Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator

TAC Notice: What's Changing on TAC Web

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send

Contents

Introduction
Prerequisites
- Requirements
- Components Used
- Conventions

DOCSIS Configuration File Generation Tools
Installing the Cisco Standalone CPE Configurator
Creating Simple DOCSIS 1.0 Configuration Files
- Creating a standard.cm File
- Creating a premium.cm File
- Creating a disabled.cm Configuration File

Setting SNMP Variables
- Setting an SNMP Community String
- Modification of standard.cm to Include SNMP Parameters
- Modification of premium.cm to Include SNMP Parameters
- Modification of disabled.cm to Include SNMP Parameters
- IP and LLC Filters
- Other SNMP Variables

Cisco Vendor-Specific Fields
- IOS Configuration File Download
- Cisco IOS Configuration Commands
- Number of Phone Lines and Upstream Rate Limiting on IP Precedence

Performing a Firmware Upgrade via the DOCSIS Configuration File
Overriding the Downstream Frequency used by a Cable Modem
Overriding the Upstream Channel used by a Cable Modem
Miscellaneous Settings
- Configuring a DOCSIS Configuration File Shared-Secret

Downloadable DOCSIS Configuration Files
Conclusion
NetPro Discussion Forums - Featured Conversations
Related Information

Introduction

The Data-over-Cable Service Interface Specifications (DOCSIS) requires that a DOCSIS-compliant cable modem download a DOCSIS configuration file during its power-on or reset sequence. A Trivial File Transfer Protocol (TFTP) server is used for this purpose. This file contains important operational parameters and information for the cable modem, such as the maximum allowed upstream (US) and downstream (DS) rates, the

number of customer premises equipment (CPE) allowed to be supported by the modem, and whether the connected CPE is even allowed access to the service provider's network. This file must be in the format described in the DOCSIS Radio Frequency Specification (SP-RFI-IOS-991105). The information stored in the DOCSIS configuration files is in binary format.

This document describes how to create a simple DOCSIS configuration file with the Cisco Standalone Configurator tool, and it explains how to set the most frequently used fields. In addition, some advanced DOCSIS configuration file examples are presented.

Prerequisites

Requirements

The reader should have a basic understanding of the DOCSIS protocol.

Components Used

The information in this document is based on the DOCSIS CPE Configurator version 3.7 (version 3.2 is no longer available).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

DOCSIS Configuration File Generation Tools

There are a number of tools available that allow you to create and edit DOCSIS configuration files. In this document, the Cisco Standalone DOCSIS CPE Configurator version 3.2 is used in all examples. Since then, Cisco has developed version 3.7, and now the most current version is 4.0. If you are a registered user, you can order the latest version Cisco Broadband Configurator Release 4.0 (CBC 4.0). CBC 4.0 has advanced features, as it also contains DOCSIS 1.1 capabilities. You can still configure DOCSIS 1.0 with the CBC 4.0 tool to satisfy this document.

Another commonly used tool is the online DOCSIS CPE Configurator (registered customers only) . This tool may be used to create DOCSIS configuration files; it can not, however, directly edit DOCSIS configuration files.

Both Cisco tools have extensive help included and provide information on what each field means and how to use them properly. It also colors mandatory fields red, to differentiate them from optional fields.

Other DOCSIS cable modem and cable modem termination system (CMTS) vendors also publish DOCSIS configuration file generation and editing tools. The concepts presented in this document should apply to these other tools, as well as to the Cisco tools.

Installing the Cisco Standalone CPE Configurator

CBC 4.0 runs on Windows, Solaris, and Linux platforms. Instructions to successfully install CBC 4.0 can be found in the Quick Start Guide for Installing Cisco Broadband Configurator Release 4.0.

Creating Simple DOCSIS 1.0 Configuration Files

Creating a standard.cm File

The first DOCSIS configuration file example that is going to be created is a file called standard.cm. This file directs a cable modem to allow a downstream rate of 500 kbps and an upstream rate of 64 kbps. In addition, only one CPE device is allowed to connect to the cable modem. This file is created in the DOCSIS 1.0 compliant format.

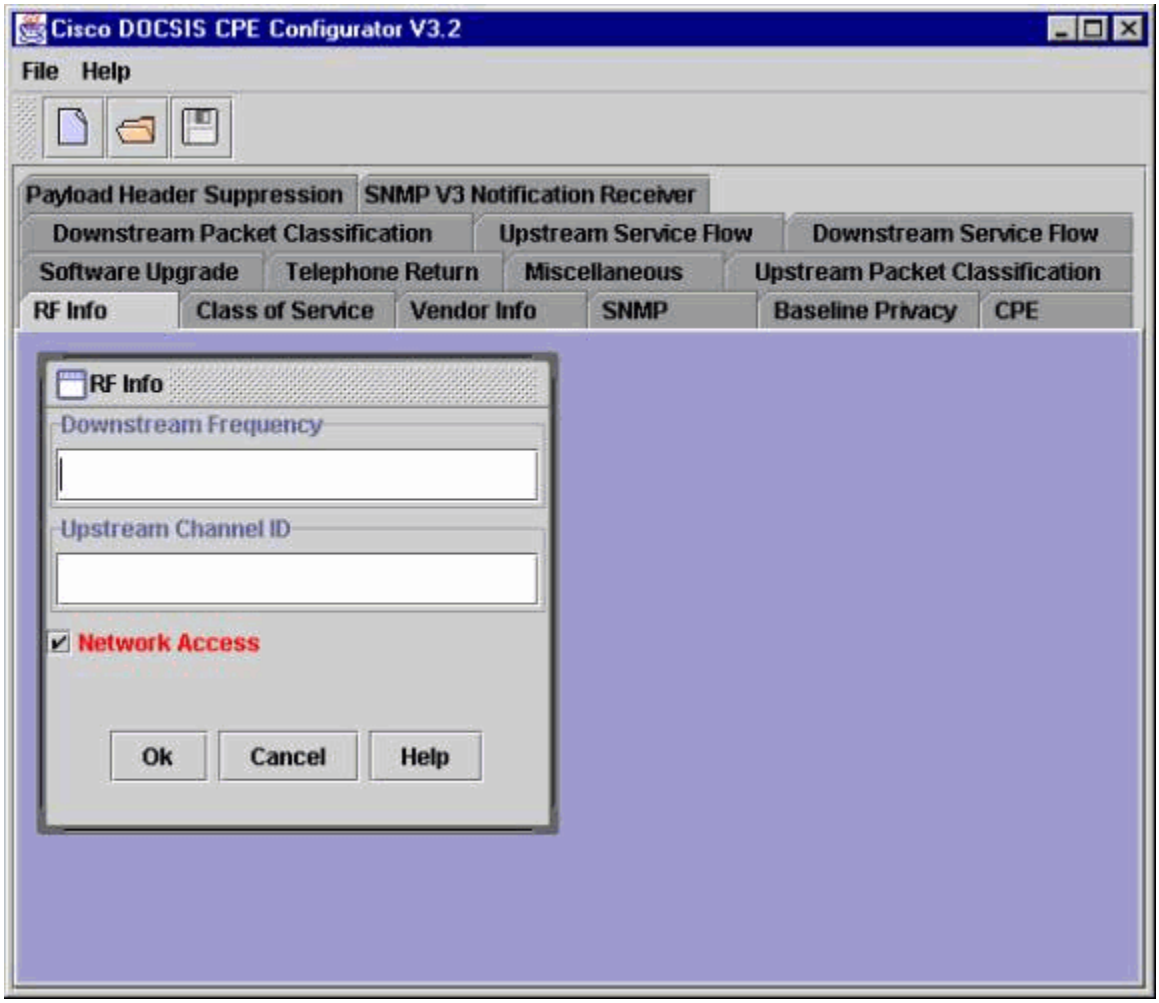
1. Launch the Configurator.

   The RF Info tab appears.

2. Check the **Network Access** check box. This is a mandatory field.

   Make sure that the Network Access box is checked; otherwise the CPE does not have network connectivity and no CPE devices behind the cable modem are allowed to obtain network access. For a detailed explanation on what the Downstream Frequency and Upstream Channel ID mean and when to set those values, click the **Help** button at the bottom of the tab.

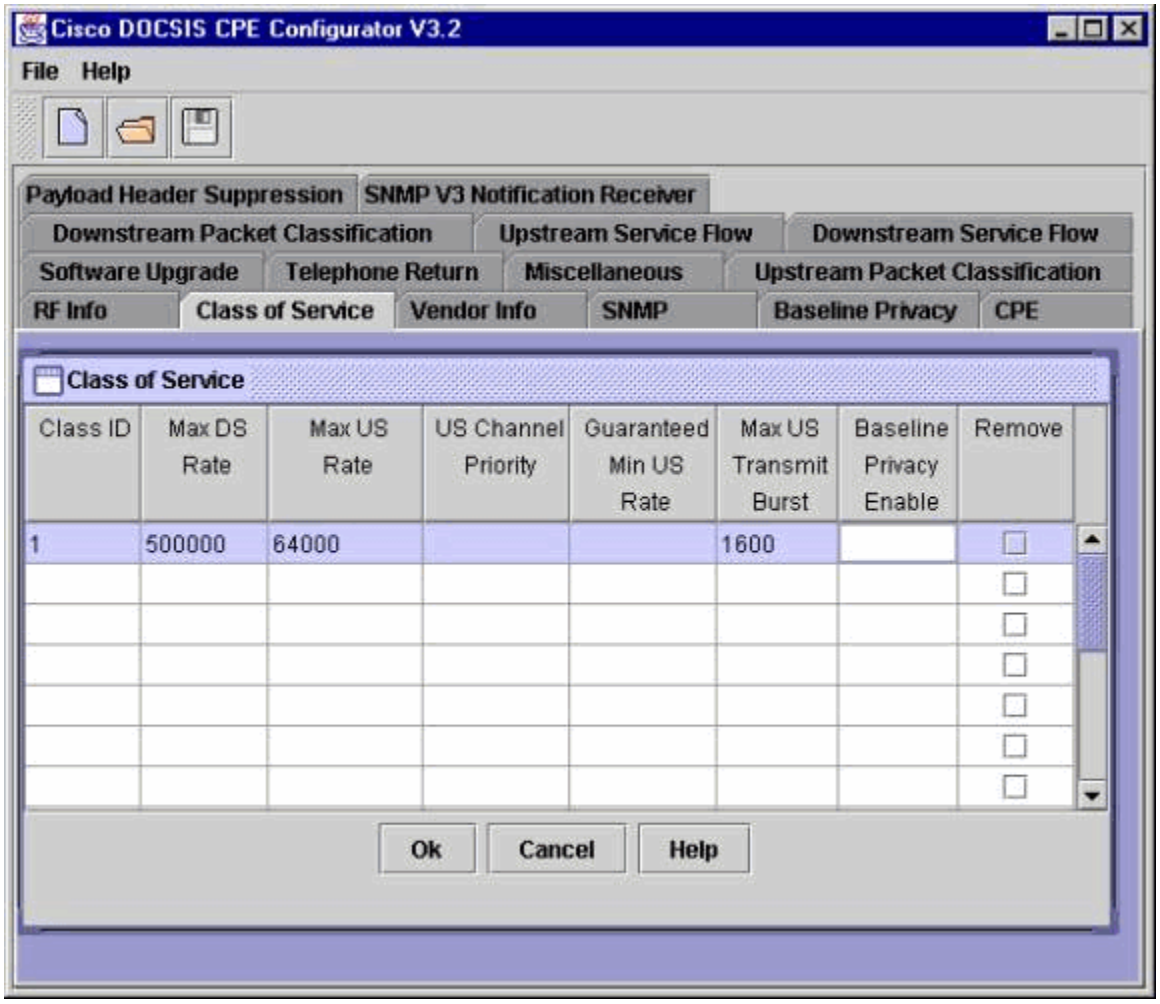
   Figure 1



3. Click the **Class of Service** tab to set the maximum downstream and upstream rates for the cable modems.

Normally, only one class of service (CoS) is ever configured here for DOCSIS 1.0.

Figure 2



4. On the Class of Service tab, identify a **Class ID**.

   This is an arbitrary identifier for the class of service that you are setting up; it is normally set to **1**. If there is not a number specified in this field, the system defaults to 1.

5. Set the Max DS Rate to **500000** bits per second (bps) and the Max US Rate to **64000** bps to describe the maximum downstream and upstream bit rates.

   Note: These rates are not guaranteed; rather, they are the maximum allowed rates.

6. Enter the Max US Transmit Burst.

   This value gives the modem an upper limit on the number of bytes of data that a cable modem can send in one burst. In DOCSIS 1.0 systems, this value could be set to 0 to indicate that there was no limit on the amount of data that a cable modem could transmit in one burst. A 0 value, however, might not be acceptable when a DOCSIS 1.0 modem is being operated in a DOCSIS 1.1-enabled environment. For this reason, a value that allows for the transmission of one full-sized Ethernet frame is generally used (typically, 1600 bytes).

