Using the Network Inventory Manager

The Network Inventory Manager allows you to create, query, modify, and delete your network inventory and provision the supported devices. It allows you to set up the download method for downloading a configuration and its authentication to a specific device.

Understanding the Network Inventory Window

The Network Inventory Manager Tree View displays a hierarchical view of the network and CPEs inventoried in the Cisco Convergent Network Solution Center: Subscriber Provisioning Repository. The inventoried objects can include:

- Network partitions in the form of subnetworks and complexes (MGX and ESR10K complexes)
- T1 CPEs (Cisco 2421, Cisco 3660, and Cisco 3810)
- Cisco 3660 Gateways
- Cisco 7200 routers
- Cisco ESR10K edge service routers

Note The Network Inventory Manager Tree View window appears when you click **Network Inventory Manager** in the CCNSC Subscriber Provisioning Control Center window.

From the Network Inventory Manager Tree View, you can create your network inventory or you can select an existing inventoried object that you want to manage. Figure 3-1 shows an expanded view of the CCNSC Subscriber Provisioning Network Inventory Manager Tree View.

Figure 3-1   Network Inventory Manager—Expanded Window
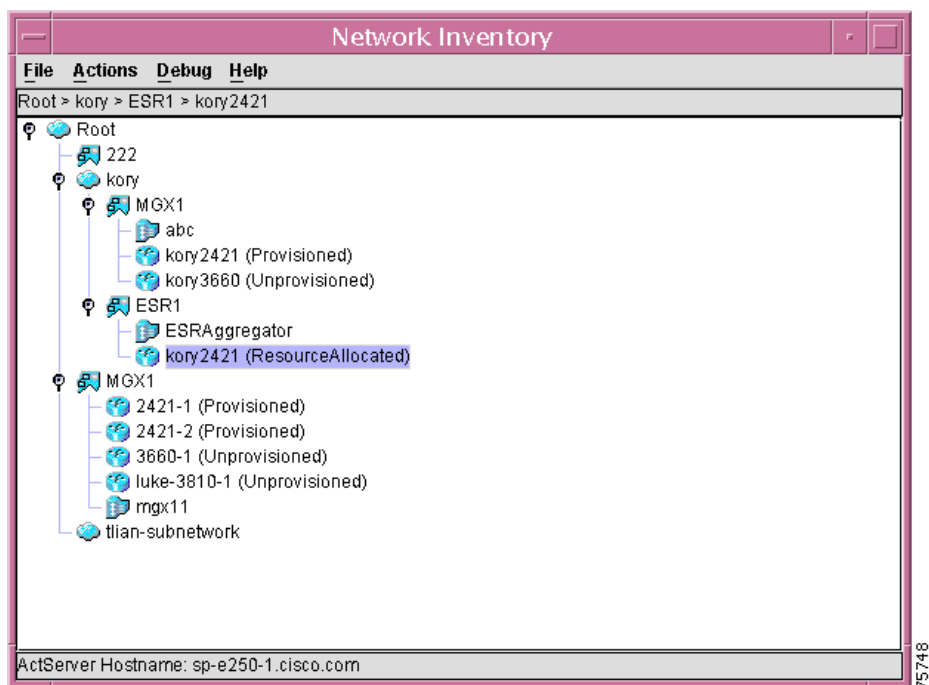
The Network Inventory window also provides the Tree View menu bar, which allows you to select various operations to perform from several drop-down menus. You can also select an operation from a context menu by right-clicking on the icon within the Tree View. The Tree View menu bar provides the following drop-down menus:

Table 3-1   Tree View Menu Options

Menu	Description
File	Allows you to close the Network Inventory Manager. The **Close** option stops the Network Inventory Manager process.
Actions	Allows you to perform the following operations: **Refresh**—provides four options: • **Refresh Tree View**—refreshes the Tree View • **Refresh Server Configuration**—refreshes the configuration of the ACT server • **Refresh Config Delivery Manager Configuration**—refreshes the configuration for the Configuration Delivery Manager • **Refresh Access Manager Configuration**—refreshes the configuration for the Access Manager. **Subnetwork**—creates subnetworks and other complexes. This option is enabled when a subnetwork is selected. **Aggregator Complex**—identifies the operations that can be performed for a selected aggregator complex. This option is enabled when an aggregator complex is enabled. **Device**—identifies all of the operations that can be performed for a selected device. This option is enabled when a device is selected. The operations that are enabled within these drop-down menus depend upon whether or not the particular network element exists. If it exists, all operations are enabled. If it does not exist, the operations are disabled and appear gray.
Debug	Allows you to set the debug level for the CCNSC Subscriber Provisioning Client and the CCNSC Subscriber Provisioning Server. For information about the possible debug levels and their meanings, see the "Setting Debug Levels" section on page 3-87.

The Network Tree shows all of the objects that are currently defined in CCNSC Subscriber Provisioning. The Network Tree uses the following conventions:

• Item in the Network Tree can be preceded by a ⊕ icon to indicate that the tree can be expanded. Click the icon to expand to the next level of the hierarchy.

  When the Network Tree first appears (or when refreshed), you must click on an item the first time for the ⊕ icon to appear. The icon remains in place for as long as the Network Tree window remains open (and unrefreshed).

  The 💡 icon indicates that you have reached the lowest level in the hierarchy for that network object. Click the icon to collapse to the previous level of the hierarchy.

• Root in the hierarchy is preceded by the 📂 icon. The root is the highest level network object and can be made up of any number of subnetworks and complexes.

• Subnetworks in the hierarchy are preceded by the ☁ icon. A subnetwork is a logical partition of your network and can optionally be made up of any number of other subnetworks and Complexes. Subnetworks are arbitrarily determined by a network administrator in order to provide a multilevel hierarchical structure.

• Complexes in the hierarchy are preceded by the 🖧 icon. A Complex is a logical partition of your network. A Complex can be created subordinate to a subnetwork or can be created to be at the same hierarchical level as a Subnetwork. A Complex is arbitrarily determined by a network administrator in order to provide a multilevel hierarchical structure.

- Aggregators in the hierarchy are preceded by the ![icon] icon. An aggregator is a device that aggregates data from a number of devices that are connected to the aggregator. An aggregator can be created subordinate to a complex.

- CPE devices in the hierarchy are preceded by the ![icon] icon. A device can be subordinate to a Subnetwork or a Complex. Devices that are subordinate to a MGX Complex are Cisco 2421s, Cisco 3810s, or Cisco 3660s. Objects that are subordinate to an ESR10K Complex are Cisco 2421s. A device defined for the subnet or a Complex can be a new device or a deployed device. A new device means that you are creating it for the first time. A deployed device is an existing device that has been provisioned outside of CCNSC Subscriber Provisioning but you want to bring it under the management of CCNSC Subscriber Provisioning. The current state of the device is shown in parentheses, such as Unprovisioned, ResourceAllocated, and Provisioned. For more information about device states and transitions, see the "Device States and Transitions" section on page 3-28. Devices are at the customer site. This is the lowest level network object displayed in the Network Tree.

- 911 Gateway, Cisco 7200, or ESR10K devices in the hierarchy are preceded by the ![icon] icon. These devices are subordinate to a Subnetwork. A device is part of the core network. This is the lowest level network object displayed in the Network Tree.

To be managed by the Network Inventory Manager, the network object must be listed in the Network Tree. If the network object is not listed, try expanding the hierarchy. If it is still not listed, it has not been inventoried in the CCNSC Subscriber Provisioning Repository. If it is a network element that you want to manage, you can create it or bring it under CCNSC Subscriber Provisioning management.

Working with the Root Node

The Root node is the highest level network object and can be made up of any number of subnetworks and complexes. The actions available for the Root node are as follows and are described in these sections:

- the "Creating a Subnetwork" section on page 3-5

- the "Creating a Complex" section on page 3-15

- the "Viewing and Modifying Telnet Gateway Properties" section on page 3-71.

Working with Subnetworks and Complexes

A subnetwork is a logical partition of your network and can optionally be made up of any number of other subnetworks. A complex is a group of devices that feed data to an ESR10K or an MGX device. Subnetworks are arbitrarily *determined* by a network administrator in order to provide a multilevel hierarchical structure. The actions available for subnetworks are as follows:

- the "Creating a Subnetwork" section on page 3-5

- the "Creating a Complex" section on page 3-15

- the "Creating New Devices" section on page 3-35

- the "Viewing and Modifying Telnet Gateway Properties" section on page 3-71

- the "Deleting a Network Object" section on page 3-81

- the "Deleting a Channel for a CPE Device" section on page 3-82.

Creating a Subnetwork

When you create a subnetwork, you are arbitrarily segmenting your network to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. You can create a subnetwork to be directly subordinate to the Root node or to another subnetwork.

Procedure

Step 1 Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2 Select **Actions > SubNetwork > Create Subnetwork** or right-click and select **Create Subnetwork** from the context menu.

The Create Subnetwork window appears, with the **Subnetwork** tab enabled, as shown in Figure 3-2.

Figure 3-2   Create Subnetwork Window

Step 3 Enter a name for the subnetwork in the **Name** field.

Step 4 Pull down the **Subnetwork Type** menu and select a subnetwork type.

You can specify the following subnetwork types:

- **Subnetwork**—select this type if you are creating a subnetwork under an existing subnetwork.

The Network Inventory Manager automatically retrieves and selects the configured values of the Parent, Configuration Delivery Servers, Call Agent, and Resource Allocation Servers from various configuration files. If more than one value is configured for a particular field, you can select from a drop-down list. The Parent and Call Agent information always have only one value, therefore, you do not need to select a value for these fields.

Step 5   Check the value for the Parent.

The parent for the network object you are creating is automatically provided for you based on the Root node or subnetwork under which you are creating this network object. This identifies the Network Inventory Manager Root as it is defined in the ACT server. The top level parent is always **/Root**. You cannot select a different value.

Step 6   Enter a name to identify the subnetwork you are creating.

Step 7   Enter the name of the domain to which this subnetwork is to belong.

A domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on organization-type or geography. This domain name must be configured to match the one defined in DNS.

Step 8   Select a Telnet Gateway from the drop-down list.

The Configuration Delivery Manager will send the configuration for downloading onto the device using this Telnet Gateway. The Network Inventory Manager retrieves this information from the **/opt/CSCOcnscs/cdm/cdm.properties** file. The Telnet Gateway method can be used for downloading configurations to devices. If you select this method, you must also define terminal server attributes and connectivity attributes.

Step 9   Select a Cisco Intelligence Engine 2100 (Cisco IE2100) Server from the drop-down list.

You are now ready to specify protocol attributes for the subnetwork.

Specifying Protocol Attributes for a Subnetwork

Step 1   Click the **Protocol** tab.

The **Protocol** tab is enabled. There are two subtabs in this window—the **ATM** tab and the **IP** tab.

Step 2   Specify ATM attributes, IP attributes, or both, depending upon the subnetwork type.

See the following sections for specific information:

- the "Specifying ATM Attributes for a Subnetwork" section on page 3-7
- the "Specifying IP Attributes for a Subnetwork" section on page 3-8.

Step 3   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes in all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for the subnetwork, see the following sections:

- the "Specifying Connectivity Attributes for a Subnetwork" section on page 3-11
- the "Specifying Terminal Server Attributes for a Subnetwork" section on page 3-13.

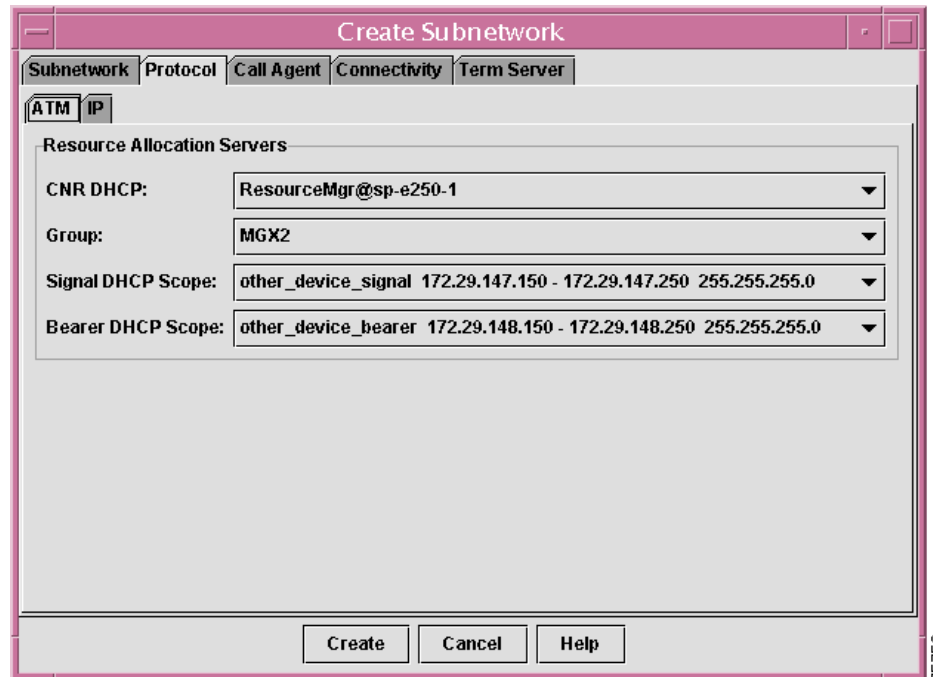**Step 4**   Click **Cancel** to close this window and return to the Tree View.

Specifying ATM Attributes for a Subnetwork

Step 1 Click the **ATM** tab.

The **ATM** tab is enabled, as shown in Figure 3-3.

Figure 3-3   Create Subnetwork - ATM Window

Step 2 Select a CNR host name from the drop-down list.

The Cisco Network Registrar provides a DHCP service and DNS. CNR clients can use CNR to obtain their IP address assignments and other configuration information through the DHCP service, and DNS is used to resolve the IP addresses to a hostname. The Network Inventory Manager retrieves this information from the **ipservice.cfg** file.

Step 3 Select a group name from the drop-down list.

The group name collectively identifies the IP addresses (IP address pools) within this subnetwork that are to be allocated for voice signaling and bearer PVCs. For example, MGX1. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 4 Select a Signal DHCP Scope from the drop-down list.

The Signal and Bearer DHCP scopes that you select must be in the same group.The Signal DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice signaling. The GUI displays the information in the following format:

<scope name> <IPaddress>-<IP address> <subnetmask>

For example:

```
signal 101.32.104.50–102.32.104.100 255.255.255.0
```
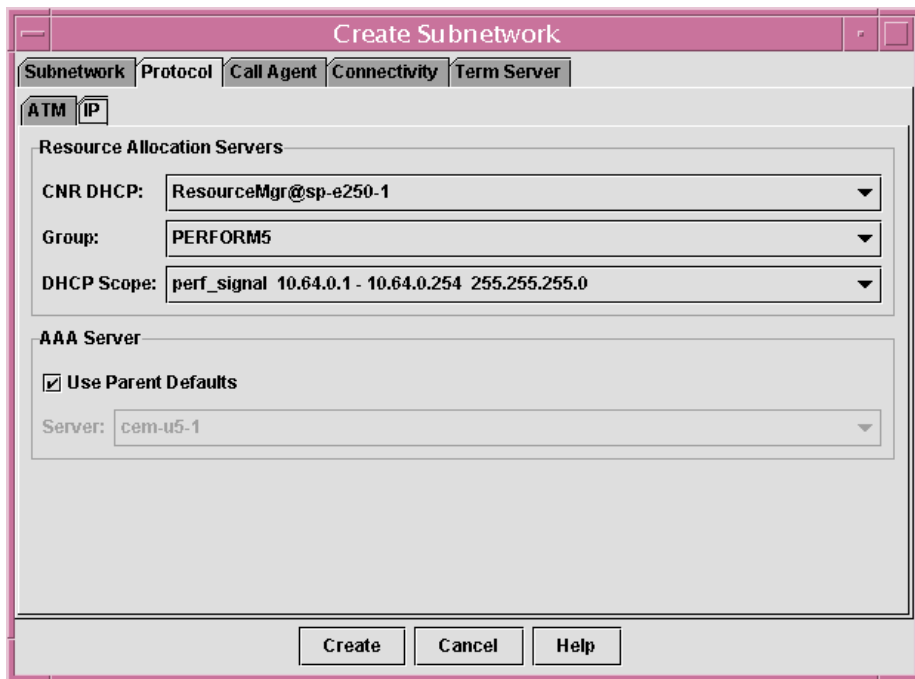
The Network Inventory Manager retrieves this information from the
/CSCOcnscs/resourceMgr/common/ipservice.cfg file.

