Configuring Broadband Access Center for Cable

This chapter describes the Broadband Access Center for Cable (BACC) configuration activities that you perform using Configuration menu options:

Configuring the Class of Service

Using the BACC administrator, you can configure the classes of service offered to your customers. For example, you can associate DOCSIS options with different DOCSIS classes of service. You use the BACC administrator user interface to add, modify, view, or delete any selected class of service. Start with the Manage Class of Service page, as shown in Figure 10-1.

Figure 10-1 Manage Class of Service Page

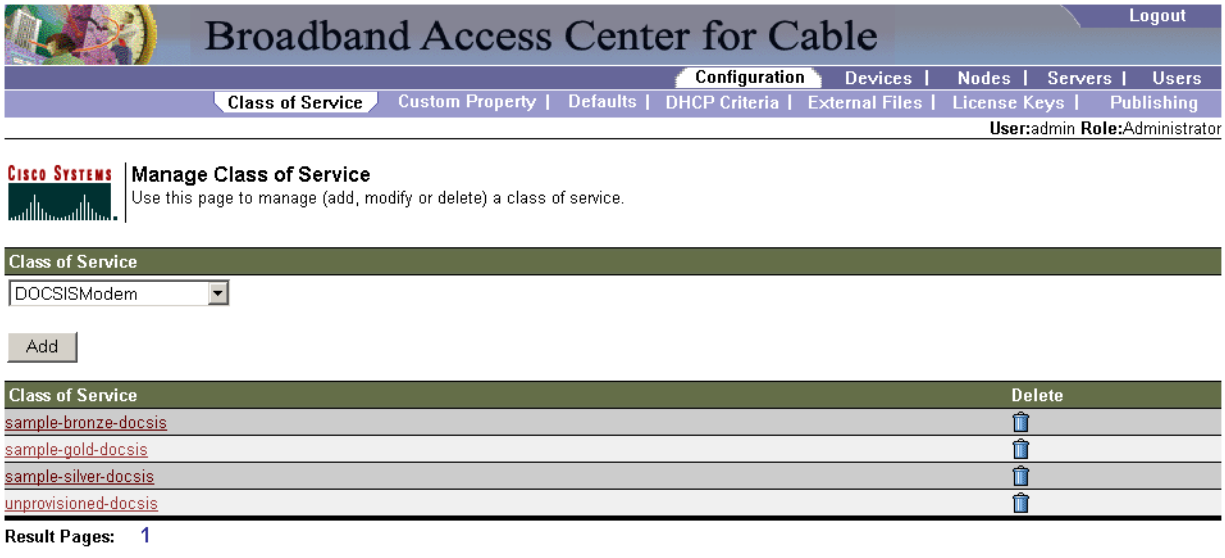


Table 10-1 identifies the fields and buttons shown in Figure 10-1.

Table 10-1 Configure Class of Service Page

Field or Button	Description
Class of Service	A drop-down list that identifies the technology classes of service that you can search for. Available selections, as they appear on screen, include: • ATA 186 • ATA 188 • CableHomeManData • CableHomeManWan • DOCSISmodem • Computer • PacketCableMTA **Note** Refer to the "Configuring Defaults" section on page 10-7, for additional information on these areas of technology.
Add	Lets you add a new class of service.
Class of Service list	Displays the attributes of any selected class of service.
Delete	Lets you delete selected classes of service.

Adding a Class of Service

To add a specific class of service:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Click **Add**. The Add Class of Service page appears. This page identifies the various settings for the selected class of service.

Step 4 Enter the name of your new class of service.

Step 5 Choose a **Class of Service Type**.

Step 6 Enter a **Property Name** and **Property Value** in the appropriate fields.

For example:

Assume that you want to create a new class of service called Gold-Classic for DOCSIS modems. You might:

a. Enter **Gold-Classic** as the Class of Service Name.

b. Choose **DOCSIS** from the service type drop-down list.

c. Choose the /cos/docsis/file property file name.

d. Enter **Gold-Classic.cm** in the Property Value field and then continue with the rest of this procedure.

Step 7 Click **Add** to add the property to the defining class of service.

Step 8 Click **Submit** to finalize the process or **Reset** to return all fields to their previous setting. After submitting the class of service, the Manage Class of Service page appears to show the newly added class of service for that particular device type.

Note Multiple Property Name:Property Value pairs could appear on this page. You use the **Delete** button to remove any unwanted pairs from the class of service.

Caution When adding a DOCSISModem class of service, you must specify the /cos/docsis/file property with the value being the name of a previously added external file. This file is used when provisioning a DOCSIS device that has this class of service.

When adding a PacketCable class of service, you must specify the /cos/packetCableMTA/file property with the value being the name of a previously added external file. This file will be used when provisioning a Packetcable device that has this class of service.

When adding a CableHomeWanMan class of service, you must specify the /cos/cableHomeWanMan/file property with the value being the name of a previously added external file. This file will be used when provisioning a CableHomeWanMan device that has this class of service.

Table 10-2 identifies the fields and buttons shown in the Add Class of Service page.

Table 10-2 Add Class of Service Page

Field or Button		Description
Class of Service Name and Type		
	Class of Service Name	Lets you enter the name of the new class of service.
	Class of Service Type	A drop-down list that identifies the types of classes of service that you can select.
Property Name/Value		
	Property Name	Specifies the appropriate property. You can select the desired property from the drop-down list.
	Property Value	Specifies the value for the property name selected.
Add		Adds the new Property Name:Property Value pair to create the new class of service.
Submit		Activates or implements the changes you have made.
Reset		Returns all settings to their previous setting.

Modifying a Class of Service

You modify your classes of service by selecting the various properties and assigning appropriate property values. When creating a class of service for the first time you must select all the required properties and assign values to them. If you make a mistake, or your business requirements for a certain class of service change, you can either change the property value before submitting your previous changes or delete the Property Name:Property Value pair altogether.

Note Subsequent device configurations will include the changes you implement here. All existing configurations are regenerated, although the devices on the network will not get the new configuration until they reboot.

To add, delete, or modify class of service properties:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Choose the class of service to be modified.

Step 4 Click the link corresponding to the desired class of service. The Modify Class of Service page appears; note that the selected class of service name and type are displayed below the page description.

- To add a new property to the selected class of service:
  - Select the first property that you want assigned to the selected class of service, from the Property Name drop-down and then, after entering the appropriate value for that property, click **Add**.
  - Repeat for any other properties you want to assign to the selected class of service.

- To delete a property for the selected class of service:
  - Locate the unwanted property in the list immediately above the Property Name drop-down.
  - Click **Delete**.
- To modify the value currently assigned to a property:
  - Delete the appropriate property as described above.
  - Add the same property back to the class of service while entering the new Property Value.

Note If you delete a required property you must add it back, and select the appropriate value, before you submit the change.

Step 5 Click **Submit** to make the modifications to the class of service. Each property added to a class of service, is displayed when you click **Submit**. After doing so, a confirmation page appears to regenerate the configuration for the devices with the selected Class of Service.

Step 6 Click **OK** and the modified class of service will be available in the Manage Class of Service page.

Deleting a Class of Service

You can delete any existing Class of Service but, before you attempt to do so, you must ensure that there are no devices associated with that Class of Service.

Tip Where there are large numbers of devices associated with a Class of Service to be deleted, use the BACC application programmers interface (API) to write a program to iterate through these devices to reassign another class of service to the devices.

If you try to delete a Class of Service with devices associated with it, this error message is displayed:

```
The following error(s) occurred while processing your request.
Error: Class Of Service [sample-COS] has devices associated with it, unable to delete

Please correct the error(s) and resubmit your request.
```

The specific class of Service is specified within the error message. In this example this is represented by *sample-COS*.

To delete a class of service:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Click **Delete** for any desired class of service, and a confirmation dialog box appears.

Note You cannot delete the default ‘unprovisioned-docsis’ Class of Service.

Step 4 Click **OK** to delete the file, or **Cancel** to return to the Manage Class of Service page. (See Figure 10-1.)

Note A class of service cannot be deleted if devices are associated with it or, if it is designated as the default class of service.

Configuring Custom Properties

Custom properties let you specify additional customizable device information to be stored in the RDU database. The Custom Property configuration page is found under the Configuration menu and you use this page to add or delete custom properties.

Caution Although you can delete custom properties if they are currently in use, doing so could cause extreme difficulty to other areas where the properties are in use.

To configure custom properties:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Custom Property** from the Secondary Navigation bar and the Configure Custom Properties page appears.

- To add a custom property:
  - Click **Add** on the Configure Custom Properties page, and the Add Custom Property page appears.
  - Enter the name of the new custom property.
  - Choose a custom property type from the drop-down list.
  - Click **Submit** when complete. After the property has been added to the administrative database, the Configure Custom Properties page appears.
- To delete a custom property:
  - Identify the custom property to be deleted from the Configure Custom Properties page.
  - Click the **Delete** icon corresponding to the desired custom property, and the custom properties deletion dialog box appears.
  - Click **OK** to delete the custom property.

Step 3 After clicking **Submit** or **OK**, and your custom property is added or deleted, the Configure Custom Properties page appears.

Configuring Defaults

The Defaults page, found under the Configuration option, lets you access the default settings for the overall system, including the regional distribution unit (RDU), Network Registration extensions, and all supported technologies.

Selecting Configuration Options

The procedure for configuring specific default types is identical. Complete this procedure to access the desired defaults page and then refer to the appropriate section within this chapter for a description of the various page components.

Step 1 Choose **Configuration** on either the Primary Navigation bar or Main Menu page.

Step 2 Choose **Defaults** from the Secondary Navigation bar and the Configure Defaults page appears.

Step 3 Choose the desired default type from the list to the left of the screen. The appropriate defaults page appears.

ATA 186 Defaults

The Cisco ATA 186 is a handset-to-Ethernet adaptor that turns a traditional telephone into an Ethernet IP telephone. You can take advantage of the many IP telephony applications by connecting an existing analog telephone to this device.

The Configure ATA 186 Defaults page (Figure 10-2) displays a list of default values currently available to support the ATA 186.