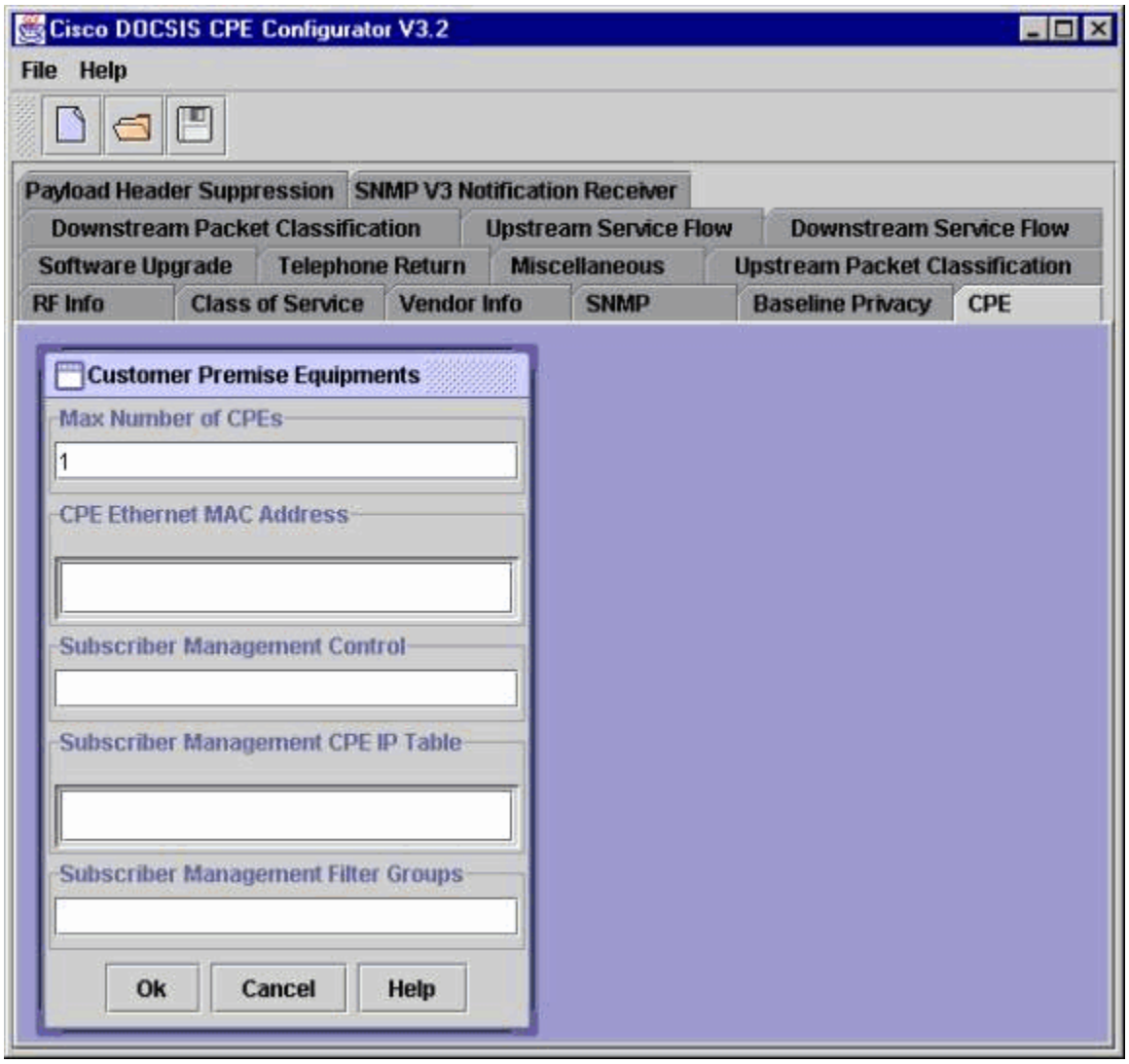
   Note: Cisco IOS® Software Release 12.1(4)CX is the first DOCSIS 1.1-enabled IOS for the uBR7200

Series. The maximum value allowed in this field was 1522 bytes. In Cisco IOS Software Release 12.2(4) BC and later, the upper limit has been raised to 2000 bytes. Additionally, in a DOCSIS 1.1 environment with a CMTS that runs Cisco IOS Software Release 12.2(8)BC1 and later, you are allowed to have a 0 burst value configured in the DOCSIS configuration file for cable modems that run DOCSIS 1.0 code.

7. Click the **CPE** tab and enter the Max Number of CPEs.

   This field indicates how many CPE devices connected to the cable modem are allowed network access. If this field is left blank then the cable modem allows one CPE device to have connectivity. For standard.cm you only want to allow access to one CPE; but, for this example, enter a value of 1 in this field anyway.

   Figure 3

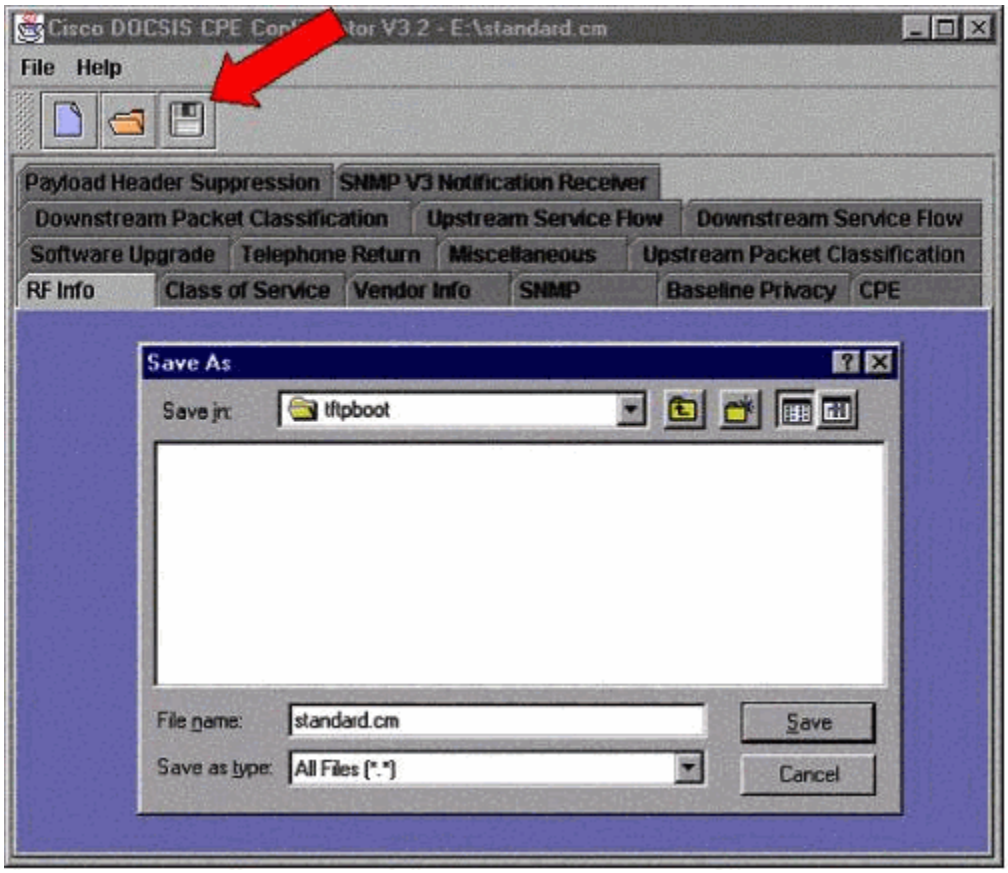


8. Review each of the tabs for which you just entered information to make sure that all of the entries that you have made are correct.

9. Save the file.

   Either click the **diskette** icon (see the red arrow in Figure 4) or choose **File > Save**.

   Figure 4



10. After the file has been saved, the file can be moved to the TFTP server so that cable modems can download it.

Click standard.cm to download this file.

Creating a premium.cm File

This procedure explains how to create the next example DOCSIS configuration file premium.cm. Cable modems that belong to users who have paid for a higher level of service should download this file. This file directs a cable modem to allow:

- A downstream rate of 2 Mbps.
- An upload rate of 256 kbps.
- A reserved minimum guaranteed upstream rate of 64 kbps.
- A higher upstream transmission priority than standard.cm users.
- Up to five CPE devices may connect to cable modems that download this file.
- Baseline Privacy is turned on, in order to ensure that a premium user's traffic is encrypted on the cable network.

Note: This file is created in the DOCSIS 1.0-compliant format.

1. In order to start work on a new file, click the **blank page** button or choose **File > New**.

2. On the RF Info tab, ensure that the **Network Access** check box is checked.

3. Click the **Class of Service** tab to enter the premium level class of service parameters:

   a. Set the Class ID to **1**.

   b. Set the Max DS Rate to **2000000** bps.

   c. Set the Max US Rate to **256000** bps.

4. Set the Upstream Channel Priority to **1** for premium.cm.

   When several cable modems are requesting upstream bandwidth from the CMTS at the same time, the requests from cable modems that use a class of service with a higher Upstream Channel Priority are answered first. This field defaults to 0 and can be set to 0 through 7, where 0 is the lowest priority and 7 is the highest. Because standard.cm users have this value set to the default of 0, you set this value to 1 for premium.cm so that upstream bandwidth requests from premium modems get answered first.

5. Set a reserved minimum upstream rate in the Guaranteed Min US Rate field.

   Note: If the cumulative total of all of the guaranteed minimum upstream rates of all the cable modems on a particular upstream is greater than the actual bandwidth available on the upstream port, then this value can no longer be guaranteed.

6. Activate the upstream admission control feature on the CMTS to ensure that cable modems can obtain their provisioned guaranteed minimum upstream rate.

   This feature totals the guaranteed minimum upstream throughput reserved by cable modems on an upstream interface; once the total exceeds an allowable level, no more cable modems that require a guaranteed minimum upstream rate are allowed online on that upstream port.

   On a Cisco CMTS, admission control is turned off by default and must be activated with the **cable upstream *port* admission-control [*percentage*]** cable interface command.

   ```
   7246VXR(config-if)# cable upstream 0 admission-control ?

   ??? Max Reservation Limit As Percentage of Raw Channel Capacity
   ```

   The *port* parameter is the upstream port on which admission control is enabled. The optional *percentage* parameter specifies the overbooking rate used when the amount of bandwidth that is available to be guaranteed is decided. So, if *percentage* is left blank or set to 100 percent, the CMTS only allows a total up to the real available upstream bandwidth to be guaranteed. If *percentage* is set to its maximum of 1000, then up to ten times the real interface bandwidth may be guaranteed.

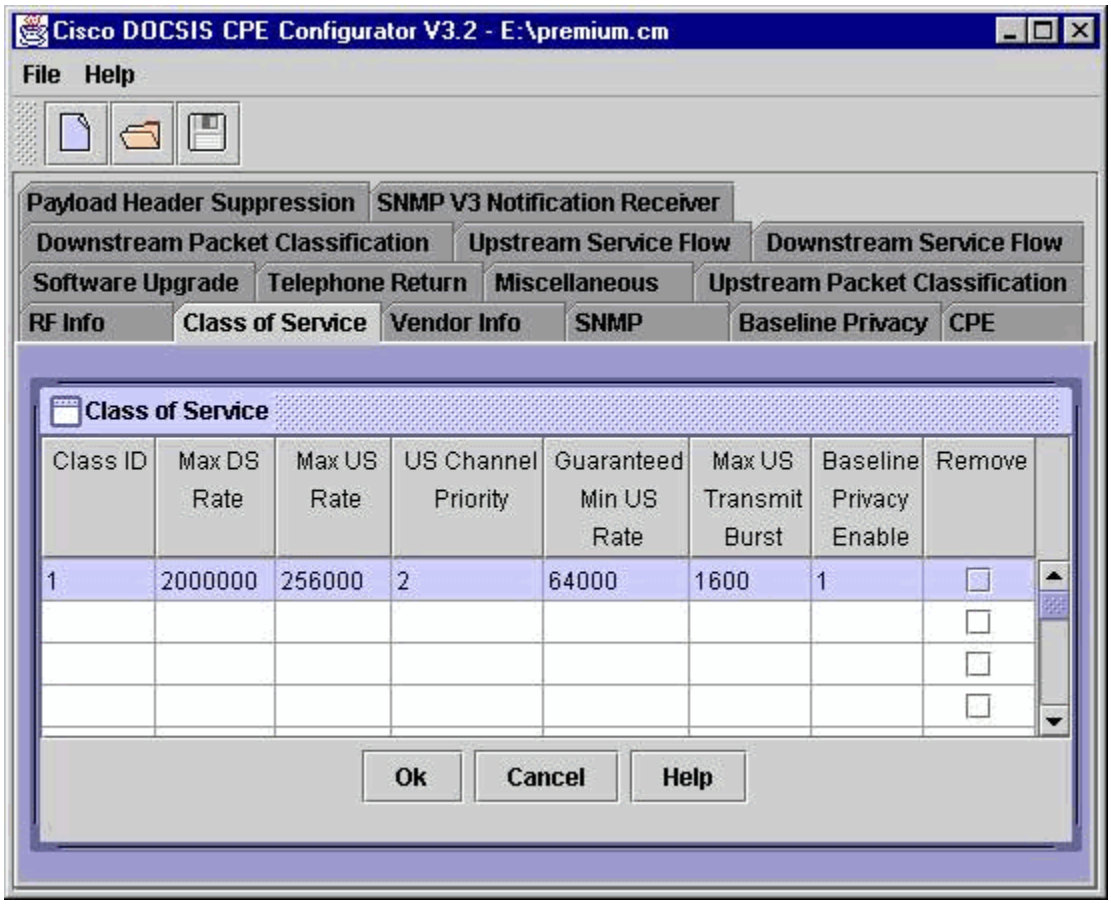
   Refer to **cable upstream admission-control** for more details on admission control and how to monitor its progress.

7. For premium.cm, specify **64000** bps as a minimum upstream rate in the Guaranteed Min US Rate field.

8. On the Class of Service tab, set the Baseline Privacy Enable field to **1** to turn on baseline privacy.

   If the Baseline Privacy Enable field is not set or is set to 0, baseline privacy interface (BPI) encryption is disabled.