Step 5   Select a Bearer DHCP Scope from the drop-down list.

The Signaling and Bearer DHCP scopes that you select must be in the same group. The Bearer DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice bearer. The GUI displays the information in the following format:

<scope name> <IPaddress>- <IP address> <subnetmask>

For example:

```
bearer 101.32.105.50-102.32.105.100 255.255.255.0
```

The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Specifying IP Attributes for a Subnetwork

Step 1   Click the **IP** tab.

The **IP** tab is enabled, as shown in Figure 3-4.

Figure 3-4   Create Subnetwork - IP Window

Step 2   Select a Cisco Network Registrar (CNR) host name from the drop-down list.

Cisco Network Registrar provides a DHCP service and DNS. CNR clients can use CNR to obtain their IP address assignments and other configuration information through the DHCP service while DNS is used to resolve the IP addresses to a hostname. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/resourceMgr.cfg** file.

Step 3   Select a group name from the drop-down list.

The group name collectively identifies the IP addresses (IP address pools) within this subnetwork that are to be allocated for voice signaling and bearer PVCs. For example, MGX1. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 4   Select a DHCP Scope from the drop-down list.

The DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice signaling. The GUI displays the information in the following format:

<scope name> <IPaddress>-<IP address> <subnetmask>

For example:

```
signal 101.32.104.50-102.32.104.100 255.255.255.0
```

The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 5   If you selected the PPP option during installation (you set the **Cisco AR** field to **yes**), then the AAA server section is enabled. Do one of the following:

- If you want to use the attributes of the parent node in the inventory tree, check the **Use Parent Defaults** box.
- To specify a server other than the parent, leave the checkbox unchecked and select the server name from the drop down list.

Specifying Call Agent Attributes for a Subnetwork

Step 1   Click the **Call Agent** tab.

The **Call Agent** tab is enabled, as shown in Figure 3-5.

Figure 3-5   Create Subnetwork - Call Agent Window

Step 2   Check the Call Agent information.

A call agent is an external control element that provides call control intelligence for VoIP networks. You can have only one call agent configured for your system. The call agent attributes can only be set from the root subnetwork. In all other subnetworks, call agent information is read-only.

The information is as follows:

- **IP Address**—The IP address of the Service Manager call agent. The Service Manager call agent is the external control element that uses protocols such as GCP, SGCP, and MGCP to control the Voice over IP gateways.

- **Protocol Type**—The protocol employed by the call agent to control the Voice over IP gateway. The possible values are:

    – **Media Gateway Control Protocol (MGCP)**—is used to establish, maintain, and disconnect calls over several types of bearer networks: IP and ATM networks

    – Others may be supported in the future.

- **Service Type**—The protocol employed by the call agent to control the Voice over IP gateway. The possible values are:

    – **Simple Gateway Control Protocol (SGCP)**—is used to establish, maintain, and disconnect calls over an IP network.

    – Others may be supported in the future.

- **Protocol Version**—The version of the protocol that is currently being used by the call agent.

Step 3   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes at all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for the subnetwork, see the following sections:

- Specifying Connectivity Attributes for a Subnetwork, page 3-11
- Specifying Terminal Server Attributes for a Subnetwork, page 3-13.

Step 4   Click **Cancel** to close this window and return to the Tree View.

Specifying Connectivity Attributes for a Subnetwork

The connectivity attributes are used when you are using the Telnet or Console mode to download. If you are using the Console mode to download, the applicable attributes are as follows:

- Console User ID
- Console Password.

All other connectivity attributes apply when using Telnet mode to download.

This is the second tab when creating a subnetwork.

Before You Begin

Step 1   Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2   Select **Actions > SubNetwork > Create Subnetwork** or right-click and select **Create Subnetwork** from the context menu.

The **Create Subnetwork** window appears with the **Subnetwork Attributes** tab enabled.

Follow the instructions described in the "Creating a Subnetwork" section on page 3-5.

Procedure

Step 1   Click the **Connectivity Attributes** tab.

The **Connectivity Attributes** tab is enabled, as shown in Figure 3-6.

Figure 3-6   Create Subnetwork - Connectivity Attributes Window

The Network Inventory Manager automatically retrieves the Connectivity attributes defined for the parent of the network object you are creating when the **Use Parent Defaults** checkbox is enabled. It is enabled by default. If you do not want to use the parent values, be sure the check box is disabled.

Step 2   Enter a value in the **User ID** field. This is the user ID that the system uses to establish a Telnet session with the device to be configured.

Step 3   Enter a value in the **Password** field. This is the password that the system uses to establish a Telnet session with the device to be configured.

Step 4   Enter an enable password.

The enable password depends upon the privilege level set at the router.

Step 5   Enter a value for the **Prompt Timeout** field.

The number of seconds that can elapse before a response to a router prompt is required. If this timeout expires, an error message is generated. The default is 20 seconds. This value is retrieved from the **cnscs.properties.initial** file, but you can change it at this window. If you have checked the **Use Parent Defaults** checkbox, the Network Inventory Manager retrieves this value from the object's parent.

Step 6   Enter a value for the **Operation Timeout** field.

The number of seconds that a router runtime operation has to complete. If this timeout expires, an error message is generated. The default is 240 seconds. This value is retrieved from the **cnscs.properties.initial** file, but you can change it at this window. If you have checked the **Use Parent Defaults** checkbox, the Network Inventory Manager retrieves this value from the object's parent.

Step 7   Enter a value for the **Console User ID** field.

Step 8   Enter a value for the **Console Password** field.

Step 9   Enter a value in the **Read Community String** field.

Step 10   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes at all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for your subnetwork, see the following sections:

- Creating a Subnetwork, page 3-5
- Specifying Terminal Server Attributes for a Subnetwork, page 3-13.

Step 11   Click **Cancel** to close this window and return to the Tree View.

Specifying Terminal Server Attributes for a Subnetwork

The terminal server attributes define information used only when using the Console mode to download.This is the third tab when creating a subnetwork.

Before You Begin

Step 1   Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2   Select **Actions > SubNetwork > Create Subnetwork** or right-click and select **Create Subnetwork** from the context menu.

The **Create Subnetwork** window appears with the **Subnetwork Attributes** tab enabled.

Follow the instructions described in the "Creating a Subnetwork" section on page 3-5.

Procedure

Step 1   Click the **Term Server** tab.

The **Term Server** tab is enabled, as shown in Figure 3-7.

Figure 3-7   Create Subnetwork - Term Server Attributes Window

If the **Use Parent Defaults** checkbox is enabled, the Network Inventory Manager automatically retrieves the Terminal Server attributes defined for the parent of the network object you are creating. It is enabled by default. If you do not want to use the parent values, be sure the check box is disabled.

Step 2   Enter an IP address for the Terminal Server.

Step 3   Enter a value in the **User ID** field. This is the user ID that the system uses to log in to the terminal server.

Step 4   Enter a value in the **Password** field. This is the password that the system uses to log in to the terminal server.

Step 5   Enter a value in the **Secret User Password** field.

This is the encrypted enable password on the router. If the encrypted password is not used on the router, this is the enable password.

Step 6   Enter a value in the **Port User Password** field. This must be the value that is set on the terminal server.

CCNSC SP does not support port username configuration directly.

Step 7   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes at all the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for your subnetwork, see the following sections:

- Creating a Subnetwork, page 3-5
- Specifying Connectivity Attributes for a Subnetwork, page 3-11.

Step 8   Click **Cancel** to close this window and return to the Tree View.

Creating a Complex

When you create a complex, you are arbitrarily segmenting your network to provide a multilevel, hierarchical routing structure while shielding the complex from the addressing complexity of attached networks. You can create a complex to be directly subordinate to the Root node or a subnetwork.

Procedure

Step 1   Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2   Select **Actions>SubNetwork>Create Complex** or right-click and select **Create Complex** from the context menu.

The Create Complex window appears, with the **IP Aggregator Complex** tab enabled, as shown in Figure 3-8.

Figure 3-8   Create Complex - IP Aggregator Complex Window

Step 3   Pull down the **Complex Type** menu and select a complex type.

You can select the following complex types:

- **MGX**—creates an MGX complex
- **ESR10K**—creates an ESR10K complex.

The Network Inventory Manager automatically retrieves and selects the configured values of the Parent, Configuration Delivery Servers, Call Agent, and Resource Allocation Servers from various configuration files. If more than one value is configured for a particular field, you can select from a drop-down list. The Parent and Call Agent information always have only one value, therefore you will not need to select a value for these fields.

If you selected an MGX complex, the **FR Aggregator Complex** tab appears.

If you selected an ESR10K complex type, the **IP Aggregator Complex** tab appears.

Step 4   Check the value for the Parent.

The parent for the network object you are creating is automatically provided for you based on the Root node or subnetwork under which you are creating this network object. This identifies the Network Inventory Manager Root as it is defined in the ACT server. The top level parent is always **/Root**. You cannot select a different value.

Step 5   Enter a name to identify the complex you are creating.

Step 6   Enter the name of the domain to which this complex is to belong.

A domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on organization-type or geography. This domain name must be configured to match the one defined in DNS.

Step 7   Select a Telnet Gateway from the drop-down list.

The Configuration Delivery Manager will send the configuration for downloading onto the device using this Telnet Gateway. The Network Inventory Manager retrieves this information from the **cdm.properties** file in the **/opt/CSCOcnscs/cdm** directory. The Telnet Gateway method can be used for downloading configurations to devices. If you select this method, you must also define terminal server attributes and connectivity attributes.

Step 8   Select a Cisco IE2100 Server from the drop-down list

You are now ready to specify aggregator attributes.

Specifying Aggregator Attributes

Step 1   Click the **Aggregator** tab.

The **Aggregator** tab is enabled.

Step 2   Enter a name for the Aggregator.

This name must be unique among all inventoried aggregators. If you specify a name that is not unique, an error message is returned.

Step 3   If you are creating an ESR10K complex, specify an IP address for the aggregator.

Step 4   Enter a Location for the aggregator (optional).

Step 5   Click **Create** to update the information in this window or specify other attributes for your complex.

Clicking **Create** saves attributes for all tabs and closes the window.

Step 6   Click **Cancel** to close this window and return to the Tree View.
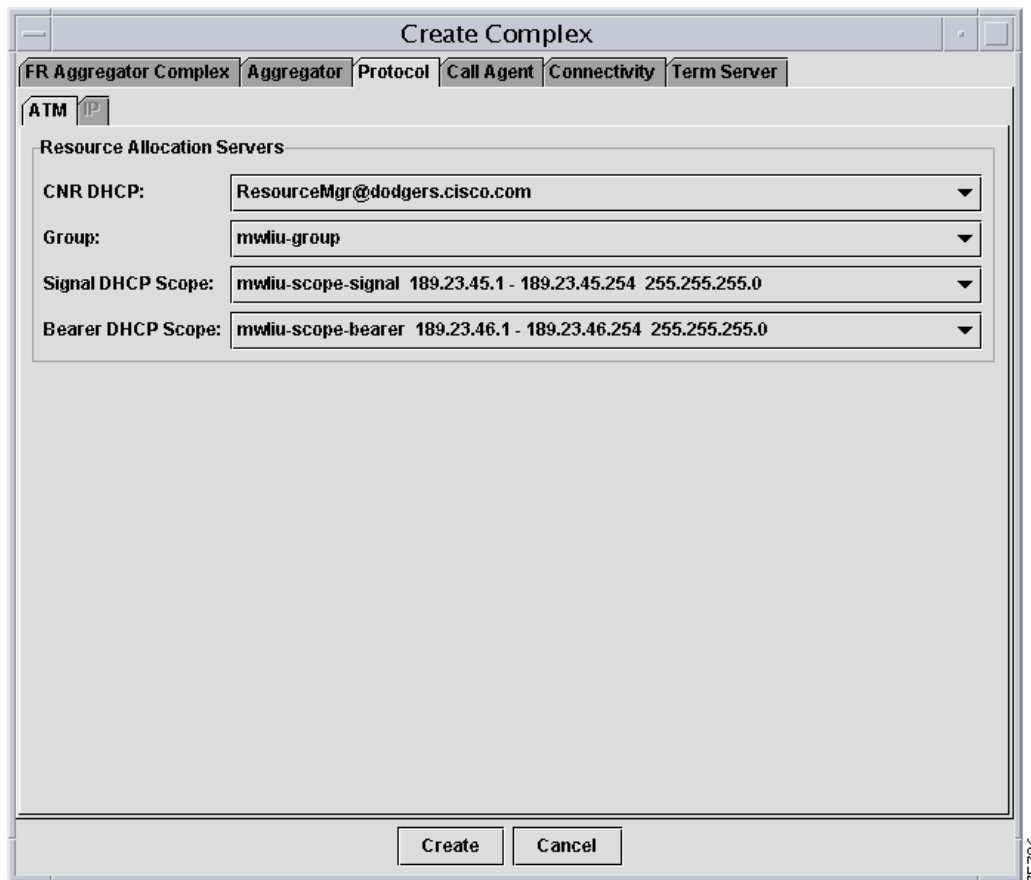
Specifying Protocol Attributes for a Complex

Step 1   Click the **Protocol** tab.

The **Protocol** tab is enabled. There are two subtabs in this window—the **ATM** tab and the **IP** tab. If the complex type is **ESR10K**, only the **IP** tab is enabled. If the complex type is **MGX**, only the **ATM** tab is enabled.

Step 2   Specify ATM attributes or IP attributes, depending upon the complex type.

See the following sections for specific information:

- the "Specifying ATM Attributes for a Subnetwork" section on page 3-7
- the "Specifying IP Attributes for a Subnetwork" section on page 3-8.

Step 3   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes in all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for the subnetwork, see the following sections:

- the "Specifying Connectivity Attributes for a Subnetwork" section on page 3-11
- the "Specifying Terminal Server Attributes for a Subnetwork" section on page 3-13.

Step 4   Click **Cancel** to close this window and return to the Tree View.

Specifying ATM Attributes for a Complex

Step 1   Click the **ATM** tab.

The **ATM** tab is enabled, as shown in Figure 3-9.

Figure 3-9   Create Subnetwork - ATM Window

Step 2   Select a CNR host name from the drop-down list.

The Cisco Network Registrar provides a DHCP service and DNS. CNR clients can use CNR to obtain their IP address assignments and other configuration information through the DHCP service while DNS is used to resolve the IP addresses to a hostname. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ResourceMgr.cfg** file.

Step 3   Select a group name from the drop-down list.