Figure 10-2 Configure ATA 186 Defaults Page

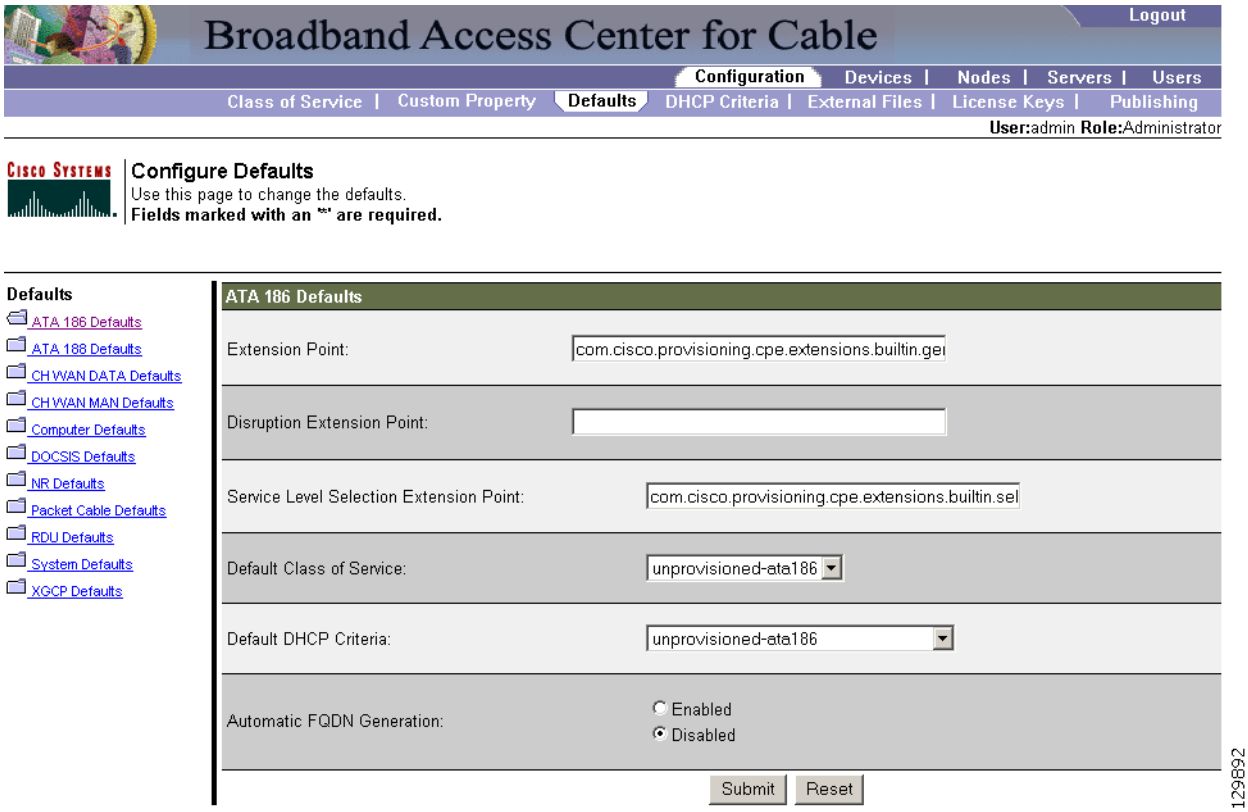


Table 10-3 identifies the fields and buttons shown in Figure 10-2. In many cases, the parameters that appear on this page also appear in other default pages.

Table 10-3 Configure ATA 186 Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a device of this technology.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a device of this technology.
Service Level Selection Extension Point	Identifies the extension used to determine the DHCP criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default class of service for a specific device technology, in this example, ATA186. New, unrecognized devices of that technology type will be assigned to this class of service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP criteria for a specific device technology, in this example, ATA186. New, unrecognized devices of that technology type will have this default DHCP criteria assigned. Use the drop-down list to select a new default value.

Table 10-3 Configure ATA 186 Defaults Page (continued)

Field or Button	Description (continued)
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automatic generation of the FQDN is disabled. **Note** See the "Automatic FQDN Generation" section on page 10-35 for additional information.
Submit	Activates the changes you have made. After the administrative database has been updated the Configure Defaults page will reflect the changes you have made.
Reset	Returns all settings to their previous setting.

ATA 188 Defaults

The Cisco ATA 188 interfaces regular telephones with IP-based ethernet telephony networks. The ATA 188 provides true, next-generation voice-over-IP (VoIP) terminations to support the needs of the enterprise, small-office environments, and emerging VoIP managed voice services and local services market.

The Configure ATA 188 Defaults page displays a list of default values currently available to support the ATA 188. The default parameters displayed for the ATA 188 are identical to those displayed for the ATA 186 although the values you select could be different.

CableHome WAN Defaults

There are two distinct CableHome WAN default screens; one for WAN-Data devices and one for WAN-Man devices.

WAN-Data devices, which are entirely dependent on their corresponding WAN-Man devices, are not unlike computers operating in the promiscuous mode, relative to their cable modems. A WAN-Data device is simply a MAC address and an IP address.

In either case, select the desired default from the displayed list to display the appropriate page. Each WAN default page contains the same fields and buttons, as identified in Table 10-4.

Table 10-4 Configure WAN MAN /WAN Data Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a WAN device.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a WAN device.
Service Level Selection Extension Point	Identifies the extension used to determine the DHCP criteria and Class of Service required for a device.

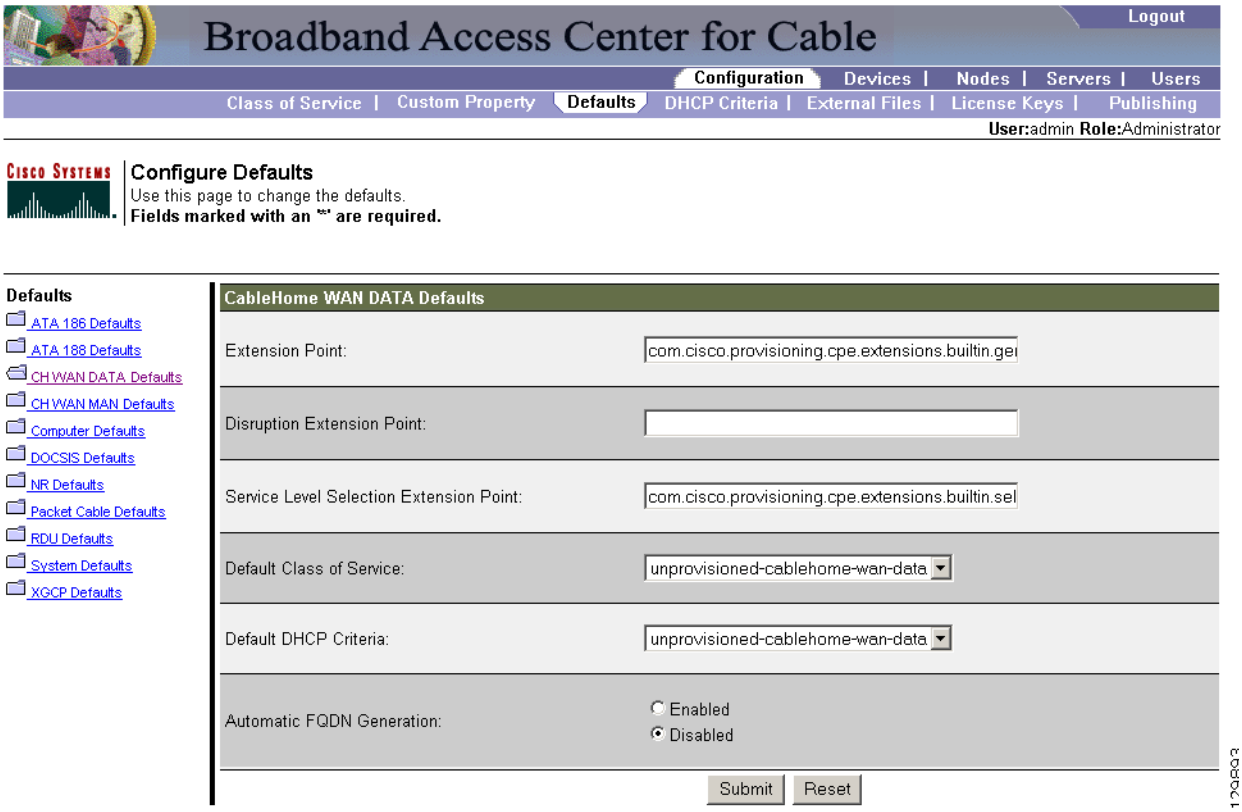
Table 10-4 Configure WAN MAN /WAN Data Defaults Page (continued)

Field or Button	Description
Default Class of Service	Identifies the current default class of service for a WAN-Data. New, unrecognized WAN devices are assigned to this class of service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP criteria for a specific device technology. New, unrecognized WAN devices are assigned this default DHCP criteria. Use the drop-down list to select a new default value.
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automated FQDN generation is disabled. **Note** See the "Automatic FQDN Generation" section on page 10-35 for additional information.

CableHome WAN Data Defaults

When you select the CableHome wide area network (WAN) Data defaults link, the CableHome Defaults page (see Figure 10-3) appears. Use this page to configure the WAN-Data device type.

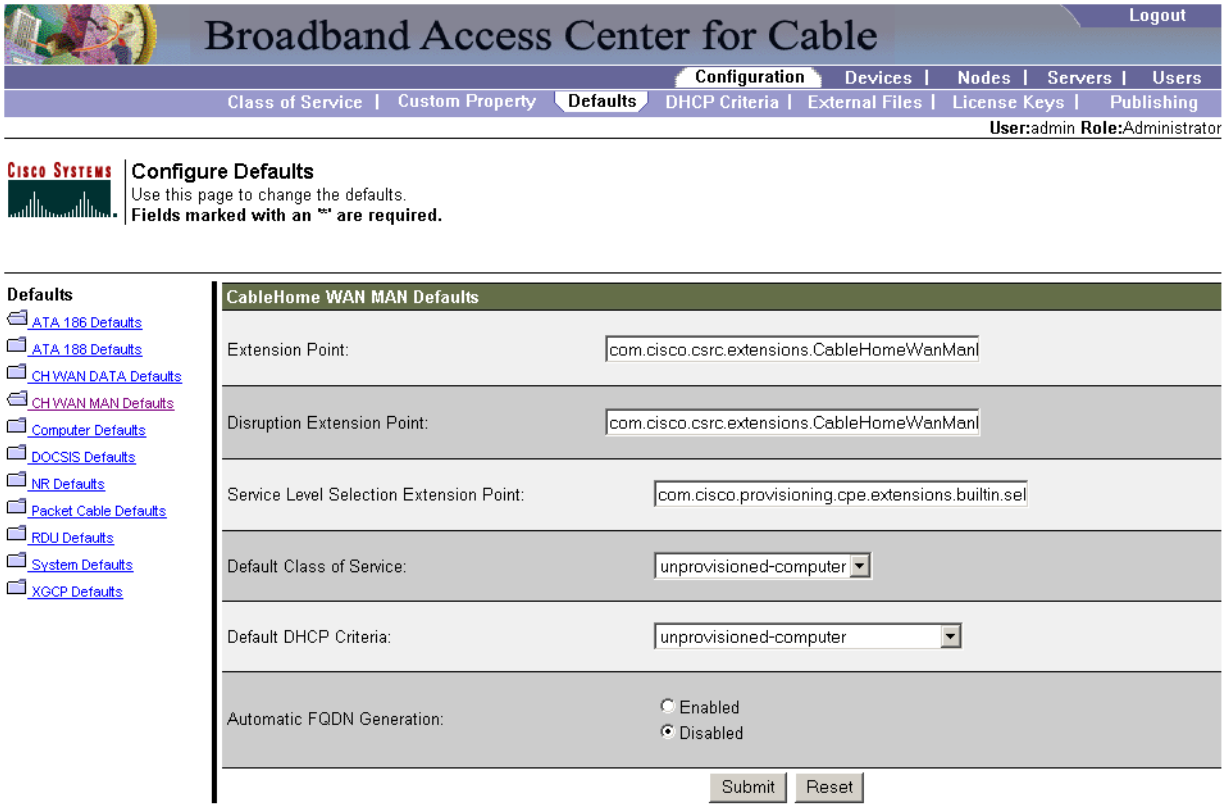
Figure 10-3 Configure CableHome WAN-Data Defaults Page



CableHome WAN-Man Defaults

When you select the CableHome WAN-Man defaults link, the CableHome WAN-Man Defaults page (see Figure 10-4) appears. Use this page to configure the WAN-Man device type.