Figure 5



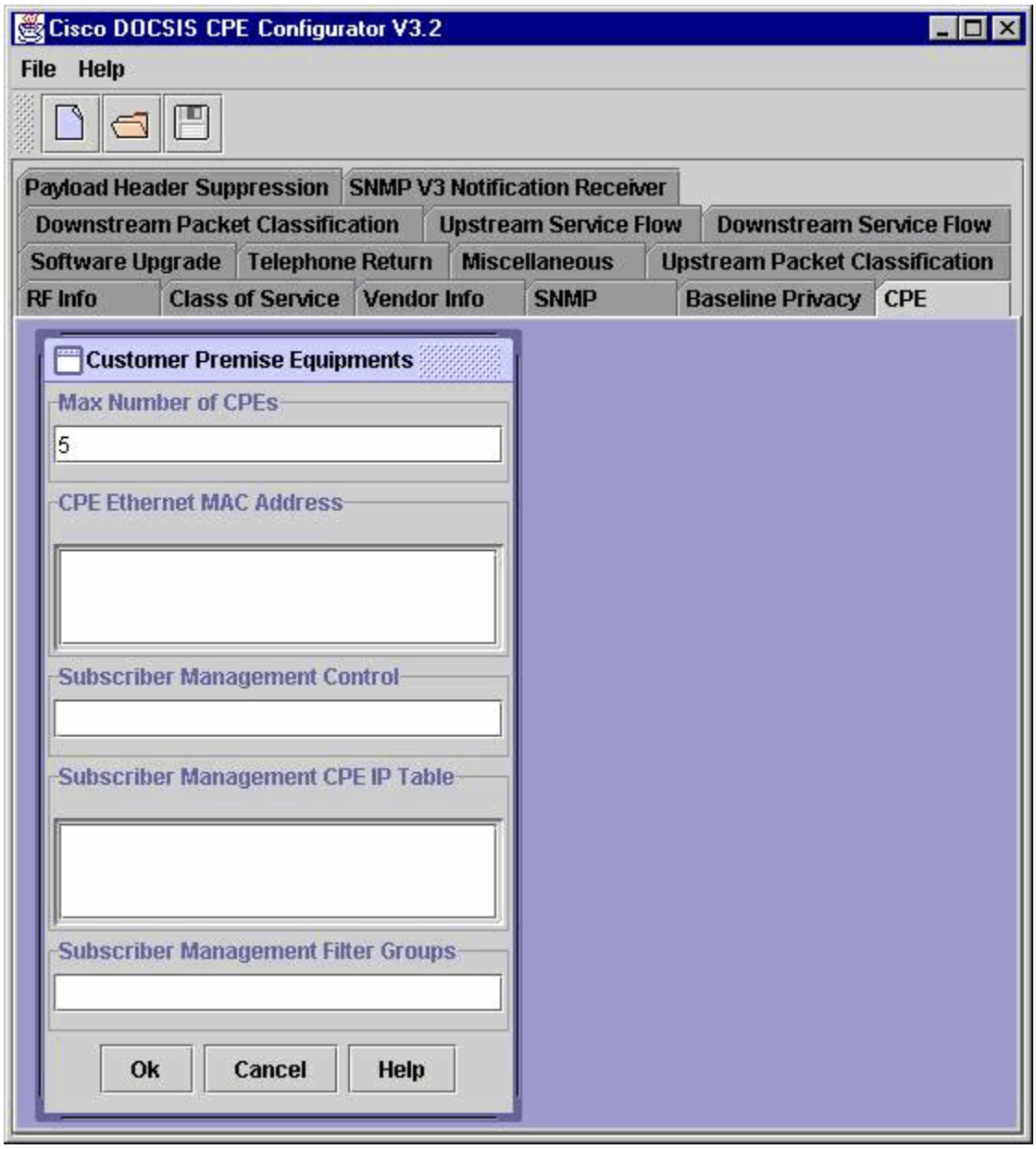
9. On the CPE tab, set the Max Number of CPEs field to **5**.

   Premium users are now allowed to attach up to five CPE devices to their cable modems.

   Note: The valid MAX CPE address range is 1 through 3 for bridging operation with Cisco IOS Software Release 12.0(4)XI1 in a Cisco uBR924. In Cisco IOS Software Release 12.0(5)T or later interim images, the valid MAX CPE address range is 1 through 254 for bridging operation. In addition, a number of third party cable modems have limits on the number of CPE devices that they can bridge. Check with your cable modem vendor for details.

   For information about the rest of the fields on the CPE tab, click the **Help** button at the bottom of the tab. This provides detailed explanation of those fields and examples.

   Figure 6



10. Save the **premium.cm** DOCSIS configuration file and move it to the TFTP server.

Click premium.cm to download this file.

Creating a disabled.cm Configuration File

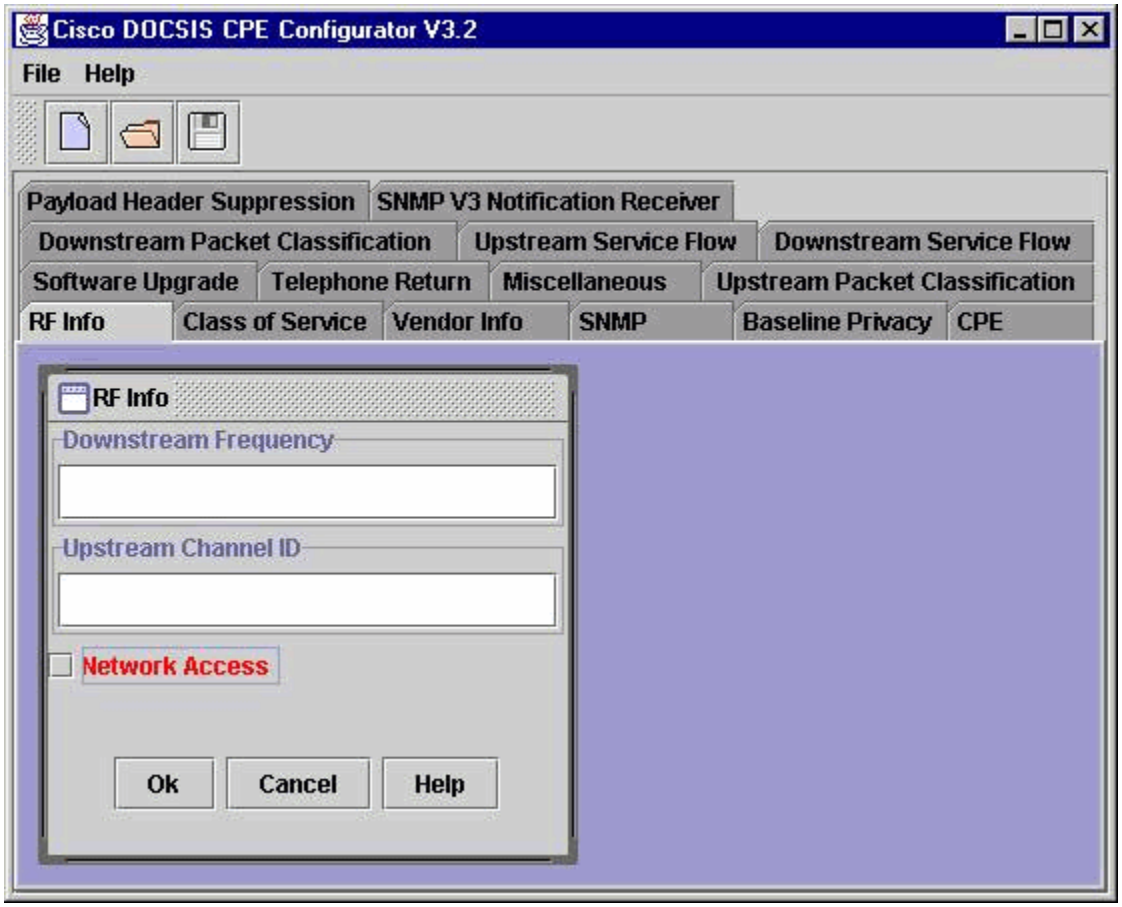
The last DOCSIS 1.0 example configuration file is disabled.cm. This file is downloaded by cable modems that are not authorized to be connected to the cable network or by cable modems that belong to customers who have not paid their bill. This configuration file allows a modem to come online but it stops CPE devices connected to the modem from getting access to the service provider's network.

It is better to let unauthorized cable modems come online and receive a DOCSIS configuration file similar to disabled.cm than to not let such modems online: an unauthorized cable modem that attempts to come online and is rejected every few minutes consumes far more resources than a cable modem that sits in the "online but disabled" state.

1. On the RF Info tab, uncheck the **Network Access** check box.

This denies the CPE access to the network.

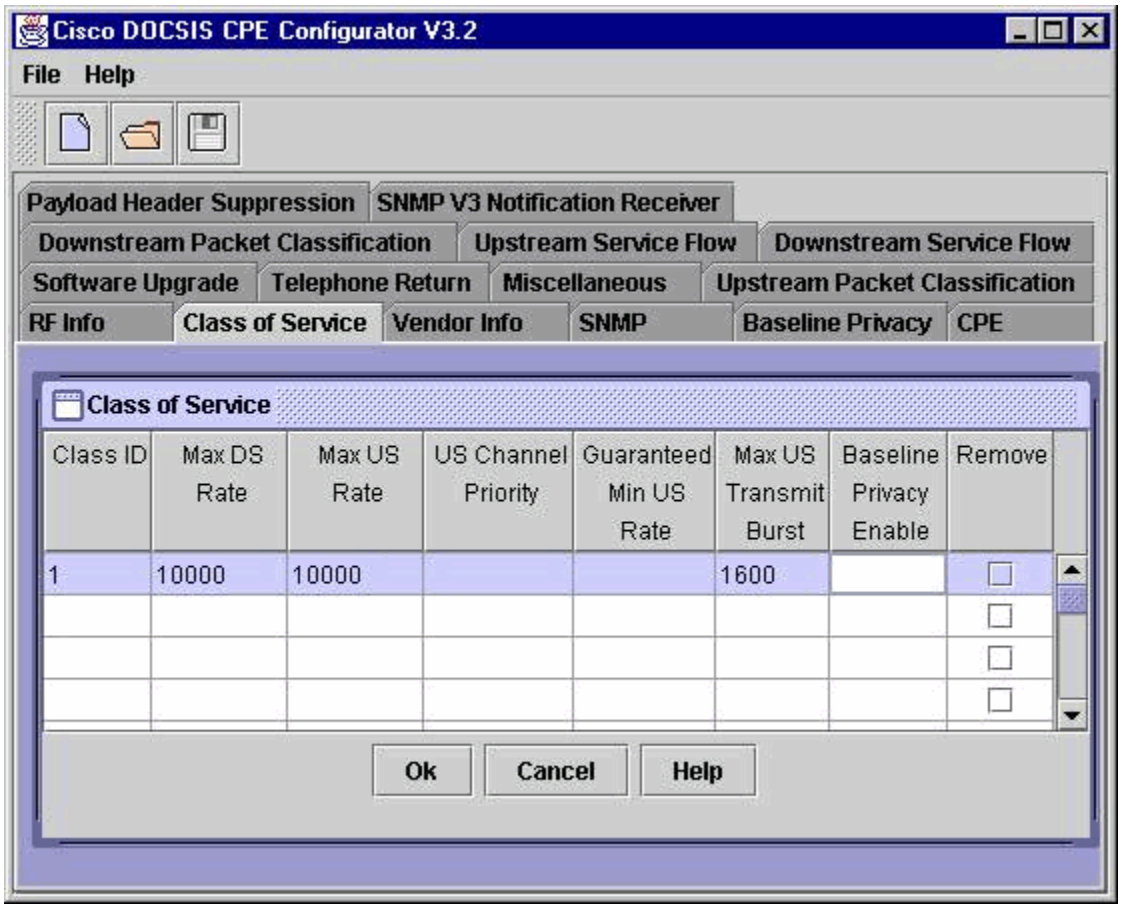
Figure 7



2. On the Class of Service tab, set the Max DS Rate and the Max US Rate to **10000** bps.

   This is slower than a typical dial-up modem connection and is almost useless for Internet access; but it is enough throughput for the service provider to perform basic management of the modem.

   Figure 8



Click disabled.cm to download this file.

Setting SNMP Variables

Setting an SNMP Community String

Cable modems may be managed with the Simple Network Management Protocol (SNMP). Refer to Simple Network Management Protocol (SNMP) for more information.

In order to make sure that only the appropriate parties and devices can manage a cable modem through SNMP, it is possible to send a set of *community strings* to the cable modem with the DOCSIS configuration file. Then, only SNMP requests that contain the correct community string are answered. In addition, it is possible to restrict the allowed source IP address of SNMP requests.

To set community strings with a DOCSIS configuration file, you need to set values for the SNMP MIB Objects fields on the SNMP tab.

Each row of the SNMP MIB Objects table has three fields. The first field is *Object ID (OID)*, which is a code that identifies the SNMP variable that is being set. This can be specified by a dotted Object ID number or by a well known Object ID Name (ASCII variable). The second field is *Type*, which identifies what type of value the variable takes. The third field is *Value*, which contains the actual value that you want to set for the variable.

When an Object ID has an **X** as a suffix, the variable may be specified several times with an index of **X**. The use of this index will become clearer in the examples.

The Object ID for most DOCSIS-specific SNMP variables begins with the sequence 1.3.6.1.2.1.69. Variables

that start with this sequence belong to the mib-2.docsDev branch of the SNMP tree. In older versions of the DOCSIS specification, these same variables belonged to a different branch of the SNMP tree.

Note: The sequence 1.3.6.1.2.1.69 (mib-2.docsDev) in the OID numbers may need to be interchanged with 1.3.6.1.3.83 (mib-2.docsDev) when you are dealing with older cable modem firmware, like uBR900 series modems that run Cisco IOS Software Release 12.0T and that are compliant with older versions of the DOCSIS 1.0 specification. If you are in doubt about which prefix to use when you specify SNMP variables, try to use the 1.3.6.1.2.1.69 prefix first; if this does not work then use the older 1.3.6.1.3.83 prefix. Consult you cable modem vendor for precise details.

Table 1 – Object IDs, Types, and the Most Commonly Used Values in Cable Environments

Object ID Number and Name	Type	Value
1.3.6.1.2.1.69.1.2.1.2.X docsDevNmAccessIp.X	IP Address	The IP address (or subnet) of the network management station allowed to manage the modem. The address 255.255.255.255 is defined to mean any host. If SNMP traps are enabled for this entry, then the value must be the address of a specific device.
1.3.6.1.2.1.69.1.2.1.3.X docsDevNmAccessIpMask.X	IP Address	The IP subnet mask of the network management stations. If traps are enabled for this entry, then the value must be 255.255.255.255.
1.3.6.1.2.1.69.1.2.1.4.X docsDevNmAccessCommunity.X	Octet String	The community string to be matched for access by this entry. For example “public”.
1.3.6.1.2.1.69.1.2.1.5.X docsDevNmAccessControl.X	Integer	The type of SNMP access that the docsDevNmAccessCommunity.X community string allows. • 2—read-only access • 3—read-write access • 4—read-only with traps • 5—read-write with traps • 6—Traps only
1.3.6.1.2.1.69.1.2.1.6.X docsDevNmAccessInterfaces.X	Octet String	The interfaces from which SNMP requests are accepted. • 0x40—Cable interface • 0x80—Ethernet interface

		• 0xC0 or 0x00—Both interfaces
1.3.6.1.2.1.69.1.2.1.7.X docsDevNmAccessStatus.X	Integer	Control over the state and creation of this entry. • 1—Activate • 2—Deactivate • 4—Create and activate • 5—Create and deactivate • 6—Delete

Modification of standard.cm to Include SNMP Parameters

As an example, you can modify standard.cm so that it programs a cable modem to allow read-only access to any host through the "public" community string. In addition, you can also specify the read-write community string "private," which allows access only through the cable interface from workstations in the 10.0.0.0/255.0.0.0 network. In other words, the cable modems only respond to SNMP requests if the request comes from a Network Management workstation with these requirements:

- It is on the cable side of the cable modem; it is not a CPE device.
- Its IP address is within the range 10.0.0.0 through 10.0.0.8.