The group name collectively identifies the IP addresses (IP address pools) within this subnetwork that are to be allocated for voice signaling and bearer PVCs. For example, MGX1. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 4   Select a Signal DHCP Scope from the drop-down list.

The Signal and Bearer DHCP scopes that you select must be in the same group.The Signal DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice signaling. The GUI displays the information in the following format:

<scope name> <IPaddress>-<IP address> <subnetmask>

For example:

```
signal 101.32.104.50-102.32.104.100 255.255.255.0
```

The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 5   Select a Bearer DHCP Scope from the drop-down list.

The Signaling and Bearer DHCP scopes that you select must be in the same group.The Bearer DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice bearer. The GUI displays the information in the following format:

<scope name> <IPaddress>- <IP address> <subnetmask>

For example:

```
bearer 101.32.105.50–102.32.105.100 255.255.255.0
```

The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Specifying IP Attributes for a Complex

Step 1   Click the **IP** tab.

The **IP** tab is enabled, as shown in Figure 3-10.

Figure 3-10   Create Subnetwork Window - IP

Step 2 Select a CNR host name from the drop-down list.

The Cisco Network Registrar provides a DHCP service and DNS. CNR clients can use CNR to obtain their IP address assignments and other configuration information through the DHCP service, and DNS is used to resolve the IP addresses to a hostname. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ResourceMgr.cfg** file.

Step 3 Select a group name from the drop-down list.

The group name collectively identifies the IP addresses (IP address pools) within this subnetwork that are to be allocated for voice signaling and bearer PVCs. For example, MGX1. The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 4 Select a DHCP Scope from the drop-down list.

The DHCP scope identifies the name of the IP address pool, IP address range, and subnet mask that are to be used for IP address allocation for voice signaling. The GUI displays the information in the following format:

<scope name> <IPaddress>-<IP address> <subnetmask>

For example:

```
signal 101.32.104.50-102.32.104.100 255.255.255.0
```

The Network Inventory Manager retrieves this information from the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file.

Step 5 If you selected the PPP option during CCNSC SP installation (you set the **Cisco AR** field to **yes**), then the AAA server section is enabled. Do one of the following:

- If you want to use the attributes of the parent node in the inventory tree, check the **Use Parent Defaults** box.

- To specify a server other than the parent, leave the checkbox unchecked and select the server name from the drop down list.

Specifying Call Agent Attributes

Step 1 Click the **Call Agent** tab.

The **Call Agent** tab is enabled, as shown in Figure 3-11.

Figure 3-11   Create Subnetwork - Call Agent Window

Step 2 Check the Call Agent information.

A call agent is an external control element that provides call control intelligence for VoIP networks. You can have only one call agent configured for your system. The call agent attributes can only be set from the root subnetwork. In all other subnetworks, call agent information is read-only.

The information is as follows:

- **IP Address**—The IP address of the Service Manager call agent. The Service Manager call agent is the external control element that uses protocols such as GCP, SGCP, and MGCP to control the Voice over IP gateways.

- **Protocol Type**—The protocol employed by the call agent to control the Voice over IP gateway. The possible values are:
    - **Media Gateway Control Protocol (MGCP)**—is used to establish, maintain, and disconnect calls over several types of bearer networks: IP and ATM networks
    - Others may be supported in the future.

- **Service Type**—The protocol employed by the call agent to control the Voice over IP gateway. The possible values are:
    - **Simple Gateway Control Protocol (SGCP)**—is used to establish, maintain, and disconnect calls over an IP network.
    - Others may be supported in the future.

- **Protocol Version**—The version of the protocol that is currently being used by the call agent.

Step 3   Click **Create** to update the information in this window or specify other attributes for your complex.

Clicking **Create** saves attributes at all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for the subnetwork, see the following sections:

- Specifying Connectivity Attributes for a Subnetwork, page 3-11
- Specifying Terminal Server Attributes for a Subnetwork, page 3-13.

Step 4   Click **Cancel** to close this window and return to the Tree View.

Specifying Connectivity Attributes for a Complex

The connectivity attributes are used when you are using the Telnet or Console mode to download. If you are using the Console mode to download, the applicable attributes are as follows:

- Console User ID
- Console Password

All other connectivity attributes apply when using Telnet mode to download.

This is the second tab when creating a subnetwork.

Before You Begin

Step 1   Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2   Select **Actions > SubNetwork > Create Complex** or right-click and select **Create Complex** from the context menu.

The **Create Complex** window appears with the **Subnetwork Attributes** tab enabled.

Follow the instructions described in the "Creating a Subnetwork" section on page 3-5.

Procedure

Step 1   Click the **Connectivity** tab.

The **Device Connectivity Attributes** tab is enabled, as shown in Figure 3-12.

Figure 3-12   Create Subnetwork - Connectivity Attributes Window

The Network Inventory Manager automatically retrieves the Connectivity attributes defined for the parent of the network object you are creating when the **Use Parent Defaults** checkbox is enabled. It is enabled by default. If you do not want to use the parent values, be sure the check box is disabled.

Step 2   Enter a value in the **User ID** field. This is the user ID that the system uses to establish a Telnet session with the device to be configured.

Step 3   Enter a value in the **Password** field. This is the password that the system uses to establish a Telnet session with the device to be configured.

Step 4   Enter an enable password.

The enable password depends upon the privilege level set at the router.

Step 5   Enter a value for the **Prompt Timeout** field.

The number of seconds that can elapse before a response to a router prompt is required. If this timeout expires, an error message is generated. The default is 20 seconds. This value is retrieved from the **cnscs.properties** file, but you can change it at this window. If you have checked the **Use Parent Defaults** checkbox, the Network Inventory Manager retrieves this value from the object's parent.

Step 6   Enter a value for the **Operation Timeout** field.

The number of seconds that a router runtime operation has to complete. If this timeout expires, an error message is generated. The default is 240 seconds. This value is retrieved from the **cnscs.properties** file, but you can change it at this window. If you have checked the **Use Parent Defaults** checkbox, the Network Inventory Manager retrieves this value from the object's parent.

Step 7   Enter a value for the **Console User ID** field.

Step 8   Enter a value for the **Console Password** field.

Step 9   Enter a value in the **Read Community String** field.

Step 10   Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes at all of the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for your subnetwork, see the following sections:

- Creating a Complex, page 3-15
- Specifying Connectivity Attributes for a Complex, page 3-22.

Step 11   Click **Cancel** to close this window and return to the Tree View.

Specifying Terminal Server Attributes for a Complex

The terminal server attributes define information used only when using the Console mode to download.This is the third tab when creating a complex.

Before You Begin

Step 1   Select the Root node or subnetwork from the Tree View that you want this subnetwork to be created under.

Step 2   Select **Actions > SubNetwork > Create Complex** or right-click and select **Create Complex** from the context menu.

The **Create Complex** window appears with the **IP Aggregator Attributes** tab enabled.

Follow the instructions described in the "Creating a Subnetwork" section on page 3-5.

Procedure

Step 1   Click the **Term Server Attributes** tab.

The **Term Server Attributes** tab becomes enabled, as shown in Figure 3-13.

Figure 3-13   Create Subnetwork - Term Server Attributes Window

If the **Use Parent Defaults** checkbox is enabled, the Network Inventory Manager automatically retrieves the Terminal Server attributes defined for the parent of the network object you are creating. It is enabled by default. If you do not want to use the parent values, be sure the check box is disabled.

Step 2   Enter an IP address for the Terminal Server.

Step 3   Enter a value in the **User ID** field. This is the user ID that the system uses to log in to the terminal server

Step 4   Enter a value in the **Password** field. This is the password that the system uses to log in to the terminal server

Step 5   Enter a value in the **Secret User Password** field.

This is the encrypted enable password on the router. If the encrypted password is not used on the router, this is the enable password.

Step 6   Enter a value in the **Port User Password** field. This must be the value that is set on the terminal server.

CCNSC SP does not support port username configuration directly.

Step 7 Click **Create** to update the information in this window or specify other attributes for your subnetwork.

Clicking **Create** saves attributes at all the tabs and closes the window. Only the fields in the **Subnetwork Attributes** tab are required to create a subnetwork. If you wish to fill in values for other tabs, wait to click **Create** until you have filled them all in.

To specify other attributes for your subnetwork, see the following sections:

- Creating a Complex, page 3-15
- Specifying Connectivity Attributes for a Complex, page 3-22.

Step 8 Click **Cancel** to close this window and return to the Tree View.

Viewing and Modifying Subnetwork or Complex Properties

You can view and modify the currently configured properties of a subnetwork or a complex. The Network Inventory Manager automatically retrieves the configured subnetwork, connectivity, and terminal server attributes.

The interface for viewing and modifying subnetwork properties is identical to the interface for creating subnetworks, except that the Name field is not editable and the Aggregator tab is not included.

For information on Aggregator properties see the "Specifying Protocol Attributes for a Subnetwork" section on page 3-6.

Viewing and Modifying Aggregator Properties

You can view and modify the currently configured properties of an aggregator associated with a Aggregator Complex. The Network Inventory Manager automatically retrieves the configured aggregator attributes.

Procedure

Step 1 Select an Aggregator Complex from the Tree View.

Step 2 Select **Actions > Device > Properties** or right-click and select **Properties** from the context menu.

The Aggregator Properties window appears, as shown in Figure 3-14, with the **Aggregator Attributes** tab enabled. The window for both ESR10K and MGX aggregators is similar, however, in the window for the MGX, the IP address is optional.

Figure 3-14   Aggregator Properties - Aggregator Window

If you want to change the connectivity attributes for this aggregator, click the **Connectivity** tab. The Aggregator Properties window now displays the connectivity properties, as shown in Figure 3-15.

Figure 3-15   Aggregator Properties - Connectivity Window

Once you have created an aggregator, you can modify its attributes. For detailed information about these attributes, see the "Specifying Protocol Attributes for a Subnetwork" section on page 3-6 and the "Specifying Connectivity Attributes for a Subnetwork" section on page 3-11.

Step 3   Click **OK** or **Apply** to update the information in this window or **Cancel** to cancel changes you have made

You are returned to the Tree View.

Working with Devices

CCNSC Subscriber Provisioning supports T1 CPEs used with Voice over IP over T1 solutions and, in addition, supports provisioning of the following devices:

- Cisco 3660s used with 911 gateways
- Cisco ESR10K edge service routers
- Cisco 7200s

You can create devices at the Network Inventory Manager windows to be managed by CCNSC Subscriber Provisioning (new CPEs), or you can select existing provisioned devices to be managed by CCNSC Subscriber Provisioning (CPEs deployed only in an ESR10K complex). The actions available for the devices depend upon the device type. The following sections indicate the specific actions available for a device type:

- the "Creating New Devices" section on page 3-35
- the "Adding a Service to a New CPE" section on page 3-37.

When configuring devices, it may be useful to understand the states and state transitions for the devices. Seethe "Device States and Transitions" section on page 3-28 for more information.

Device States and Transitions

CCNSC Subscriber Provisioning supports several states for an ESR10K complex or an MGX complex. In addition, CCNSC Subscriber Provisioning defines the states a device can transition to and from.

Devices in an ESR10K complex can be in only one of the following states at any given time:

- **Unprovisioned**—resources have not been allocated for the CPE and the CPE has not been configured with voice and/or data service. However, the CPE may have some partial configuration (for example, connectivity for the management interface) or it may be up and running (that is, its operational state can be "up").

- **ResourceAllocated**—resources for voice and/or data service have been allocated and reserved for the CPE, however, the CPE has not been configured for voice and/or service. This means that CCNSC Subscriber Provisioning or the OSS has assigned an IP address and FQDN for signaling and IP address for bearer.

- **Provisioned**—full configuration, including voice service, for the CPE has been generated and delivered through a router console or though Telnet. The CPE may or may not be up running. This means the CPE's operational state may be "up", ready for voice, or "down", the configuration file has been generated and is waiting to be downloaded.

Figure 3-16 shows the state transitions for devices in an ESR10K complex.

Figure 3-16   State Transitions for Devices in an ESR10K Complex
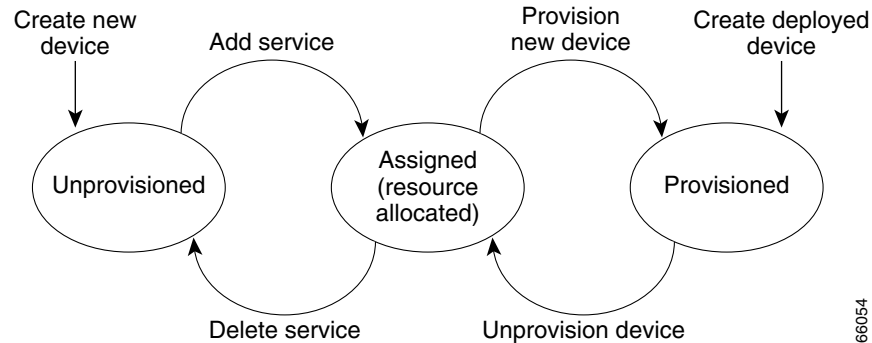
If you are provisioning the device using a Cisco IE2100, there is one additional state, as shown in Figure 3-17.

- **PendingProvisioned**—Provisioning is pending download of the configuration from the Cisco IE2100 device.

Figure 3-17   State Transitions for Devices in an ESR10K Complex (with Cisco IE2100 Provisioning)
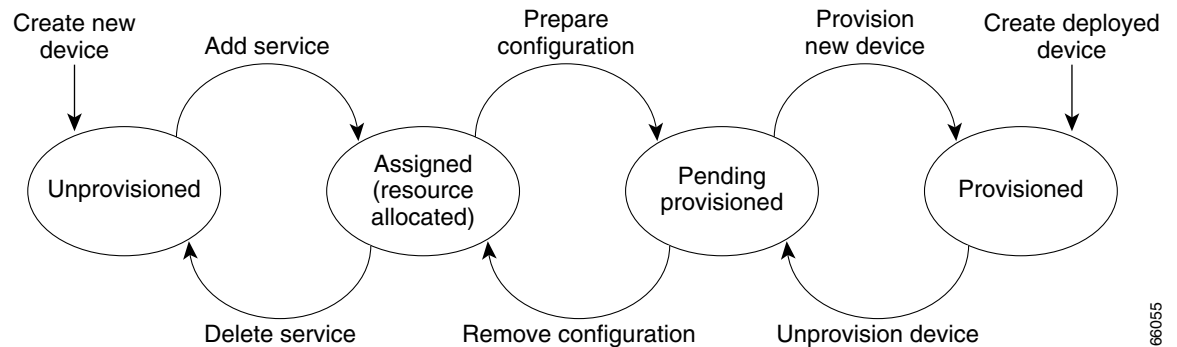
The devices in an MGX complex can have two additional states:

- **Channel resources allocated**—Channels have been allocated for the device but have not yet been provisioned.
- **Channels provisioned**—Channels have been allocated and provisioned.

Figure 3-18 shows a state diagram for devices in an MGX complex.

