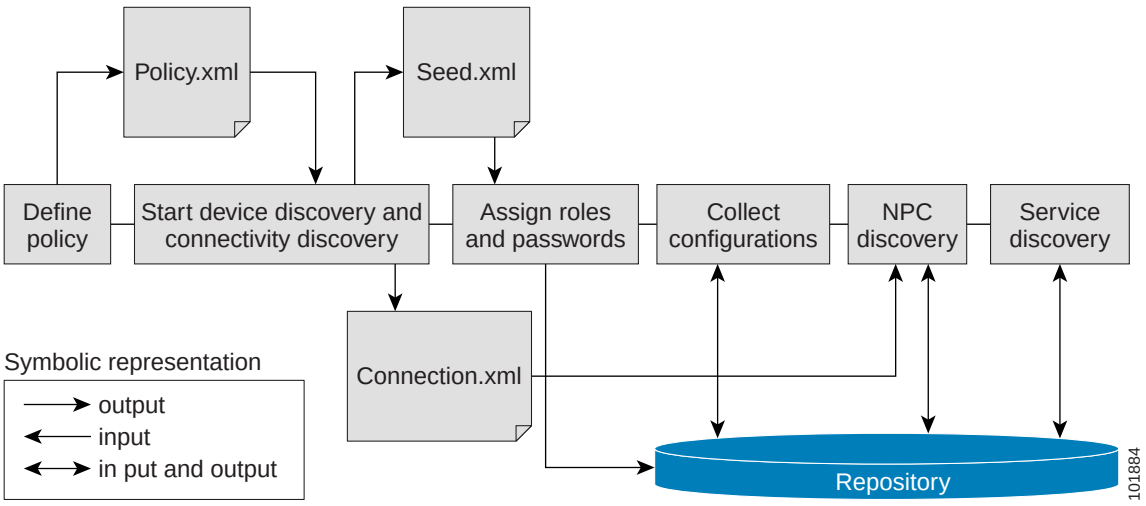
Before running Auto Discovery, you should do the following:

- Enable SNMP on all devices.
- Enable CDP on all devices you want to discover.
- Have a lab diagram that shows how the network is set up.
- Disable all NAT IP address mapping in the network. (**This feature is not supported in this release.)**
- Not have multiple installations of ISC in one subnet.

Process Flow

Figure 4-128 shows the Auto Discovery Process.

Figure 4-128 Auto Discovery Process Flow



Cornerstone Bridge Log is available for viewing from an internet browser.

User Interface

There are two user interfaces available for running Auto Discovery:

- Inventory Manager GUI
- UNIX Command Line Interface (UNIX CLI)

Inventory Manager GUI

To use Auto Discovery within Inventory Manager, follow these steps:

Step 1 Choose **File** > **New** > **New Dynamic Device List** to create a **policy.xml** file.

Step 2 Choose **Tasks** > **Start Auto Discovery**.

Step 3 Choose your own location and names to save the seed file and connection output file.

Step 4 Assign roles and passwords.

Step 5 Choose **Tasks** > **Collect Latest Config Files**.

Step 6 Choose **Tasks** > **Start NPC Discovery** using the connection output file.

Step 7 Choose **Tasks** > **Start Service Discovery** to do Common and Service Discovery.

To see the results of the Auto Discovery and Service Discovery processes, the following screens are available:

- Choose **Service Inventory** > **Inventory and Connection Manager** > **Service Requests** to see Service Requests.
- Choose **Service Inventory** > **Inventory and Connection Manager** > **Named Physical Circuits** to see NPC.
- Choose **Service Inventory** > **Inventory and Connection Manager** > **NPC Rings** to see Ring Topologies.

UNIX Command Line Interface (UNIX CLI)

To use the UNIX CLI, follow these steps:

Step 1 Edit **policy.xml** in **$ISC_HOME/bin**.

Step 2 Run **$ISC_HOME/bin/invokeDiscovery.sh** for device and connection discovery.

Step 3 Output files are saved in **$ISC_HOME/tmp/seed.xml** and **$ISC_HOME/tmp/connection.xml** automatically.

Step 4 Use Inventory Manager to assign roles and passwords for devices and collect configuration files. See Creating a New Customer with Devices, page 4-10.

Step 5 Run **$ISC_HOME/bin/runDiscoverNPC.sh** to populate connections.

Step 6 Run **$ISC_HOME/bin-/runCommonDiscovery.sh** for all service discovery.

Step 7 Log available via standard output.

Service Discovery

This section describes the types of Service Discovery that ISC currently supports. It contains the following sections:

MPLS Service Discovery

This section describes the process for MPLS Service Discovery. This section contains the following sections:

MPLS Service Discovery Overview

The IP Solution Center (ISC) provides a mechanism to discover the state of the network. Using Inventory Manager, you can discover information about the following network features:

- Devices (Network hardware)
- Connections (Named Physical Circuits)
- Services (L2 VPN and L3 MPLS VPN service requests)

MPLS VPN Service Discovery provides the following benefits:

- When you create an MPLS VPN service request, less information needs to be added.
- Services provisioned by non-ISC applications can be discovered and managed by ISC.