Table 2 shows OIDs, their types, and the values used to achieve those requirements. It shows settings for the cable modem to allow read-only access to any host via the "public" community string and specifies the read-write community string "private," which allows access only through the cable interface from workstations in the 10.0.0.0/255.0.0.0 network.

Caution: Never assign the well-known community strings "public" and "private" in a production network. These community strings are very common and would be easily guessed by unauthorized parties.

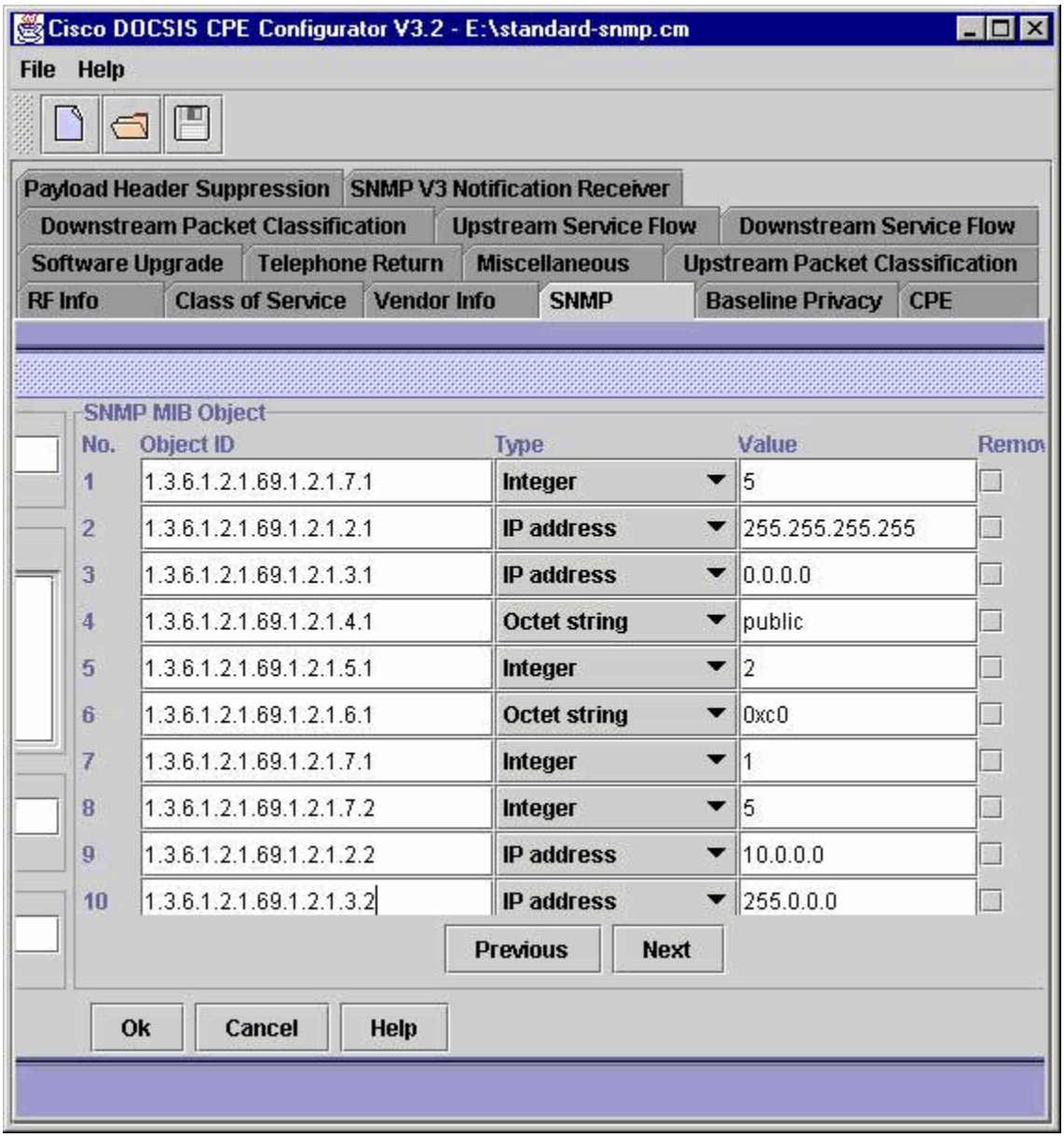
Table 2 – Settings for Cable Modems

Object ID Number and Name	Type	Value	Meaning
1.3.6.1.2.1.69.1.2.1.7.1 docsDevNmAccessStatus.1	Integer	5	Create the SNMP table entry number 1 but do not activate it yet.
1.3.6.1.2.1.69.1.2.1.2.1 docsDevNmAccessIp.1	IP Address	255.255.255.255	Allow SNMP requests from any source IP address.
1.3.6.1.2.1.69.1.2.1.3.1 docsDevNmAccessIpMask.1	IP Address	0.0.0.0	Mask associated with the docsDevNmAccessIp.1 IP address.
1.3.6.1.2.1.69.1.2.1.4.1			

docsDevNmAccessCommunity.1	Octet String	Public	Set the community string to “public” for this entry.
1.3.6.1.2.1.69.1.2.1.5.1 docsDevNmAccessControl.1	Integer	2	Allow read-only (2) access.
1.3.6.1.2.1.69.1.2.1.6.1 docsDevNmAccessInterfaces.1	Octet String	0xC0 (or 0x00)	Allow access from any interface on the modem.
1.3.6.1.2.1.69.1.2.1.7.1 docsDevNmAccessStatus.1	Integer	1	Activate this entry now that it is completed.
1.3.6.1.2.1.69.1.2.1.7.2 docsDevNmAccessStatus.2	Integer	5	Create the SNMP table entry number 2 but do not activate it yet.
1.3.6.1.2.1.69.1.2.1.2.2 docsDevNmAccessIp.2	IP Address	10.0.0.0	Allow SNMP requests from hosts in the 10.0.0.0 network.
1.3.6.1.2.1.69.1.2.1.3.2 docsDevNmAccessIpMask.2	IP Address	255.0.0.0	Mask associated with the network 10.0.0.0.
1.3.6.1.2.1.69.1.2.1.4.2 docsDevNmAccessCommunity.2	Octet String	Private	Set the community string to “private” for this entry.
1.3.6.1.2.1.69.1.2.1.5.2 docsDevNmAccessControl.2	Integer	3	Allow read-write (3) access.
1.3.6.1.2.1.69.1.2.1.6.2 docsDevNmAccessInterfaces.2	Octet String	0x40	Allow access only through the cable interface.
1.3.6.1.2.1.69.1.2.1.7.2 docsDevNmAccessStatus.1	Integer	1	Activate this entry now that it is completed.

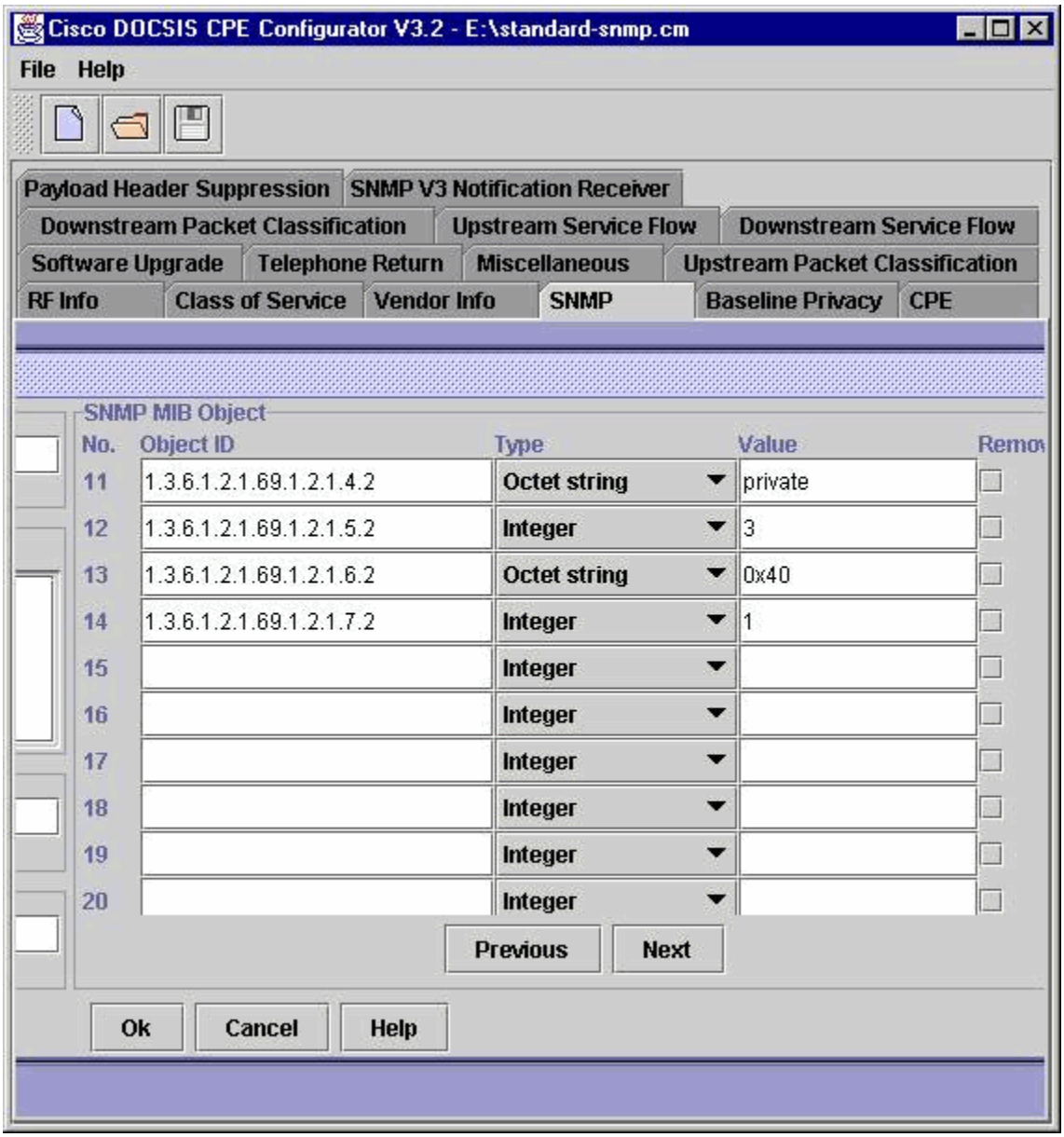
Figures 9 and 10 show how the values from Table 2 are entered into the Cisco DOCSIS CPE Configurator tool . For these examples, the numerical OID is entered; the equivalent OID names could have been used instead.

Figure 9



Those are the first set of SNMP variables added to standard.cm. Click **Next** to get to another screen of variables.

Figure 10

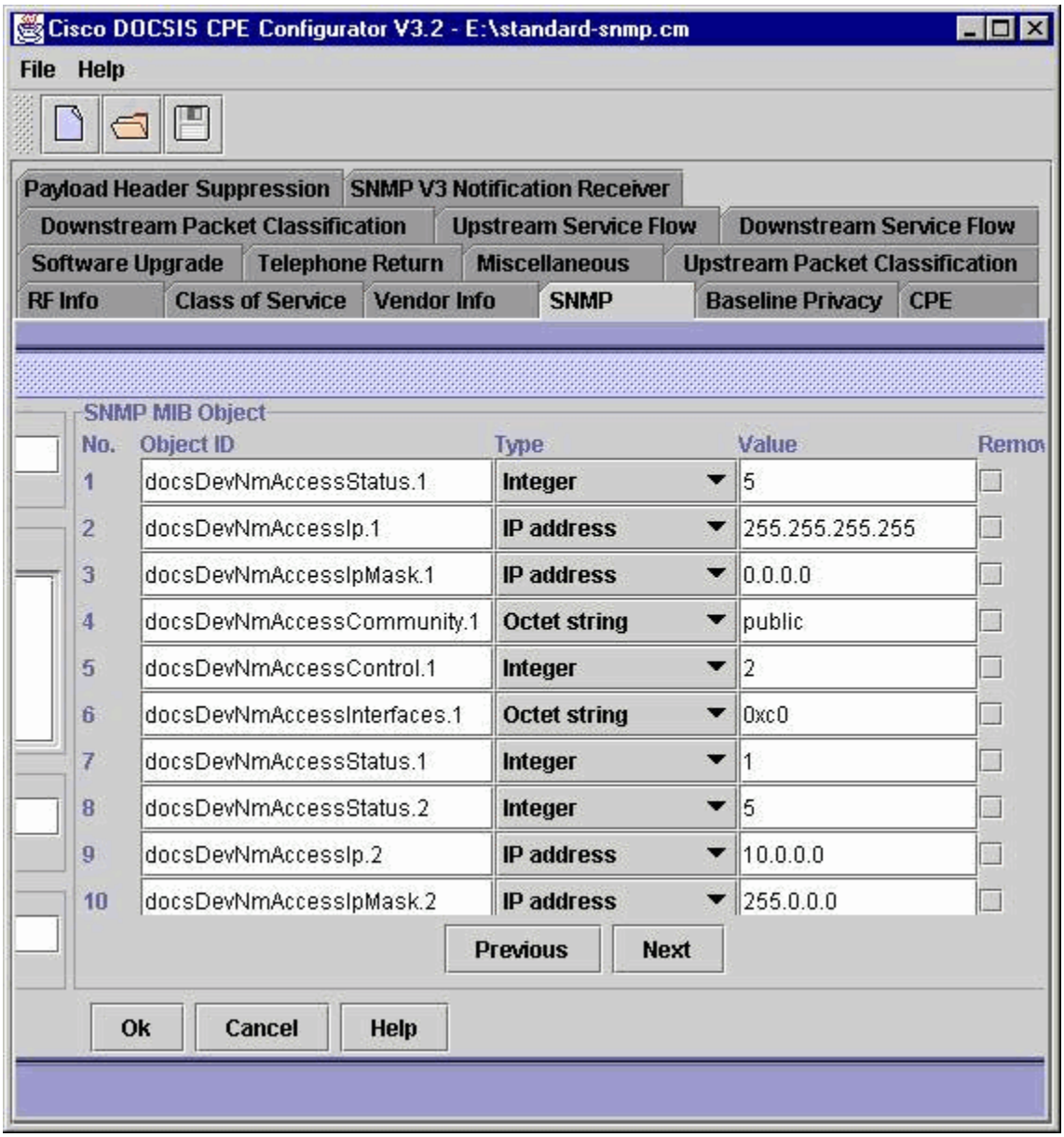


Those are the next set of SNMP values. Click **Next** to get to another screen of variables.