Figure 3-18   State Transitions for Devices in an MGX Complex
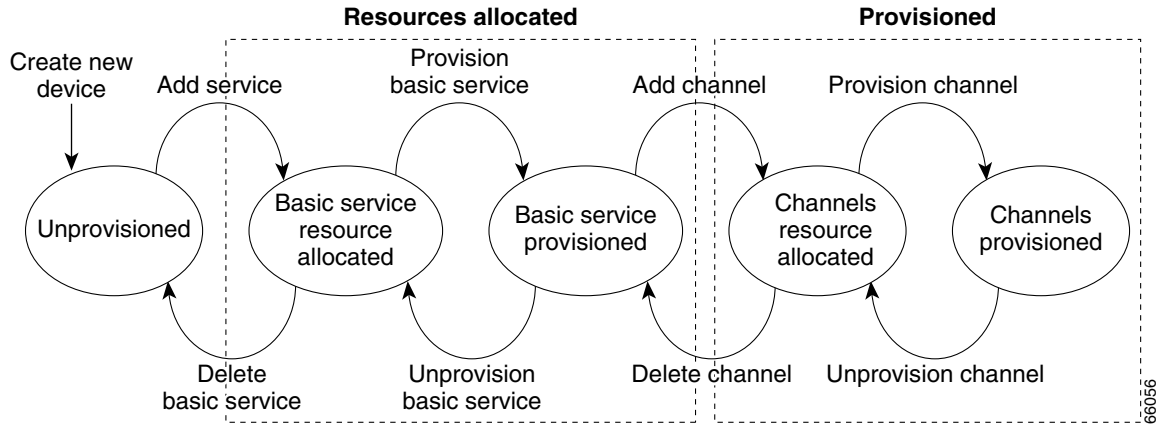
Table 3-2 lists and describes the state transitions supported in CCNSC Subscriber Provisioning.

Table 3-2   Supported CPE State Transitions

From State	To State	Description
external unprovisioned CPE	Unprovisioned CPE in CCNSC Subscriber Provisioning (Unprovisioned)	This state transition allows a new CPE (unprovisioned) to be added to the CCNSC Subscriber Provisioning inventory. CCNSC Subscriber Provisioning creates a CPE object in its inventory with these attributes: • Subscriber ID (optional) • device type and model: CPE, T1 CPE • device name • Subnetwork names: for example, region, site, central office where the CPE belongs.
Unprovisioned	Assigned CPE (ResourcesAllocated)	This state transition allocates and reserves resources for the CPE. The resources allocated depend upon the service type. For voice signaling PVC, CCNSC Subscriber Provisioning allocates and reserves IP addresses in DHCP and updates DNS. The DNS update may take time, therefore, a CPE may not be in the "Assigned" state until FQDNs are updated. If successful, CCNSC Subscriber Provisioning updates the CPE object with these attributes: • Service features: for example, Voice and data service, NAT, DHCP, CHAP • Service request number (optional) • Management • IP address • Subnet mask • Scope • FQDN • ESR port • T1 framing • T1 channel group • T1 line code • T1 channel group speed

Table 3-2   Supported CPE State Transitions (continued)

From State	To State	Description
		• Data
		• Element IP address
		• Element subnet mask
		• DHCP
		– Domain name
		– Start IP address
		– End IP address
		• NAT
		• CHAP
		If the DNS update fails, an error message is logged and displayed in the GUI; you will be required to fix the DNS problem. Note, upon failure, IP addresses allocated by CCNSC Subscriber Provisioning are deallocated (rolled back), and the CPE will remain in the "Unprovisioned" state.
Assigned CPE	Provisioned CPE (Provisioned)	This state transition generates the configuration file using the allocated resources, downloads and applies the configuration to the CPE, and places the CPE in the Provisioned state. CCNSC Subscriber Provisioning also updates the CPE object with these attributes: operation (create/update/delete) Template data

Table 3-2   Supported CPE State Transitions (continued)

From State	To State	Description

external deployed CPE	provisioned CPE in CCNSC Subscriber Provisioning
	
	(Provisioned)
		This state transition allows a deployed CPE (that is a CPE provisioned outside of CCNSC Subscriber Provisioning) to be introduced into its inventory. The CPE's operational state is "up". When a deployed CPE is introduced to CCNSC Subscriber Provisioning, CCNSC Subscriber Provisioning creates a CPE object with attributes you provide at the relevant GUI windows and keeps the object in its persistent store:
		
		• Service features: for example, Voice and data service, NAT, DHCP, CHAP
		
		• Service request number (optional)
		
		• Management
		
		• IP address
		
		• Subnet mask
		
		• Scope
		
		• FQDN
		
		• ESR port
		
		• T1 framing
		
		• T1 channel group
		
		• T1 line code
		
		• T1 channel group speed
		
		• Data PVC (if present)
		
		• Element IP address
		
		• Element subnet mask
		
		• DHCP
		  – Domain name
		  – Start IP address
		  – End IP address
		
		• NAT
		
		• CHAP
		
		• template data

provisioned CPE	assigned CPE	This state transition removes the configuration related to voice/data services from the CPE. CCNSC Subscriber Provisioning generates the configuration file and delivers it to the CPE.

Table 3-2   Supported CPE State Transitions (continued)

From State	To State	Description
assigned CPE	Unprovisioned CPE	This state transition deallocates resources used by the CPE, that is, it deallocates IP addresses from DHCP, and updates DNS. If DNS updates fail, an error message will be logged and displayed in the GUI, which will require you to to fix DNS problem. The CPE will transition to the Unprovisioned state.
unprovisioned CPE	deleted CPE	This state transition removes a CPE object from CCNSC Subscriber Provisioning. The CPE's configuration files are also deleted from the FTP server.

Working with New Devices

A new device is a T1 CPE for an MGX complex (a Cisco 3660, Cisco 2421, or Cisco 3810 CPE device), a T1 device for and ESR10K complex, or a new device for a subnetwork (a 911 Gateway, ESR10K, or Cisco 7200) that you are creating in the Network Inventory Manager. You can provision T1 CPEs. The 911 gateway provides gateway service to 911 servers, which are designed to handle emergency 911 calls. You must use the Telnet Gateway download method for 911 gateways, Cisco 7200s, and ESR10K routers.

Note   The 911 server is not a Cisco product. For more information about this server, refer to the product documentation provided by your vendor.

The actions available for New CPE devices are as follows:

- "Creating New Devices" section on page 3-35
- "Adding a Service to a New CPE" section on page 3-37
- "Provisioning a New CPE Device for an ESR10K Complex" section on page 3-67
- "Viewing CPE Properties" section on page 3-72
- "Viewing and Modifying Element Properties" section on page 3-73
- "Generating and Downloading a Configuration File to a CPE" section on page 3-76
- "Downloading a Configuration Using a Telnet Gateway" section on page 3-79
- "Deleting a Network Object" section on page 3-81
- "Deleting Provisioning of CPE Device" section on page 3-81
- "Deleting a Service for a CPE Device" section on page 3-82

Creating New Devices

Before You Begin

- You can create T1 CPE devices only under an MGX complex or an ESR10K complex. Before you do this, you must first create an MGX complex or an ESR10K complex.

- You can create 911 Gateway objects, ESR10K objects, or Cisco 7200 objects only under a subnetwork. Therefore, you must first create a subnetwork as described in "Creating a Subnetwork" section on page 3-5.

Procedure

Step 1   Select the subnetwork, MGX complex, or ESR10K complex from the Tree View that you want this device to be created under.

Step 2   Do one of the following:

- If you are creating a device under an MGX complex or an ESR complex, select **Actions > Aggregator Complex > Create New Device** or right-click and select **Create New Device** from the Subnetwork context menu

- If you are creating a device under a subnetwork, select **Actions > SubNetwork > Create New Device** or right-click and select **Create New Device** from the **Subnetwork** context menu.

The Create New Device window appears.

Figure 3-19 shows the Create New Device window for T1 CPE devices.

Figure 3-19   Create New Device Dialog Box for a T1 CPE Device
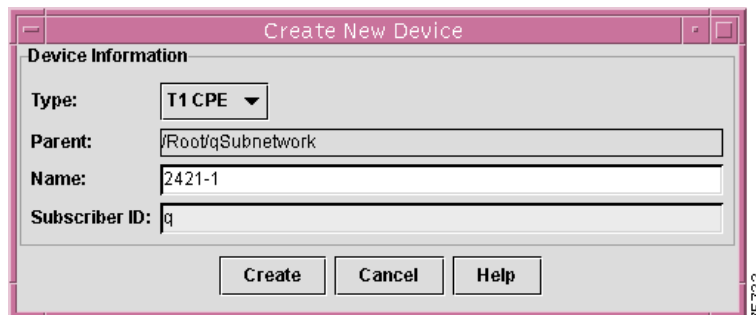
Figure 3-20 shows the Create New Device window for 911 Gateway, ESR10K, and Cisco 7200 devices.

Figure 3-20   Create New Device Dialog Box for 911 Gateway, ESR10K, or Cisco 7200

Step 3   Select a device type from the drop-down list.

The types listed in the drop-down list depend upon whether you are creating the device under a subnetwork or a Aggregator Complex. You can create the following device types:

- T1 CPE— CPE that can be created only under an MGX complex or an ESR10K complex. Under an ESR10K complex you can create only a Cisco 2421 device; under an MGX complex you can create a Cisco 3660, Cisco 2421, or Cisco 3810 T1 device.
- Device—911 Gateway that can be created only under a subnetwork.
- ESR10K—Cisco ESR10K edge services router that can be created only under a subnetwork.
- 7200—Cisco 7200 device that can be created only under a subnetwork.

Step 4   Enter a value in the **Name** field.

This name uniquely identifies the device throughout its subnetwork. If a device with this name already exists, an error is returned and an entry is created in the log file.

Step 5   Enter a value in the **Subscriber ID** field.

This is an arbitrary number that provides a unique ID to a subscriber. It does not apply to 3660s. This ID can be used to track log information in the Log Viewer. This field is optional. For information about using the Log Viewer, see Chapter 6, "Using the Log Viewer."

Step 6   For a 3660 device, ESR10K device, or Cisco 7200, also specify an IP address and an (optional) location

The location helps you to identify the physical site of the 3660 device, for example, San Jose-Bldg 3. This is informational only and has no effect on the operation of the device.

Step 7   Click **Create** to create the device or **Cancel** to close this window and return to the Tree View.

When you create a CPE device, it appears in the Tree View and is followed with (Unprovisioned) to indicate that this device has not been provisioned or had resources allocated for it.

For more information about device states and transitions between them, see "Device States and Transitions" section on page 3-28.

Note   An error window appears if you did not supply information in all of the required fields.

Proceed to "Adding a Service to a New CPE" to continue provisioning the new T1 CPE.

Adding a Service to a New CPE

When you add a service to a new CPE, you identify the service that you want for this particular device and you allocate IP addresses from the specified scope (IP address pool). The possible voice and data selections are:

- Voice and Data
- Voice
- Data

The interface for adding a service varies depending upon which type of device you are adding and whether you are adding it to an MGX complex or an ESR10K complex. You can add services for the following devices in the following contexts:

- **T1 CPE (3660 under an MGX complex**—Go to the "Adding a Service to a 3660 in an MGX Complex" section on page 3-37 for specific instructions.
- T**1 CPE (2421) or T1 CPE (3810) under an MGX complex**— Go to the "Adding a Service to a Cisco 2421 or a Cisco 3810 in an MGX Complex" section on page 3-48 for specific instructions.
- **T1 CPE (2421) under an ESR10K complex**—Go to the "Adding a Service to a 2421 in an ESR10K Complex" section on page 3-59 for specific instructions.

The following sections describe adding services for particular devices.

Adding a Service to a 3660 in an MGX Complex

Before You Begin

- You create 3660 T1 CPE devices under an MGX complex. Therefore, you must first create a MGX complex as described in the "Creating a Complex" section on page 3-15.
- You must first create a new CPE device as described in "Creating New Devices" section on page 3-35.

Adding a Basic Service for a 3660 CPE Device

Step 1   From the Tree View, select the newly created 3660 T1 device.

Step 2   Select **Actions > Device > Add Basic Service** or right-click and select **Add Service** from the **Device** context menu.

An Add Service window appears, with the **Port Info** tab enabled, as shown in Figure 3-21.

Figure 3-21   Add Basic Service - Port Info Window

The Service Request Info that displays at this window corresponds with the information you specified at the Create New Device window. For more information about these fields, see the "Creating New Devices" section on page 3-35.

Step 3   Make a voice and data selection for this device from the drop down list.

T1 CPEs support the following voice and data selections:

- Voice and Data—signaling and bearer plus data
- Voice—signaling and bearer
- Data—data only.

✎

Note   If you select the Data service for this CPE, voice services are disabled.

Step 4   Enter slot and port information for the device.

a.   Click the checkbox under **Slot#** for the slots in which you have cards installed. After you click the checkbox, default port information appears.

b.   Click on the **Num Ports** field for each slot you are configuring and select the number of ports from the pull down menu. You can specify 4 ports or 8 ports for each card.

c.   In the port number fields for each selected slot, assign an IMA number.

Step 5   Click the **Device** tab.

The **Device** tab is enabled, as shown in Figure 3-22.

Figure 3-22   Add Basic Service - Devices Window

For each slot that you have enabled, specify the following information:

- **IP Address**—IP address of the PVC.
- **Subnet Mask**—subnet mask for the PVC.
- **PVC VPI/VCI**—virtual path identifier/virtual connection identifier. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transit on its way to its final destination. These are required fields.

Step 6   Click the **Allocate and Preview Download** button.

The Configuration File Generation window appears. This window shows router configuration commands that have been generated based upon the configuration options you selected.

Step 7   Edit the commands shown in the Configuration File Generation window as required.

Step 8   Do one of the following:

- If you want to save the configuration to a file for later use, click the **Save** button and then specify the path and filename for the file in which you want to save the configuration.
- If you are ready to download the configuration, click the **Download** button.
- To abandon the configuration, click the **Cancel** button.

If the IP address you specified is incorrect or unreachable, an error message appears.

If you cancel the configuration, the device is marked as **ResourceAllocated** in the Tree View.

The device is now in the Provisioned state.

Adding a Channel for a 3660 CPE Device

Once you have added basic service for the 3660 device, you can provision voice and data channels.

Step 1   Select the device to provision in the Tree View.

Step 2   Select **Actions>Device>Add Channels** or select **Add Channels** from the **Device** context menu.

The **Add Channels** window appears, as shown in Figure 3-23.

Figure 3-23   Add Channels Window

Step 3   To add voice channels, click the **Voice Channels** tab.

The **Add Channels** window for voice channels appears, as shown in Figure 3-24.

Figure 3-24   Add Channels - Voice Channels Window

Channels for which resources have been allocated but which have not been provisioned are highlighted in blue. Provisioned channels appear in black.

Step 4   To add a voice channel, click the **Add Signalling/Bearer Channel** button.

The Signal and Bearer Channel Entry window appears, as shown in Figure 3-25.

Figure 3-25   Signal and Bearer Channel Entry Window

If you are using Cisco Network Registrar, then CNR will update the signalling IP address to the value assigned by CNR's Domain Name Service (DNS) server. Make sure that the IP address is set up properly to allow DNS update in the CNR server.

The back end processor will only use the information that you specify in the **Signal Channel** area of the window; however, you must still specify information in the fields in the **Bearer Channel** area of the window.

Complete these steps to specify signal channel information:

a. If you want the system to generate the IP address, subnet mask, and FQDN for the signal channel, check the **Auto Assign Addresses** checkbox.

b. If you want to manually assign information to identify the signal channel, specify the following information:

   – **IP address**—Enter the IP address for the channel.

   – **Subnet mask**—Enter the subnet mask for the channel.

   – **FQDN**—Enter the Fully Qualified Domain Name for the channel.

c. Enter the VPI and VCI for the signal channel.

d. In the QoS field for the signal channel, pull down the QoS menu and select a QoS type for the signal channel.

   You can select the following QoS types:

   – UBR

   – UBR+

   – VBR-rt

> – VBR-nrt
>
> – CBR
>
> – ABR

e. In the **QoS** field for the bearer channel, pull down the **QoS** menu and select a QoS type for the bearer channel.

