



# Usage Based Billing for the Cisco CMTS

---

## Document Revision History

Date	Revision	Reason
2/13/2006	Rev. B0	Added Document Revision History table and feature enhancements introduced in Cisco IOS Release 12.3(17a)BC.
5/06/2009	Rev. B1	Modified <b>show cable metering</b> output examples.

This document describes the Usage-Based Billing feature for the Cisco Cable Modem Termination System (CMTS), which provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

## Feature Specifications for Usage-Based Billing

Feature History	
Release	Modification
Release 12.3(9a)BC	This feature was introduced on Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.  Feature support includes the new CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format.
Release 12.3(17a)BC	This feature includes additional MIBs that support OSSI specifications as well as enhanced billing reports. For more information about DOCSIS 2.0, see the Cable Labs document t <a href="#">Data-Over-Cable Service Interface Specifications DOCSIS 2.0 Operations Support System Interface Specification</a> .  Support for Secure Socket Layer (SSL) Servers introduced with certification support.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

12.3(21)BC	<p>This feature provides enhancements to specify the source interface for billing packets in the Subscriber Account Management Interface Specification (SAMIS).</p> <p>The <b>cable metering source-interface &lt;interface&gt;</b> command was introduced.</p> <p>Support also includes a new object <code>ccmtrCollectionSrcIfIndex</code> in <code>CISCO-CABLE-METERING-MIB.my</code>.</p>
12.2(33)SCB	SAMIS over Internet Protocol Detail Record (IPDR) was introduced.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

This document includes the following major sections:

- [Prerequisites for Usage-Based Billing, page 2](#)
- [Restrictions for Usage-Based Billing, page 3](#)
- [Information About Usage-Based Billing, page 4](#)
- [How to Configure the Usage-Based Billing Feature, page 10](#)
- [Monitoring the Usage-Based Billing Feature, page 35](#)
- [Configuration Examples for Usage-Based Billing, page 36](#)
- [Additional References, page 38](#)
- [Command Reference, page 40](#)

## Prerequisites for Usage-Based Billing

The Usage-Based Billing feature has the following prerequisites:

- The Usage-Based Billing feature is supported only on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
- The Usage-Based Billing feature is supported for cable modems compliant with DOCSIS 1.0, DOCSIS 1.1 and DOCSIS 2.0 in Cisco IOS Release 12.3(9a)BC.
- The Cisco CMTS router must be running Cisco IOS Release 12.3(9a)BC or later Cisco IOS Release 12.3 BC release.
- Cable modems that are being monitored should use a DOCSIS configuration file that defines upstream and downstream primary service flows using Service Class Naming (SCN) (TLV 24/25, subTLV 4). If dynamically-created service flows are to be monitored, they should also be created with SCN names.

- When the feature is operating in File mode, an external billing server must log into the Cisco CMTS to copy the billing records to the external server, using either Secure Copy (SCP) or Trivial File Transfer Protocol (TFTP). The Cisco CMTS cannot operate as a FTP or secure FTP (SFTP) server.
- When the feature is operating in Streaming mode in non-secure mode, an external billing server must be configured to receive the billing records at a configurable TCP port.
- When the feature is operating in Streaming mode in secure mode, the following are required:
  - The external billing server must be configured to receive the billing records at a configurable TCP port using a secure socket layer (SSL) connection.

**Tip**

---

Several third-party solutions for SSL support on the billing application server are available.

---

- A Certificate Authority (CA) must be configured and available to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

## Restrictions for Usage-Based Billing

The Usage-Based Billing feature has the following restrictions and limitations:

- SNMP commands can be used to display or modify the Usage-Based Billing configuration, and SNMP traps can be used to notify the billing application system when a billing record is available. However, SNMP commands cannot be used to retrieve billing records.
- Cisco IOS Release 12.3(9a)BC does not support Usage-Based Billing with 1:N or Route Processor Redundancy (RPR):
  - When HCCP N+1 switchover events occur to a Protect cable interface, usage-based billing is suspended until the system returns to the Working cable interface.
  - On the Cisco uBR10012 router, when the system switches over to the secondary PRE1 module, usage-based billing is suspended unless you have also preconfigured the usage-based billing on the secondary PRE1 module.
- Billing records do not include information about multicast service flows and traffic counters.
- The packet counters displayed by CLI commands are reset to zero whenever the Cisco CMTS router is rebooted. The packet counters displayed by SNMP commands are not retained across router reloads, and SNMP MIB counters cannot be preserved during reloads. These counters are 64-bit values and could roll over to zero during periods of heavy usage.
- When configuring cable metering in the Usage-Based Billing File Mode, the source-interface cannot be specified immediately after using the **cable metering filesystem** command. Once the **cable metering filesystem** command is used, the cable metering file will write to the bootflash. Until this operation is complete, no cable metering configuration will be allowed.

After the file write operation is complete, the source-interface command (**cable metering source-interface**) can then be configured; and the metering file in the bootflash would need to be removed so that billing packets have the source-interface's IP address.

**Note**

---

This cable metering restriction will not be a problem during reload.

---

- When configuring cable metering in the Usage-Based Billing Streaming Mode, make sure that the loopback interface is accessible from the collector server. Telnetting to the loopback interface's IP address from the collector server is a good method of testing whether the loopback interface is accessible from the collector server or not.

## Information About Usage-Based Billing

This section describes the Usage-Based Billing feature:

- [Feature Overview, page 4](#)
- [Usage-Based Billing and DOCSIS Support on the Cisco CMTS, page 5](#)
- [Standards, page 5](#)
- [Modes of Operation, page 6](#)
- [Billing Record Format, page 6](#)
- [SNMP Support, page 9](#)
- [Benefits, page 10](#)

## Feature Overview

The Usage-Based Billing feature provides a standards-based, open application approach to recording and retrieving traffic billing information for DOCSIS networks. When enabled, this feature provides the following billing information about the cable modems and customer premises equipment (CPE) devices that are using the cable network:

- IP and MAC addresses of the cable modem.
- Service flows being used (both upstream and downstream service flows are tracked).
- IP addresses for the CPE devices that are using the cable modem.
- Total number of octets and packets received by the cable modem (downstream) or transmitted by the cable modem (upstream) during the collection period.
- Total number of downstream packets for the cable modem that the CMTS dropped or delayed because they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA).

Billing records are maintained in a standardized text format that the service provider can easily integrate into their existing billing applications. Service providers can use this information to determine which users might be potential customers for service upgrades, as well as those customers that might be trying to exceed their SLA limits on a regular basis.

## Usage-Based Billing and DOCSIS Support on the Cisco CMTS

The Usage-Based Billing feature supports these DOCSIS features on the Cisco CMTS:

- DOCSIS 1.0, DOCSIS 1.1, and DOCSIS 2.0-compliant cable modems are supported.
- Best Effort service flows are supported for DOCSIS-compliant cable modems.
- Secondary service flows are supported for DOCSIS-compliant cable modems.
- Dynamic service flows are supported for DOCSIS-compliant cable modems.

- Information about deleted service flows is available only for DOCSIS 1.1 service flows but not for DOCSIS 1.0 service flows.
- Support for terminated service flows must be enabled using the **cable sflog** global configuration command. Refer to the [“Enabling Usage-Based Billing Feature \(File Mode\)—Using CLI Commands” section on page 10](#).

## Standards

The Usage-Based Billing feature is based on several open standards, allowing it to be supported by a wide range of commercial and custom-written billing applications. The following standards provide the major guidelines for writing and using the billing records that the CMTS produces:

- Extensible Markup Language (XML)—A metalanguage that in turn can easily define other markup languages to contain any kind of structured information, such as billing records. An XML-based approach allows the collected billing information to be used by and distributed among many different billing applications from different vendors. It also allows the format to be easily updated and customized to meet the needs of different providers.
- IP Detail Record (IPDR)—An open, vendor-independent standard, defined in the *Network Data Management—Usage (NDM-U) For IP-Based Services* specification, to simplify billing and usage record-keeping for any type of services that can be delivered over an IP-based network. Service providers can use IPDR to create unified billing applications for all of their services, such as DOCSIS or Voice-over-IP, even though those services use different protocols and application servers.
- DOCSIS Operations Support System Interface (OSSI) specification—A DOCSIS specification that defines the requirements for the network management of a DOCSIS network, including a Subscriber Account Management Interface Specification (SAMIS) for a billing record interface. The DOCSIS 2.0 version of this specification states that a CMTS is not required to provide a billing interface, but if the CMTS does provide a billing interface, it must be based on the IPDR/XML standards.