At this stage, the file can be saved as standard-snmp.cm. Click standard-snmp.cm to download this file.

When you open standard-snmp.cm, notice that the known numerical OID values have been converted into their equivalent, easier-to-read MIB variable names (see Figure 11).

Figure 11



Modification of premium.cm to Include SNMP Parameters

In addition to the private and public community strings, premium.cm can be modified to include details that set up a host to which a cable modem can send SNMP traps. SNMP parameters that send public community strings, private community strings, and SNMP traps are shown in Table 3.

Table 3 – SNMP Parameters to Send public and private Community String and SNMP Traps

Object ID Number and Name	Type	Value	Meaning
1.3.6.1.2.1.69.1.2.1.7.3 docsDevNmAccessStatus.3	Integer	5	Create the SNMP table entry number 3 but do not activate it yet.
1.3.6.1.2.1.69.1.2.1.2.3 docsDevNmAccessIp.3	IP Address	10.2.10.1	Send SNMP traps to 10.2.10.1.

1.3.6.1.2.1.69.1.2.1.3.3 docsDevNmAccessIpMask.3	IP Address	255.255.255.255	Network mask for docsDevNmAccessIp value.
1.3.6.1.2.1.69.1.2.1.4.3 docsDevNmAccessCommunity.3	Octet String	Public	Set the community string to “public” for this entry.
1.3.6.1.2.1.69.1.2.1.5.3 docsDevNmAccessControl.3	Integer	6	This entry will only generate traps (6).
1.3.6.1.2.1.69.1.2.1.6.3 docsDevNmAccessInterfaces.3	Octet String	0xC0	Because this entry is not used to access the cable modem, this field becomes irrelevant and can be set to any value.
1.3.6.1.2.1.69.1.2.1.7.3 docsDevNmAccessStatus.3	Integer	1	Activate this entry now that it is completed.

Note: The address 10.2.10.1 is the IP address of the Network Management Station that receives the SNMP traps.

Click premium-snmp.cm to download this file.

Modification of disabled.cm to Include SNMP Parameters

Finally, disabled.cm may also be modified to allow SNMP management of online but disabled cable modems. The file disabled-snmp.cm is a modified version of disabled.cm that has the same SNMP community strings as standard-snmp.cm.

Click disabled-snmp.cm to download this file.

IP and LLC Filters

It is possible to implement IP and Logical Link Control (LLC) layer filtering on a cable modem. You might wish to implement LLC filters to specify which Layer 3 protocols may pass through a cable modem. This would typically be used to stop non-IP-related traffic—such as IPX and NetBEUI traffic—from reaching the service provider network. You might also wish to implement IP filters to protect CPE devices from inadvertent file sharing or to stop end users from running potentially disruptive services such as a DHCP server.

Table 4 shows the relevant OIDs for LLC filtering of different Layer 3 protocols. As when you specify SNMP community strings, the numerical OID prefix 1.3.6.1.2.1.69 might need to be replaced by 1.3.6.1.3.83 for modems that run older firmware.

Table 4 – OIDs for LLC Filtering of Different Layer 3 Protocols

Object ID Number and Name	Type	Value
		If set to discard (1), any Layer 2 packet that does not match at least one of

1.3.6.1.2.1.69.1.6.1.0 docsDevFilterLLCUnmatchedAction.0	Integer	the filters in the docsDevFilterLLC series is discarded. If set to accept (2), any Layer 2 packet that does not match at least one of the filters in the docsDevFilterLLC series is allowed to pass through the cable modem for further processing.
1.3.6.1.2.1.69.1.6.2.1.2.X docsDevFilterLLCStatus.X	Integer	Control the state and creation of this entry. • 1—Activate • 2—Deactivate • 4—Create and activate • 5—Create and deactivate • 6—Delete
1.3.6.1.2.1.69.1.6.2.1.3.X docsDevFilterLLCIfIndex.X	Integer	The interface to which this filter entry applies. • 0—Both • 1—Ethernet Interface • 2—Cable Interface
1.3.6.1.2.1.69.1.6.2.1.4.X docsDevFilterLLCProtocolType.X	Integer	Can be set to EtherType (1) or DSAP (2) to describe the format of docsDevFilterLLCProtocol.
1.3.6.1.2.1.69.1.6.2.1.5.X docsDevFilterLLCProtocol.X	Integer	The layer three protocol for which this filter applies. • 2048—IP • 2054—IP ARP • 33079—IPX

As an example, you can add SNMP variables to a DOCSIS configuration file to program a cable modem to allow only IP and IP Address Resolution Protocol (ARP) traffic to pass through. This way, if an end user is running another Layer 3 protocol—such as Internetwork Packet Exchange (IPX)—you can make sure that unwanted traffic that is generated by this protocol does not consume upstream resources. Table 5 shows OID numbers, their types, and the values used to program a cable modem to allow only IP and IP ARP traffic to pass

through.

Caution: Be aware of Cisco bug ID CSCdt94942, in which the ARP traffic is not passed after you enable LLC filters in the DOCSIS configuration file. This happens in Cisco cable modems that run Cisco IOS Software Releases 12.1 and 12.1T.

Table 5 – OIDs to Allow Only IP and IP ARP Traffic to Pass Through

Object ID Number and Name	Type	Value	Meaning
1.3.6.1.2.1.69.1.6.1.0 docsDevFilterLLCUnmatchedAction.0	Integer	1	Discard any traffic that does not match one of the next LLC filters.
1.3.6.1.2.1.69.1.6.2.1.2.1 docsDevFilterLLCStatus.1	Integer	5	Create the LLC filter table entry number 1 but do not activate it yet.
1.3.6.1.2.1.69.1.6.2.1.3.1 docsDevFilterLLCIfIndex.1	Integer	0	Apply this filter to both the Ethernet and the Cable interface.
1.3.6.1.2.1.69.1.6.2.1.4.1 docsDevFilterLLCProtocolType.1	Integer	1	Specify the next Protocol Type as an EtherType.
1.3.6.1.2.1.69.1.6.2.1.5.1 docsDevFilterLLCProtocol.1	Integer	2048	Allow frames that carry IP traffic to pass.
1.3.6.1.2.1.69.1.6.2.1.2.1 docsDevFilterLLCStatus.1	Integer	1	Activate this LLC filter table entry.
1.3.6.1.2.1.69.1.6.2.1.2.2	Integer	5	Create the LLC filter table entry number 2

docsDevFilterLLCStatus.2			but do not activate it yet.
1.3.6.1.2.1.69.1.6.2.1.3.2 docsDevFilterLLCIfIndex.2	Integer	0	Apply this filter to both the Ethernet and Cable interface.
1.3.6.1.2.1.69.1.6.2.1.4.2 docsDevFilterLLCProtocolType.2	Integer	1	Specify the next Protocol Type as an EtherType.
1.3.6.1.2.1.69.1.6.2.1.5.2 docsDevFilterLLCProtocol.2	Integer	2054	Allow frames that carry IP ARP traffic to pass.
1.3.6.1.2.1.69.1.6.2.1.2.2 docsDevFilterLLCStatus.2	Integer	1	Activate this LLC filter table entry.

These filters have been added to standard.cm to make standard-llc.cm.

Note: These filters could have been added to standard-snmp.cm as well.

Table 6 shows the relevant OIDs that you use to filter at the IP layer.

Table 6 – OIDs to Filter at the IP Layer

Object ID Number and Name	Type	Value
1.3.6.1.2.1.69.1.6.3.0 docsDevFilterIpDefault.0	Integer	If set to discard (1), any IP packet that does not match one of the filters in the docsDevFilterIP series is discarded. If set to accept (2), any Layer 2 packet that does not match one of the filters in the docsDevFilterIP series is allowed to pass for further processing.
		Control the state and creation of this entry. (See the **Note** at the end of the table.)

1.3.6.1.2.1.69.1.6.4.1.2.X docsDevFilterIpStatus.X	Integer	• 1—Activate • 2—Deactivate • 4—Create and activate • 5—Create and deactivate • 6—Delete
1.3.6.1.2.1.69.1.6.4.1.3.X docsDevFilterIpControl.X	Integer	If set to discard (1), all packets that match this filter are discarded. If set to accept (2), all packets that match this filter are allowed to pass through the cable modem for further processing.
1.3.6.1.2.1.69.1.6.4.1.4.X docsDevFilterIpIfIndex.X	Integer	The interface to which this filter entry applies. • 0—Both • 1—Ethernet Interface • 2—Cable Interface
1.3.6.1.2.1.69.1.6.4.1.5.X docsDevFilterIpDirection.X	Integer	Determines whether the filter is applied to inbound (1) traffic, outbound (2) traffic, or traffic in both (3) directions.
1.3.6.1.2.1.69.1.6.4.1.6.X docsDevFilterIpBroadcast.X	Integer	If set to true (1), the filter only applies to multicast and broadcast traffic. If set to false (2), the filter applies to all traffic.
1.3.6.1.2.1.69.1.6.4.1.7.X docsDevFilterIpSaddr.X	IP Address	The source IP address, or portion thereof, that is to be matched for this filter. The source address is first masked against docsDevFilterIpSmask before it is compared to

		this value. A value of 0 for this object and 0 for the mask matches all IP addresses.
1.3.6.1.2.1.69.1.6.4.1.8.X docsDevFilterIpSmask.X	IP Address	A network mask that is to be applied to the source address prior to matching.
1.3.6.1.2.1.69.1.6.4.1.9.X docsDevFilterIpDaddr.X	IP Address	The same as docsDevFilterIpSaddr, except for the destination IP address.
1.3.6.1.2.1.69.1.6.4.1.10.X docsDevFilterIpDmask.X	IP Address	The same as docsDevFilterIpSmask, except for the destination IP address.
1.3.6.1.2.1.69.1.6.4.1.11.X docsDevFilterIpProtocol.X	Integer	The IP protocol number that is to be matched. For example: • 1—ICMP • 6—TCP • 17—UDP • 256—Any protocol
1.3.6.1.2.1.69.1.6.4.1.12.X DocsDevFilterIpSourcePortLow.X	Integer	If docsDevFilterIpProtocol is UDP or TCP, this is the inclusive lower bound of the UDP or TCP source port range that is to be matched. Otherwise, it is ignored during matching.
1.3.6.1.2.1.69.1.6.4.1.13.X DocsDevFilterIpSourcePortHigh.X	Integer	The inclusive upper bound of the UDP or TCP source port range to be matched.
1.3.6.1.2.1.69.1.6.4.1.14.X docsDevFilterIpDestPortLow.X	Integer	The inclusive lower bound of the UDP or TCP destination port range to be matched.
1.3.6.1.2.1.69.1.6.4.1.15.X DocsDevFilterIpDestPortHigh.X	Integer	The inclusive upper bound of the UDP or TCP destination port range to be matched.

Note: DocsDevFilterIpStatus.X values 1 and 5 are no longer supported, now that Cisco bug ID CSCdw86385 is fixed. As of Cisco IOS Software Releases 12.2(11)T and 12.2(11), only value 4 is supported.

As an example, you can add SNMP variables to a DOCSIS configuration file to program a cable modem to not allow any Microsoft Networking Traffic (for example, traffic to UDP and TCP ports 137 to 139) to leave or enter any interface on the cable modem. This would inhibit inadvertent file sharing. In addition, you can apply a filter to the Ethernet interface to block IP traffic from CPE devices that are configured as DHCP servers (for example, traffic from UDP port 67). Table 7 shows the SNMP variables that you can use to accomplish these objectives.

Table 7 – OIDs to Block Traffic to TCP and UDP Ports 137 – 139 and UDP Port 67

Object ID Number and Name	Type	Value	Meaning
1.3.6.1.2.1.69.1.6.3.0 docsDevFilterIpDefault.0	Integer	2	If an IP packet does not match a filter then let it pass.
1.3.6.1.2.1.69.1.6.4.1.2.1 docsDevFilterIpStatus.1	Integer	5	Create the IP filter table entry number 1 but do not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.1 docsDevFilterIpControl.1	Integer	1	All IP packets that match filter number 1 are discarded.
1.3.6.1.2.1.69.1.6.4.1.4.1 docsDevFilterIpIfIndex.1	Integer	0	This filter applies to both the Ethernet and cable interfaces.
1.3.6.1.2.1.69.1.6.4.1.5.1 docsDevFilterIpDirection.1	Integer	3	This filter applies to both inbound and outbound traffic.
1.3.6.1.2.1.69.1.6.4.1.6.1 docsDevFilterIpBroadcast.1	Integer	2	This filter applies to all traffic, including multicasts and

			broadcasts.
1.3.6.1.2.1.69.1.6.4.1.7.1 docsDevFilterIpSaddr.1	IP Address	0.0.0.0	The source IP address for this filter may be any IP address.
1.3.6.1.2.1.69.1.6.4.1.8.1 docsDevFilterIpSmask.1	IP Address	0.0.0.0	
1.3.6.1.2.1.69.1.6.4.1.9.1 docsDevFilterIpDaddr.1	IP Address	0.0.0.0	The destination IP address for this filter may be any IP address.
1.3.6.1.2.1.69.1.6.4.1.10.1 docsDevFilterIpDmask.1	IP Address	0.0.0.0	
1.3.6.1.2.1.69.1.6.4.1.11.1 docsDevFilterIpProtocol.1	Integer	6	This filter matches TCP packets.
1.3.6.1.2.1.69.1.6.4.1.12.1 docsDevFilterIpSourcePortLow.1	Integer	0	This filter matches traffic from any source port.
1.3.6.1.2.1.69.1.6.4.1.13.1 docsDevFilterIpSourcePortHigh.1	Integer	65535	
1.3.6.1.2.1.69.1.6.4.1.14.1 docsDevFilterIpDestPortLow.1	Integer	137	This filter matches traffic to destination ports 137 through 139.
1.3.6.1.2.1.69.1.6.4.1.15.1 docsDevFilterIpDestPortHigh.1	Integer	139	
1.3.6.1.2.1.69.1.6.4.1.2.1 docsDevFilterIpStatus.1	Integer	1	Activate IP filter table entry number 1.
1.3.6.1.2.1.69.1.6.4.1.2.2 docsDevFilterIpStatus.2	Integer	5	Create the IP filter table entry number 2 but do not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.2 docsDevFilterIpControl.2	Integer	1	All IP packets that filter number 2 are discarded.