You can select the following QoS types:

> – UBR
>
> – UBR+
>
> – VBR-rt
>
> – VBR-nrt
>
> – CBR
>
> – ABR

f. Enter the following information for the bearer channel:

> – **Peak Cell Rate**—Enter a value between 64 and 6000
>
> – **Sustainable Cell Rate**—Enter a value between 0and 6000
>
> – **Maximum Burst Size**—Enter a value between 1 and 64000

Step 5 To add data channels, complete these steps:

a. In the **Add Channels** window, click the **Data Channels** tab.

The **Data Channels** tab is enabled, as shown in Figure 3-26.

Figure 3-26   Add Channels - Data Channels Window

Data channels that are already provisioned are highlighted in blue. Unprovisioned data channels appear in black.

b.   To add a new data channel, click the **Add Data Channel** button.

The **Data Channel Entry** window appears, as shown in .

Figure 3-27   Data Channel Entry Window

c. On the **Data Channel Entry** window, specify the following information:

   – **DLCI**—the data-link connection identifier for the data channel.

   – **Interface Type**—Pull down the drop down menu and select **Serial** or **HSSI** (High Speed Serial Interface), then specify the port and slot for the interface.

   – **FRF**—pull down the menu and select an FRF value.

   – **PVC VPI/VCI**—the VPI and VCI for the private virtual circuit.

   – **QoS**—pull down the **QoS** menu and select a QoS type for the data channel. You can specify the following QoS types:

   UBR

   UBR+

   VBR-rt

   VBR-nrt

   CBR

   ABR

   – **Peak Cell Rate**—Enter a number between 64 and 6000 to specify highest cell rate allowed for this channel).

   – **Description**—(optional) Enter a description for the data channel.

d. When you are done specifying the data channel configuration, click the **Allocate** button.

   The channel is allocated.

Step 6   When you are done specifying channel information for the device, click the **Preview Download** button.

The Preview Channels window appears, as shown in Figure 3-28.

*Figure 3-28   Preview Channels Window*

Step 7   Review the information in this window.

Step 8   Do one of the following:

- If the information is correct, click the **Preview Configuration** button.

- If the information is incorrect, click the **Cancel** button to return to the Add Channels window.

If you select **Preview Configuration**, the Configuration File Generation window appears, as shown in Figure 3-29. This window shows router commands that have been generated as a result of your selections.

Figure 3-29   Configuration File Generation Window
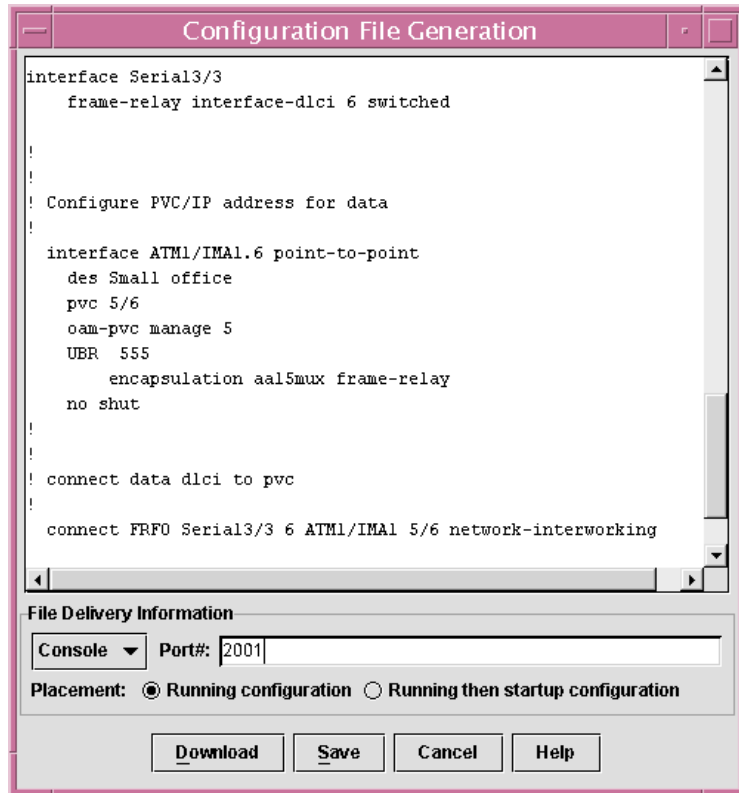
Step 9   Review the router configuration commands in the Configuration File Generation window.

Step 10   Do one of the following:

- If you want to save the configuration for future use, click the **Save** button and then specify the path and filename for the file to which you want to save the configuration.

- If the router configuration is correct, complete these steps:

a.   Pull down the File Delivery Information menu and select a file delivery method. You can specify the following delivery methods:

- **Console**—downloads the file to a router. The router administrator can then specify **config t** to enter configuration mode and apply the configuration.

- **Telnet**—downloads the file to the device via Telnet.

- **File**—saves the configuration to a specified file.

b.   Select the Placement method:

- To download the configuration and make it the running configuration, click the **Running configuration** button.

- To download the configuration and make it the running configuration and also the startup configuration when the device is rebooted, click the **Running then startup configuration** button.

c.   Click the **Download** button to complete the download.

Initial configuration for the 3660 device is complete. You can now add multiple voice channels or multiple data channels.

Adding a Service to a Cisco 2421 or a Cisco 3810 in an MGX Complex

Before You Begin

- You create 2421 or 3810 T1 CPE devices under an MGX complex. Therefore, you must first create an MGX complex as described in the "Creating a Complex" section on page 3-15.

- You must first create a new CPE device as described in "Creating New Devices" section on page 3-35 and select a device type of 2421 or 3810.

Adding a Basic Service for a 2421 or a 3810 CPE Device

Step 1 From the Tree View, select the newly created 2421 or 3810 T1 device.

Step 2 Select **Actions > Device > Add Basic Service** or right-click and select **Add Service** from the Device context menu. The Add Basic Service window appears, with the **Port Info** tab enabled, as shown in Figure 3-30.

Figure 3-30   Add Basic Service - Port Info Window

The Service Request Info that displays at this window corresponds with the information you specified at the Create New Device window. For more information about these fields, see the "Creating New Devices" section on page 3-35.

Step 3   Make a voice and data selection for this device from the drop down list.

T1 CPEs support the following voice and data selections:

- **Voice and Data**—signaling and bearer plus data
- **Voice**—signaling and bearer
- **Data**—data only.

✎

Note   If you select the Data service for this CPE, voice services are disabled.

Step 4   Enter slot and port information for the device.

    d.   Click the checkbox under **Use** for the slot in which you have cards installed. After you click the checkbox, default port information appears.

    e.   Click on the **Num Ports** field for each slot you are configuring and select the number of ports from the pull down menu. You can specify 1 port or 2 ports for each card.

Step 5   Click the **Device** tab.

The **Device** tab is enabled, as shown in Figure 3-31.

Figure 3-31   Add Basic Service - Devices Window

For each port that you have enabled, specify the following information:

- **IP Address**—IP address of the PVC

- **Subnet Mask**—subnet mask for the PVC

- **PVC VPI/VCI**—virtual path identifier/virtual connection identifier. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transit on its way to its final destination. These are required fields.

Step 6   Click the **Allocate and Preview Download** button.

The Configuration File Generation window appears. This window shows router configuration commands that have been generated based upon the configuration options you selected.

Step 7   Edit the commands shown in the Configuration File Generation window as required.

Step 8   Do one of the following:

- If you want to save the configuration to a file for later use, click the **Save** button and then specify the path and filename for the file in which you want to save the configuration.

- If you are ready to download the configuration, click the **Download** button.

- To abandon the configuration, click the **Cancel** button.

If the IP address you specified is incorrect or unreachable, an error message appears.

If you cancel the configuration, the device is marked as **ResourceAllocated** in the Tree View.

If you clicked the **Download** button, the device is now in the Provisioned state.

You are now ready to add Voice and/or Data channels for the device.

Adding a Channel for a 2421 or a 3810 CPE Device

Once you have added basic service for the 2421 or 3810 device, you can provision voice and data channels.

Step 1   Select the device to provision in the Tree View.

Step 2   Select **Actions>Device>Add Channels** or select **Add Channels** from the **Device** context menu.

The Add Channels window appears, as shown in Figure 3-32.

Figure 3-32   Add Channels Window

Step 3   To add a voice channel, click the **Voice Channels** tab.

The Add Channels window for voice channels appears, as shown in Figure 3-33.

Figure 3-33   Add Channels - Voice Window

Channels for which resources have been allocated but have not been provisioned are highlighted in blue. Provisioned channels appear in black.

Step 4   If you have not previously specified a bearer channel, click the **Add Signalling/Bearer Channel** button.

Note   If you have previously added a channel, the **Add Signalling/Bearer Channel** button is disabled.

The Signal and Bearer Channel Entry window appears, as shown in Figure 3-34.

Figure 3-34   Signal and Bearer Channel Entry Window

The back end processor will only use the information that you specify in the **Signal Channel** area of the window; however, you must still specify information in the fields in the **Bearer Channel** area of the window.

Complete these steps to specify signal channel information:

a. If you want the system to generate the IP address, subnet mask, and FQDN for the signal channel, check the **Auto Assign Addresses** checkbox.

b. If you want to manually assign information to identify the signal channel, specify the following information:

  – **IP address**—specify the IP address for the channel

  – **Subnet mask**—specify the subnet mask for the channel

  – **FQDN**—specify the Fully Qualified Domain Name (FQDN) for the channel.

Note   If you are using Cisco Network Registrar with Cisco Convergent Network Solution Center: Subscriber Provisioning, then the back end processor will update the signal channel IP address to a value specified in the CNR's DNS server. Therefore, you must ensure that the IP address you specify is within the range specified in the CNR configuration.

c. Enter the VPI and VCI for the signal channel.

d. In the **QoS** field, pull down the **QoS** menu and select a QoS type for the signal channel.

  You can select the following QoS types:

  – UBR

  – UBR+

–   VBR-rt

–   VBR-nrt

–   CBR

–   ABR

e.   Enter a number between 64 and 6000 to specify the **Peak Cell Rate** for the signal channel.

f.   If you want to manually assign information to identify the bearer channel, specify the following information:

–   **IP address**—specify the IP address for the channel

–   **Subnet mask**—specify the subnet mask for the channel.

g.   Enter the VPI and VPC for the bearer channel.

h.   In the **QoS** field, pull down the **QoS** menu and select a QoS type for the bearer channel.

You can select the following QoS types:

–   UBR

–   UBR+

–   VBR-rt

–   VBR-nrt

–   CBR

–   ABR

i.   Enter the following information for the bearer channel:

–   **Peak Cell Rat**e—specify a value between 64 and 6000 to specify the peak cell rate.

Step 5   To add data channels, complete these steps:

a.   On the **Add Channels** window, click the **Data Channels** tab.

The **Data Channels** tab is enabled, as shown in Figure 3-35.

Figure 3-35   Add Channels - Data Channels Window

Data channels that are already provisioned are highlighted in blue. Unprovisioned data channels appear in black.

b. To add a new data channel, click the **Add Data Channel** button.

The Data Channel Entry window appears, as shown in Figure 3-36.

Figure 3-36   Data Channel Entry Window

c.   In the **Data Channel Entry** window, specify the following information:

–   **DLCI**—the data-link connection identifier for the data channel

–   **FRF**—pull down the **FRF** menu and select an FRF value

–   Pull down the **Interface** menu and select the interface type (**Serial** or **HSSI**). Then specify the port and the slot for the interface.

–   **PVC VPI/VCI**—the VPI and VCI for the private virtual circuit

–   **QoS**—pull down the **QoS** menu and select a QoS type for the data channel. You can specify the following QoS types:

UBR

UBR+

VBR-rt

VBR-nrt

CBR

ABR

–   **Peak Cell Rate**—specify the a value between 64 and 6000 to specify the highest cell rate allowed for this channel

–   **Minimum Cell Rate**—specify a minimum cell rate between 0 and 64 for the data channel

–   **Description** (optional)—specify an optional description for the data channel.

d.   When you are done specifying the data channel configuration, click the **Allocate** button.

The channel is allocated.

Step 6   When you are done specifying channel information for the 3810 or 2421 device, click the **Preview Download** button.

The Preview Channels window appears, as shown in Figure 3-37.

Figure 3-37   Preview Channels Window

Step 7   Review the information in this window and do one of the following:

- If the information is correct, click the **Preview Configuration** button.

- If the information is incorrect, click the **Cancel** button to return to the Add Channels window.

If you select **Preview Configuration**, the **Configuration File Generation** window appears, as shown in
Figure 3-38. This window shows router commands that have been generated as a result of your
selections.

Figure 3-38   Configuration File Generation Window
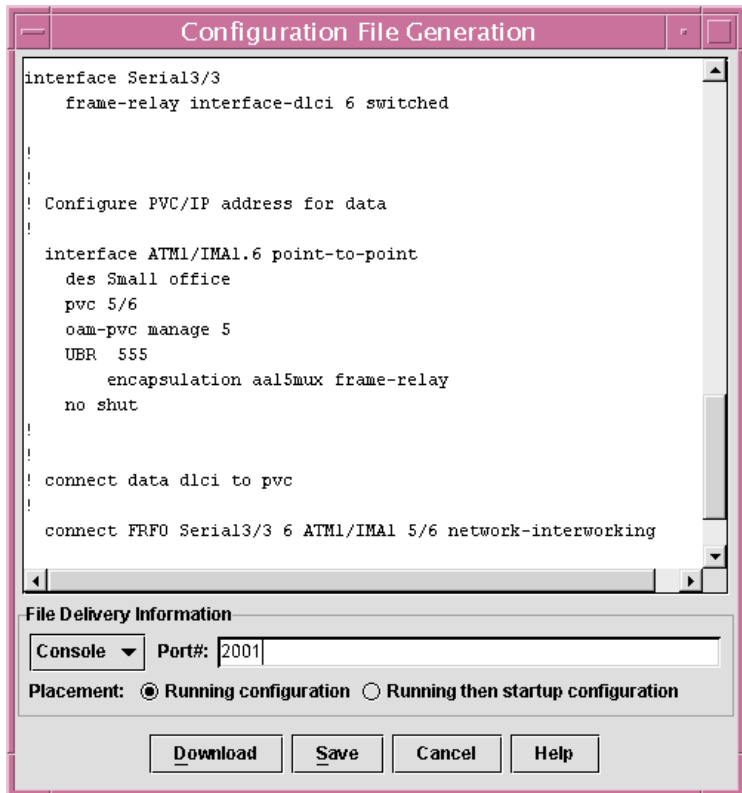
```
interface Serial3/3
    frame-relay interface-dlci 6 switched
!
!
! Configure PVC/IP address for data
!
  interface ATM1/IMA1.6 point-to-point
    des Small office
    pvc 5/6
    oam-pvc manage 5
    UBR  555
        encapsulation aal5mux frame-relay
    no shut
!
!
! connect data dlci to pvc
!
  connect FRF0 Serial3/3 6 ATM1/IMA1 5/6 network-interworking
```

File Delivery Information

Console ▼ Port#: 2001

Placement: ⦿ Running configuration ○ Running then startup configuration

Download   Save   Cancel   Help

Step 8   Review the router configuration commands in the **Configuration File Generation** window.

Step 9   To download the file, complete these steps:

    a.   Pull down the **File Delivery Information** menu and select a file delivery method. You can specify the following delivery methods:

        – **Console**—downloads the file to a router. The router administrator can then specify **config t** to enter configuration mode and apply the configuration.