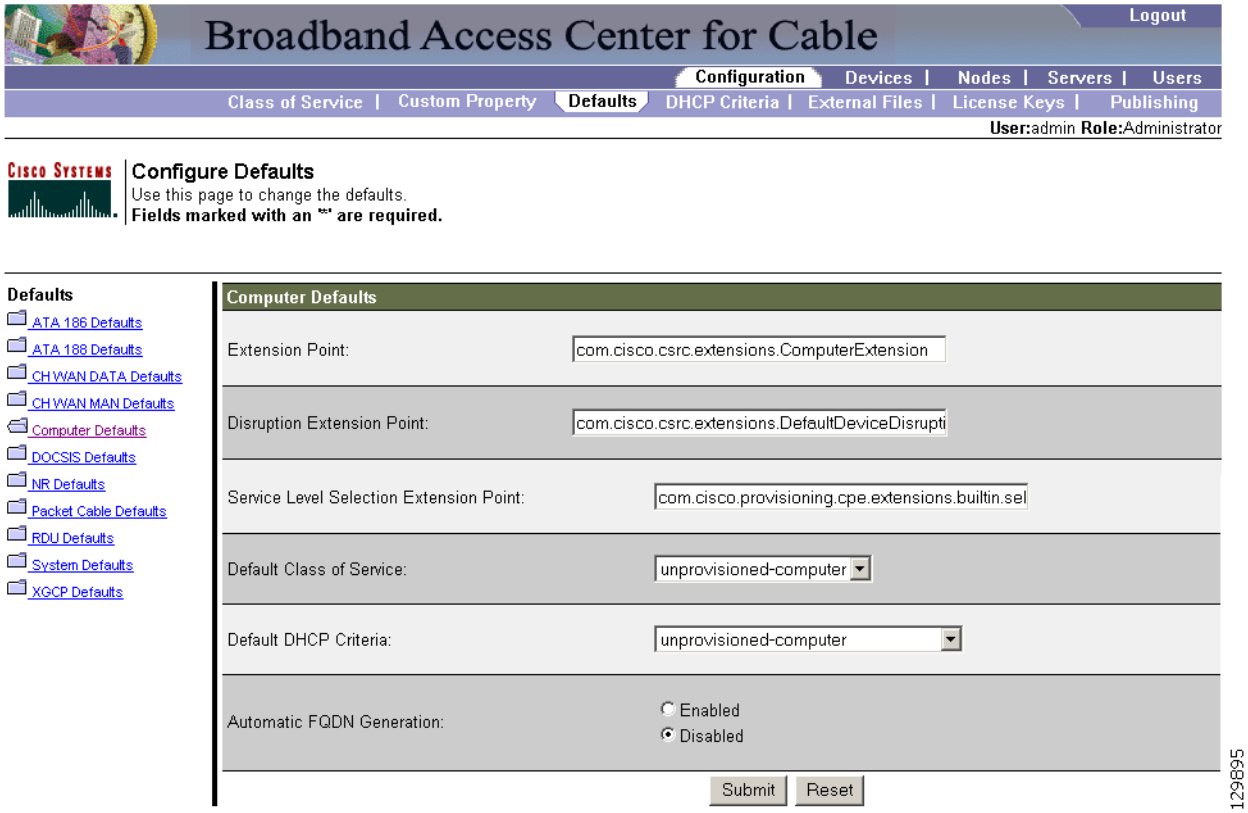
Figure 10-4 Configure CableHome WAN-Man Defaults Page



Computer Defaults

The Computer Defaults page (Figure 10-5) displays a list of default values currently applied to the computers supported by BACC.

Figure 10-5 Configure Computer Defaults Page



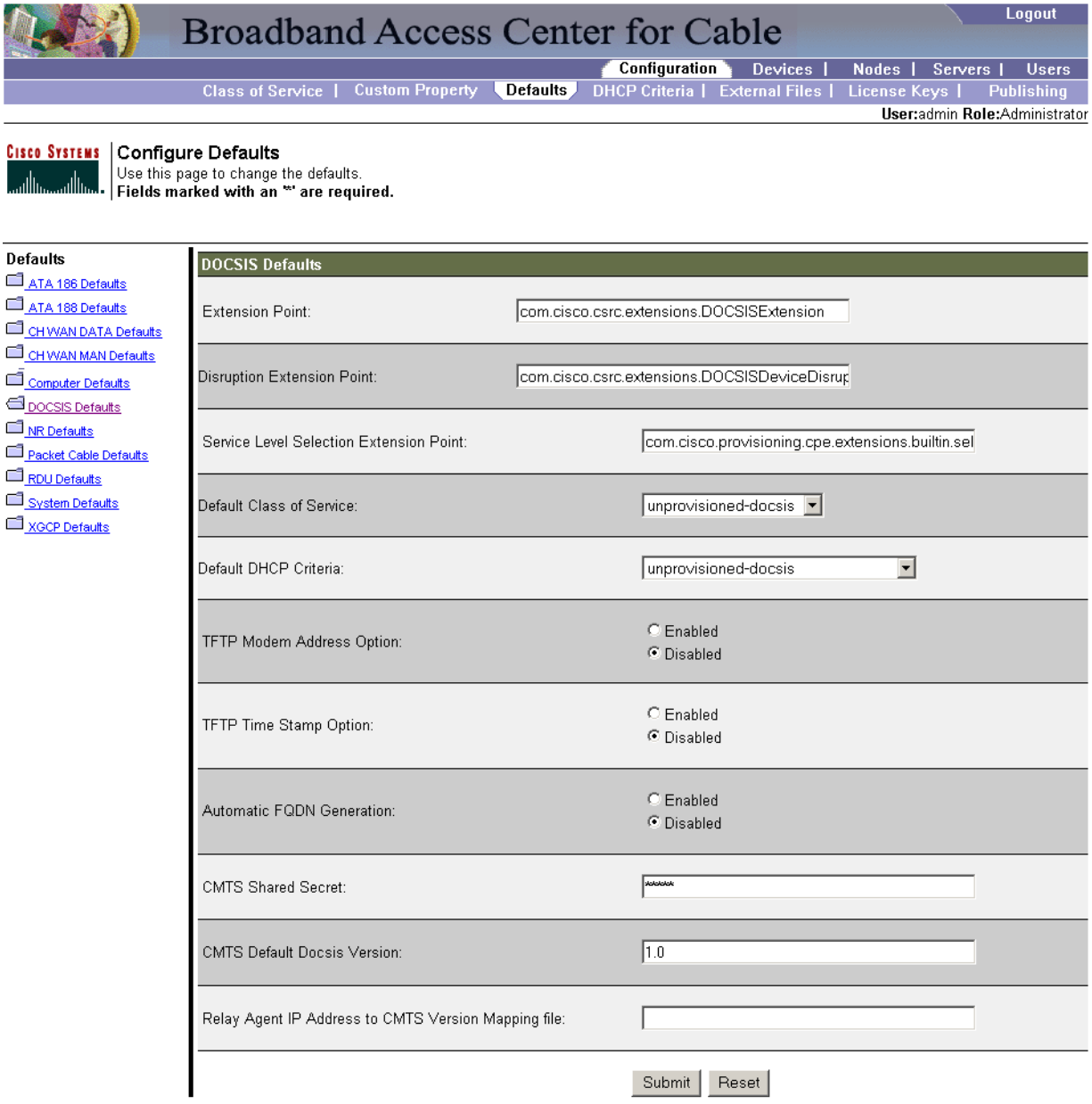
Refer to Table 10-3 for the description of all fields and buttons appearing in Figure 10-5.

Note Changes to the default Class of Service and default DHCP Criteria cause regeneration to occur. Any other changes made to this page will not affect the current devices.

DOCSIS Defaults

When the DOCSIS Defaults option is selected, the DOCSIS Defaults page appears. This page (Figure 10-6) displays a list of default DOCSIS values currently applied to cable modems supported by BACC.

Figure 10-6 Configure DOCSIS Defaults Page



Refer to Table 10-5 for the description of all fields and buttons appearing in Figure 10-6.

Note Changes to the default Class of Service and default DHCP Criteria cause regeneration to occur. Changes to any TFTP option come into effect starting from the next TFTP transfer.

Table 10-5 identifies the fields and buttons that are unique to this defaults page.

Table 10-5 Configure DOCSIS Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a DOCSIS device.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a DOCSIS device.
Service Level Selection Extension Point	Identifies the extension used to determine the DHCP criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default class of service for a device. New, unrecognized devices are assigned to this class of service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP criteria for a specific device technology. New, unrecognized devices are assigned this default DHCP criteria. Use the drop-down list to select a new default value.
TFTP Modem Address Option	Identifies whether the TFTP modem address option is enabled.
TFTP Time Stamp	Identifies whether the TFTP server will issue a time stamp.
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automated FQDN generation is disabled. **Note** See the "Automatic FQDN Generation" section on page 10-35 for additional information.
CMTS Shared Secret	Identifies the character string that BACC uses in the calculation of the CMTS MIC in the configuration file. The CMTS uses it to authenticate the configuration file that a cable modem submits to the CMTS for authorization.
CMTS Default Docsis Version	Specifies the default DOCSIS version used by all CMTSs. If you do not enter a DOCSIS version in this field, it will default to version 1.0.
Relay Agent IP Address to CMTS Version Mapping file	Identifies the mapping file used by the CMTS. This file specifies the DOCSIS version that the CMTS will use.