1.3.6.1.2.1.69.1.6.4.1.4.2 docsDevFilterIpIfIndex.2	Integer	0	This filter applies to both the Ethernet and cable interfaces.
1.3.6.1.2.1.69.1.6.4.1.5.2 docsDevFilterIpDirection.2	Integer	3	This filter applies to both inbound and outbound traffic.
1.3.6.1.2.1.69.1.6.4.1.6.2 docsDevFilterIpBroadcast.2	Integer	2	This filter applies to all traffic, including multicasts and broadcasts.
1.3.6.1.2.1.69.1.6.4.1.7.2 docsDevFilterIpSaddr.2	IP Address	0.0.0.0	The source IP address for this filter may be any IP address.
1.3.6.1.2.1.69.1.6.4.1.8.2 docsDevFilterIpSmask.2	IP Address	0.0.0.0	
1.3.6.1.2.1.69.1.6.4.1.9.2 docsDevFilterIpDaddr.2	IP Address	0.0.0.0	The destination IP address for this filter may be any IP address.
1.3.6.1.2.1.69.1.6.4.1.10.2 docsDevFilterIpDmask.2	IP Address	0.0.0.0	
1.3.6.1.2.1.69.1.6.4.1.11.2 docsDevFilterIpProtocol.2	Integer	17	This filter matches UDP packets.
1.3.6.1.2.1.69.1.6.4.1.12.2 docsDevFilterIpSourcePortLow.2	Integer	0	This filter matches traffic from any source port.
1.3.6.1.2.1.69.1.6.4.1.13.2 docsDevFilterIpSourcePortHigh.2	Integer	65535	
1.3.6.1.2.1.69.1.6.4.1.14.2 docsDevFilterIpDestPortLow.2	Integer	137	This filter matches traffic to destination ports 137
1.3.6.1.2.1.69.1.6.4.1.15.2			

docsDevFilterIpDestPortHigh.2	Integer	139	through 139.
1.3.6.1.2.1.69.1.6.4.1.2.2 docsDevFilterIpStatus.2	Integer	1	Activate IP filter table entry number 2.
1.3.6.1.2.1.69.1.6.4.1.2.3 docsDevFilterIpStatus.3	Integer	5	Create the IP filter table entry number 3 but do not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.3 docsDevFilterIpControl.3	Integer	1	All IP packets that match filter number 3 are discarded.
1.3.6.1.2.1.69.1.6.4.1.4.3 docsDevFilterIpIfIndex.3	Integer	1	This filter applies to the Ethernet interface only.
1.3.6.1.2.1.69.1.6.4.1.5.3 docsDevFilterIpDirection.3	Integer	1	This filter applies to inbound traffic only.
1.3.6.1.2.1.69.1.6.4.1.6.3 docsDevFilterIpBroadcast.3	Integer	2	This filter applies to all traffic, including multicasts and broadcasts.
1.3.6.1.2.1.69.1.6.4.1.7.3 docsDevFilterIpSaddr.3	IP Address	0.0.0.0	The source IP address for this filter may be any IP address.
1.3.6.1.2.1.69.1.6.4.1.8.3 docsDevFilterIpSmask.3	IP Address	0.0.0.0	
1.3.6.1.2.1.69.1.6.4.1.9.3 docsDevFilterIpDaddr.3	IP Address	0.0.0.0	The destination IP address for this filter may be any IP
1.3.6.1.2.1.69.1.6.4.1.10.3	IP Address	0.0.0.0	

docsDevFilterIpDmask.3			address.
1.3.6.1.2.1.69.1.6.4.1.11.3 docsDevFilterIpProtocol.3	Integer	17	This filter matches UDP packets.
1.3.6.1.2.1.69.1.6.4.1.12.3 docsDevFilterIpSourcePortLow.3	Integer	67	This filter matches traffic only from a source port of 67.
1.3.6.1.2.1.69.1.6.4.1.13.3 docsDevFilterIpSourcePortHigh.3	Integer	67	
1.3.6.1.2.1.69.1.6.4.1.14.3 docsDevFilterIpDestPortLow.3	Integer	0	This filter matches traffic to any destination port.
1.3.6.1.2.1.69.1.6.4.1.15.3 docsDevFilterIpDestPortHigh.3	Integer	65535	
1.3.6.1.2.1.69.1.6.4.1.2.3 docsDevFilterIpStatus.3	Integer	1	Activate IP filter table entry number 3.

These filters have been added to standard.cm to make standard-ip.cm. Click standard-ip.cm to download this file.

Other SNMP Variables

You can use the SNMP MIB Object table section of the DOCSIS configuration file to set other parameters. RFC2669 - DOCSIS Cable Device MIB describes the set of SNMP objects common to all DOCSIS-compliant cable modems that can be changed with the DOCSIS configuration file. The MIBs that are supported on the uBR7200 are listed in the uBR7200 Series MIB Support Lists.

Cisco Vendor-Specific Fields

Cisco cable modems can accept a range of extra fields in the DOCSIS configuration file, which cater to the enhanced functionality within Cisco cable modems. Some of these fields only apply to cable modems that contain Voice over IP (VoIP) plain old telephone service (POTS) ports, such as the uBR924 and CVA120 series.

IOS Configuration File Download

It is possible to direct a Cisco cable modem to download a Cisco IOS Software configuration file. Set the IOS Filename field (on the Vendor Info tab) to the name of a Cisco IOS Software configuration file. This configuration file is stored on the same TFTP server as the DOCSIS configuration file, and it should be in plain text (TXT) format.

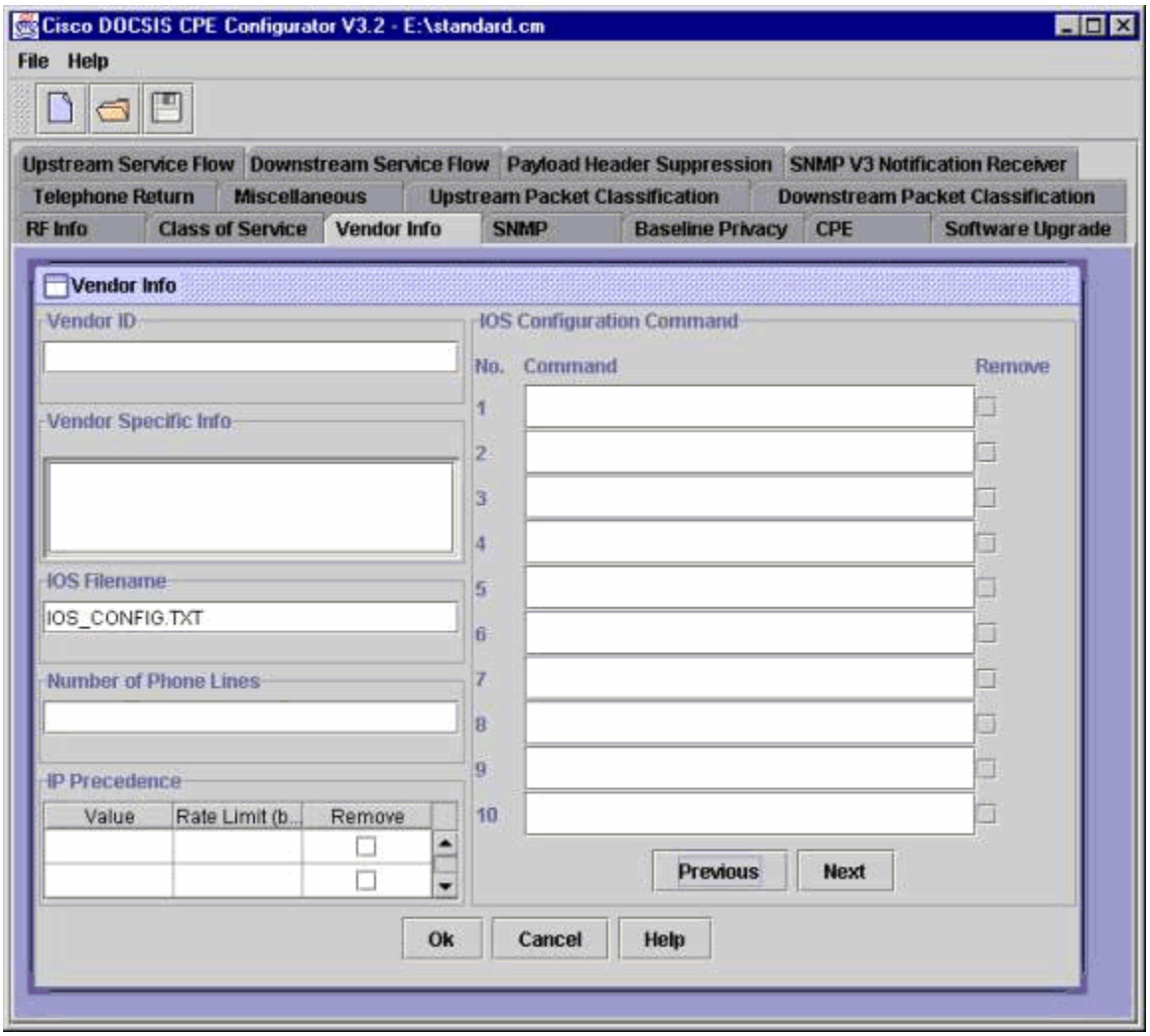
This example shows a typical IOS configuration file called IOS_CONFIG.TXT, which could be downloaded to a Cisco cable modem:

```
IOS_CONFIG.TXT

!

hostname uBR

!

enable secret cisco?

!

line vty 0 4

?password cisco

end
```

That configuration file adds lines to the cable modem's IOS configuration that specify the hostname, the Telnet password, and the enable secret. If any of these already exist on the Cisco cable modem's current configuration, they are overwritten. This type of Cisco IOS Software configuration file is especially useful for devices like the Cisco Cable Voice Adapters (CVA 120) series because, by default, a CVA does not have Telnet or enable password installed.

Figure 12 shows one way to set the IOS Filename field on the Vendor Info tab. When the IOS Filename field is filled in, a Cisco cable modem attempts to download the specified file, to include its contents in the running configuration.

Figure 12



Note: After a Cisco cable modem downloads a Cisco IOS Software configuration file through this method, the console port of the modem is disabled. This is so that service providers can make use of this feature to stop end users from misconfiguring their Cisco cable modems after they come online. There is no way to circumvent this behavior. For more detailed information, refer to Console or Telnet Access to Cable Modem Is Disabled.

Standard.cm has been modified to include these changes in standard-ios-config.cm. Click IOS_CONFIG.TXT to review the content of the IOS_CONFIG.TXT file.

Note: When you use Cisco Configurator tools, all of the Cisco vendor-specific fields—such as IOS Filename and Number of Phone Lines—automatically specify a Vendor ID field that corresponds to Cisco in the binary DOCSIS configuration file. Thus, there is no need to enter a value in the Vendor ID field. If you are using a third party Configurator, you must specify a Vendor ID field value of **00-00-0c**, which corresponds to Cisco Systems.

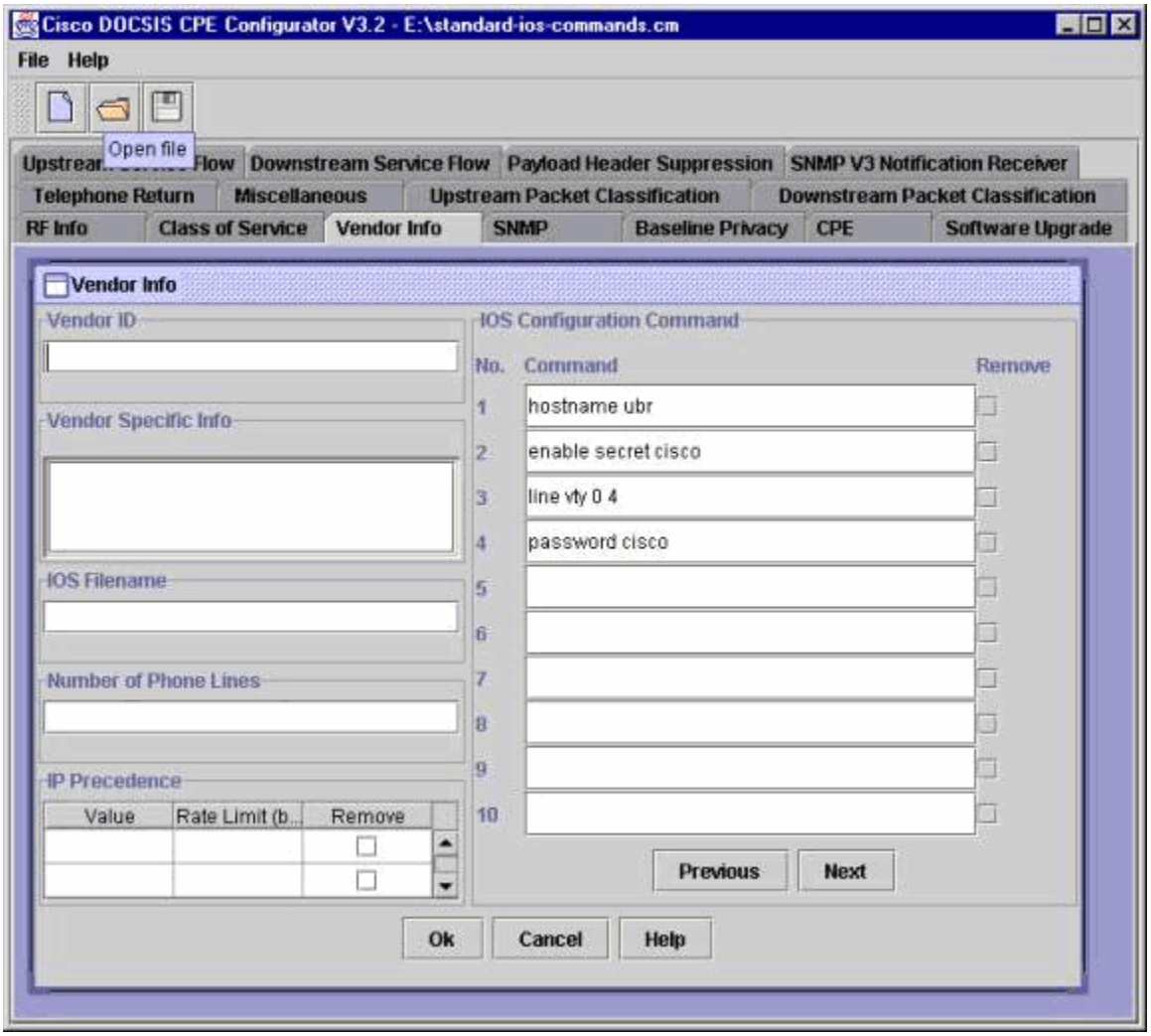
Cisco IOS Configuration Commands

Rather than have a Cisco cable modem download a separate Cisco IOS Software configuration file, you can specify a few individual IOS configuration commands within the DOCSIS configuration file. This can be done in the IOS Configuration Command area of the Vendor Info tab.