        – **Telnet**—downloads the file to the device via Telnet

        – **File**—saves the configuration to a specified file.

    b.   Select the **Placement** method:

        •   To download the configuration and make it the running configuration, click the **Running configuration** button.

        •   To download the configuration and make it the running configuration and also the startup configuration when the device is rebooted, click the **Running then startup configuration** button.

    c.   Click the **Download** button to complete the download.

Step 10   Do one of the following:

    •   If you want to save the configuration for future use, click the **Save** button and then specify the path and filename for the file to which you want to save the configuration.

    •   If the router configuration is correct, click the **Download** button to download the configuration to the device

Configuration for the 3810 or 2421device is complete. If you clicked **Download**, the device is now marked as **Provisioned** in the Tree View.

Adding a Service to a 2421 in an ESR10K Complex

Once you have created an ESR10K complex and have added devices to it, you can add services to the complex.

Before You Begin

- You can create 2421 T1 CPE devices under an ESR10K complex. Therefore, you must first create an ESR10K complex as described in the "Creating a Complex" section on page 3-15.

- You must first create a new CPE device as described in "Creating New Devices" section on page 3-35.

Adding a Basic Service for a 2421 CPE Device in an ESR10K Complex

Step 1   From the Tree View, select the newly created 2421 T1 device.

Step 2   Select **Actions>Device>Add Service** or right-click and select **Add Service** from the Device context menu.

The Allocate Resources window appears, with the **Management** tab enabled, as shown in Figure 3-39.

Figure 3-39   Allocate Resources - Management Window

The Service Request Info that displays at this window corresponds with the information you specified at the **Create New Device** window. For more information about these fields, see the "Creating New Devices" section on page 3-35.

Step 3   Make a voice and data selection for this device from the drop down list.

T1 CPEs support the following voice and data selections:

- **Voice and Data**—signaling and bearer plus data
- **Voice**—signaling and bearer
- **Data**—data only.

✎

Note   If you select the Data service for this CPE, voice services are disabled.

Step 4   If a DHCP service was specified during installation and you want the system to automatically assign addresses, check the **Auto Assign Addresses** checkbox.

Step 5   If you want to manually assign addresses, specify the following information:

- **IP Address**—specify the IP address for the device
- **Subnet mask**—specify the subnet mask for the device
- **FQDN**—specify the Fully Qualified Domain Name (FQDN) for the device.

Step 6   Click the **Data Services** tab.

The **Data Services** tab is enabled, as shown in Figure 3-40.

Figure 3-40   Allocate Resources - Data Services Window

Step 7   On the Data Services tab, specify the following information:

- **Ethernet IP Address**—specify the Ethernet address for the device
- **Ethernet Subnet Mask**—specify the Ethernet subnet mask for the device.

Step 8   Click the **DHCP** tab.

The **DHCP** tab is enabled, as shown in Figure 3-41.

Figure 3-41   Allocate Resources - DHCP Window

Step 9   Do one of the following:

- If you want to use a Dynamic Host Configuration Protocol (DHCP) server to assign an IP address for the device, check the **Enable DHCP server** checkbox.

- If you do not want to use DHCP to assign an address, leave the **Enable DHCP server** box unchecked. If you leave the checkbox unchecked, the entry fields in the DHCP tab are disabled.

Step 10   If you checked the **Enable DHCP** server checkbox, specify the following information:

- **Domain Name**—specify the domain name for the DHCP server you will use to allocate an IP address for the device

- **Start IP Address**—specify the starting IP address for the range of IP addresses from which you want the DHCP server to allocate an address

- **End IP Address**—specify the ending IP address for the range of IP addresses from which you want the DHCP server to allocate an address.

Step 11   Click the **NAT** (network address translation) tab.

The **NAT** tab is enabled, as shown in Figure 3-42.

Figure 3-42   Allocate Resources - NAT Window

Step 12   If you want to enable NAT, check the **Enable NAT** checkbox; otherwise leave the checkbox unchecked.

You can use NAT to enable users to access Internet services when there is an insufficient number of IP addresses for all users who need access.

If you leave the **Enable NAT** checkbox unchecked, the entry fields in the NAT tab are disabled.

Step 13   If you checked the Enable NAT checkbox, specify the following information:

- **Start IP Address**—specify the starting IP address in a range of IP addresses from which you want to allocate an address for the device
- **End IP Address**—specify the ending IP address in a range of addresses from which you want to allocate an address for the device
- **Netmask**—specify the netmask for the NAT address

Step 14   If the Challenge Handshake Authentication Protocol (CHAP) was enabled when Cisco Convergent Network Solution Center: Subscriber Provisioning was installed, click the **CHAP** tab.

Step 15   The **CHAP** tab is enabled, as shown in Figure 3-43.

Figure 3-43   Allocate Resources - CHAP Window

Step 16   Do one of the following:

- If you want to disabled Point-to-Point Protocol (PPP) authentication using CHAP for this CPE device, check the **Do NOT use PPP authentication with this CPE** checkbox.

- If you want to enable CHAP authentication on this CPE device, leave the checkbox unchecked.

If the **Do Not use PPP authentication with this CPE** checkbox is checked, then the entry fields in the **CHAP** tab are disabled.

Step 17   If you did not check the **Do NOT use PPP authentication with this CPE** checkbox, complete these steps:

   a.   Select a **Domain Path** for the AAA server.

   b.   Select a method for password authentication:

   – **Default**—if you specified a default password and username in the Subscriber Access Manager, click the **Use Default** button.

   – **Provide Unique**—if you want to require users connecting through this device to provide a unique username and password that PPP will use to authenticate them, click the **Provide Unique** button and then specify the Username and Password that users must provide.

Step 18   When you have completed specifying the configuration parameters for the device, click the **Add Service** button.

The Allocate Resources window appears. The entry fields are greyed out, as shown in Figure 3-44.

Figure 3-44   Allocate Resources Window

Step 19   Do one of the following:

- If you want to provision the device at this point, click the **Provision** button.
- If you want to save the configuration and apply the provisioning settings later, click the Done button.

If you click **Done**, the device is marked with the indication **ResourceAllocated**.

If you click **Provision**, the New Provision window appears, as shown in Figure 3-45.

Figure 3-45   New Provision Window

Step 20   Review the information in the New Provision Screen.

Step 21   If the information is correct, click the **Download Preview** button. If the information is not correct, click the **Cancel** button.

The Configuration File Generation window appears, as shown in Figure 3-46.

Figure 3-46   Configuration File Generation Window
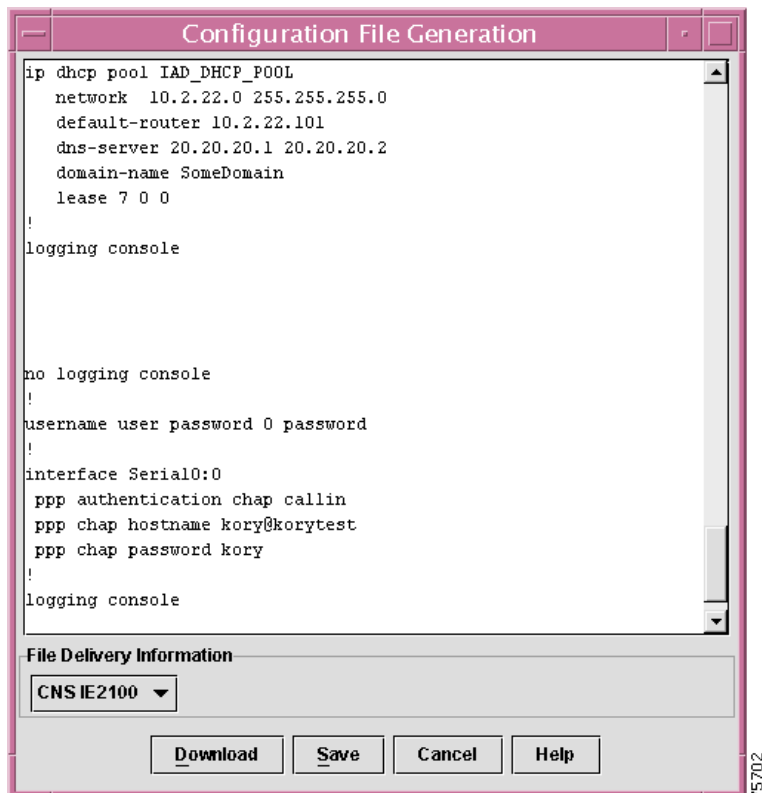
```
Configuration File Generation

ip dhcp pool IAD_DHCP_POOL
   network  10.2.22.0 255.255.255.0
   default-router 10.2.22.101
   dns-server 20.20.20.1 20.20.20.2
   domain-name SomeDomain
   lease 7 0 0
!
logging console




no logging console
!
username user password 0 password
!
interface Serial0:0
 ppp authentication chap callin
 ppp chap hostname kory@korytest
 ppp chap password kory
!
logging console
```

File Delivery Information

CNS IE2100 ▼

[Download]   [Save]   [Cancel]   [Help]

The Configuration File Generation window shows router configuration commands that have been generated based upon your selections in the Allocate Resources window.

Step 22   Review the router configuration commands shown in the Configuration File Generation window.

Step 23   Do one of the following.

- If the commands are incorrect, click **Cancel** to cancel the download. The device will now be marked in the Tree View with the indicator **ResourceAllocated**. You can then modify the configuration.

- If you want to save the configuration in a file and download it to the device at a later time, click the **Save** button and then specify the path and the filename for the file to which you want to save the configuration.

- To download the file, complete these steps:

a.   Pull down the File Delivery Information menu and select a file delivery method. You can specify the following delivery methods:

- **CNSIE2100**—Downloads the file to a Cisco Intelligence Engine 2100 Series device

- **Console**—Downloads the file to a router. The router administrator can then specify **config t** to enter configuration mode and apply the configuration.

- **Telnet**—downloads the file to the device via Telnet

- **File**—saves the configuration to a specified file.

b.   Click the **Download** button to complete the download.

The device is now marked as **Provisioned** in the Tree View.

Provisioning a New CPE Device for an ESR10K Complex

You can provision a new CPE device (Cisco 2421 CPE) under and ESR10K complex in two ways:

1. By following the steps described above in the "Adding a Service to a 2421 in an ESR10K Complex" section on page 3-59 and then downloading the file.

2. If you saved the configuration to a file or cancelled the process for adding the service, by selecting the device from the Tree View, selecting **Actions>Device>New Provision**, and then downloading the configuration.

The information you provide at this window will be provided as input to the appropriate template. Based upon the service type you have selected, CCNSC Subscriber Provisioning provisions voice or data services. Once CCNSC Subscriber Provisioning updates the template, it generates a configuration file. It then stores this configuration file in the CCNSC Subscriber Provisioning Repository, specifically the Oracle database, until it is downloaded onto the device. For information about the templates supported in CCNSC Subscriber Provisioning, see Chapter 4, "Using the Template Manager."

Before You Begin

*   If you are provisioning a T1 CPE device, you must first:
    *   Create an ESR10K complex as described in the "Creating a Complex" section on page 3-15.
    *   Create a new CPE device as described in "Creating New Devices" section on page 3-35.
    *   Add a service to the CPE device as described in "Adding a Service to a New CPE" section on page 3-37

Procedure

Step 1   From the Tree View, select a newly created CPE device in the ResourceAllocated state and select **Actions>Device>New Provision** or right-click and select **New Provision** from the **Device** context menu.

The **New Provision** window appears, as shown in Figure 3-47.

Figure 3-47   New Provision Window
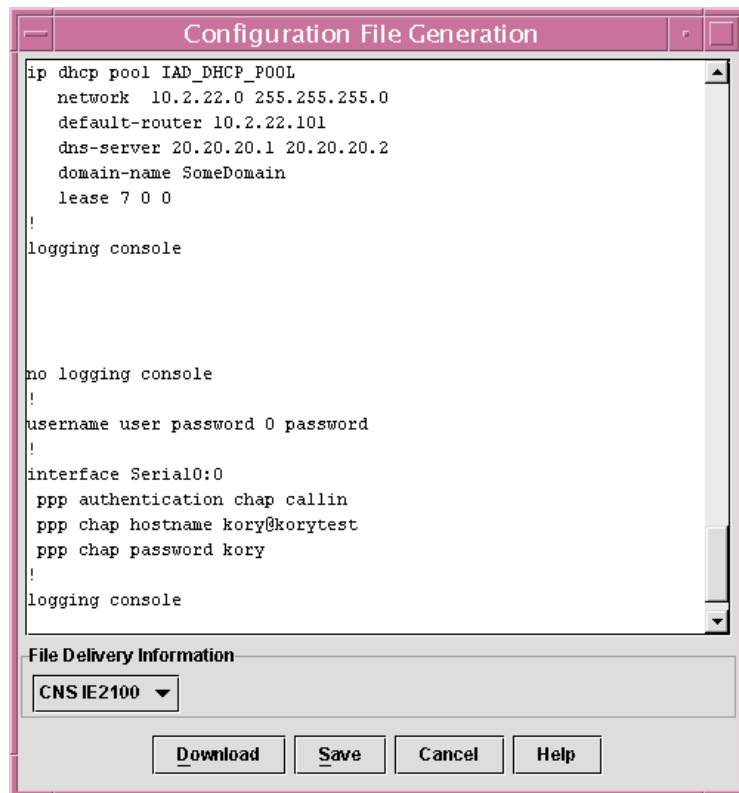

Step 2   Click **Download Preview**.

The Configuration File Generation window appears, as shown in Figure 3-48.

Figure 3-48   Configuration File Generation Window

The Configuration File Generation window shows router configuration commands that have been generated based upon your selections in the Allocate Resources window.

Step 3   Review the router configuration commands shown in the Configuration File Generation window.

Step 4   Do one of the following.

- If the commands are incorrect, click **Cancel** to cancel the download. The device will now be marked in the Tree View with the indicator **ResourceAllocated**. You can then modify the configuration.

- If you want to save the configuration in a file and download it to the device at a later time, click the **Save** button and then specify the path and the filename for the file to which you want to save the configuration.

- To download the file, complete these steps:

    a.   Pull down the File Delivery Information menu and select a file delivery method. You can specify the following delivery methods:

    - **CNSIE2100**—downloads the file to a Cisco Intelligence Engine 2100 Series device

    - **Console**—downloads the file to a router The router administrator can then specify **config t** to enter configuration mode and apply the configuration.

    - **Telnet**—downloads the file to the device via Telnet

    - **File**—saves the configuration to a specified file.

    b.   Click the **Download** button to complete the download.

The device is now marked as **Provisioned** in the Tree View.

Refreshing the Tree View

Refreshing the Tree View updates the Device Tree with any changes that have been made since the last refresh.

Procedure

Step 1   Select any or none of the objects in the Tree View

Step 2   Select **Actions > Refresh > Refresh TreeView**.

The Tree View is updated with any changes you have made.

Refreshing the Server Configuration

Refreshing the server configuration updates the information in the CCNSC Subscriber Provisioning Repository with changes you have made to the **ResourceMgr.cfg** file. These changes are reflected at the appropriate windows throughout the Network Inventory Manager.

You should refresh the server configuration when you make changes to the **ResourceMgr.cfg** or **/CSCOcnscs/resourceMgr/common/ipservice.cfg** files. If you do not refresh the server after making changes to these files, your changes will not be visible in the GUI.

If you change the CNR server, FTP server, or Telnet Gateway in the **ResourceMgr.cfg** file for a subnetwork or Aggregator complex, the values for these servers in Properties window for the subnetwork or Aggregator complex are empty after you refresh the server configuration.