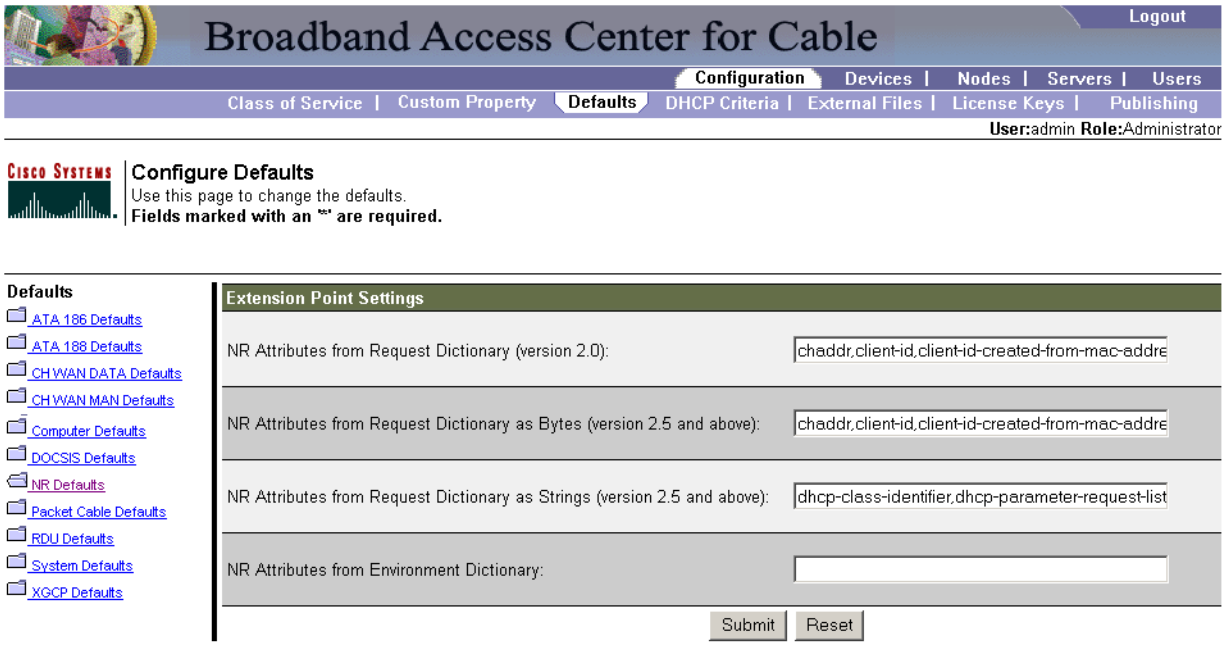
Note If you enable either or both of the TFTP options on this page, that appropriate TFTP information will be included in the TFTP file before it is sent to the DOCSIS cable modem.

Network Registrar Defaults

BACC provides Network Registrar (NR) extension points that allow BACC to pull information from an incoming DHCP packet(s) to detect a device's technology. They also let BACC respond to device DHCP requests with options that correspond to the configuration stored at the DPE.

When the NR Defaults option is selected, the NR Defaults page (see Figure 10-7) appears.

Figure 10-7 Configure Network Registrar Defaults Page



Refer to Table 10-6 for the description of all fields and buttons appearing in Figure 10-7.

Table 10-6 Configure Network Registrar Defaults Page

Field or Button	Description
NR Attributes from Request Dictionary (for 2.0 Extensions)	Identifies a comma-separated list of attributes pulled from the Network Registrar request dictionary, as strings, when sending a request to the RDU to generate a configuration for the current device. **Note** This property applies only to the BPR 2.0 Network Registrar extensions.
NR Attributes from Request Dictionary as Bytes (for 2.5 Extensions)	Identifies a comma-separated list of attributes pulled out of the Network Registrar request dictionary as bytes when sending a request to the RDU to generate a configuration for the current device. **Note** This property applies only to the BACC 2.5 (or higher) Network Registrar extensions.

Table 10-6 Configure Network Registrar Defaults Page (continued)

Field or Button	Description
NR Attributes from Request Directory as Strings (for 2.5 Extensions)	Identifies a comma-separated list of attributes pulled from the Network Registrar request dictionary as strings when sending a request to the RDU to generate a configuration for the current device. **Note** This property applies only to the BACC 2.5 (or higher) Network Registrar extensions.
NR Attributes from Environment Directory	Identifies a comma-separated list of attributes pulled out of the Network Registrar environment dictionary as strings when sending a request to the RDU to generate a configuration for the current device. **Note** This property applies to both BPR 2.0 and BACC 2.5 (or higher) Network Registrar extensions.
Submit	Activates or implements the changes you have made. After the administrative database has been updated to reflect the changes you make, modified changes appear in the Configure Defaults page.
Reset	Returns all settings to their previous setting.

Note Changes made to this page do not take effect until the Network Registrar extensions are reloaded.

PacketCable Defaults

The PacketCable Defaults page identifies those defaults necessary to support the PacketCable voice technology. When selected the PacketCable Defaults page (see Figure 10-8) appears.

Figure 10-8 Configure PacketCable (Voice Technology) Defaults Page

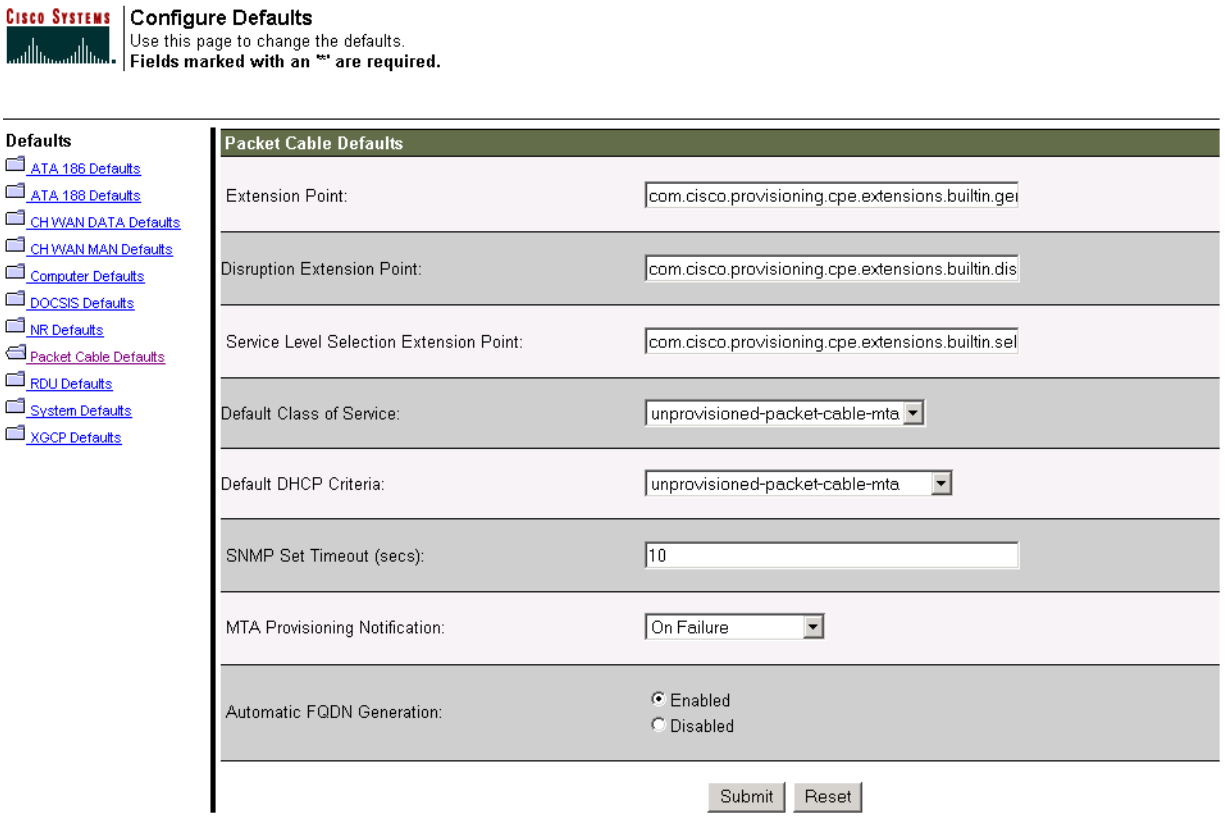


Table 10-7 identifies the fields and buttons that are unique to this defaults page.

Table 10-7 Configure PacketCable (Voice Technology) Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a device of this technology.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a device of this technology.
Service Level Selection Extension Point	Identifies the extension used to determine what DHCP criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default class of service for a device. New, unrecognized devices are assigned to this class of service. Use the drop-down list to select a new default value.

Table 10-7 Configure PacketCable (Voice Technology) Defaults Page (continued)

Field or Button	Description
Default DHCP Criteria	Identifies the current default DHCP criteria for a specific device technology. New, unrecognized devices are assigned this default DHCP criteria. Use the drop-down list to select a new default value.
SNMP Set Timeout	Identifies the SNMP set timeout in seconds.
MTA Provisioning Notification	Notification that an MTA event has taken place. An event occurs when the MTA sends its provisioning complete inform based on the selected choice. Options available include: • On Failure • On Success • During Provisioning • Always • Never
Automatic FQDN Generation	Identifies whether a fully qualified domain name (FQDN) will be generated.

RDU Defaults

When you select the RDU defaults link, the RDU Defaults page (see Figure 10-9) appears. Use this page to configure the RDU to communicate with Network Registrar. See the *Cisco CNS Network Registrar User's Guide* for additional information.