Cisco IOS Software configuration commands are entered in these fields in the order in which they would be entered from the configuration mode prompt on a Cisco router. Figure 13 shows the commands that are equivalent to those seen previously in IOS_CONFIG.TXT.

Note: The console port is *not* disabled when commands are specified in the IOS Configuration Command area.

Figure 13



Note: The **end** keyword is not required as the last command.

Only Cisco cable modems that run versions of Cisco IOS Software Release 12.1(1)T and later can understand the IOS Configuration Commands vendor-specific fields. For Cisco cable modems that run earlier versions of Cisco IOS Software, use the IOS Filename field instead.

Number of Phone Lines and Upstream Rate Limiting on IP Precedence

Cisco cable modems with voice ports may be provisioned to allow telephone calls to be made from the in-built VoIP telephony ports. When you specify an allowed number of simultaneous phone calls (in the Number of Phone Lines field on the Vendor Info tab), you can restrict the resources granted to a cable modem to support the Class of Service requirements of a phone call. Refer to Frequently Asked Questions on DOCSIS 1.0+ for more details on how resources are dynamically assigned to VoIP phone calls from cable modems.

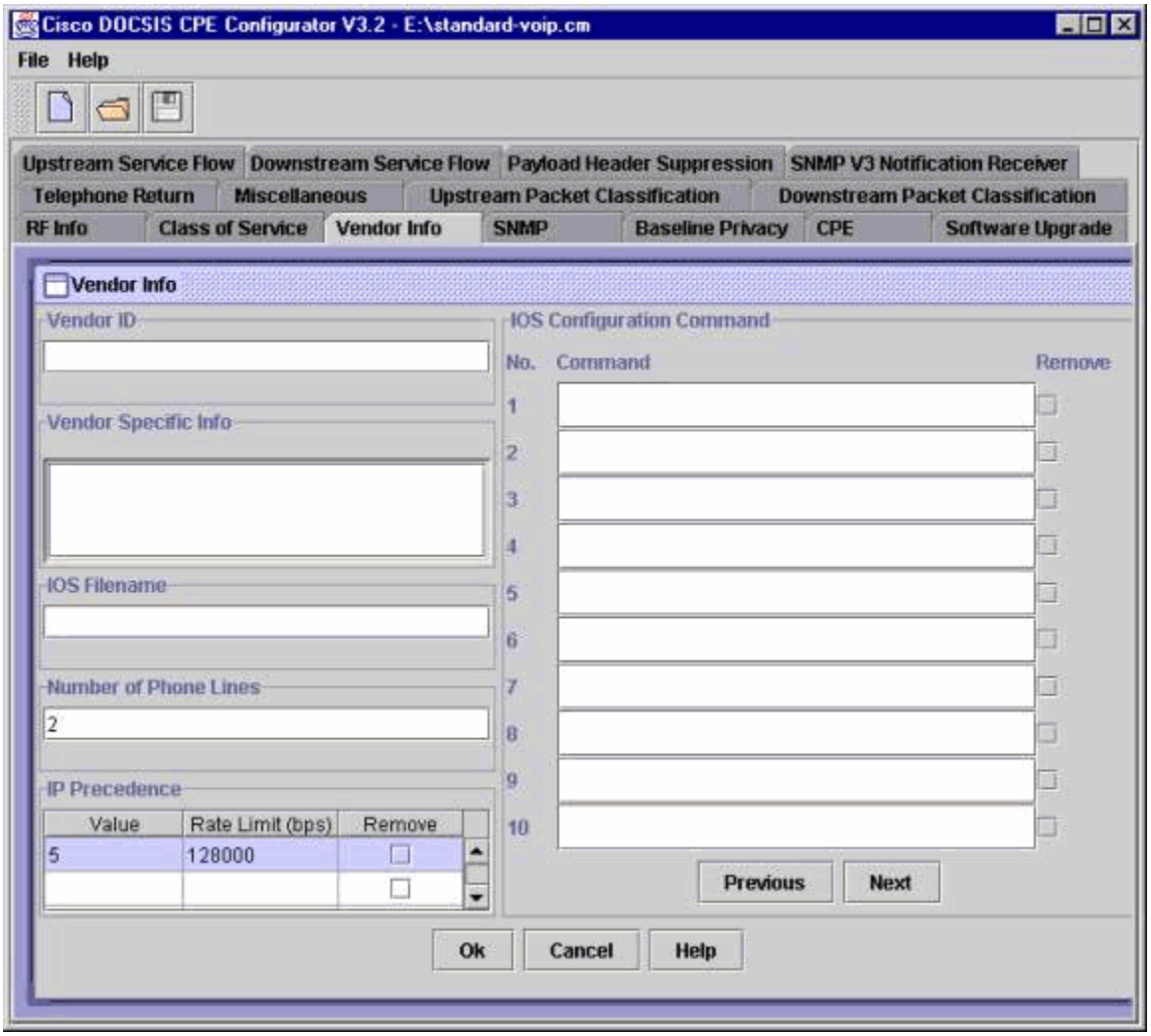
In addition to specifying the number of phone calls that may have dedicated resources assigned to them, the cable modem can be commanded to rate limit IP traffic in the upstream direction based on the IP precedence of the traffic. The reason for this feature is that VoIP packets are normally sent with an IP precedence of 5. Some service providers may have their backhaul networks configured to give a better class of service to IP traffic with precedence 5, to minimize delay for VoIP data packets.

When you rate limit IP traffic based on the precedence level, you can restrict the amount of traffic sent in this manner and hence discourage end users from engaging in this behavior. Typically, IP precedence 5 traffic is rate limited to the amount of bandwidth expected to be used by the maximum allowed number of VoIP phone calls.

It is not strictly necessary to specify upstream IP precedence rate limiting when phone lines are provisioned. In addition, you can specify that you prefer to perform upstream rate limiting on IP traffic with certain precedence settings without provisioning any phone lines. This means that you can perform IP precedence rate limiting on Cisco cable modems without telephony ports.

Figure 14 is an example of a Cisco cable modem that is provisioned to allow resources for up to two simultaneous VoIP phone calls. In addition, IP traffic with precedence 5 is rate limited in the upstream path to 128 kbps.

Figure 14



To get a copy of a DOCSIS configuration file that contains the Number of Phone Lines and IP Precedence parameters, click standard-voip.cm.

Performing a Firmware Upgrade via the DOCSIS Configuration File

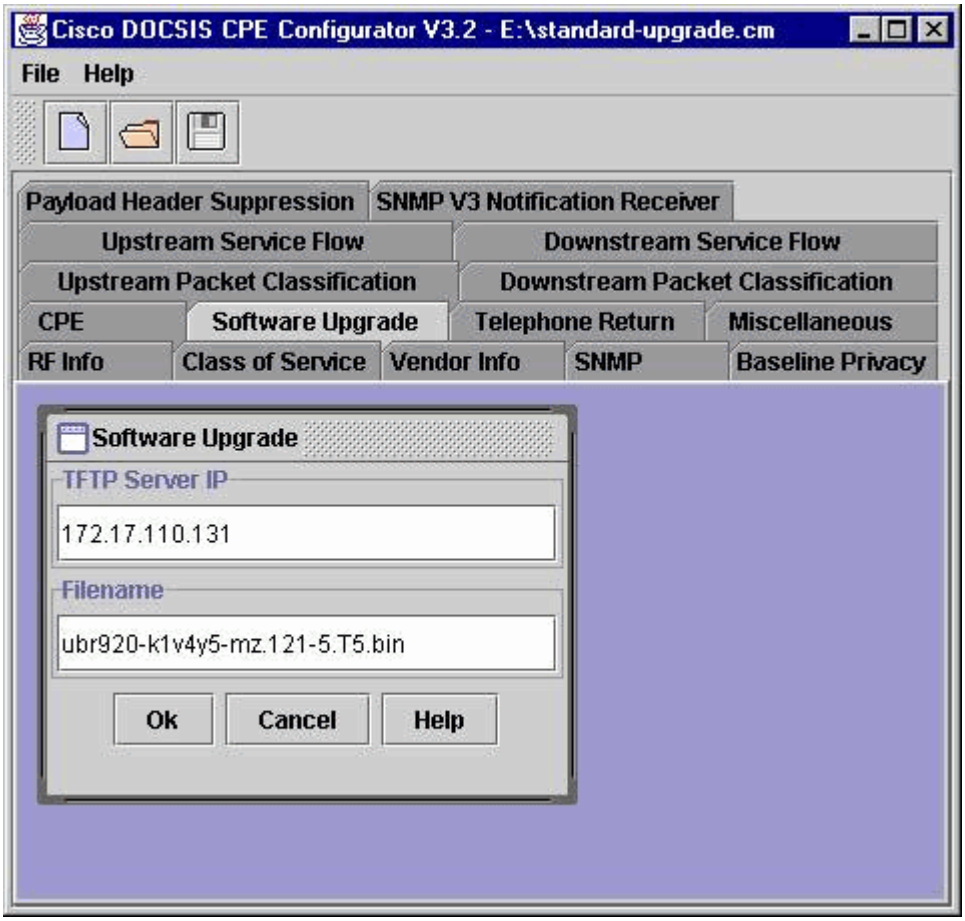
It is possible to command cable modems to upgrade themselves through TFTP: specify the name and location of

a new version of cable modem firmware in the DOCSIS configuration file.

On the Software Upgrade tab, the TFTP Server IP field is set to the IP address of a TFTP server that contains the firmware image; the Filename field is set to the file name of the firmware image.

Figure 15 shows that a uBR924 cable modem that receives this DOCSIS configuration file will attempt to download ubr920-k1v4y5-mz.121-5.T5.bin from the TFTP server on 172.17.110.131.

Figure 15



Note: If a cable modem downloads an image that is either corrupt or belongs to another vendor's cable modem, then it should perform a checksum calculation on the image to detect such an error. If the image can be understood by the cable modem and its checksum is correct, then the cable modem automatically reboots and runs the new version of firmware. If the image is corrupted or is intended to be used with another type of cable modem, then the cable modem should ignore the new image and remain online.

If the name of the firmware image in the DOCSIS configuration file is the same as the firmware image name that is currently on the cable modem, then the cable modem should ignore the upgrade step because it is already running the correct firmware image.

Note: Always test with upgrades of a few of a particular vendor's cable modems before you begin a mass upgrade; there may be bugs or unexpected problems associated with the upgrade process. It is clearly better to be prudent and perform tests to discover potential problems before you do a mass upgrade, find an unexpected problem, and then have to physically replace every cable modem in a system.

The sample DOCSIS configuration file standard-upgrade.cm contains parameters that command cable modems

to download a uBR924 image. Click standard-upgrade.cm to download this file.

Overriding the Downstream Frequency used by a Cable Modem

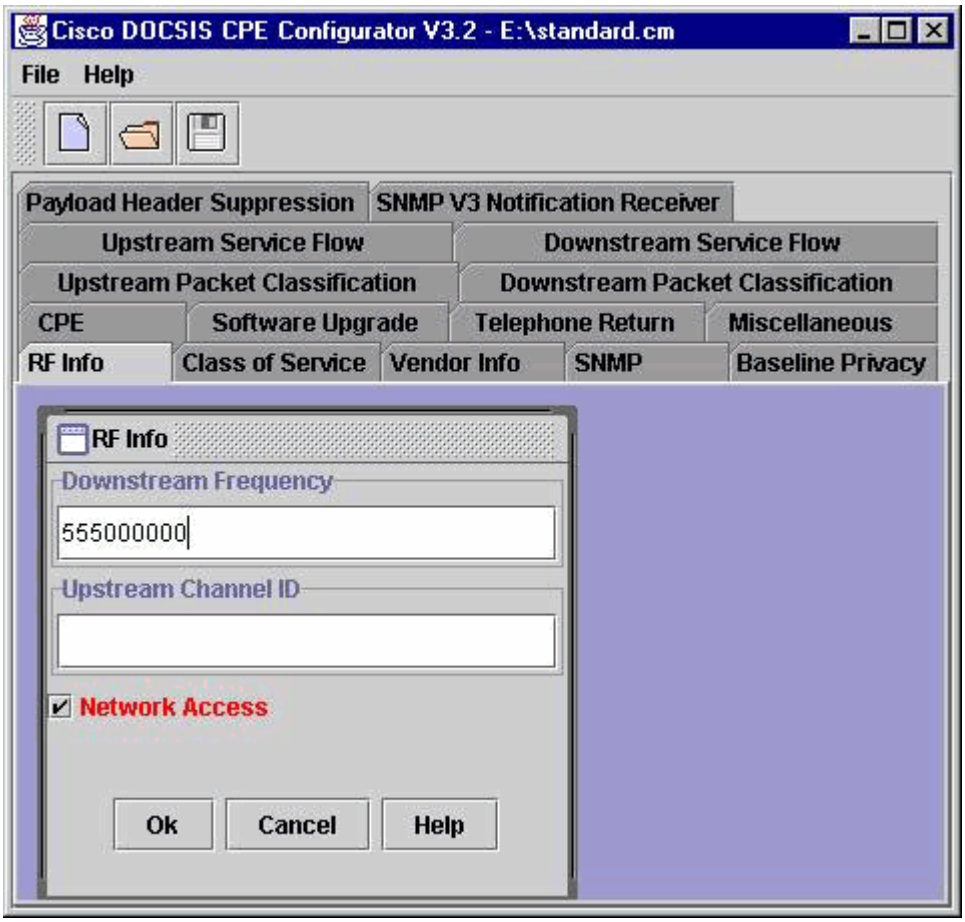
In situations where several CMTS devices serve the one cable segment, it might be desirable for certain cable modems to connect to one CMTS and not to the other. One method to force cable modems that have come online with the wrong CMTS to move to the right one is to use the Downstream Frequency override field on the RF Info tab. Specify an alternate downstream frequency (in Hz) in this field. If a cable modem downloads a DOCSIS configuration file with this field set, it disconnects from the CMTS onto which it initially locked, and it tries to come online with the CMTS that is sending a signal at the downstream frequency specified in the DOCSIS configuration file.