Note   If you change the **Nimtree.properties** file, which is a client file, it is not updated when you refresh the server configuration. If you want changes to the **Nimtree.properties** file to take effect, you must shut down the GUI and restart it. See the *Cisco Convergent Network Solution Center: Subscriber Provisioning Installation Guide*.

Procedure

Step 1   Select any or none of the objects in the Tree View

Step 2   Select **Actions > Refresh > Refresh Server Configuration**.

The CCNSC Subscriber Provisioning Repository is updated and so are the Network Inventory Manager windows that are affected by the changed information.

Viewing and Modifying Telnet Gateway Properties

You can view and modify the current configured properties of the Telnet Gateway. The Telnet Gateway operates in conjunction with the TFTP server. The Network Inventory Manager automatically retrieves the configured properties.

> **Note**   Only the admin user can edit the Telnet Gateway properties.

Procedure

Step 1   Log in as the **admin** user.

Step 2   Select the Root, a Subnetwork, or an Aggregator Complex in the Tree View.

Step 3   Select **Actions > SubNetwork > Telnet Gateway Properties** or **Actions > Aggregator Complex > Telnet Gateway Properties** or right-click and select **Telnet Gateway Properties** from the context menu.

The Telnet Gateway Properties window appears with the **Properties** tab enabled, as shown in Figure 3-49.

Figure 3-49   Telnet Gateway Properties Window
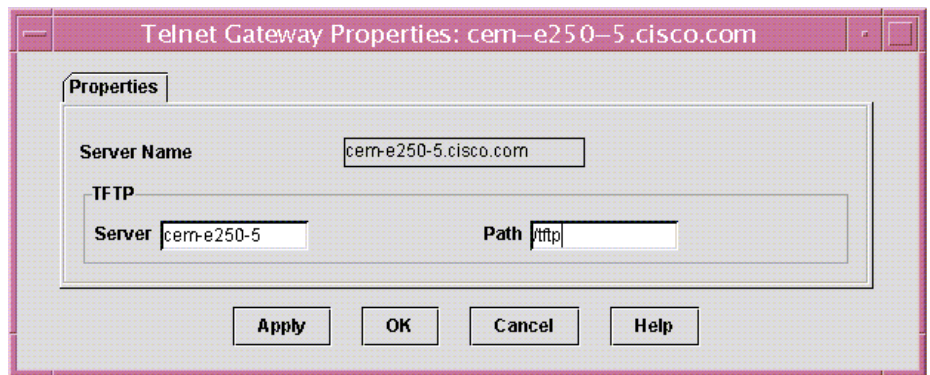
You can view all properties, but you cannot modify all of them. Table 3-3 describes the Telnet Gateway properties.

Table 3-3   Telnet Gateway Properties

Property Name	Description
Server Name	You cannot modify this property.
TFTP Server	The IP address of the TFTP server you want to establish a Telnet connection to in order to download configurations to the device. The TFTP server can reside on the same machine as the CCNSC Subscriber Provisioning software or it can be on a separate machine.
Path	The path you want used to establish a Telnet connection to the TFTP server. The default path is **/tftpboot** as the mount point. You can modify this path, but you must always start with the mount point. In the GUI, you specify the relative path. For example, in the GUI you would specify **pluto**. The full path would be **/tftpboot/pluto**. You can modify this property.

Step 4   Click **Apply** to update the information in this window.

Step 5   Click **OK** to save these Telnet Gateway properties or **Cancel** to close this window without saving any changes.

You are returned to the Tree View.

Viewing CPE Properties

Procedure

Step 1   Select the CPE from the Tree View.

Step 2   Select **Actions > Device > Properties** or right-click and select **Properties** from the context menu.

The CPE Properties window appears, as shown in Figure 3-50. The following figure shows the CPE Properties window for a 2421 device under and ESR10K complex.

Figure 3-50   CPE Properties Window

The properties displayed at this window cannot be modified. See "Creating New Devices" section on page 3-35 for information about these fields.

Step 3   Click **Show Subnetwork Properties**, if you want to view or modify any of the subnetwork properties.

The Properties window for the subnetwork appears. For information about these fields, see "Creating a Subnetwork" section on page 3-5.

Step 4   Click **Cancel** to return to the Tree View.

Viewing and Modifying Element Properties

You can view and modify all currently configured element properties for a CPE, 911 gateway. Cisco 7200, or Cisco ESR10K; the properties you can define are the same whether you are working with a T1 CPE another device. The Network Inventory Manager automatically retrieves the configured General and Terminal Server attributes for the parent object making modification of the element properties optional. However, if you want to override the properties of the parent object for a specific device, you can do so at the Element Properties window.

Procedure

Step 1   Select a CPE, 911 gateway, Cisco 7200, or Cisco ESR10K from the Tree View.

Step 2   Select **Actions>Device>Element Properties** or right-click and select **Element Properties** from the context menu.

The Element Properties window appears, with the **General** tab enabled, as shown in Figure 3-51.

Figure 3-51   Element Properties Window

Table 3-4 describes the general properties you can view and modify for an element.

Table 3-4   General Element Properties

Property Name	Description
Device IP Address	The IP address of the device. This identifies the IP address if using the Telnet VTY to access the device.
Prompt Timeout	The number of seconds that can elapse before a response to a router prompt is required. If this timeout expires, an error message is generated. The default is 20 seconds. This value is retrieved from the **cnscs.properties** file, but you can change it at this window.
Operation Timeout	The number of seconds that a router runtime operation has to complete. If this timeout expires, an error message is generated. The default is 240 seconds. This value is retrieved from the **cnscs.properties** file, but you can change it at this window.
User ID	The user name that the system uses to establish a Telnet session with the device.
User Password	The user password that the system uses to establish a Telnet session with the device.
Enable Password	The enable password sets a local password to control access to various privilege levels. Privilege levels define the operations available to a user after they have logged in to a network device. This property is optional.
Console User ID	The User ID for accessing the console port on the device.
Console Password	The password for accessing the console port on the device.

Step 3   Click **Apply** to update the information in this window.

Step 4   Click **OK** to save these General properties.

To view and modify other properties, see the following section:

- Viewing and Modifying Terminal Server Attributes for a CPE, page 3-74

Step 5   Click **Cancel** to close this window without saving any changes.

You are returned to the Tree View.

Viewing and Modifying Terminal Server Attributes for a CPE

The terminal server attributes define information about the terminal server that will be used to download the configuration to a device. The terminal server attributes define information used only when using Console mode to download.

Procedure

Step 1   Select the CPE, or 911 gateway, ESR10K, or Cisco 7200 from the Tree View.

Step 2   Select **Actions > Device > Element Properties** or right-click and select **Element Properties** from the context menu.

Step 3   Click the **Terminal Server** tab.

The **Terminal Server** tab becomes enabled, as shown in Figure 3-52.

Figure 3-52   Element Properties - Terminal Server Window

Table 3-5 describes the Terminal Server properties you can view and modify for an element.

Table 3-5   Terminal Server Properties

Property Name	Description
Port Number	The port number over which the Terminal Server will communicate with the device. This value is retrieved if the Console download mode is selected to download a configuration to a device as described in "Generating and Downloading a Configuration File to a CPE" section on page 3-76.
Server IP Address	The IP address of the Terminal Server.
Server User ID	The user name for logging into the Terminal Server for purposes of establishing a connection to the device.
Server User Password	The user password for logging into the Terminal Server for purposes of establishing a connection to the device.
Port Password	The password for logging into the Terminal Server port used to access the device. Note that currently Cisco Convergent Network Solution Center: Subscriber Provisioning does not support port usernames.

Step 4   Click **Apply** to update the information in this window.

Step 5   Click **OK** to save these Terminal Server properties.

To view and modify other properties, see the "Viewing and Modifying Element Properties" section on page 3-73

Step 6   Click **Cancel** to close this window without saving any changes.

You are returned to the Tree View.

Generating and Downloading a Configuration File to a CPE

The Network Inventory Manager uses the information you provided at the New Provision or Modify Provision window to generate a configuration file and download it onto the device. This task applies to new CPEs and deployed CPEs.

Before You Begin

- If you are generating a configuration file for a T1 CPE device, you must first:
    - Create a subnetwork as described in the "Creating a Subnetwork" section on page 3-5 or create a complex as described in the "Creating a Complex" section on page 3-15.
    - Create a new CPE device as described in "Creating New Devices" section on page 3-35.
    - Add a service to the CPE device as described in "Adding a Service to a New CPE" section on page 3-37
    - Provision a device as described in "Provisioning a New CPE Device for an ESR10K Complex" section on page 3-67 or as described in "Generating and Downloading a Configuration File to a CPE" section on page 3-76.
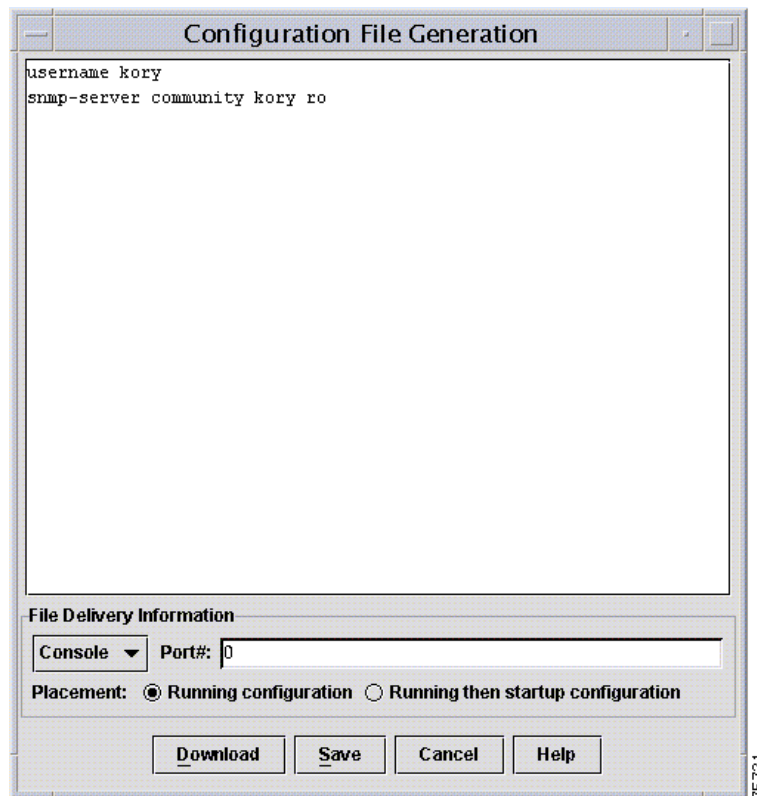
Procedure

Step 1   Continue directly from the New Provision or Modify Provision window at which you clicked **Download Preview**.

The **Configuration File Generation** window appears, as shown in Figure 3-53.

Figure 3-53   Configuration File Generation Window

Step 2   Select the **Download** mode.

See Table 3-6 for a description of the download mode options.

Table 3-6   Download Options

Mode	Device	Description
Console	T1 CPE under MGX Complex or ESR10K Complex	Downloads the configuration file using the Console download mode. If you select this file delivery method, you must provide the console port number on the device to which you are downloading the configuration file. This mode is available only for new provisions.
File	T1 CPE under MGX Complex or ESR10K Complex	Saves the configuration file to a file. It can be downloaded at a later time. You can either specify a filename or select one from the browser. If you successfully download using this option, CCNSC Subscriber Provisioning registers the device as provisioned and it appears in the Network Inventory Manager, as provisioned. However, to download the configuration to the device, you will need to download it through the Telnet Gateway download method. For more information about this method, see the "Downloading a Configuration Using a Telnet Gateway" section on page 3-79. This mode is available only for new provisions.

Table 3-6   Download Options (continued)

Mode	Device	Description
CNSIE2100	T1 CPE under an ESR10K Complex	Transfers the configuration file, using the Hypertext Transfer Protocol (HTTP), for new and deleted provisioning. Modification of an existing configuration is available only through calls to the Cisco Convergent Network Solution Center: Subscriber Provisioning Application Programming Interface (API) functions.
Telnet	T1 CPE under MGX Complex or ESR10K Complex	Uses the Telnet Gateway server defined in the Subnetwork properties window to copy the configuration file to the path specified in the TG Properties window. This mode can be used for new and deleted provisioning. Modification of existing provisioning can only be done using the Cisco Convergent Network Solution Center: Subscriber Provisioning API functions.

Step 3   If you have selected the Console download mode, specify a port number.

This value is retrieved from the **Terminal Server Attributes** tab of the Element Properties window. If you change the port number at this window, the Element Properties window is not updated with your change. However, if you make a change at the Element Properties window as described in "Viewing and Modifying Terminal Server Attributes for a CPE" section on page 3-74, it will be reflected in this field.

**Step 4**   Select the **Placement** type.

The options are as follows:

- Running Configuration—download is dynamic; changes will be lost upon restart
- Running then startup configuration—download takes effect immediately and sends a copy to startup configuration.

Step 5   Select one of the following options:

- **Save**—saves the configuration file
- **Download** — downloads the configuration file to the device
- **Cancel**—cancels the provision operation and returns to the Tree View.

If you clicked **Download**, the Download Results window appears, as shown in Figure 3-54.

Figure 3-54   Download Results Window
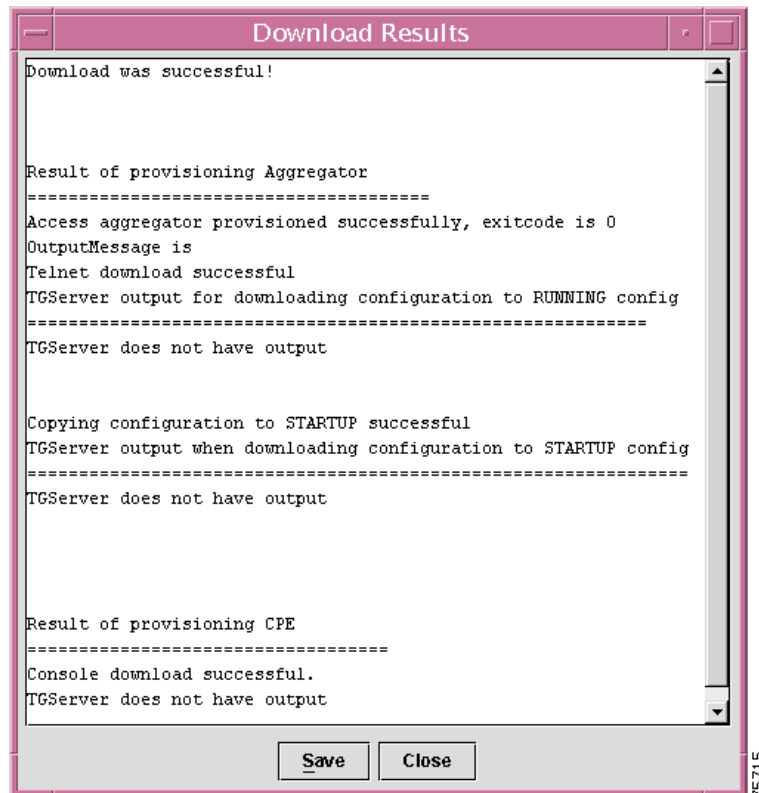
The information displayed includes whether the download was successful or error messages as to why the download failed.

Step 6   Click **Close**.

Step 7   Click **Close** at the New Provision window.

The device appears as (**Provisioned**) in the Tree view.