Tip

For further information about these standards, see the documents listed in the [“Standards” section on page 38](#).

## Modes of Operation

The Usage-Based Billing feature can operate in two modes:

- File Mode—In file mode, the CMTS collects the billing record information and writes the billing records to a file on a local file system, using a file name that consists of the router’s hostname followed by a timestamp of when the file was written. A remote application can then log into the CMTS and transfer the billing record file to an external server where the billing application can access it.

The remote application can use the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP) to transfer the file. After a successful transfer, the remote application then deletes the billing record file, which signals the CMTS that it can create a new file. The remote application can either periodically log into the CMTS to transfer the billing record file, or it can wait until the CMTS sends an SNMPv3 trap to notify the application that a billing record file is available.

- **Streaming Mode**—In streaming mode, the CMTS collects the billing record information and then regularly transmits the billing record file to an application on an external server, using either a non-secure TCP connection or a secure sockets layer (SSL) connection. The billing record data collected is streamed on the fly; and if streaming is unsuccessful, then the SAMIS data will be sent the next interval only.

If the CMTS fails to establish a successful connection with the external server, it retries the connection between 1 and 3 times, depending on the configuration. If the CMTS continues to be unable to connect with the external server, the CMTS can send an SNMPv3 trap to notify an SNMP manager that this failure occurred.

In streaming mode, you configure the CMTS to transmit the billing record file at regular intervals. Typically, the interval chosen would depend on the number of cable modems and the size of the billing record files that the CMTS produces.

## Billing Record Format

Each billing record is an ASCII text file using XML formatting to encode the billing record objects that are required by the DOCSIS specifications. This file can be read by any billing application that can be configured to parse XML data files.

**Table 1** lists the objects that are contained in each billing record that the CMTS generates. This table shows the object's name, as it appears in the billing record, and a description of that object.

**Table 1** Billing Record Objects

Object Name	Description
IPDRcreationTime	(Appears in header of billing record) Date and time that the CMTS created the billing record.
serviceClassName	Service Class Name (SCN) identifying the service flow (for example, BronzeDS).  <b>Note</b> Cisco IOS Release 12.3(9a) supports DOCSIS 1.0 and DOCSIS 1.1 cable modems with the following differences between them: <ul style="list-style-type: none"> <li>• Because DOCSIS 1.0 cable modems do not have service class names, the SCN field is always blank and the service flow ID (SFID) is the same as the service ID (SID).</li> <li>• For DOCSIS 1.1 cable modems, the value for the SCN field is that which is configured and the SFID.</li> </ul>
CMmacAddress	MAC Address of the cable modem, expressed as six hexadecimal bytes separated by dashes (for example, 00-00-0C-01-02-03).
CMipAddress	IP address for the cable modem, expressed in dotted decimal notation (for example, 192.168.100.101).
CMdocsisMode	Version of DOCSIS that the cable modem is currently using (DOCSIS 10, 11, 20).
CPEipAddress	IP address for each CPE device that is using this cable modem, expressed in dotted decimal notation. This object is optional and can be suppressed to improve performance by reducing the size of the billing record files.
CMTSipAddress	IP address for the CMTS, expressed in dotted decimal notation.
CMTShostName	Fully qualified hostname for the CMTS (for example, cmts01.cisco.com).
CMTSsysUpTime	Amount of time, in hundredths of a second, since the last initialization of the CMTS management interface, expressed as a 32-bit decimal number (0 to 4,294,967,296).

Table 1 Billing Record Objects (continued)

Object Name	Description
RecType (SFTType renamed to RecType in Cisco IOS Release 12.3(17a)BC)	Type of service flow being described: <ul style="list-style-type: none"> <li>• <b>Interim</b> = the service flow was active throughout the collection period and should be reported as 1.</li> <li>• <b>Stop</b> = the service flow was deleted at some point during the collection period and should be reported as 2.</li> </ul>
serviceIdentifier	Service flow ID assigned to this service flow by the CMTS, expressed as a decimal number. <b>Note</b> For DOCSIS 1.0 cable modems, the SFID field always shows the primary service flow for the upstream or downstream.
serviceDirection	Direction for the service flow ( <b>Downstream</b> or <b>Upstream</b> ).
serviceOctetsPassed	Total number of octets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
servicePktsPassed	Total number of packets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
SLAdropPkts	(Downstream service flows only) Total number of downstream packets for the cable modem that the CMTS dropped because otherwise they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
SLAdelayPkts	(Downstream service flows only) Total number of packets that the CMTS delayed transmitting on the downstream to the cable modem because otherwise they would have exceeded bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
CMTScatvIfIndex	The ifIndex of the MAC interface.
CMTScatvIfName	The ifName of the CMTS CATV (MAC) interface associated with this cable modem.
CMTSupIfName	The ifName of the CMTS Upstream interface associated with this cable modem.
CMTSdownIfName	The ifName of the CMTS Downstream interface associated with this cable modem.
CMcpeFqdn	FQDNs for cable modem associated CPEs.
serviceTimeCreated	Timestamp for SF creation (consistent with QoS MIB model).
serviceTimeActive	The active time of the SF in seconds.

**Note** Because the byte and packet counters are 64-bit values, it is possible for them to wrap around to zero during a billing period. The billing application should use the sysUpTime value along with the counters to determine whether the counters have wrapped since the last billing period. If a counter appears to regress, and if the current sysUpTime indicates this billing cycle is the next scheduled cycle for this particular cable modem, you can assume that the counter has wrapped during the billing cycle.

**Note**

These billing record objects are defined in Appendix B, *IPDR Standards Submission for Cable Data Systems Subscriber Usage Billing Records*, in the *DOCSIS 2.0 OSS I Specification* (SP-OSSIV2.0-IO3-021218).

The following example shows a sample IPDR billing record for a downstream service flow:

```
<?xml version="1.0" encoding="UTF-8"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```

xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="C341A679-0000-0000-0000-000BBF54D000"
creationTime="2002-05-25T14:41:29Z"
IPDRRecorderInfo="CMTS01"
version="3.1">
</IPDR>
<IPDR xsi:type="DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315 </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-AB-D4-53</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.3</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>2</serviceDirection>
<serviceOctetsPassed>23457</ServiceOctetsPassed>
<servicePktsPassed>223</ServicePktsPassed>
<serviceSlaDropPkts>2</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>

```

The following example shows a sample IPDR billing record for an upstream service flow:

```

<?xml version="1.0" encoding="UTF-8"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
  docId="C3146152-0000-0000-0000-000BBF7D5800"
  creationTime="2003-09-18T16:52:34Z"
  IPDRRecorderInfo="CMTS01-UBR7246.cisco.com"
  version="3.1">
<IPDR xsi:type=" DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315 </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-18-8A-4D</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.14</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>1</serviceDirection>
<serviceOctetsPassed>1404</ServiceOctetsPassed>
<servicePktsPassed>6</ServicePktsPassed>
<serviceSlaDropPkts>0</serviceSlaDropPkts>