An MPLS VPN service request consists of one or more MPLS VPN links. ISC supports Service Discovery for two types of MPLS VPN links:

- PE-CE
- PE-NoCE

The Unmanaged CE option is also supported for the PE-CE type.

Limitations

In cases where Auto Discovery is used, ISC has the following Auto Discovery limitations:

- Auto Discovery does not support creating Service Requests with an MVRF CE PE-CE links.
- Auto Discovery does not support creating Service Requests for commands not supported by ISC.

MPLS Service Discovery Process

The MPLS Service Discovery process creates one MPLS VPN Service Request for each VRF-enabled interface. A VRF-enabled interface is an interface on which the **ip vrf forwarding** command is configured on the PE.

Note MPLS Service Discovery can be invoked only after Device Discovery and NPC Discovery have been completed *successfully.*

The following steps describe the logic MPLS Service Discovery uses to create Service Requests and populate the Repository:

Step 1 Find all the PE devices in the Repository with the role of PE-POP.

Step 2 Analyze the configuration file for each PE found in the previous step.

Step 3 Identify all the VRF-enabled interfaces (these interfaces can also be sub-interfaces).

Step 4 Check each VRF-enabled interface for valid Service Requests (SR).

Step 5 If a valid SR exists, ignore the VRF-enabled interface.

Otherwise, for each VRF-enabled interface, find the CE connected to the interface in the Named Physical Circuit (NPC) table, which was populated by the NPC Discovery process.

Note An NPC is a collection of physical links. By traversing the physical links, you can find the terminating logical device for the VPN link.

Step 6 Find the sub-interface on the CE that connects the MPLS link with the PE.

Step 7 If no terminating CE is found in the NPC table, create an SR without the CE.

Step 8 Create a generic MPLS Service Policy for each PE-CE link, and attach it to the Customer associated with the CE.

Note An MPLS Service Policy provides defaults to simplify the provisioning of service requests.

Step 9 Create a generic MPLS Service Policy for each PE-Only link, and attach it to the Provider associated with the PE.

Step 10 Analyze the PE and CE configuration files, and determine the routing protocols, based on the IP addresses of the participating interfaces.

Note Some of the routing protocols, for example BGP and EIGRP, cannot be deduced in the PE-Only SR, because the CE configuration file is not available.

Step 11 Analyze the configuration files, capture all the available redistribution related information, and then populate the Repository.

Step 12 Analyze a list of export and import route targets for each VRF.

Step 13 Create CERCs and CERC Membership.

Step 14 Turn on the override VRF Name and RD Flag for the MPLS VPN Link. (This information is captured from the configuration file.)

Step 15 Save the MPLS SR with the MPLS VPN Link in the Repository with a flag indicating that this service request was discovered.

Synchronization

The MPLS Service Discovery process does not synchronize existing services. If it is determined that an SR exists in the Repository for a particular interface, the Discovery process ignores the interface. But, if you have manually added a service on a new interface and ISC is not aware of it, the Service Discovery process creates the newly added service in the Repository.

CERC Creation

Given a list of Route Targets in the configuration files for each of the VRFs, the MPLS VPN Service Discovery module needs to re-create the CERC according to the ISC service model. MPLS VPN Service Discovery assumes that the services provisioned on the network are provisioned manually and do not follow the conventions adopted by ISC for topologies (CERC Route Target Allocation). As a result, a CERC created to fit into the service model supported by ISC is not associated with any VPN. You must create the VPN and associate it to the CERC created by discovery.

User Input After Discovery

After Service Discovery, a Policy and an SR are created. When a CE is discovered, a Customer-owned Policy is created. When no CE is discovered, a Provider-owned Policy and Global SR are created. After the Service Discovery process is complete, you cannot modify the relationship between the Customer and the SR. This restriction applies to both the Customer-owned and Global SRs.

The Service Discovery process ends with the newly created Service Requests in a PENDING state and the related objects in the Repository. After the completion of the Discovery process, you must go to the GUI, create the VPN, and connect the VPN with the CERC.

You cannot modify the Policy or the SR or associate an SR with a Customer or Provider at this point.

Because the CERC is a logical concept used within ISC to represent topologies, Service Discovery is unable to connect the way you have manually configured the services with CERC.

Note The configuration files that Discovery processes upload from device are logged under **$ISC_HOME/tmp/autodiscovery**.

Grey Management Discovery

This section describes the process of Grey Management Discovery.

The following steps describe the logic MPLS Service Discovery uses to create Grey Management Service Requests and populate the Repository:

Step 1 The discovery process scans the PE configuration files to determine if there is a VRF provisioned by ISC (VRF name starts with grey_mgmt_vpn).

Step 2 After finding a VRF, the discovery process scans the NPC connection table to determine if there is an NPC on that interface, and if a Managed CE (MCE) is connected to the PE on this interface.

Step 3 If an MCE is found, the discovery process scans the Route Target entries in the Management VRF for the Management CERC, and attaches it to the Management VPN.