Downloading a Configuration Using a Telnet Gateway

You can use the Telnet Gateway method to download a configuration to any ESR10K, Cisco 7200, or 911 gateway. When you use this download method, the configuration is downloaded over the Console or the Telnet-vty port of the device.

Before You Begin

Provision the device to which you want to download the configuration.

Create a subnetwork as described in the "Creating a Subnetwork" section on page 3-5 and then create a new device as described in the "Creating New Devices" section on page 3-35.

Procedure

Step 1   Select a provisioned device.

Step 2   Select **Actions > Device > Telnet Download** or right-click and select **Telnet Download** from the device context menu.

The Select Configuration file for download window appears.

Step 3   Select the file you want to download to the device.

Step 4   Click **Open**.

The Download Options window appears.

Step 5   Select the options you want applied for this download.

The options are as follows:

- Running Configuration—download is dynamic; the configuration takes effect immediately. This is console +configt mode. It reads the configuration file line by line to the device. This applies only to a running configuration. It is the current configuration of the IOS router.

- Startup configuration—download takes effect only after the router reboots. If you select this option, you can use only the Telnet vty port to establish a connection to the device.

- Telnet-vty—connection is made to the Telnet-vty port on the device. This is the management interface. This download operation uses the TFTP download method.

- Console—connection is made to the console port of the device. The download operation uses configure terminal mode (line-by-line transfer).

- Update Startup Configuration after Download to Running Config—downloads to running configuration and copies running configuration to startup configuration.This option is enabled only if you have selected Running Config in the Download To group. This option allows you to choose whether or not the device's startup configuration is updated after the running configuration has been downloaded.

- Reload Element after Download—after download, resends a command to the device to restart it. This option forces the device to reboot after the configuration has been downloaded.

Step 6   Click **Download**.

The Download Status window appears. The information displayed includes whether the download was successful or failed.

Step 7   Click **ShowErrors**.

Step 8   Click **Close**.

Deleting a Network Object

When you delete a network object, all information about the object is removed from the CCNSC Subscriber Provisioning Repository. You can delete subnetworks, Aggregator Complexes, T1 CPEs (2421s), 3660s, Cisco 7200s, and Cisco ESR10K objects.

Before You Begin

- For T1 CPE devices, you must delete the provisioning and service for the device, before you delete the device.

- You must delete all of the subordinate objects, before deleting a Aggregator Complex or Subnetwork.

Procedure

Step 1   Select the network object from the Tree View that you want to delete.

Step 2   Select **Actions > Device > Delete**, **Actions > Subnetwork > Delete**, **Actions > Device > Delete**, or right-click and select **Delete** from the context menu.

The Delete Confirmation window appears.

Step 3   Select **Yes** to delete the network object or **No** to cancel the delete operation.

Whether you selected **Yes** or **No**, you will be returned to the Tree View. However, if you selected **Yes**, the object no longer appears in the Tree View.

Deleting Provisioning of CPE Device

When you delete the provisioning information for the device, a delete configuration file is downloaded to the device. You can delete provisioning for T1 CPEs (2421s).

Procedure

Step 1   Select the device from the Tree View for which you want to delete provisioning.

Step 2   Select **Actions > Device > Delete Provision** or right-click and select **Delete Provision** from the device context menu.

The CPE Provision window appears.

Step 3   Enter a value in the **Service Request ID** field.

Provide a service request ID to identify this particular request. You can use it to search the Log Viewer log.

The system automatically selects the appropriate template based upon which service has been provisioned.

Step 4   Click **Download Preview** or **Cancel**.

- **Cancel**—cancels the provision operation and returns to the Tree View.
- **Download Preview**—displays the Configuration File Generation window and shows the configuration file that is to be downloaded. The variable information is to be filled in with values provided in this service request.

If the delete template it successfully downloaded, the state of the device changes to ResourceAllocated and appears following the device in the Tree View.

Deleting a Service for a CPE Device

Procedure

Step 1   Select the CPE device from the Tree View that you want to delete.

Step 2   Select **Actions > Device > Delete Service**, or right-click and select **Delete Service** from the context menu.

The Delete Confirmation window appears.

Step 3   Select **Yes** to delete the service or **No** to cancel the delete operation.

Whether you selected **Yes** or **No**, you will be returned to the Tree View. However, if you selected **Yes**, the CPE state changes to Unprovisioned and appears following the device in the Tree View.

Deleting a Channel for a CPE Device

You can delete channels for a device to which you have added channels. For 3660, 3810, or 2421 devices, choose VoIPoATM devices.

Complete these steps to delete channels:

Step 1   On the Tree View, select a device for which you have allocated channels.

Step 2   Select **Actions>Device>Delete Channels**.

Step 3   If you are deleting a voice channel, select the **Voice Channel** tab.

The **Delete Channels** window for voice channels appears, as shown in Figure 3-55.

Figure 3-55   Delete Channels - Voice Window

Step 4   If you are deleting data channel, click the **Data Channel**s tab.

The Delete Channels window for data channels appears, as shown in Figure 3-56.

Figure 3-56   Delete Channels - Data Window

Step 5   Click the **Delete Channel** checkbox next to any channels that you want to delete.

Step 6   Click the **Preview Download** button.

The Preview Channels window appears, as shown in Figure 3-57.

Figure 3-57   Preview Channels Window

Step 7   Do one of the following:

- If you want to Cancel the delete channels operation, click the **Cancel** button.

- To continue with the deletion, click the **Preview Configuration** button.

The Configuration File Generation window appears, as shown in .

Figure 3-58   Configuration File Generation Window
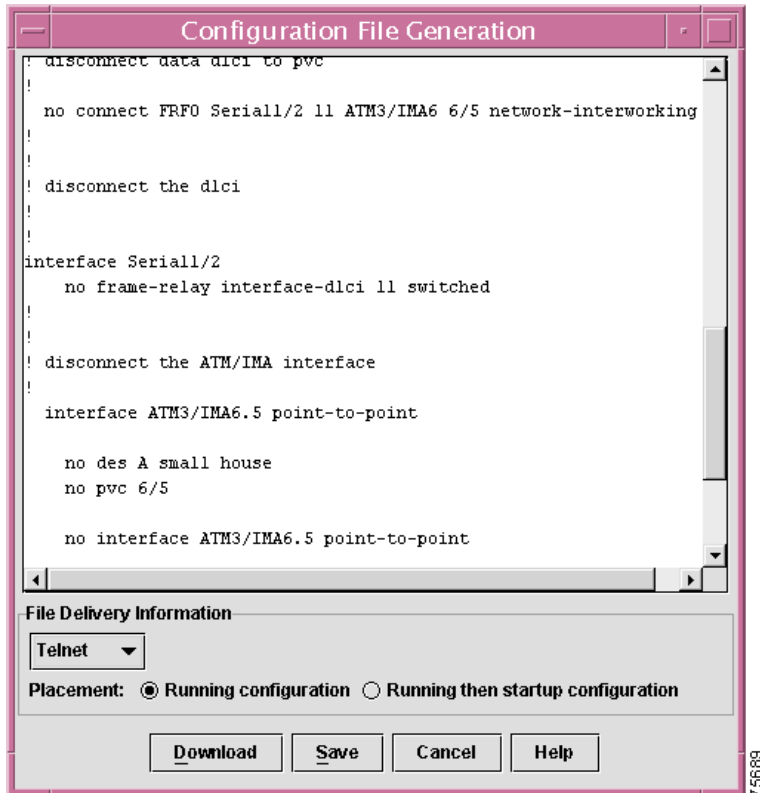
Step 8   Review the router configuration commands in the Configuration File Generation window.

Step 9   Do one of the following:

- If you want to save the configuration for future use, click the **Save** button and then specify the path and filename for the file to which you want to save the configuration.

- If the router configuration is correct, complete these steps:

a.   Pull down the **File Delivery Information** menu and select a file delivery method. You can specify the following delivery methods:

   – **Console**—Downloads the file to a Trivial File Transfer Protocol (TFTP) server. The file can then be downloaded from the TFTP server to the 2421 device. If you specify Console, then you must specify the console port number on the device to which you are downloading the configuration.

   – **Telnet**—Downloads the file to the device via Telnet.

   – **File**—Saves the configuration to a specified file.

b.   Select the **Placement** method:

- To download the configuration and make it the running configuration, click the **Running configuration** button.

- To download the configuration and make it the running configuration and also the startup configuration when the device is rebooted, click the **Running then startup configuration** button.

If you click **Download**, the channel configuration is updated.

Setting Debug Levels

You can independently set debug levels for the CCNSC Subscriber Provisioning Client and the CCNSC Subscriber Provisioning Server.

The debug level determines how much debug information will be displayed in the log. Each log level includes the previous level. For example, if you select the Error log level, which is the default, the log will include all Error level and Emergency level messages.

The log level is set in the **Nimtree.properties** file for the client and the **cnscs.properties** file for the server. However, you can update the log level value in these files from the GUI.

CCNSC Subscriber Provisioning provides a **logEmerg.log** file. This log is used to capture Emergency level errors that occur before the other processes used to log information in an audit trail or debugging log can be initialized. For example, the Behavior Manager will write to the **logEmerg.log** file at startup time when either of the following occur:

- The Behavior Manager cannot read the **/CSCOcnscs/resourceMgr/common/ipservice.cfg** file, **cnscs.properties** file, or the **cnscs.properties.initial** file.

As a result, any Emergency level errors logged in the **logEmerg.log** file before the other processes come up, will not appear in an audit trail or in the debugging log.

Procedure

Step 1 Select **Debug>Set Debug Level** from the Tool bar.

The Debug Level Settings window appears, as shown in Figure 3-59.

Figure 3-59   Debug Level Settings Window
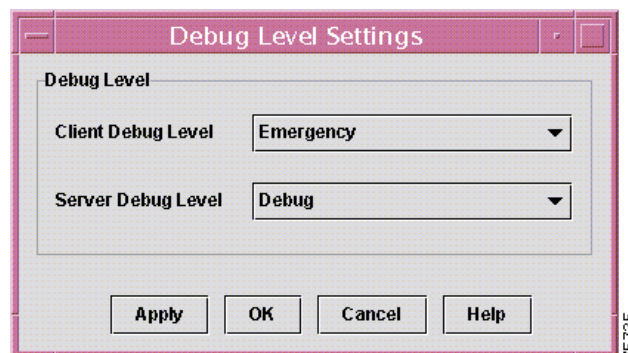
Step 2 Select the log level you want for the client and the server.

The possible log levels are described in Table 3-7.

Table 3-7   Debug Levels

Debug Level	Description
Emergency	Displays messages that require immediate operator intervention. These messages is display regardless of the level you select.
Error	Displays error messages that are sent to the log. Some of these messages may need operator intervention in order to continue. This is the default.
Warning	Displays warning messages that are sent to the log but do not require operator intervention for processing to continue.
Information	Displays informational messages that are sent to the log.
Debug	Displays debug messages that are helpful to developers and testers.

Step 3   Click **Apply** or **OK** to commit the changes.

After the Tree View is refreshed, "debug" changes back to the default, which is "error," unless changes are made in the **Nimtree.properties** file for the client or the **cnscs.properties** file for the server.

Setting Up the Automatic Configuration Feature

If you use CCNSC SP in conjunction with the Cisco Intelligence Engine 2100 (Cisco IE2100), you can then set up CCNSC SP to use the Cisco IE2100 to provision the IAD2421devices that it manages.

In order to use the Cisco IE2100 to provision devices managed by CCNSC SP, you must complete these steps:

1. Configure Cisco Convergent Network Solution Center: Subscriber Provisioning to use the Cisco IE2100 Configuration Registrar to provision devices. For information on this topic, refer to Chapter 4, "CCNSC Subscriber Provisioning Configuration," in the *Cisco Convergent Network Solution Center: Subscriber Provisioning Installation Guide*.

2. Configure each IAD2421 that will be provisioned through the Cisco IE2100 to communicate with the Cisco IE2100.

3. Ensure that the complex properties page has the correct Cisco IE2100 server name.

4. Establish a connection between the IAD2421 and the Cisco IE2100.

Configuring Routers to Communicate with the Cisco IE2100

Complete these steps to configure each IAD2421 that will use the Cisco IE2100 and CCNSC SP to obtain a configuration file.

Step 1   Make sure the Cisco IE2100 is running and is reachable through IP.

Step 2   Make sure that the **startup config** file on each IAD2421 device that will be provisioned through the Cisco IE2100 contains the following commands:

```
cns config initial <Cisco IE2100 ipaddress or DNS name> event
cns id serial <serial interface #> ipaddress
cns event <Cisco IE2100 ip or DNS name> keepalive <timeout> <retry>
```

The following example shows the use of these commands:

```
ip name server 172.29.145.233
cns config init RM1.pluto.cisco.com event
cns id serial 0:0 ipaddress
cns event RM1.pluto.cisco.com keepalive 5 5
```

> **Note**   If the IAD2421 is using the Cisco IE2100's DNS name, make sure that the IAD2421 has an **ip name server <*DNS server IP*>** command in its **startup config** file pointing to the DNS server that can resolve the Cisco IE2100's DNS name.

Ensuring That the Complex Properties Page Has the Correct Cisco IE2100 Name

Complete these steps to ensure that the Complex Properties page has the correct Cisco IE2100 name.

Step 1   When you complete the ESR10K complex that contains the IAD2421 devices that will be provisioned through the Cisco IE2100, pull down the menu for the Cisco IE2100 server field and select the Cisco IE2100 that will be used to provision the devices in the complex.

For specific instructions, refer to the .

Step 2   When you add a service to the IAD2421 device and the Configuration File Generation window appears, choose **CNSIE2100** as the File Delivery Method.

For specific instructions, refer to the .

Establishing the Connection Between the IAD2421 and the Cisco IE2100

Complete these steps to establish a connection between the IAD2421 and the Cisco IE2100.

Step 1   Reload the IAD2421 to simulate a first time power-on connection to the ESR10K.

The IAD2421 should read in the CNS agent configuration and use HTTP to get a configuration file from the Cisco IE2100.

Once the IAD2421 finishes downloading the configuration, it remove the **cns config init x.x.x.x event** command from its **startup config** file and sends out an event.

Step 2   Check the device's state in the Tree View.

The CCNSC SP server receives the event and changes the IAD2421's object state from **PendingProvisioned** to **Provisioned**. You need to manually refresh the NIM tree to see this.

The Cisco Convergent Network Solution Center: Subscriber Provisioning CDM server appends the **cns config partial x.x.x.x** command to the end of the generated configuration file. Once the configuration download is complete, the IAD2421 should have the following three CNS command lines:

```
cns config partial <Cisco IE2100 IP address or DNS name>
cns id serial <port#> ipaddress
cns event <Cisco IE2100 IP or DNS name>keepalive <timeout> <retry>
```

After this, the IAD2421 listens for incremental configuration update events

Note the following points:

1. When the IAD2421 is in the **Pending Provisioned** state, you can execute a Delete Configuration only. This operation removes the object and its associated configuration file from the Cisco IE2100. It also unprovisions port information from the ESR10K.

2. After you perform a Delete Configuration operation, the object state changes to **ResourceAllocated**.

3. When the IAD2421 is in the **Provisioned** state, you can execute a Delete Provision operation. This operation uses a Cisco IE2100 event to push down the configuration to the IAD2421. Once the configuration is successfully removed from the IAD2421, it sends out an event.

4. After the Delete Provision operation, the object state changes to **ResourceAllocated**.

5. If an error occurs during processing, the object icon for the device changes to red.

6. Any warning messages from the operation do not result in an error—instead the operation is regarded as successful. You can find further information on the traces in the Telnet Gateway trace files.