Figure 10-9 Configure RDU Defaults Page

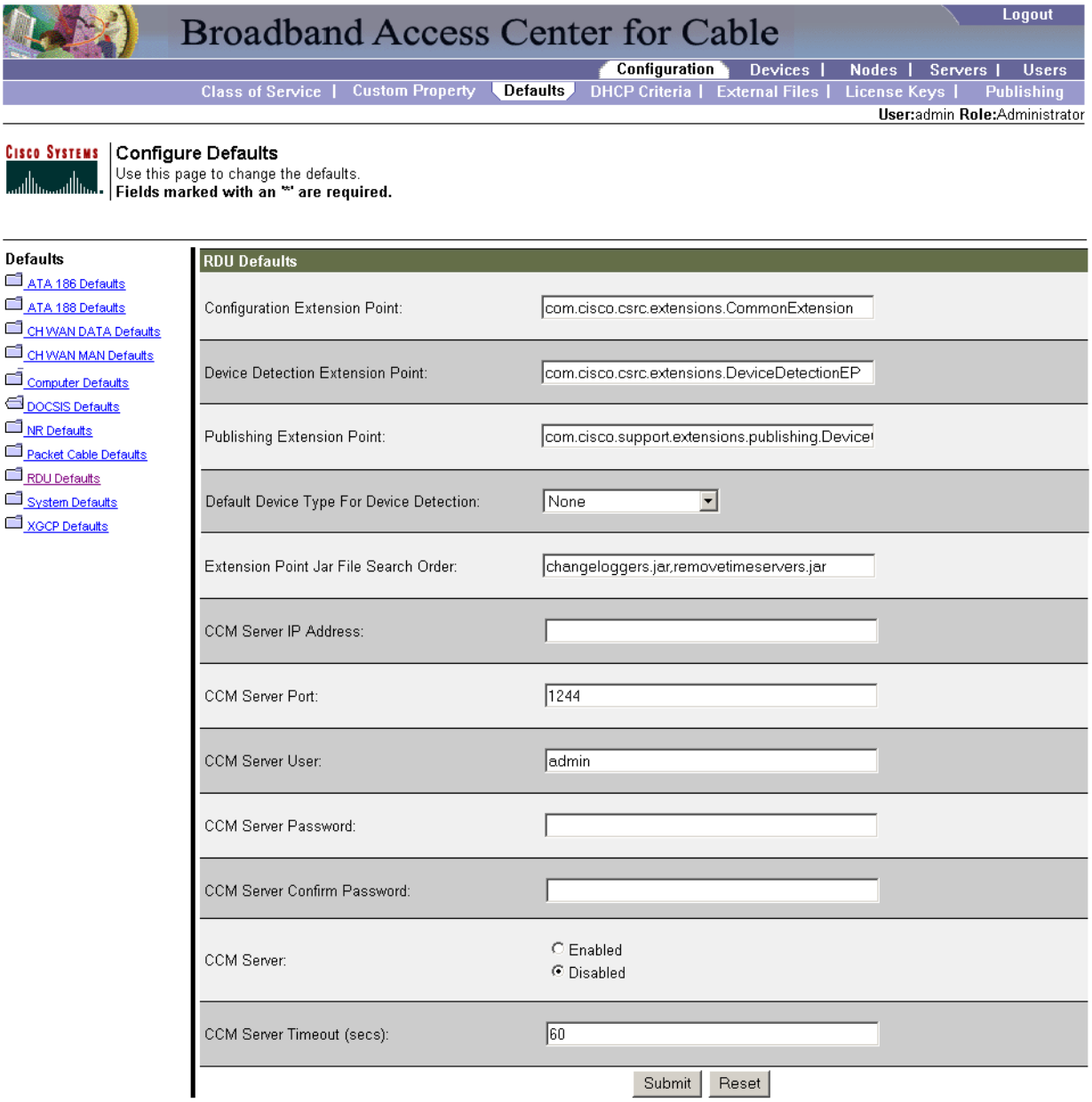


Table 10-8 describes all fields and buttons appearing in Figure 10-9.

Table 10-8 Configure RDU Defaults Page

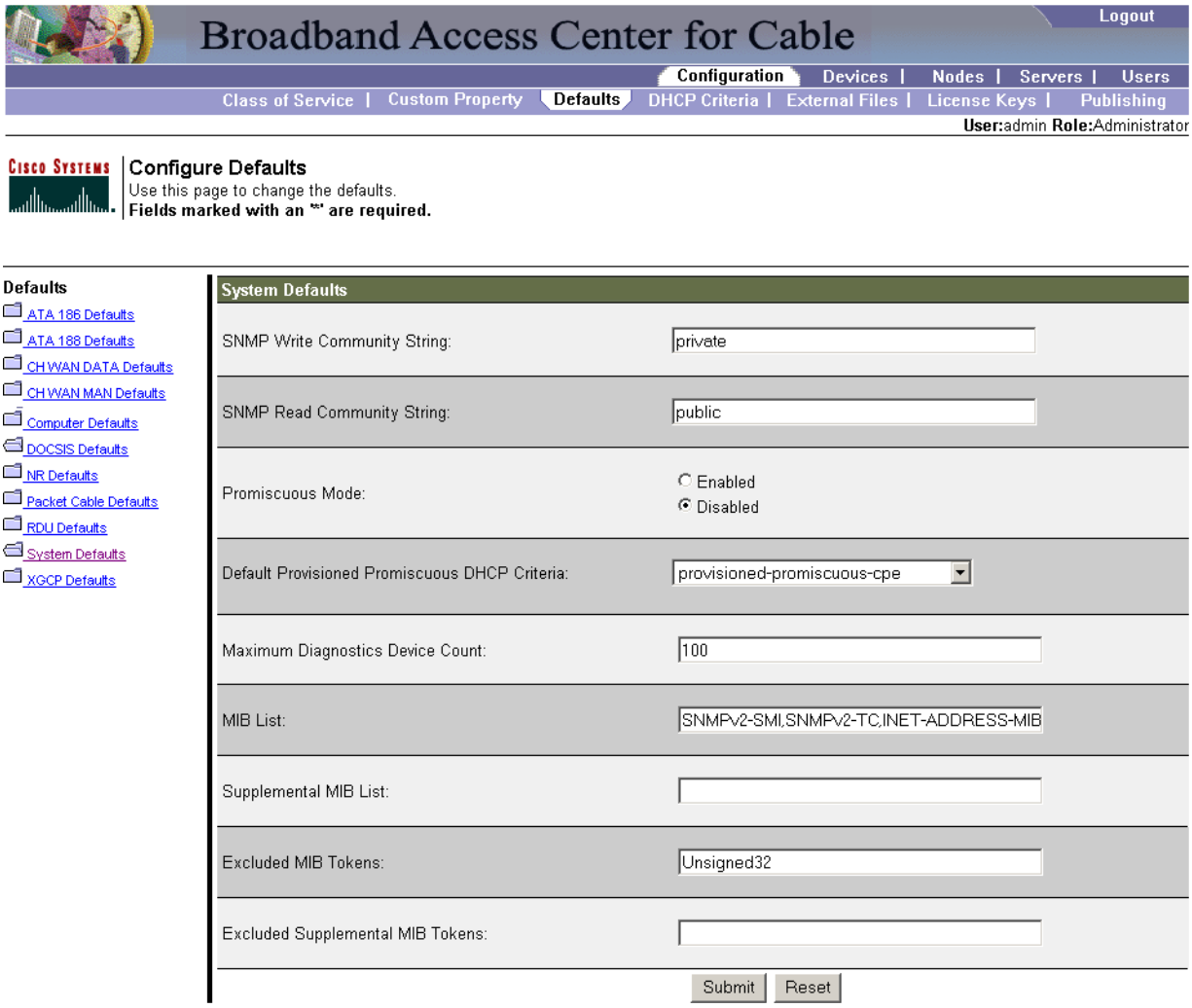
Field or Button	Description
Configuration Extension Point	Identifies the common extension points executed before any other technology extension point is executed.
Device Detection Extension Point	Identifies the extension point used to determine a device's type (for example DOCSIS or computer) based on information pulled from the device's DHCP DISCOVER requests.
Publishing Extension Point	Identifies the extension point to be used for an RDU publishing plug-in.This is useful when you need to publish RDU data into another database.
Extension Point Jar File Search Order	Specifies the sequence in which the classes are searched in the Jar files that are listed in the preceding four fields.
CCM Server IP Address	Identifies the CCM server's IP address.
CCM Server Port	Identifies the CCM server port on which BACC communicates.
CCM Server User	Identifies the CCM server user name and is used in conjunction with the password fields.
CCM Server Password	Identifies the password used to authenticate the CCM Server User.
CCM Server Confirm Password	Authenticates the CCM Server Password.
CCM Server	Specifies whether the BACC interface to the CCM Server is enabled or disabled.
CCM Server Timeout (ms)	Specifies the length of time that BACC attempts to connect with the CCM Server until BACC declares the connection down.

Note See the Managing Regional Distribution Unit Extensions, page 10-31 for related information on RDU extension points.

System Defaults

When you select the Systems Defaults link, the System Defaults page (see Figure 10-10) appears.

Figure 10-10 System Defaults Page



Note You can configure the default values using the BACC application program interface.

Table 10-9 describes all fields and buttons appearing in Figure 10-10.

Table 10-9 Configure System Defaults Page

Field or Button	Description
SNMP Write Community String	Identifies the default write community string for any device that may require SNMP information. The default write community string is **private**.

Table 10-9 Configure System Defaults Page (continued)

Field or Button	Description
SNMP Read Community String	Identifies the default read community string for any device that can read or access the SNMP MIB. The default read community string is **public**.
Promiscuous Mode	Identifies whether the Promiscuous mode is enabled. There are two options: • Enable—Enables the Promiscuous mode within BACC. • Disable—Disables the Promiscuous mode within BACC.
Default Provisioned Promiscuous DHCP Criteria	Identifies the default DHCP criteria used to provision a CPE in the Promiscuous mode, when the device that the CPE is behind does not have a CPE DHCP criteria specified.
Maximum Diagnostic Device Count	Identifies the maximum number of MAC addresses (devices) that you can troubleshoot at any one time.
MIB List	Identifies a list of MIBs used by the RDU that do not require restarting the RDU.
Supplemental MIB List	Identifies an extended list of MIBs used by the RDU.
Excluded MIB Tokens	Defines those key words, or tokens, that cannot be redefined by a MIB.
Excluded Supplemental MIB Tokens	Defines those additional key words, or tokens, that cannot be redefined by a MIB and do not appear in the Excluded MIB Tokens list.

Gateway (xGCP) Control Protocol Defaults

XGCP is a gateway control protocol that lets external call agents control gateways in a Voice over IP (VoIP) environment. The Configure XGCP Defaults page (Figure 10-11) displays a list of default values currently applied to the xGCP gateway devices supported by BACC.