```

```
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

## SNMP Support

Cisco IOS Release 12.3(9a)BC supports the [CISCO-CABLE-METERING-MIB](#) MIB, which provides the following SNMPv3 support for the Usage-Based Billing feature:

- Configuring the Usage-Based Billing feature using SNMPv3 commands.
- Displaying the current Usage-Based Billing configuration using SNMPv3 commands.
- Sending SNMPv3 traps upon the following usage-based billing events:
  - The CMTS is reporting that a new billing record is available.
  - The CMTS is reporting that a failure occurred in writing the most recent billing record (for example, the disk is full).
  - The CMTS is reporting that it could not successfully open a secure SSL connection to stream a billing record to the billing server.

For more information on this support, see the [CISCO-CABLE-METERING-MIB](#).

In addition, information about deleted service flows (DOCSIS 1.1 service flows only) is maintained in the docsQosServiceFlowLogTable in the [DOCS-QOS-MIB](#). (Logging of deleted service flows must be enabled using the **cable sflog** global configuration command.)

## Benefits

The Usage-Based Billing feature provides the following benefits to cable service providers and their partners and customers:

- Allows service providers to integrate their billing applications for DOCSIS services with their other XML-capable billing applications.
- Standards-based approach that supports existing networks and services, such as DOCSIS and PacketCable, and is easily extensible to support future services as they are supported on the Cisco CMTS.

## How to Configure the Usage-Based Billing Feature

This section describes the following tasks that are required to implement the Usage-Based Billing feature:

- [Enabling Usage-Based Billing Feature \(File Mode\)—Using CLI Commands, page 10](#)
- [Enabling Usage-Based Billing Feature \(File Mode\)—Using SNMP Commands, page 12](#)
- [Enabling Usage-Based Billing Feature \(Streaming Mode\)—Using CLI Commands, page 15](#)
- [Enabling Usage-Based Billing Feature \(Streaming Mode\)—Using SNMP Commands, page 17](#)
- [Enabling and Configuring Secure Copy \(optional\), page 21](#)
- [Configuring the Cisco CMTS for SSL Operation, page 24](#)

- [Retrieving Records from a Cisco CMTS in File Mode, page 25](#)
- [Disabling the Usage-Based Billing Feature, page 32](#)
- [Configuring Certified SSL Servers for Usage-Based Billing, page 33](#)

## Enabling Usage-Based Billing Feature (File Mode)—Using CLI Commands

This section describes how to enable and configure the Usage-Based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable metering filesystem *filesys* [flow-aggregate] [cpe-list-suppress]**
4. **snmp-server enable traps cable metering**
5. **cable sflog max-entry *number* entry-duration *time***
6. **cable metering source-interface *interface***
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable Router#</p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 3	<p><b>cable metering filesystem <i>filesys</i></b> <b>[flow-aggregate] [cpe-list-suppress]</b></p> <p><b>Example:</b> Router(config)# cable metering filesystem disk1: Router(config)#</p>	<p>Enables the Usage-Based Billing feature for file mode and configures it with the following parameters:</p> <ul style="list-style-type: none"> <li>• <i>filesys</i> = Specifies the file system to contain the billing records. The <i>filesys</i> has a maximum length of 25 characters and must specify a valid file system on the router (such as disk0: or slot1:). (The system will write the billing records on this filesystem using a file name that consists of the router's hostname followed by a timestamp when the record was written.)</li> <li>• <b>flow-aggregate</b> = (Optional) Combines all information for an individual cable modem into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction.</li> <li>• <b>cpe-list-suppress</b> = (Optional) Eliminates the customer premises equipment (CPE) IP addresses from the billing records to improve performance.</li> </ul>
Step 4	<p><b>snmp-server enable traps cable metering</b></p> <p><b>Example:</b> Router(config)# snmp-server enable traps cable metering Router(config)#</p>	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

	Command or Action	Purpose
Step 5	<p><b>cable sflog max-entry</b> <i>number</i> <b>entry-duration</b> <i>time</i></p> <p><b>Example:</b>  Router(config)# cable sflog max-entry 2000  entry-duration 7200  Router(config)#</p>	<p>(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.</p> <ul style="list-style-type: none"> <li><i>number</i>—Specifies the maximum number of entries in the service flow log. When the log becomes full, the oldest entries are deleted to make room for new entries. The valid range is 0 to 59999, with a default of 0 (which disables service flow logging).</li> <li><i>time</i>—Specifies how long, in seconds, entries can remain in the service flow log. The CMTS deletes entries in the log that are older than this value, so this should specify a long enough time period for at least one billing cycle. The valid range is 1 to 86400 seconds, with a default value of 3600 seconds (1 hour).</li> </ul>
Step 6	<p><b>cable metering source-interface</b> <i>interface</i></p> <p><b>Example:</b>  Router(config)# cable metering source-interface loopback100  Router(config)#</p>	<p>(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.</p>
Step 7	<p><b>end</b></p> <p><b>Example:</b>  Router(config)# end  Router#</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

## Enabling Usage-Based Billing Feature (File Mode)—Using SNMP Commands

This section describes how to enable and configure the Usage-Based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

### SUMMARY STEPS

To configure the Cisco CMTS for Usage-Based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB. [Table 2](#) describes each of these objects, and whether they are required or optional.



#### Note

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command. Refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

**Table 2** *SNMP Objects to be Configured for File Mode*

Object	Type	Description
ccmtrCollectionType	Integer	<p>Enables or disables the Usage-Based Billing feature. The valid values are:</p> <ul style="list-style-type: none"> <li>• 1 = none. The Usage-Based Billing feature is disabled (default).</li> <li>• 2 = local. The Usage-Based Billing feature is enabled and configured for file mode.</li> <li>• 3 = stream. The Usage-Based Billing feature is enabled and configured for streaming mode.</li> </ul> <p>Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.</p>
ccmtrCollectionFilesystem	DisplayString	<p>Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash).</p> <p><b>Note</b> The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.</p>
ccmtrCollectionCpeList	TruthValue	<p>(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following:</p> <ul style="list-style-type: none"> <li>• true = CPE information is present (default).</li> <li>• false = CPE information is omitted.</li> </ul> <p><b>Note</b> When set to true, a maximum of 5 CPE IP addresses for each cable modem.</p>
ccmtrCollectionAggregate	TruthValue	<p>(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows:</p> <ul style="list-style-type: none"> <li>• true = All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank.</li> <li>• false = Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).</li> </ul>
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

**DETAILED STEPS****Note**

The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

- Step 1** Set the `ccmtrCollectionType` object to 2, to enable the Usage-Based Billing feature and to configure it for file mode:

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionType.0 -i 2
workstation#
```

- Step 2** Set the `ccmtrCollectionFilesystem` object to the local file system where the Cisco CMTS should write the billing records:

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionFilesystem.0
-D disk0:
workstation#
```

- Step 3** (Optional) To omit the IP addresses of CPE devices from the billing records, set the `ccmtrCollectionCpeList` object to 2 (false). The default is to include the CPE information.

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionCpeList.0 -i 2
workstation#
```

- Step 4** (Optional) To aggregate all service flow information for each cable modem in a single record, set the `ccmtrCollectionAggregate` object to 1 (true). The default is for each service flow to be written in a separate record:

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionAggregate.0 -i 1
workstation#
```

- Step 5** (Optional) To specify the source-interface for the billing packets, set the `ccmtrCollectionSrcIfIndex` object to 1 (true). The default is for the billing packets to automatically select a source-interface.

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

## Examples

The following example shows the Usage-Based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-Based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB
ccmtrCollectionType.0 = none(1)
ccmtrCollectionFilesystem.0 =
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = 0
ccmtrCollectionDestination.0 =
ccmtrCollectionTimestamp.0 = 00 00 00 00 00 00 00 00
ccmtrCollectionNotifEnable.0 = true(1)
```

```
workstation#
```

The following SNMP commands are then given to enable the Usage-Based Billing feature and to configure it for file mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionType.0 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionFilesystem.0 -D disk1:
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering
```

```
cable metering filesystem disk1:
```

```
Router#
```

The following SNMP display shows the new configuration, after the Cisco CMTS has successfully written a billing record:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

cmtrCollectionType.0 = local(2)
cmtrCollectionFilesystem.0 = disk1:
cmtrCollectionCpeList.0 = true(1)
cmtrCollectionAggregate.0 = false(2)
cmtrCollectionStatus.0 = success(1)
cmtrCollectionDestination.0 = disk1:UBR7246.cisco.com-20030925-185827
cmtrCollectionTimestamp.0 = 07 d3 09 19 12 3a 1c 00
cmtrCollectionNotifEnable.0 = true(1)

workstation#
```