The type of scenario in which this practice would be common is when two or more service providers control separate CMTSs and, as such, there are multiple downstream frequencies onto which cable modems could lock. Each service provider must agree that—if a cable modem that belongs to another service provider came online with the wrong service provider's CMTS—a DOCSIS configuration file would be sent to the cable modem to tell it to use the correct downstream frequency.

The biggest caveat with the use of the Downstream Frequency override field is that, if an incorrect downstream frequency is specified, cable modems are never able to come online. A cable modem might lock onto a CMTS downstream frequency because it scans through the downstream spectrum and then downloads a DOCSIS configuration file that specifies a downstream frequency on which no CMTS is sending a signal. The cable modem adjusts its downstream receiver to listen to the specified frequency; when it hears nothing, it continues to scan. The cable modem probably will again lock onto the first frequency it found, download the same DOCSIS configuration file with the same incorrect downstream frequency, become stuck in an endless loop, and never fully come online.

Figure 16 shows an example of how the Downstream Frequency override field is set in the Cisco Configurator to specify a new downstream frequency in Hz to which a cable modem should connect.

Figure 16



Click standard-ds.cm to download a sample DOCSIS configuration file that contains a value in the Downstream Frequency override field.

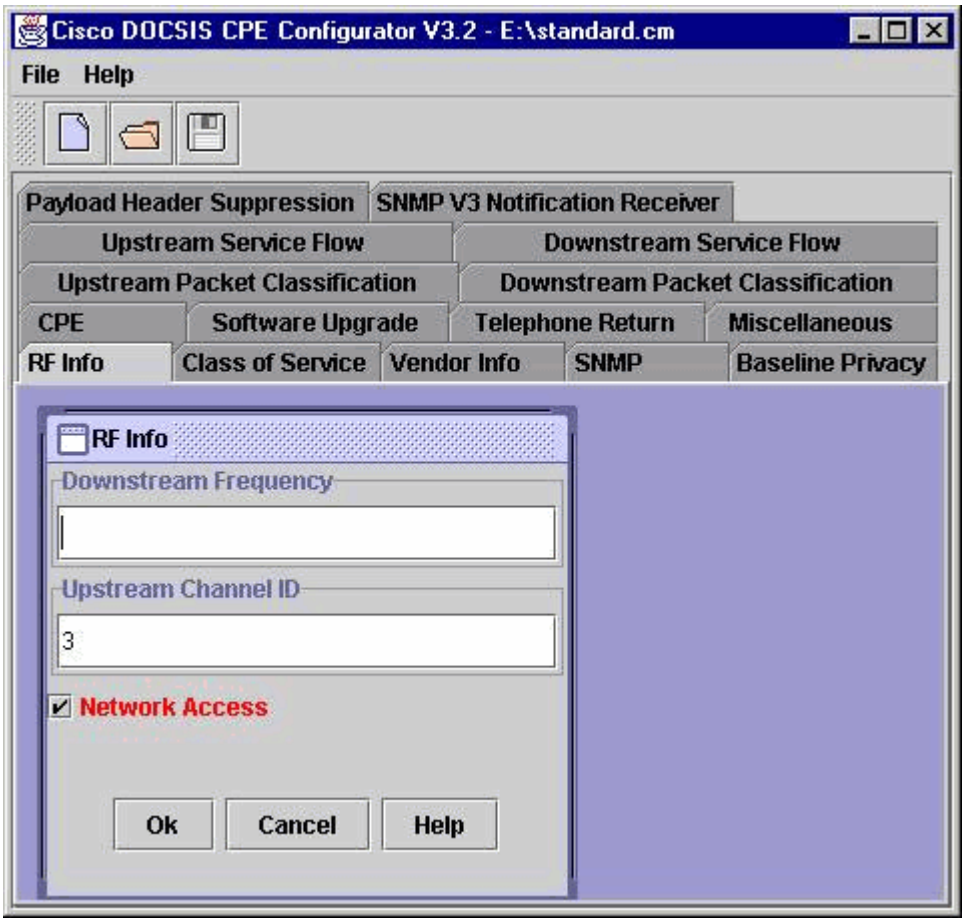
Overriding the Upstream Channel used by a Cable Modem

If several upstream channels are available for use on a particular cable segment, a cable modem should randomly select one of these channels to use when it comes online. One way to force a cable modem to use a particular upstream channel is to use the Upstream Channel ID override parameter on the RF Info tab of the Configurator. The valid range for the Upstream Channel ID is 1 through 255. It may be set to 0 only for Telco-return modems. In addition, if the Upstream Channel ID is set to a nonexistent or inactive upstream channel, or if the Upstream Channel ID specified corresponds to an upstream port that is not connected to the same cable segment as the cable modem, then the cable modem is unable to come online.

Figure 17 shows an example of how to set the Upstream Channel ID field to **3**.

Note: The Upstream Channel ID number is always one greater than the port to which it corresponds on a Cisco CMTS. For example, if Upstream Channel ID 1 is specified, this corresponds to the upstream port 0 on a Cisco CMTS.

Figure 17



In Figure 17, the upstream channel 3 in the DOCSIS configuration file corresponds to upstream port 2 on a Cisco CMTS.

Miscellaneous Settings

Configuring a DOCSIS Configuration File Shared-Secret

One problem that can occur in cable modem networks is that end users may decide to create their own DOCSIS configuration file that contains a higher level of service than that for which the user has paid. The user might then use a variety of means to make their cable modem download this forced DOCSIS configuration file rather than the service provider's version of the file and thereby receive an unauthorized level of service.

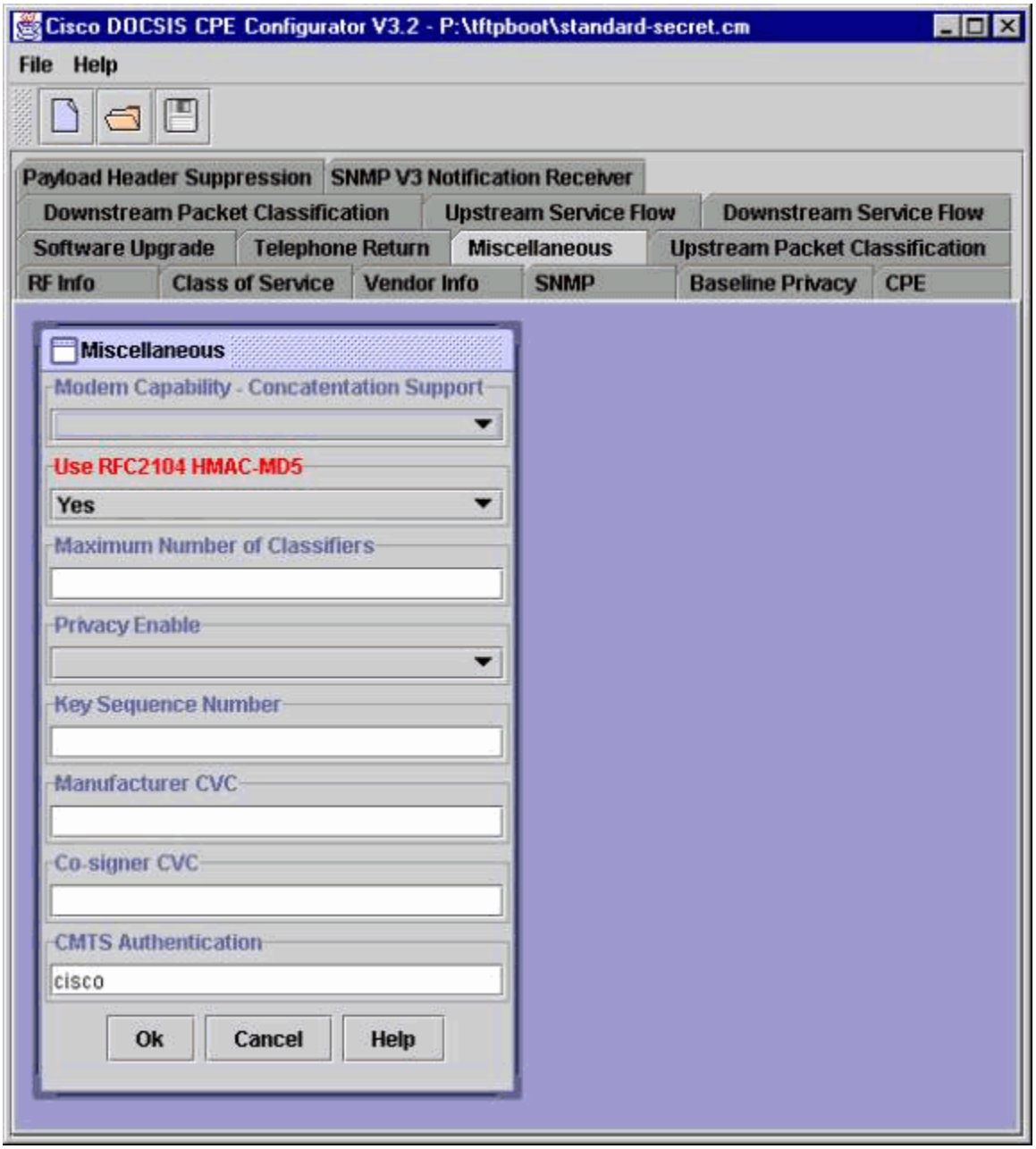
For this reason, it is possible to specify a CMTS Authentication string when you create a DOCSIS configuration file. This string is not stored in the file; it is used, however, when the file's MD5 checksum is calculated. The CMTS is also given a copy of the CMTS Authentication string and uses it to ensure that only cable modems that receive DOCSIS configuration files with the correct CMTS Authentication string are able to come online.

Because the CMTS Authentication string is not explicitly stored in the DOCSIS configuration file—but is only used as a part of the file's checksum generation—the CMTS Authentication string does not appear when a DOCSIS configuration file is viewed with the Cisco Configurator or any other tool. This means that end users can not merely obtain a copy of the DOCSIS configuration file to find the CMTS Authentication string. It also means that, if a DOCSIS configuration file is being modified, special care must be made to ensure that the CMTS Authentication string is reinserted into the DOCSIS configuration file every time it is re-saved. Otherwise, the checksum does not take into account the right CMTS Authentication string and is incorrect.

Figure 18 shows how a CMTS Authentication string is configured on the Miscellaneous tab. In this case, the

CMTS Authentication string is set to **cisco**.

Figure 18



Note: If this file is saved and re-opened, the CMTS Authentication field becomes blank and must be filled in again.

On a Cisco CMTS, the CMTS Authentication string is specified per cable interface with this cable interface command:

```
cable shared-secret string
```

The value for *string* must be identical to the CMTS Authentication string. Only one **cable shared-secret** command may be issued on each cable interface.

If a **cable shared-secret** is specified on a cable interface and a cable modem on that interface tries to come online with a DOCSIS configuration file that uses the wrong CMTS Authentication string, then the cable modem is not allowed to proceed to the online state and a message similar to this is logged on the CMTS:

```
%UBR7200-5-AUTHFAIL: Authorization failed for Cable Modem 0001.9E89.64C1
                     on interface Cable6/0
```

The cable modem also has a status of `reject(m)` instead of `online`.

Downloadable DOCSIS Configuration Files

Use Table 8 to download and find more information about a specific configuration file.

Table 8 – Downloads and Information

File Download (Save to disk)	More Information about the File
disabled.cm	More Info
disabled-snmp.cm	More Info
premium.cm	More Info
premium_snmp.cm	More Info
standard.cm	More Info
standard-ds.cm	More Info
standard-ios-commands.cm	More Info
standard-ios-config.cm	More Info
standard-llc.cm	More Info
standard-snmp.cm	More Info
standard-upgrade.cm	More Info
standard_us.cm	More Info
standard-voip.cm	More Info
standard-ip.cm	More Info

Conclusion

The DOCSIS configuration file gives a service provider the power to control virtually every aspect of a cable modem's operation. The simplest kinds of DOCSIS configuration files generally only specify a maximum throughput and the number of supported CPE devices. More complicated DOCSIS configuration files can configure a modem to reserve upstream bandwidth, be managed through SNMP, and perform packet filtering (amongst other things).

When you generate new DOCSIS configuration files for use in a production network, it is critically important that you thoroughly test the effects of the files on your different vendor's cable modems before you deploy the file. Different vendor modems and different versions of firmware might react differently to certain settings. Work with your cable modem vendor to resolve any irregularities or problems.

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Cable
Network Infrastructure: Remote Access
ISDN TA and BRI dial-in to a PRI - May 28, 2004 what is the debug command for modem allocation? - May 27, 2004 Cant VPN out of from my LAN - May 27, 2004 uBR question: cable modem online with no IP - May 27, 2004 2610XM as a ras server - May 27, 2004

Related Information

- **The DOCSIS RFI Specifications**
- **RFC 2669 - DOCSIS Cable Device MIB**
- **Port Numbers for protocol numbers and TCP/UDP Port Numbers**
- **Cisco DOCSIS CPE Configurator (V2.0.4 collects information to generate a DOCSIS configuration file.)**
- **Broadband Cable Technologies**
- **Broadband Cable Technology Support**
- **Technical Support - Cisco Systems**

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.