Figure 10-11 Configure XGCP Page

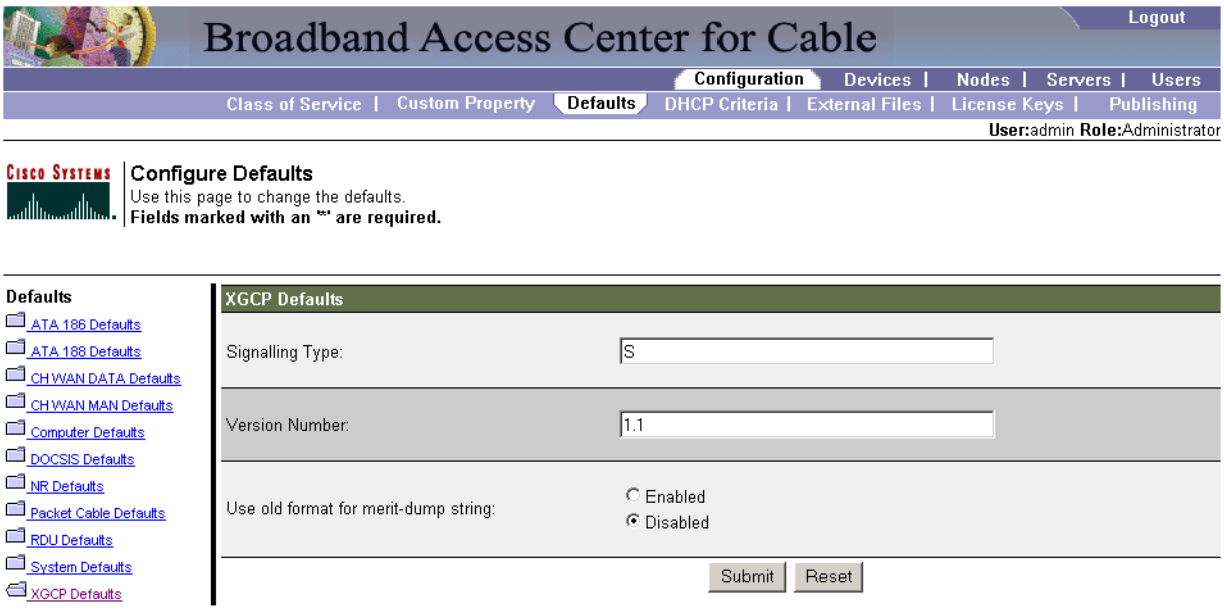


Table 10-10 describes all fields and buttons appearing in Figure 10-11.

Table 10-10 Configure XGCP Defaults Page

Field or Button	Description
Signalling Type	Identifies the xGCP signalling type, such as: S, M, and so on.
Version Number	Identifies the xGCP version number in use.
Use old format for merit-dump string	Enables or disables the use of the old string format, which does not include the version number.

Note Subsequent device configurations will include the changes you implement here. However, all existing configurations are not changed. To make the changes in any existing configuration, you must regenerate the configuration using the application programming interface (API).

Configuring DHCP Criteria

In BACC, DHCP criteria describe the specific criteria for a device when selecting a scope in Network Registrar. For example, a DHCP criteria called **provisioned-docsis** has an inclusion selection tag called **tagProvisioned**. The DHCP criteria is associated with a DOCSIS modem. When this modem requests an IP address from the Network Registrar, Network Registrar looks for scopes associated with the scope selection tag **tagProvisioned**.

To access the DHCP Criteria page:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **DHCP Criteria** from the Secondary Navigation bar and the Manage DHCP Criteria page appears.

Adding DHCP Criteria

To add a DHCP criteria:

Step 1 Click **Add**, on the DHCP Criteria page, and the Add DHCP Criteria page appears.

Step 2 Enter the name of the DHCP criteria you want to create.

Step 3 Enter the DHCP Criteria client-class name.

Step 4 Enter the inclusion and exclusion selection tags.

Note When creating new DHCP criteria, the client-class and Inclusion and Exclusion selection tag names you enter must be the exact names from within Network Registrar. Refer to the *Network Registrar User's Guide* and the *Network Registrar CLI Reference* for additional information about client-class and selection tags. You should specify either the Client Class, Inclusion Selection Tag or Exclusion Selection Tag names when creating a new DHCP criteria.

Step 5 You can add or modify the properties that are added on the DHCP criteria. Enter or select a Property Name, or select an existing name, and enter or modify the appropriate Property Value.

Step 6 Click **Add** after changing or creating the property name-property value pair.

Step 7 Click **Submit**. After the DHCP criteria is successfully added in the RDU database, it will be visible in the Manage DHCP Criteria Page.

Modifying DHCP Criteria

To modify existing DHCP criteria:

Step 1 On the Manage DHCP criteria page, click the DHCP criteria link that you want to modify and the Modify DHCP Criteria page appears.

Step 2 Make the desired changes to the client-class, inclusion and exclusion selection tags, and the property value settings.

Step 3 Click **Submit**. After successful modification of the DHCP criteria in the RDU Database, the Manage DHCP Criteria page appears.

Note Subsequent device configurations will include the changes you implement here. All existing configurations are regenerated, although the devices on the network will not get the new configuration until they are rebooted.

Deleting DHCP Criteria

Deleting DHCP criteria using the administrator application does not delete the actual DHCP server configurations from the DHCP server. You must delete the DHCP server configurations manually. To delete an existing criteria:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **DHCP Criteria** from the Secondary Navigation bar and the Manage DHCP Criteria page appears.

Step 3 Click the **Delete** icon corresponding to the criteria you want to delete, and a deletion dialog box appears.

Step 4 Click **OK** to delete the criteria or click **Cancel** to abort the operation. The Manage DHCP Criteria page appears.

Note You can delete a DHCP criteria only if there are no devices associated with that criteria, and it is not designated as the default DHCP criteria. If a DHCP criteria has devices associated, you must associate a different DHCP criteria before deleting the criteria.

Managing External Files

Using the BACC administrative user interface, you can manage the TFTP server files or template files for dynamic generation for DOCSIS, PacketCable MTAs, and WAN-Man files, or software images for devices (see Figure 10-12). You can add, delete, replace, or export any file type, including:

- Template files—These are text files that contain either DOCSIS, PacketCable, or CableHome options and values that, when used in conjunction with a particular class of service, provide dynamic file generation.

  Note Template files can be created in any text editor, but must have a tmpl file extension. Refer to the "Developing Template Files" section on page 12-1 for additional template information.

- Static configuration files—These files are used as a configuration file for a device. For example, a static configuration file called gold.cm would identify the gold DOCSIS class of service. BACC treats this file type like any other binary file.
- IOS images—These are images stored in firmware for a Cisco device. The Cisco device can upload the image to upgrade its functionality. BACC treats this file type like any other binary file.

Note Figure 10-12 is displayed after clicking the Search button on the Manage External Files page.

Figure 10-12 Manage External Files Page

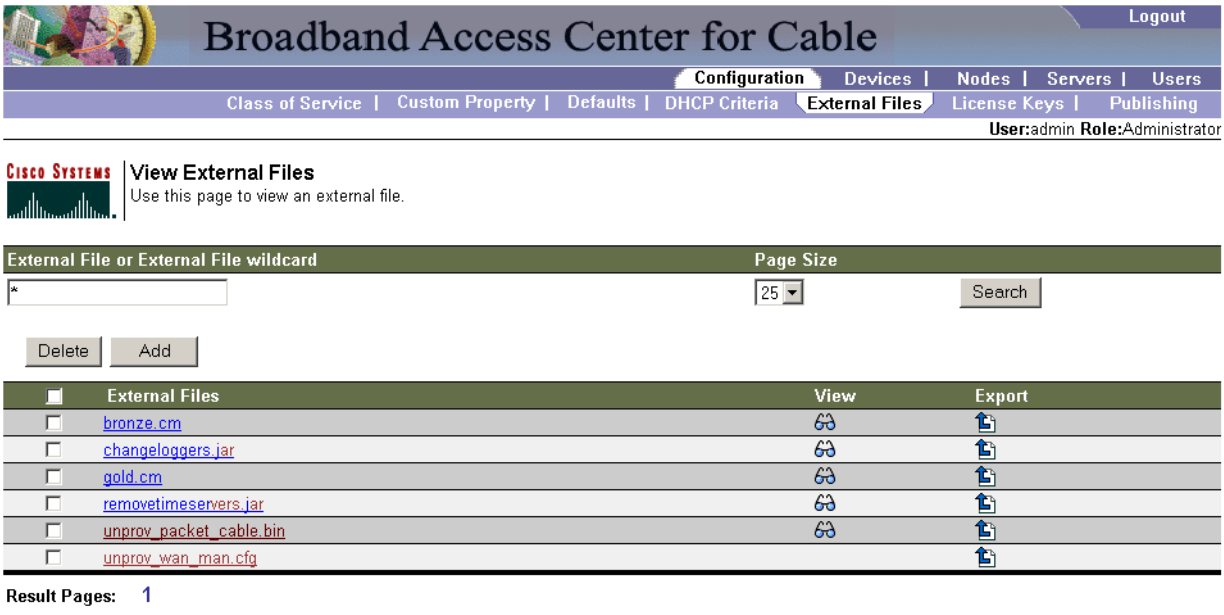


Table 10-11 identifies the fields and buttons shown in Figure 10-12.

Table 10-11 Manage External Files Page

Field or Button	Description
External Files	Identifies the filename. An asterisk (*) can be used as a wildcard character to allow searching for partial filenames. For example, you can enter ***.cm** to list all external files ending with the .cm extension. An example of an invalid wildcard is bronze*.
Page Size	Identifies the length of page to be displayed.
Search	Initiates the search for an external file with a name that matches the entry in the External Files field.
Delete	Removes any selected external file from the database.
Add	Adds a new file.
External Files list	Displays a list of external files that match the search criteria. **Note** The check boxes immediately to the left of any selected item in this list must be checked before it can be deleted.
View	Displays the details of the selected binary file.
Export	Exports any selected file to the client's computer.

Adding External Files

To add an existing external file:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **External Files** from the Secondary Navigation bar. The Manage External Files page appears.

Step 3 Click **Add** and the Add External Files page appears.

Step 4 Enter the **Source filename** and the **External filename**.

Note If you do not know the exact name of the source file, use the **Browse** function to navigate to the desired directory and select the file. By default, file sizes up to 12 MB are supported.

Step 5 Click **Submit.** The Manage External Files page appears to indicate that the file has been added.