## Enabling Usage-Based Billing Feature (Streaming Mode)—Using CLI Commands

This section describes how to enable and configure the Usage-Based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable metering destination** *ip-address port [ip-address2 port2] retries minutes {non-secure | secure} [flow-aggregate] [cpe-list-suppress]*
4. **snmp-server enable traps cable metering**
5. **cable sflog max-entry** *number entry-duration time*
6. **cable metering source-interface** *interface*
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable Router#</p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 3	<p><b>cable metering destination</b> <i>ip-address port</i> <i>[ip-address2 port2] retries minutes</i> <i>{non-secure   secure}</i> <i>[flow-aggregate] [cpe-list-suppress]</i></p> <p><b>Example:</b> Router(config)# cable metering destination 10.10.21.3 5300 10.10.21.4 5300 2 30 secure Router(config)#</p>	<p>Enables the Usage-Based Billing feature for streaming mode and configures it with the following parameters:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i> and <i>port</i> = Specifies the IP address and TCP port number for the billing application on an external server that will collect the records. The valid range for <i>port</i> is 0 to 65535.</li> <li>• <i>ip-address2</i> and <i>port2</i> = (Optional) Specifies an IP address and TCP port number for the billing application on a secondary external server that will be used if the primary server fails to respond. The valid range for <i>port</i> is 0 to 65535.</li> <li>• <i>retries</i> = Specifies the number of retry attempts that the CMTS will make to establish a connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range is 0 to, with a no default.</li> <li>• <i>minutes</i> = Specifies how often, in minutes, the billing records are streamed to the external server. The valid range is 15 to 1440 minutes (24 hours), with no default.</li> <li>• <b>non-secure</b> = Specifies that the Cisco CMTS should use an unencrypted TCP connection when connecting to the billing application on the external server.</li> <li>• <b>secure</b> = Specifies that the Cisco CMTS should use a secure socket layer (SSL) connection when connecting to the billing application on the external server.</li> <li>• <b>flow-aggregate</b> = (Optional) Combines all information for an individual cable modem into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction.</li> <li>• <b>cpe-list-suppress</b> = (Optional) Eliminates the IP addresses for customer premises equipment (CPE) from the billing records, so as to improve performance.</li> </ul>

	Command or Action	Purpose
Step 4	<pre>snmp-server enable traps cable metering</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server enable traps cable metering Router(config)#</pre>	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.
Step 5	<pre>cable sflog max-entry number entry-duration time</pre> <p><b>Example:</b></p> <pre>Router(config)# cable sflog max-entry 2000 entry-duration 7200 Router(config)#</pre>	(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows. <ul style="list-style-type: none"> <li><i>number</i>—Specifies the maximum number of entries in the service flow log. When the log becomes full, the oldest entries are deleted to make room for new entries. The valid range is 0 to 59999, with a default of 0 (which disables service flow logging).</li> <li><i>time</i>—Specifies how long, in seconds, entries can remain in the service flow log. The CMTS deletes entries in the log that are older than this value, so this should specify a long enough time period for at least one billing cycle. The valid range is 1 to 86400 seconds, with a default value of 3600 seconds (1 hour).</li> </ul>
Step 6	<pre>cable metering source-interface interface</pre> <p><b>Example:</b></p> <pre>Router(config)# cable metering source-interface loopback100 Router(config)#</pre>	(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.
Step 7	<pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end Router#</pre>	Exits global configuration mode and returns to privileged EXEC mode.

## Enabling Usage-Based Billing Feature (Streaming Mode)—Using SNMP Commands

This section describes how to use SNMP commands to enable and configure the Usage-Based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

### SUMMARY STEPS

To configure the Cisco CMTS for Usage-Based Billing feature in streaming mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB. [Table 3](#) describes each of these objects, and whether they are required or optional.

**Note**

In addition, to include information about deleted service flows (DOCSIS 1.1 service flows only) in the billing records, you must enable the logging of deleted service flows, using the **cable sflog** global configuration command. Refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

**Table 3** *SNMP Objects to be Configured for Streaming Mode*

Object	Type	Description
ccmCollectionType	Integer	Enables or disables the Usage-Based Billing feature. The valid values are: <ul style="list-style-type: none"> <li>• 1 = none. The Usage-Based Billing feature is disabled (default).</li> <li>• 2 = local. The Usage-Based Billing feature is enabled and configured for file mode.</li> <li>• 3 = stream. The Usage-Based Billing feature is enabled and configured for streaming mode.</li> </ul> Set ccmCollectionType to 3 (stream) to enable the feature for streaming mode.
ccmCollectionIpAddress	InetAddress	IP address for the external collection server. This value must be specified.
ccmCollectionPort	Unsigned32	TCP port number at the external collection server to which the billing records should be sent. The valid range is 0 to 65535, but you should not specify a port in the well-known range of 0 to 1024. This value must be specified.
<p><b>Note</b> You can configure the ccmCollectionIpAddress and ccmCollectionPort objects twice, to specify a primary collection server and a secondary collection server.</p>		
ccmCollectionIpAddrType	InetAddressType	(Optional) Type of IP address being used for the collection server. The only valid value is ipv4, which is the default value.
ccmCollectionInterval	Unsigned32	(Optional) Specifies how often, in minutes, the billing records are streamed to the external server. The valid range is 15 to 1440 minutes (24 hours), with a default of 30 minutes. (Cisco recommends a minimum interval of 30 minutes.)
ccmCollectionRetries	Unsigned32	(Optional) Specifies the number of retry attempts that the CMTS will make to establish a secure connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range for <i>n</i> is 0 to 5, with a default of 0.

**Note** The ccmCollectionInterval and ccmCollectionRetries parameters are optional when configuring Usage-Based Billing for streaming mode with SNMP commands, but these parameters are required when configuring the feature with CLI commands.

**Table 3** SNMP Objects to be Configured for Streaming Mode (continued)

Object	Type	Description
ccmCollectionSecure	TruthValue	<p>(Optional) Specifies whether the Cisco CMTS should use a secure socket layer (SSL) connection when connecting with the billing application on the external server. The valid values are:</p> <ul style="list-style-type: none"> <li>• true(1) = The Cisco CMTS uses a SSL connection. This option is available only on CMTS software images that support Baseline Privacy Interface (BPI) encryption.</li> <li>• false(2) = The Cisco CMTS uses an unencrypted TCP connection. This is the default value.</li> </ul>
ccmCollectionCpeList	TruthValue	<p>(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following:</p> <ul style="list-style-type: none"> <li>• true = CPE information is present (default).</li> <li>• false = CPE information is omitted.</li> </ul> <p><b>Note</b> When set to true, a maximum of 5 CPE IP addresses for each cable modem.</p>
ccmCollectionAggregate	TruthValue	<p>(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows:</p> <ul style="list-style-type: none"> <li>• true = All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank.</li> <li>• false = Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).</li> </ul>
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

**DETAILED STEPS****Note**

The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

**Step 1** Set the `ccmCollectionType` object to 3, to enable the Usage-Based Billing feature and to configure it for streaming mode:

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionType.0 -i 3
workstation#
```

**Step 2** Set the `ccmCollectionIpAddress` and `ccmCollectionPort` objects to the IP address of the external collection server and the TCP port number to which billing records should be sent:

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionIpAddress.1 -o '0a 08
06 0b'
workstation# setany -v2c ip-address rw-community-string ccmCollectionPort.1 -g 6789
workstation#
```

- Step 3** (Optional) Set the `ccmCollectionIpAddress` and `ccmCollectionPort` objects a second time to specify the IP address and TCP port number of a second external collection server to which billing records should be sent, in the case that the Cisco CMTS cannot connect to the primary collection server:

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionIpAddress.1 -o '0a 08
06 0c'
workstation# setany -v2c ip-address rw-community-string ccmCollectionPort.1 -g 7000
workstation#
```

- Step 4** (Optional) To change any of the other default parameters, set the appropriate objects to the desired values. For example, the following lines configure the Usage-Based Billing feature for a non-secure connection, with a collection interval of 45 minutes, and a maximum number of 3 retries.

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c ip-address rw-community-string ccmCollectionInterval.1 -i 45
workstation# setany -v2c ip-address rw-community-string ccmCollectionRetries.1 -i 3
workstation#
```

- Step 5** (Optional) To omit the IP addresses of CPE devices from the billing records, set the `ccmCollectionCpeList` object to 2 (false). The default is to include the CPE information.