The discovery process also caches the route target of the Management VRF.

Step 4 A Management SR with a corresponding Management Link for the MCE and PE connection is created in the Repository.

Step 5 If, when the new Links are created, Management Route Targets are found, they are ignored and the join Grey Management flag is turned on.

Layer 2 VPN Discovery

This section contains the following sections:

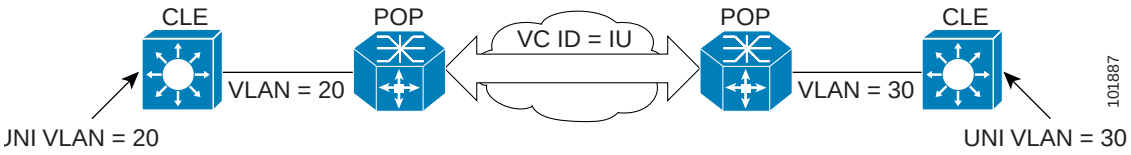
Topology

L2 VPN Discovery:

- Discovers inter-POP EWS and ERS (with No-CE) services.
- Creates all Service Requests in PENDING state. One generic VPN is generated for all discovered services.

Figure 4-129 shows the L2VPN Discovery Topology.

Figure 4-129 L2VPN Discovery Topology



Logic (MPLS Core)

The following steps describe the logic that L2VPN Service Discovery uses to create Service Requests and populate the Repository for an MPLS core:

Step 1 Gets all POPs and parses their configuration files.

Step 2 Discovers the VCs between the POPs (a pseudo wire is discovered).

Step 3 Discovers the VLAN ID that maps to the VC for each POP.

Step 4 Gets all UNIs on each POP, which is associated with a VC tunnel endpoint, and the UNIs on the associated CLE (linked via trunk mode) that allows the VLAN ID to pass.

Step 5 If there is a pair of UNIs on each side of the CORE, which shares the same VC, an SR is discovered.

Logic (L2TPv3)

L2TPv3 service discovery can be performed from Inventory Manager as described in Start Service Discovery, page 4-96.

In the case of L2TPv3, the L2VPN Service Discovery uses the following steps to create Service Requests and populate the Repository:

Step 1 Gets all POPs and parses their configuration files.

Step 2 Looks for all ATM, Serial and MFR interfaces and gets all the VCs with L2TPv3 encapsulation (for ATM the VC is under the PVC).

Step 3 Sets the interface containing the VC statement as the UNI interface.

VPLS Service Discovery

This section contains the following sections:

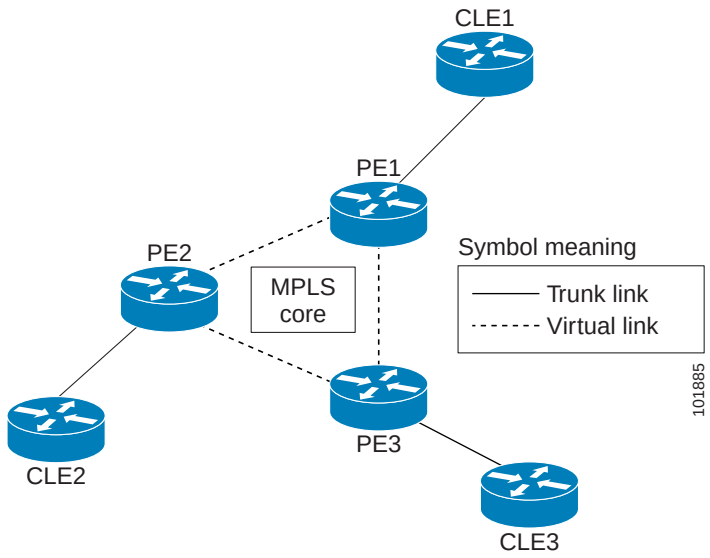
Topology

VPLS Discovery:

- Discovers only full-mesh VPLS topologies.
- Creates all Service Requests in the PENDING state.
- Creates a VPN with the name of the VPN Id for the discovered VPLS SR.

Figure 4-130 shows an MPLS core topology to help demonstrate how VPLS Service Discovery creates an SR and associates it with a VPN link.

Figure 4-130 MPLS Network



Logic

The following steps describe the logic L2VPN Service Discovery uses to create Service Requests and populate the Repository:

Step 1 Discovers virtual links that are associated with the same VPN ID among PEs across the MPLS core.

Step 2 Discovers trunk links between the PE and its associated CLEs the same way as in L2VPN.

Restrictions

Due to the existing VPLS Policy Types, VPLS Discovery has the following limitations:

- Only EWS with CE and ERS with CE, or EWS without CE and ERS without CE types of topologies can be discovered.
- EWS or ERS with a combination of CE and no CE cannot be discovered.
- Service Requests cannot be created for the above topologies.

Ring Topology Discovery (Connection Discovery)

Connection Discovery can discover ring topology NPCs. A ring of NPCs is a group of physical links that form a loop between the logical CLE devices.

Figure 4-131 shows an sample ring topology.

Figure 4-131 Sample Ring Topology