Viewing External Files

To view the contents of a DOCSIS or PacketCable voice technology external file:

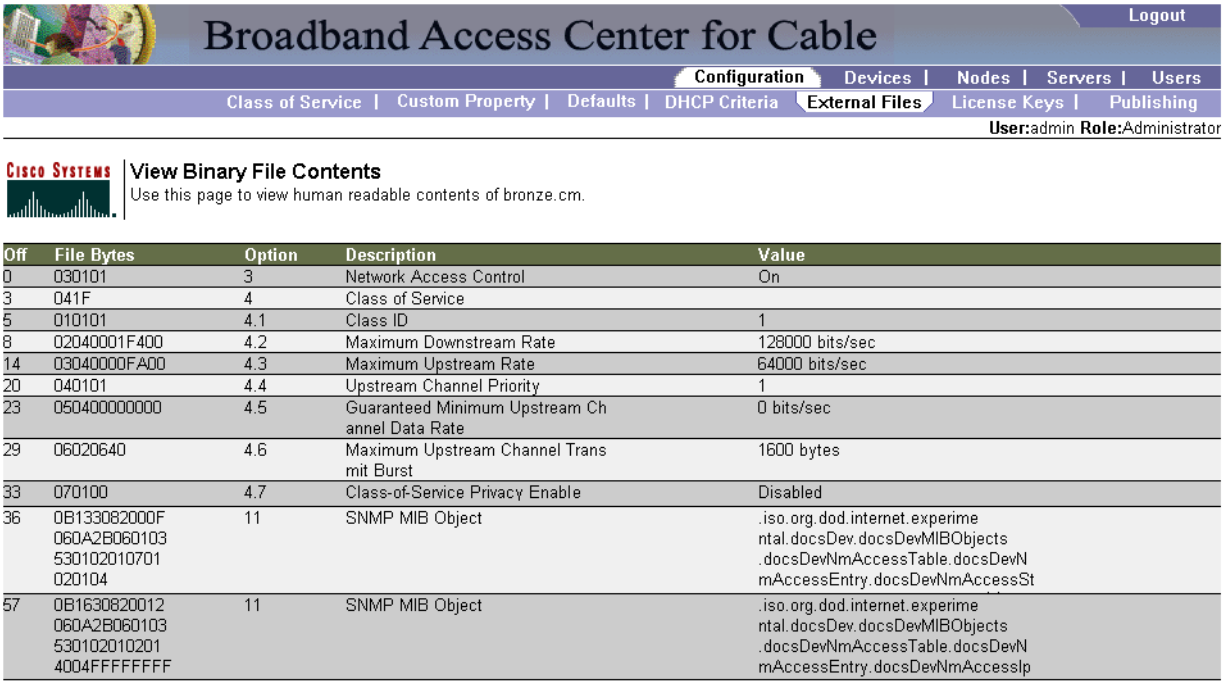
Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **External Files** from the Secondary Navigation bar. The Manage External Files page appears.

Step 3 Search for the required file using the search field and appropriate wildcard characters.

Step 4 Click the **Details** icon corresponding to the DOCSIS, CableHome WAN-Man, and PacketCable MTA binary configuration files and a View Binary File Contents page appears. Figure 10-13 identifies example binary file content and Figure 10-14 identifies example Jar file content.

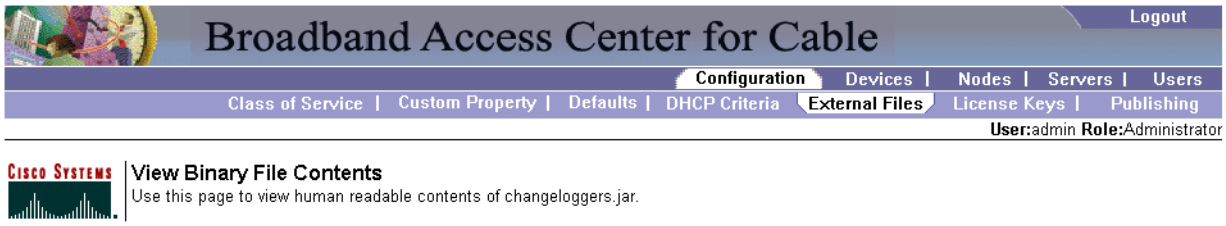
Figure 10-13 Example Binary File Content



Off	File Bytes	Option	Description	Value
0	030101	3	Network Access Control	On
3	041F	4	Class of Service	
5	010101	4.1	Class ID	1
8	02040001F400	4.2	Maximum Downstream Rate	128000 bits/sec
14	03040000FA00	4.3	Maximum Upstream Rate	64000 bits/sec
20	040101	4.4	Upstream Channel Priority	1
23	050400000000	4.5	Guaranteed Minimum Upstream Channel Data Rate	0 bits/sec
29	06020640	4.6	Maximum Upstream Channel Transmit Burst	1600 bytes
33	070100	4.7	Class-of-Service Privacy Enable	Disabled
36	0B133082000F 060A2B060103 530102010701 020104	11	SNMP MIB Object	.iso.org.dod.internet.experimental.docsDev.docsDevMIBObjects.docsDevNmAccessTable.docsDevNmAccessEntry.docsDevNmAccessSt
57	0B1630820012 060A2B060103 530102010201 4004FFFFFFFF	11	SNMP MIB Object	.iso.org.dod.internet.experimental.docsDev.docsDevMIBObjects.docsDevNmAccessTable.docsDevNmAccessEntry.docsDevNmAccessIp

129889

Figure 10-14 Example Jar File Content



Extension Point JAR File Details		
changeloggers.jar		
Main attributes		
Created-By	1.4.1_02 (Sun Microsystems Inc.)	
Implementation-Title	"Change Loggers"	
Implementation-Vendor	"Cisco Systems, Inc."	
Implementation-Version	"1.0"	
Manifest-Version	1.0	
Name	com/cisco/support/extensions/publishing	
Specification-Title	"Tracking Changes"	
Specification-Vendor	"General Cable, Inc."	
Specification-Version	"1.0"	
com.cisco.support.extensions.publishing.DeviceChangeLogger.class attributes		
Implementation-Title		"Device Change Logger"
Implementation-Version		"2.0"

129890

Replacing External Files

To replace an existing external file:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **External Files** from the Secondary Navigation bar.

Step 3 Select the link that corresponds to the file you want to replace from the search output list. The Replace External Files page appears. Note that the selected filename already appears on this page.

Step 4 Enter the path and filename of the source file to be used as a replacement for the displayed external filename.

Note If you do not know the exact name or location of the source file, use the **Browse** function to navigate to the desired directory and select the file.

Step 5 Click **Submit**. After submitting the replacement file, a confirmation page appears to indicate that, after replacement, BACC will regenerate configurations for the affected devices.

Step 6 Click **OK** and the Manage External Files page appears.

Note All devices using this file through a class of service are regenerated after the replacement is finished.

Exporting External Files

You can copy external files to your local hard drive using the export function.

Note The procedure described below assumes that you are using Internet Explorer. This procedure is different if you are using Netscape Navigator.

To export a file:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **External Files** from the Secondary Navigation bar.

Step 3 Identify the external file that you want to export.

Step 4 Click the **Export** icon and you are prompted to either open the file or save it.

Step 5 Return to the BACC user interface.

Deleting External Files

Complete this procedure to delete an existing external file:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **External Files** from the Secondary Navigation bar.

Step 3 In the **External Files** field, enter the filename of the external file that you want to modify.

Step 4 Click **Search**. The appropriate file will appear in the External Files list.

Step 5 Choose the appropriate file or files.

Step 6 Click **Delete**.

Caution Deleting a template file that is not directly linked to a class of service, but is referenced by another template file that is linked to a class of service, will cause the configuration regeneration service to fail.

Note You cannot delete a file that has a class of service associated with it. You must remove the class of service association before proceeding. See the "Configuring the Class of Service" section on page 10-1 for additional information.

Managing License Keys

Software licenses are used to activate specific features or to increase the functionality of your installation. Each license is available as either a permanent license or an evaluation license.

- Permanent—A permanent license is purchased for use in your network environment and activates the specific features for which it is intended.
- Evaluation—An evaluation license enables functionality for a specific amount of time after installation. You can upgrade an evaluation license to a permanent license by entering a new permanent license number.

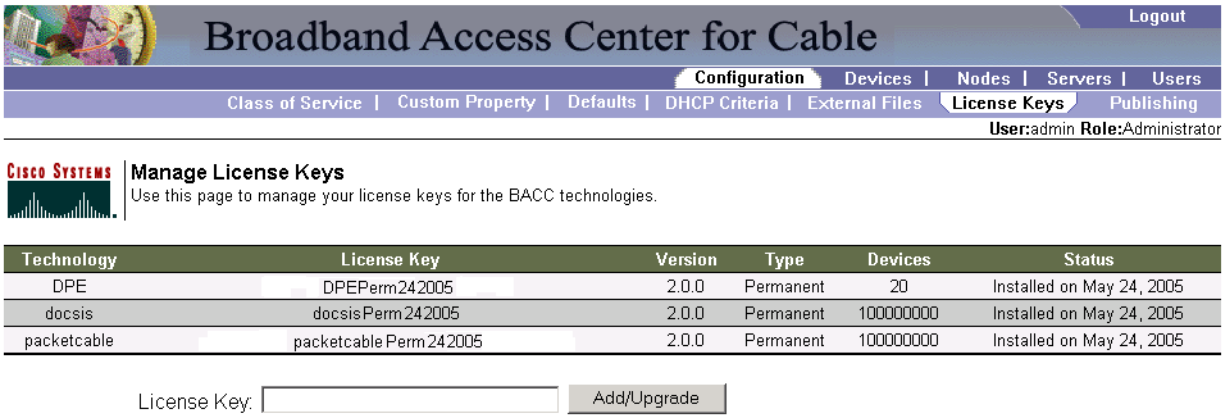
Caution Do not attempt to deploy into a fully operational network with an evaluation license key installed. Any provisioning done using an evaluation license will be disabled when that evaluation license expires.

When you upgrade from an evaluation license to a permanent license, you do not have to re-install the software. You can perform the upgrade directly from the BACC administrator user interface; you do not have to repeat the entire installation process.

The Manage License Keys page (Figure 10-15) displays a list of licenses that have been entered for your implementation. This BACC release supports both evaluation and permanent licenses for high-speed data (DOCSIS cable modems), PacketCable MTAs, ATAs, DPEs, CableHome WAN-Man and WAN-Data devices, and computers. The status of each available license is displayed as active, expired, not installed, or identifies the expiration date.

Note You can upgrade your evaluation licenses to permanent status. You can also upgrade a permanent license to increase the number of authorized devices. When you reach the limit of your number of licensed devices you cannot provision new devices, but existing devices that are already provisioned continue to receive service.

Figure 10-15 Manage License Keys Page



Adding and Modifying a License

To add, modify, or upgrade a license:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Licenses** from the Secondary Navigation bar.

Step 3 Obtain your new license key from either your Cisco Systems, Inc. representative or the Cisco Technical Assistance Center (TAC) website. See the Preface in this guide for TAC contact information.

Step 4 Enter the new license key in the License Key field.

Step 5 Click **Add/Upgrade** to install the new license key. If you enter a permanent license key, it overwrites the corresponding evaluation key (if that key was installed). If you enter a license key (permanent or evaluation) for a new technology, it will appear in the technology list.

Managing Regional Distribution Unit Extensions

Creating a custom extension point is essentially a programming activity that can, when used in conjunction with the BACC administrator' s user interface, allow you to expand the quantity of device types and technologies supported.

Managing extensions includes:

- Writing a New Class, page 10-31
- Installing RDU Custom Extension Points, page 10-31
- Viewing RDU Extensions, page 10-32

Note You can specify multiple extension points by making them run one after another. You do this by specifying the extensions points in a comma-separated list.

Writing a New Class

This procedure is included to better illustrate the entire custom extension creation process. You can create many different types of extensions; for the purposes of this procedure the a new Publishing Extension Point is used.

To write the new class:

Step 1 Create a Java source file for the custom publishing extension.