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionCpeList.0 -i 2
workstation#
```

- Step 6** (Optional) To aggregate all service flow information for each cable modem in a single record, set the `ccmCollectionAggregate` object to 1 (true). The default is for each service flow to be written in a separate record:

```
workstation# setany -v2c ip-address rw-community-string ccmCollectionAggregate.0 -i 1
workstation#
```

- Step 7** (Optional) To specify the source-interface for the billing packets, set the `ccmtrCollectionSrcIfIndex` object to 1 (true). The default is for the billing packets to automatically select a source-interface.

```
workstation# setany -v2c ip-address rw-community-string ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

## Examples

The following example shows the Usage-Based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-Based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB
ccmCollectionType.0 = none(1)
ccmCollectionFilesystem.0 =
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00 00 00 00 00 00 00
ccmCollectionNotifEnable.0 = true(1)

workstation#
```

The following SNMP commands are then given to enable the Usage-Based Billing feature and to configure it for streaming mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionType.0 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionIpAddress.1 -o '0a 08 06 0b'
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionPort.1 -g 6789
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionRetries.1 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionInterval.1 -i 45
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering destination 10.8.6.11 6789 3 45 non-secure

Router#
```

The following SNMP display shows the new configuration:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = stream(3)
ccmCollectionFilesystem.0 =
ccmCollectionIpAddrType.1 = ipv4(1)
ccmCollectionIpAddress.1 = 0a 08 06 0b
ccmCollectionPort.1 = 6789
ccmCollectionInterval.1 = 45
ccmCollectionRetries.1 = 3
ccmCollectionSecure.1 = false(2)
ccmCollectionRowStatus.1 = active(1)
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00 00 00 00 00 00 00
ccmCollectionNotifEnable.0 = true(1)

workstation#
```

## Enabling and Configuring Secure Copy (optional)

This section describes how to configure the CMTS for the Secure Copy Protocol (SCP), to allow an external server to log into the CMTS and copy the billing records from the Cisco CMTS to the external server.



### Note

For instructions on the actual procedure to be used when downloading the billing files from the Cisco CMTS router, see the [“Retrieving Records from a Cisco CMTS in File Mode”](#) section on page 25.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2...]**

5. **aaa authorization** {network | exec | commands *level* | reverse-access} {default | *list-name*} *method1* [*method2* ...]
6. **username** *name* **privilege** *level* **password** *encryption-type* *encrypted-password*
7. **ip ssh time-out** *seconds*
8. **ip ssh authentication-retries** *n*
9. **ip scp server enable**
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router(config)# aaa new-model Router(config)#	Enables the Authentication, Authorization, and Accounting (AAA) access control model.
Step 4	<b>aaa authentication login</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ...]  <b>Example:</b> Router(config)# aaa authentication login default enable Router(config)#	Enables AAA access control authentication at login, using the following parameters: <ul style="list-style-type: none"> <li>• <b>default</b> = Uses the authentication methods that are listed with this command as the default methods for when a user logs in.</li> <li>• <i>list-name</i> = Specifies the name for a list of authentication methods to be used when a user logs in.</li> <li>• <i>method1</i> [<i>method2</i> ...] = Specifies the type of login authentication that should be used when a user logs in. At least one method must be specified, but you can also specify multiple methods, if desired.</li> </ul> Valid methods include <b>enable</b> , <b>line</b> , and <b>local</b> .  <b>Note</b> This command includes additional options. For details, see the documentation listed in <a href="#">Additional References, page 38</a> .

Command or Action	Purpose
<p><b>Step 5</b></p> <pre>aaa authorization exec {default   list-name} method1 [method2 ...]</pre> <p><b>Example:</b></p> <pre>Router(config)# aaa authorization exec default local Router(config)#</pre>	<p>Configures the CMTS to allow users to run an EXEC shell and access the CLI to run the Secure Copy commands.</p> <ul style="list-style-type: none"> <li>• <b>default</b> = Uses the authorization methods that are listed with this command as the default methods for when a user logs in.</li> <li>• <b>list-name</b> = Specifies the name for a list of authorization methods be used when a user logs in.</li> <li>• <b>method1 [method2 ...]</b> = Specifies the type of login authorization that should be used when a user logs in. At least one method must be specified, but you can also specify multiple methods, if desired.</li> </ul> <p>Valid methods include <b>local</b>.</p> <p><b>Note</b> This command includes additional options. For details, see the documentation listed in <a href="#">Additional References</a>, page 38.</p>
<p><b>Step 6</b></p> <pre>username name privilege level password encryption-type password</pre> <p><b>Example:</b></p> <pre>Router(config)# username billingapp privilege 15 password 7 billing-password Router(config)#</pre>	<p>(Optional) Creates a user account for login access and specifies the privilege level and password for that account:</p> <ul style="list-style-type: none"> <li>• <b>name</b> = User name to be used for logging in.</li> <li>• <b>level</b> = Privilege level (0 to 15) of access allowed for this user.</li> <li>• <b>encryption-type</b> = Type of encryption to be used on the password when writing it to the router's configuration file: 0 is unencrypted and 7 is encrypted.</li> <li>• <b>password</b> = Password the user should enter for access.</li> </ul> <p><b>Note</b> This step is optional but for the purposes of security and management, Cisco recommends creating a unique account for the billing application to use when logging into the CMTS.</p>
<p><b>Step 7</b></p> <pre>ip ssh time-out seconds</pre> <p><b>Example:</b></p> <pre>Router(config)# ip ssh time-out 120 Router(config)#</pre>	<p>Enables Secure Shell (SSH) access on the Cisco CMTS, which is required for SCP use. The <i>seconds</i> parameter specifies the maximum time allowed for SSH authentication, in seconds, with a valid range of 0 to 120 seconds, with a default of 120 seconds.</p>
<p><b>Step 8</b></p> <pre>ip ssh authentication-retries n</pre> <p><b>Example:</b></p> <pre>Router(config)# ip ssh authentication-retries 3 Router(config)#</pre>	<p>Specifies the maximum number of login attempts a user is allowed before the router disconnects the SSH session. The valid range is 1 to 5, with a default of 3 attempts.</p>

	Command or Action	Purpose
Step 9	<code>ip scp server enable</code>  <b>Example:</b> Router(config)# ip scp server enable Router(config)#	Enables SCP access on the Cisco CMTS.
Step 10	<code>end</code>  <b>Example:</b> Router(config)# end Router#	Exits global configuration mode and returns to privileged EXEC mode.

## Configuring the Cisco CMTS for SSL Operation

This section describes the procedures to configure the Cisco CMTS for secure socket layer (SSL) operation, so that the Usage-Based Billing feature can use an SSL connection to transfer the billing record files in streaming mode.



### Note

This procedure is required only when using the **secure** option with the **cable metering destination** command.

## Prerequisites

- The billing application server must be configured for SSL operations.
- A Certificate Authority (CA) must be configured to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

## SUMMARY STEPS

To prepare the Cisco CMTS router for SSL operation, you must perform the following configuration steps:

- Configuring the router's host name and IP domain name, if not already done.
- Generating an RSA key pair.
- Declaring a Certification Authority.
- Configuring a Root CA (Trusted Root).
- Authenticating the CA.
- Requesting the Certificates.

For the detailed steps in performing these procedures, see the *Configuring Certification Authority Interoperability* chapter in the *IP Security and Encryption* section of the *Cisco IOS Security Configuration Guide*, Release 12.2, at the following URL:

[http://www.cisco.com/en/US/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c.html](http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html)

## Retrieving Records from a Cisco CMTS in File Mode

When the Usage-Based Billing feature is enabled and configured for File mode, the billing application server must regularly retrieve the billing records from the Cisco CMTS. This is typically done by a script that either logs in to the Cisco CMTS and uses CLI commands to transfer the file, or by a script that uses SNMP commands to transfer the file.

When using CLI commands, the procedure is typically as follows:

1. The billing application server receives an SNMP trap from the Cisco CMTS when a billing record is written. This notification contains the file name of the billing record that should be retrieved.
2. The billing application server starts a custom-written script to retrieve the billing record. This script would do one of the following:
  - a. If using CLI commands, the script logs in to the Cisco CMTS using a telnet connection, and then transfers the billing record to the billing application server, using the **copy** CLI command. The transfer can be done using either the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP).

**Note**

You could also use the File Transfer Protocol (FTP) to transfer files from the Cisco CMTS to an external FTP server, but this is not recommended, because the FTP protocol transmits the login username and password in cleartext.

- b. If using SNMP commands, the script sets the `ciscoFlashCopyEntry` objects in the `CISCO-FLASH-MIB` to transfer the billing record to the application server, using TFTP.
3. After transferring the billing record, the script deletes it on the Cisco CMTS file system, so that the Cisco CMTS can begin writing a new billing record.

The following sections show examples of how this can be done, using each method.

**Tip**

The following examples are given for illustration only. Typically, these commands would be incorporated in automated scripts that would retrieve the billing records.

## Using SCP

To transfer billing records using SCP, you must first enable and configure the router for SCP operation, using the procedure given in the “[Enabling and Configuring Secure Copy \(optional\)](#)” section on page 21. Then, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the SCP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an FTP server with the hostname of billserver.mso-example.com:

```
CMTS01# copy slot0:CMTS01_20030211-155025 scp://billingapp-server.mso-example.com/
Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
Password: billing-password

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 1403352/1024 bytes]

1403352 bytes copied in 17.204 secs (85631 bytes/sec)

CMTS01# delete slot0:CMTS01_20030211-155025
CMTS01# squeeze slot0:
CMTS01#
```



### Note

The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

## Using TFTP

To transfer billing records using TFTP, you must first configure an external workstation to be a TFTP server. For security, the TFTP server should be isolated from the Internet or any external networks, so that only authorized TFTP clients, such as the Cisco CMTS router, can access the server.

To transfer the billing records, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the TFTP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an TFTP server with the hostname of billserver.mso-example.com.

```
CMTS01# copy slot0:CMTS01_20030211-155025
tftp://billingapp-server.mso-example.com/incoming

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1102348/1024 bytes]

1102348 bytes copied in 14.716 secs (63631 bytes/sec)

CMTS01# delete slot0:CMTS01_20030211-155025
CMTS01# squeeze slot0:
CMTS01#

```

**Note**

The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

## Using SNMP

To transfer billing record file using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB to transfer the file to a TFTP server. After the file has been successfully transferred, you can then use SNMP commands to delete the billing record file.

**Note**

Before proceeding with these steps, ensure that the TFTP server is properly configured to receive to receive the billing records. At the very least, this means creating a directory that is readable and writable by all users. On some servers, the TFTP server software also requires that you create a file with the same name as the file that is to be received, and this file should also be readable and writable by all users.

## SUMMARY STEPS

To transfer a billing record file to a TFTP server, using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB. [Table 4](#) describes each of these objects, and whether they are required or optional.

**Table 4** Transferring a File to a TFTP Server Using SNMP Commands

Object	Type	Description
ciscoFlashCopyEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashCopyCommand	INTEGER	Type of copy command to be performed. To copy a billing record file to a TFTP server, set this object to 3 (copyFromFlash).

**Table 4** Transferring a File to a TFTP Server Using SNMP Commands (continued)

Object	Type	Description
ciscoFlashCopyServerAddress	IpAddress	IP address of the TFTP server.  <b>Note</b> This parameter defaults to the broadcast address of 255.255.255.255, which means it will transfer the billing record file to the first TFTP server that responds. For security, this object should always be set to the IP address of the authorized TFTP server.
ciscoFlashCopySourceName	DisplayString	Name of the billing record file to be transferred, including the Flash device on which it is stored.
ciscoFlashCopyDestinationName	DisplayString	(Optional) Name for the billing record, including path, on the TFTP server. If not specified, the copy operation defaults to saving the billing record at the top-most directory on the TFTP server, using the original file name.  <b>Note</b> A file with the destination file name should already exist on the TFTP server. This file should be readable and writable by all users, so that it can be replaced with the billing record file.
ciscoFlashCopyProtocol	INTEGER	(Optional) Specifies the protocol to be used when copying the file. For a TFTP transfer, set this object to 1 (tftp), which is the default.
ciscoFlashCopyNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the copy operation. The default is false (no trap is generated).

After transferring the billing records file, you must then set a number of objects in the CISCO-FLASH-MIB to delete the file, so that the Cisco CMTS can begin writing a new file. If the Flash memory is not ATA-compatible, you must also set a number of objects to squeeze the Flash memory, so as to make the deleted space available for new files. [Table 5](#) describes each of these objects, and whether they are required or optional.

**Table 5** Deleting a File Using SNMP Commands

Object	Type	Description
ciscoFlashMiscOpCommand	INTEGER	Specifies the operation to be performed: <ul style="list-style-type: none"> <li>• 3 = Delete the file.</li> <li>• 5 = Squeeze the Flash memory, so as to recover the deleted space and make it available for new files.</li> </ul>
ciscoFlashMiscOpDestinationName	DisplayString	When deleting a file, the name of the file to be deleted, including the name of the file system, up to a maximum of 255 characters.  When squeezing a file system, the name of the file system to be squeezed (slot0:, slot1:, flash:, or bootflash:).

**Table 5** Deleting a File Using SNMP Commands (continued)

Object	Type	Description
ciscoFlashMiscOpEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashMiscOpNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the operation. The default is false (no trap is generated).

**DETAILED STEPS****Note**

The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

**Copying the Billing Record File to the TFTP Server**

- Step 1** The script performing the copy should generate a 32-bit number to be used as the index entry for this copy command. The script can generate this number in any convenient way, so long as the index number is not currently being used for another operation.
- Step 2** Create the table entry for the copy command, by using the number that was generated in [Step 1](#) and setting the ciscoFlashCopyEntryStatus object to the create-and-wait state (5):
- ```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 5
workstation#
```
- Step 3** Set the ciscoFlashCopyCommand to 3 (copyFromFlash) to specify that the billing record file should be copied from the router's Flash file system:
- ```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyCommand.582
-i 3
workstation#
```
- Step 4** Set the ciscoFlashCopyServerAddress object to the IP address of the TFTP server:
- ```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyServerAddress.582
-a "172.20.12.193"
workstation#
```
- Step 5** Set the ciscoFlashCopySourceName object to the file name, including the device name, of the billing record file to be transferred:
- ```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopySourceName.582
-D "slot0:CMTS01_20030211-155025"
workstation#
```
- Step 6** (Optional) To specify a specific destination on the TFTP server, set the ciscoFlashCopyDestinationName object to the path name and file name for the billing record file on the TFTP server. (Typically, the path name and file name should already exist on the TFTP server.)
- ```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyDestinationName.582
-D "/cmts01-billing/billing-file"
workstation#
```

**Step 7** To execute the command, set the `ciscoFlashCopyEntryStatus` object to the active state (1):

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 1
workstation#
```

**Step 8** Periodically poll the `ciscoFlashCopyStatus` object until the file transfer completes:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus.582
ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus.582
ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus.582
ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation#
```

If the file transfer fails, the most common status values that are reported by the `ciscoFlashCopyStatus` object are:

- 3 = `copyInvalidOperation`. This indicates that the operation failed on the TFTP server, typically because the destination file name and path name do not exist on the TFTP server, or they exist but are not writable by all users.
- 5 = `copyInvalidSourceName`. The file name for the billing record, as specified in `ciscoFlashCopySourceName` does not exist. Verify that you specified the correct device name and that no spaces exist in the file name.
- 6 = `copyInvalidDestName`. The destination path name and file name specified in `ciscoFlashCopyDestinationName` is not accessible on the TFTP server. This could be because the path name does not exist or is not configured to allow write-access. This error could also occur if a file with the same path name and file name already exists on the TFTP server.
- 7 = `copyInvalidServerAddress`. The IP address of the TFTP server specified in `ciscoFlashCopyServerAddress` is invalid, or the TFTP server is not responding.
- 14 = `copyFileTransferError`. A network error occurred that prevented the file transfer from completing.

**Step 9** After the file transfer has completed successfully, set the `ciscoFlashCopyEntryStatus` object to 6 (delete) to delete the row entry for this copy command:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 6
workstation#
```

---

### Deleting the Billing Record File

After the billing record file has been successfully transferred, use the following procedure to delete the billing record on the Cisco CMTS flash file system, so that the Cisco CMTS can write the new billing record.

**Step 1** Generate another random number to be used as an index entry and configure the following objects in the `ciscoFlashMiscOpTable`:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus.31 -i
5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand.31 -i 3
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName.31
-D "/cmts01-billing/CMTS01_20030211-155025"
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus.31 -i
1
workstation#
```

**Step 2** Periodically poll the `ciscoFlashMiscOpStatus` object until the file transfer completes:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus.31
ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus.31
ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation#
```

**Step 3** If the Flash memory system is not ATA-compatible (slot0:, slot1:, flash:, or bootflash:), configure the following objects in the `ciscoFlashMiscOpTable` to squeeze the Flash file system to recover the deleted file space:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus.32
-i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand.32 -i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName.32
-D slot0:
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus.32
-i 1
workstation#
```

## Examples

The following SNMP commands transfer a file named `CMTS01_20030211-155025` to a TFTP server at the IP address `10.10.31.3`. After the file is successfully transferred, the row entry for this copy command is deleted.

```
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyEntryStatus.582 -i 5
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyCommand.582 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyServerAddress.582 -a
"10.10.31.3"
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopySourceName.582 -D
"slot0:CMTS01_20030211-155025"
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyDestinationName.582 -D
"/cmts01-billing/CMTS01_20030211-155025"
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyEntryStatus.582 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string ciscoFlashCopyStatus.582
ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string ciscoFlashCopyStatus.582
ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashCopyEntryStatus.582 -i 6
workstation#
```

The following commands show a billing record file being deleted on the Cisco CMTS file system, and the deleted file space being recovered by a squeeze operation:

```
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpEntryStatus.31 -i 5
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpCommand.31 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpDestinationName.31 -D
"/cmts01-billing/CMTS01_20030211-155025"
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpEntryStatus.31 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpStatus.31
ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpStatus.31
ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)

workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpEntryStatus.32 -i 5
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpCommand.32 -i 5
```

```
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpDestinationName.32 -D slot0:
workstation# setany -v2c 10.8.8.21 rw-string ciscoFlashMiscOpEntryStatus.32 -i 1
workstation#
```

## Disabling the Usage-Based Billing Feature

This section describes how to disable the Usage-Based Billing. Giving this command immediately stops the collection of billing information. If a billing record is currently written or being streamed to an external server, the CMTS completes the operation before disabling the usage-based billing feature.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cable metering**
4. **no snmp-server enable traps cable metering**
5. **no cable sflog**
6. **no cable metering source-interface**
7. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                            | Purpose                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                                                                            | Enables privileged EXEC mode. Enter your password if prompted.                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)#                                                            | Enters global configuration mode.                                                                     |
| Step 3 | <b>no cable metering</b><br><br><b>Example:</b><br>Router(config)# no cable metering<br>Router(config)#                                                      | Immediately disables the Usage-Based Billing feature and stops the collection of billing information. |
| Step 4 | <b>no snmp-server enable traps cable metering</b><br><br><b>Example:</b><br>Router(config)# no snmp-server enable traps<br>cable metering<br>Router(config)# | (Optional) Disables SNMP traps for usage-based billing events.                                        |

|        | Command or Action                                                                                                                            | Purpose                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Step 5 | <b>no cable sflog</b><br><br><b>Example:</b><br>Router(config)# no cable sflog<br>Router(config)#                                            | (Optional) Disables the logging of deleted service flows.                 |
| Step 6 | <b>no cable metering source-interface</b><br><br><b>Example:</b><br>Router(config)# no cable metering<br>source-interface<br>Router(config)# | (Optional) Disables a specified source-interface for the billing packets. |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                                        | Exits global configuration mode.                                          |

## Configuring Certified SSL Servers for Usage-Based Billing

Cisco IOS Release 12.3(17a)BC introduces support for the Secure Socket Layer (SSL) Server, used with the Usage-Based Billing feature of the Cisco CMTS. Usage-Based Billing implements the DOCSIS Subscriber Account Management Interface Specification (SAMIS) format.

This new capability enables the configuration of the SSL server between the Cisco CMTS and a collection server. Certificate creation steps and **debug** commands are added or enhanced to support the SSL Server and certificates. This section describes general steps.

Refer also to the [“Configuring the Cisco CMTS for SSL Operation”](#) section on page 24.

### Generating SSL Server Certification

These general steps describe the creation and implementation of certification for the Secure Socket Layer (SSL) Server.

1. Generate the CA key.
2. Set up the open SSL environment, to include directory and sub-directory.
3. Copy files to the appropriate directories.
4. Generate the SSL Server certification request.
5. Grant the SSL Server certification request.
6. Convert the SSL Server certification to DER format.
7. Copy the SSL certification to Bootflash memory (**write mem**).
8. Start the SSL server.

## Configuring and Testing the Cisco CMTS for Certified SSL Server Support

Perform the following steps to configure the Cisco router to support the SSL Server and certification.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain name** *domain*
4. **crypto key generate rsa**
5. **Ctrl-Z**
6. **test cable read certificate**
7. **show crypto ca certificate**
8. **configure terminal**
9. **cable metering destination** *ip-addr num-1 num-2 num-3 secure*
10. **test cable metering**

### DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# config t                                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>ip domain name</b> <i>domain</i><br><br><b>Example:</b><br>Router(config)# ip domain name Cisco.com | Defines a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. <ul style="list-style-type: none"> <li>• <i>domain</i>—Valid alphanumeric domain name</li> </ul> <b>Note</b> Refer to the <a href="#">Domain Name System (DNS)</a> document on Cisco.com for additional DNS information. |
| Step 4 | <b>crypto key generate rsa</b><br><br><b>Example:</b><br>Router(config)# crypto key generate rsa       | Generates RSA key pairs. <b>Note</b> Refer to the <a href="#">Multiple RSA Key Pair Support</a> document on Cisco.com for additional RSA key information.                                                                                                                                                                                                                                                                                                           |
| Step 5 | Ctrl-Z<br><br><b>Example:</b><br>Router(config)# Ctrl-Z<br>Router#                                     | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|         | Command or Action                                                                                                                                                | Purpose                                                                                 |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Step 6  | <b>test cable read certificate</b><br><br><b>Example:</b><br>Router# test cable read certificate                                                                 | Verifies the certificate is valid and operational on the Cisco CMTS.                    |
| Step 7  | <b>show crypto ca certificate</b><br><br><b>Example:</b><br>Router# sh crypto ca certificate                                                                     | Displays the available certificates on the Cisco CMTS.                                  |
| Step 8  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# config t<br>Router(config)#                                                                          | Enters global configuration mode.                                                       |
| Step 9  | <b>cable metering destination ip-addr num-1 num-2 num-3 secure</b><br><br><b>Example:</b><br>Router(config)# cable metering destination 1.7.7.7 6789 0 15 secure | Defines the destination IP address for cable metering, to be used with the certificate. |
| Step 10 | <b>test cable metering</b><br><br><b>Example:</b><br>Router# test cable metering                                                                                 | Tests cable metering in light of the supported SSL server and metering configuration.   |

## Monitoring the Usage-Based Billing Feature

To display the most current billing record, use the **show cable metering-status** command. The following example shows typical output when usage-based billing is configured to write the billing records to a local file system:

```
CMTS01# show cable metering-status

destination                               complete-time  flow  cpe  status
   aggr suppress
disk0:R7519-UBR7246-20000308-004428 Jun 12 09:33:05 No   No   success

CMTS01#
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to stream the billing records to an external server:

```
Router# show cable metering-status

destination                               complete-time  flow  cpe  status
   aggr supp
10.11.37.2 :1234                          Jun 12 09:33:05 No   No   success

Router#
```

The following example shows a typical output for the **show cable metering-status** command using **verbose** option:

```
Router# show cable metering-status verbose
Last export status
Destination : disk0:sunethra10k-20070129-190423
Complete Time : Jan29 19:04:38
Flow Aggregate : No
Cpe list suppression : No
Source interface : FastEthernet0/0/0
Status of last export : success
Current export status : In progress
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to use the Internet Protocol Detail Record (IPDR) Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
destination                complete-time    flow cpe  status
                        aggr supp
IPDR_Session1              Jun 12 09:33:05  N/A N/A  success
```

The following example shows a typical output for for the verbose form of the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status verbose
Last export status
Destination      : IPDR_Session1
Complete Time    : Jun 12 09:36:05
Status of last export : success
```



#### Note

If the **show cable metering-status** command displays the status of a streaming operation as “success” but the records were not received on the billing application server, verify that the Cisco CMTS and server are configured for the same type of communications (non-secure TCP or secure SSL). If the Cisco CMTS is configured for non-secure TCP and the server is configured for secure SSL, the Cisco CMTS transmits the billing record successfully, but the server discards all of the data, because it did not arrive in a secure SSL stream.



#### Tip

The **show cable metering-status** command continues to show the status of the last billing record operation, until that billing record is deleted. If the record is not deleted, no new records are created.

To display information about the state of the IPDR Exporter, use the **show ipdr exporter** command. The following example shows typical output:

```
Router#configure terminal
Router#show ipdr exporter
IPDR exporter is started.
```

## Configuration Examples for Usage-Based Billing

This section lists the following sample configurations for the Usage-Based Billing feature:

- [File Mode Configuration \(with Secure Copy\), page 36](#)

- [Non-Secure Streaming Mode Configuration, page 37](#)
- [Secure Streaming Mode Configuration, page 37](#)

## File Mode Configuration (with Secure Copy)

The following excerpt from a configuration file shows a typical configuration for the Usage-Based Billing feature when operating in file mode and enabling Secure Copy (SCP) for file transfers.

```
!
cable metering filesystem disk1:
snmp-server enable traps cable metering

...

aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
username billingapp level 15 password 7 billing-password
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

## Non-Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-Based Billing feature when operating in streaming mode and specifying both a primary and a secondary external server. The data is sent using standard TCP packets, without any security.

```
cable metering destination 10.10.10.171 5321 10.10.10.173 5321 2 30 non-secure
snmp-server enable traps cable metering
```

The following excerpt from a configuration file shows a typical configuration for the Usage-Based Billing feature when operating in streaming mode and specifying only a primary external server:

```
cable metering destination 10.10.11.181 6789 2 30 non-secure
snmp-server enable traps cable metering
```



### Note

You must ensure that the billing application server is configured for standard TCP communications. If the billing application server is configured for SSL communications when the Cisco CMTS is configured for standard TCP, the Cisco CMTS is able to send the billing records to the server, but the server discards all of that information because it is not arriving in a secure stream.

## Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-Based Billing feature when operating in streaming mode and specifying only a primary external server. Secure socket layer (SSL) TCP connections are used to transmit the data, which requires the configuration of a digital certificate.

```
cable metering destination 10.10.11.181 6789 2 30 secure cpe-list-suppress
snmp-server enable traps cable metering
```

...

```

crypto ca trustpoint SSL-CERT
!
crypto ca certificate chain SSL-CERT
certificate ca 00
 308204A6 3082038E A0030201 02020100 300D0609 2A864886 F70D0101 04050030
 8198310B 30090603 55040613 02555331 13301106 03550408 130A4361 6C69666F
 726E6961 3111300F 06035504 07130853 616E204A 6F736531 1C301A06 0355040A
 13134369 73636F20 53797374 656D732C 20496E63 2E311130 0F060355 040B1308
 4361626C 65204255 310E300C 06035504 03130553 65656D61 3120301E 06092A86
...
 3E65DBBA 337627E8 589980D6 C8836C7E 3D3C3BC1 F21973BF 7B287D7A 13B16DA2
 02B2B180 C2A125C7 368BDA4C 0B8C81B7 7D5BEFF9 A6618140 1E95D19E BD0A84F5
 B43702AB 39B5E632 87BA36AC A3A8A827 C5BAC0F1 B24B8F4D 55615C49 5B6E4B61
 B15CC48A 8EF566C8 6E449B49 BF8E9165 317C1734 9A48A240 78A356B5 403E9E9B
 88A51F5B 0FE38CC2 F431
quit
!

```

**Note**

You must ensure that the billing applications server is also configured for SSL communications.

## Additional References

For additional information related to Usage-Based Billing, refer to the following references:

## Related Documents

| Related Topic                            | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CMTS Command Reference                   | <p><i>Cisco IOS CMTS Cable Command Reference Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html">http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html</a></p>                                                                                                                                                                                                                                                                                                  |
| Cisco IOS Release 12.2 Command Reference | <p>Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL:</p> <p><a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html</a></p> <p><a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a></p>  |
| Secure Copy (SCP) Configuration          | <p><i>Secure Copy</i> feature module, at the following URL:</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html">http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html</a></p> <p>Cisco IOS Release 12.2 T Command Reference, <i>Other Security Features, Secure Shell Commands</i>, at the following URL:</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_2t/secure/command/reference/sftssh.html">http://www.cisco.com/en/US/docs/ios/12_2t/secure/command/reference/sftssh.html</a></p> |

| Related Topic                         | Document Title                                                                                                                                                                                                                               |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Sockets Layer (SSL)            | Introduction to Secure Sockets Layer white paper, at the following URL:<br><br><a href="http://www.cisco.com/en/US/tech/tk583/tk618/tech_white_papers_list.html">http://www.cisco.com/en/US/tech/tk583/tk618/tech_white_papers_list.html</a> |
| Information about IPDR                | IPDR.org web site, at the following URL:<br><br><a href="http://www.ipdr.org">http://www.ipdr.org</a>                                                                                                                                        |
| IPDR.org Software Reference Libraries | IPDR.org project page, at the following URL:<br><br><a href="http://sourceforge.net/projects/ipdr/index.html">http://sourceforge.net/projects/ipdr/index.html</a>                                                                            |

## Standards

| Standards <sup>1</sup>                 | Title                                                                                                                                                                                      |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDM-U v3.1.1                           | Network Data Management – Usage (NDM-U) For IP-Based Services, Version 3.1.1 ( <a href="http://www.ipdr.org">http://www.ipdr.org</a> )                                                     |
| <a href="#">SP-RFIV1.1-I09-020830</a>  | Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 ( <a href="http://www.cablemodem.com">http://www.cablemodem.com</a> )                |
| <a href="#">SP-OSSIV2.0-I09-050812</a> | Data-Over-Cable Service Interface Specifications DOCSIS 2.0 Operations Support System Interface (OSSI) Specification ( <a href="http://www.cablemodem.com">http://www.cablemodem.com</a> ) |
| XML Schema                             | Extensible Markup Language (XML) schema ( <a href="http://www.w3.org">http://www.w3.org</a> )                                                                                              |

1. Not all supported standards are listed.

## MIBs

| MIBs <sup>1</sup>                        | MIBs Link                                                                                                                                                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CISCO-CABLE-METERING-MIB</a> | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

1. Not all supported MIBs are listed.

## RFCs

| RFCs <sup>1</sup> | Title                               |
|-------------------|-------------------------------------|
| RFC 2233          | DOCSIS OSSI Objects Support         |
| RFC 2665          | DOCSIS Ethernet MIB Objects Support |
| RFC 2669          | Cable Device MIB                    |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# Command Reference

For information about commands, see the *Cisco IOS CMTS Command Reference* at [http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