Step 2 Create a manifest file for the Jar file that will contain the extension class.

Step 3 Create the Jar file for the custom extension point. You can give the jar file any name you wish although the name given should be descriptive in nature and not be a duplicate of any other existing Jar file.

Installing RDU Custom Extension Points

After a Jar file is created, use the administrator's user interface to install it:

Step 1 Use the "Adding External Files" procedure on page 10-26 to add the new Jar file.

Note Use the Browse function to locate the Jar file created in the "Writing a New Class" procedure on page 10-31 and select this file as the Source File; leaving the External File Name blank assigns the same file name for both source and external. The external file name is what you will see through the Administrator's user interface.

Step 2 Click **Submit**.

Note An error message is generated if the class name does not exist within the jar file or if BACC detects any other errors.

Step 3 Return to the RDU Defaults page and note that the newly added Jar file appears in the Extension Point Jar File Search Order field.

Step 4 Enter the extension class name in the Publishing Extension Point field.

Step 5 Click **Submit** to commit the changes to the RDU database.

Step 6 View the RDU extensions to ensure that the correct extensions are loaded.

Viewing RDU Extensions

You can view the attributes of all RDU extensions directly from the View Regional Distribution Unit Details page. This page displays details on the installed extension Jar files and the loaded extension class files. See Viewing Regional Distribution Unit Details, page 9-24.

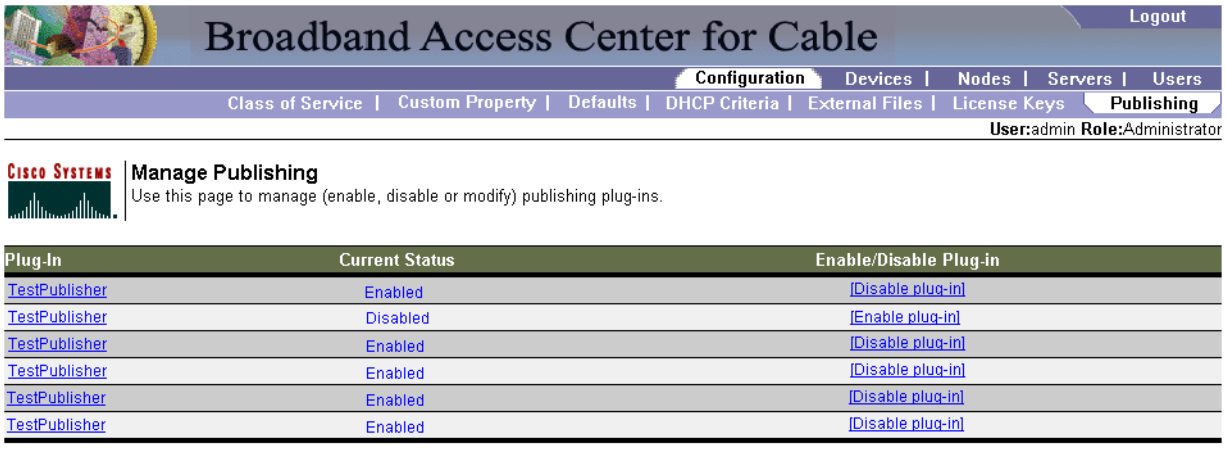
Publishing Provisioning Data

BACC has the capability to publish the provisioning data it tracks to an external datastore in real time. To do this, a publishing plug-in must be developed to write the data to the desired datastore. The Manage Publishing page, shown in Figure 10-16, identifies information such as the plug-in name, its current status (whether it is enabled or disabled), and switch to enable or disable it.

You can enable as many plug-ins as required by your implementation but care must be exercised because the use of publishing plug-ins can decrease system performance.

Note BACC does not ship with any publishing plug-ins. You must create your own plug-ins and then manage them from this page. The plug-ins shown in Figure 10-16 are for illustration only.

Figure 10-16 Manage Publishing Page



Publishing Datastore Changes

To publish changes to an external datastore:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Publishing** from the Secondary Navigation bar. The Manage Publishing page appears as shown in Figure 10-16. This page displays a list of all available database plug-ins and identifies the current status of each.

Step 3 Click on the appropriate status indicator to enable or disable the required plug-in. Note that as you click the status, it toggles from enabled to disabled. (See Figure 10-16.)

Modifying Publishing Plug-In Settings

These settings are a convenient way for plug-in writers to store plug-in settings in the RDU for their respective datastore. To modify the publishing plug-in settings:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Publishing** from the Secondary Navigation bar and the Manage Publishing page appears.

Step 3 Click the link corresponding to the plug-in you want to modify. The Modify Publishing Plug-Ins page appear.

Table 10-12 identifies the fields shown in the Modify Publishing Plug-Ins page.

Table 10-12 Modifying Publishing Plug-ins Page

Field or Button	Description
Plug-In	Identifies publishing plug-in name.
Server	Identifies the server name on which the data store resides.
Port	Identifies the port number on which the data store resides.
IP Address	Identifies the IP address of the server on which the data store resides. This is usually specified when the server name is not used.
User	Identifies the user to allow access to the data stored.
Password	Identifies the user's password which allows access to the data stored.
Confirm Password	This is used to confirm the password entered above.

Step 4 Enter the required values in the Server, Port, IP Address, User, Password, and Confirm Password fields. These are all required fields and you must supply this information before proceeding.

Step 5 Click **Submit** to make the changes to the selected plug-in, or click **Reset** to clear all fields on this page.

Configuring the SRV Record in the Network Registrar DNS Server

You must configure the Network Registrar DNS server to operate with the KDC. Refer to your Network Registrar documentation, and these instructions, to perform this configuration.

Note It is recommended that you create a zone name that matches the desired realm name, and that the only DNS record in this special zone (other than the records required by the DNS server to maintain the zone) should be the SRV record for the realm. This example assumes that the desired Kerberos realm is voice.acme.com, and that all other KDC, Network Registrar, and DPE configuration has been performed. The FQDN of the KDC is assumed to be kdc.acme.com.

Step 1 Start the **nrcmd** CLI (usually located under /opt/nwreg2/local/usrbin), and enter your username and password.

Step 2 Enter this command to create a zone for the Kerberos realm:

```
nrcmd> zone voice.acme.com create primary <address of nameserver> hostmaster
```

Step 3 Enter this command to add the SRV record to the new zone:

```
nrcmd> zone voice.acme.com. addRR _kerberos._udp. srv 0 0 88 <address of KDC>
```

Step 4 Enter these commands to save and reload the DNS server:

```
nrcmd> save
nrcmd> dns reload
```

Configuring SNMPV3 Cloning on the RDU and DPE for Secure Communication with PacketCable MTAs

BACC lets you enable an external network manager for SNMPV3 access to MTA devices. Additionally, the RDU is capable of performing SNMPV3 operations in a specific MTA.

To enable this capability, set the security key material at the DPEs and RDU. After the key material has been set, the BACC API calls that are used to create cloned SNMPV3 entries are enabled.

Note Enabling this capability will impact provisioning performance.

Creating the Key Material and Generating the Key

Creating the key material is a two-step process. First, run a script command on the RDU and then run a CLI command on the DPE.

Note This shared secret is not the same shared secret as the CMTS or the BACC shared secrets.

To create the key material:

Step 1 From the <BACC_HOME>/rdu/bin directory, run this script on the RDU:

```
generateSharedSecret.sh <password>
```

Where the <password> is any password, 6 to 20 characters in length, that you create. This password is then used to generate a 46 byte key. This key is stored in a file, called keymaterial.txt, that is located in the <BACC_HOME>/rdu/conf directory.

Step 2 Run the **packetcable snmp key-material** DPE CLI command, with the <password> used in step 1 to generate that key, on all DPEs for which this voice technology is enabled.

This generates the same 46 byte key on the DPE and ensures that the RDU and DPE(s) are synchronized and can communicate with the MTA securely.

Automatic FQDN Generation

When configuring the PacketCable voice technology, a fully qualified domain name (FQDN) must reside in the BACC database for each voice device, whenever the KDC queries the registration server for that FQDN. The BACC automatic FQDN generation feature is not limited to use by any single voice technology; it can be used by any BACC technology.

Automatically Generated FQDN Format

An automatically generated FQDN in BACC follows this format:

```
prefix<htype>-<hlen>-aa-bb-cc-dd-ee-ffsuffix.domain
```

Where:

- prefix, suffix, and domain—Identify information set using either the BACC administrators user interface or the provisioning API.

Note In the example FQDN used here, *prefix1,6,aa-bb-cc-dd-ee-ffsuffix* is the generated host name and *domain* is the domain name.

- 1,6,aa-bb-cc-dd-ee-ff—is the device MAC address

The entry of a prefix and suffix property is optional. If you do not specify these properties, and a host name is not specified during PacketCable MTA provisioning and, if neither the prefix nor suffix property is defined in the BACC property hierarchy, the device's MAC address followed by the domain name are used as the generated FQDN.

For example:

A device with the MAC address **1,6,aa:bb:cc:dd:ee:ff** will have this FQDN generated:

```
aa-bb-cc-dd-ee-ff.domain
```

Specifically, when configuring for PacketCable and many other technologies, the domain name property must also be configured. If you do not specify a domain name while provisioning a PacketCable MTA, the BACC property hierarchy is searched and, if it is not found, the MTA is not provisioned. However, if you do specify the domain name during MTA provisioning, that domain name will be used regardless of the domain name property that is specified in the BACC property hierarchy.

Properties for Automatically Generated FQDNs

Properties can be defined at any acceptable point in the BACC property hierarchy. You can use the System Defaults, Technology Defaults, DHCP Criteria, or Class of Service to accomplish this, and you can also do this at the device level.

FQDN Validation

There are a few things to consider when entering the information that is used to generate an FQDN. These include:

- Use valid alphanumeric characters only in the generated FQDN.
- Keep the length of each label (characters between the dots in the generated FQDN) to fewer than 63 characters.
- Do not allow the overall length of the generated FQDN to exceed 254 characters.

Note The FQDN supports host and domain names as per RFC1035.

Sample Automatic FQDN Generation

This section provides an example of creating an automatically generated FQDN.

Step 1 Choose the appropriate class of service, and set the /fqdn/domain property value to the DNS domain for all devices using this class of service. For the purposes of this example, assume that the domain in use is **pctest.com**, and that you want to provision a set of PacketCable devices into that domain.

Note If a domain is not specified, devices in the class of service will not receive a DHCP configuration from BACC.

Step 2 Click **Submit**.

In this example, a device with MAC address 1,6,aa:bb:cc:dd:ee:ff will yield an automatically generated FQDN of 1-6-aa-bb-cc-dd-ee-ff.pctest.com. Additionally, the Automatic FQDN Generation field should be enabled in the device's default configuration.