



## Cable Commands: cable a through cable c

---

Revised: November 13, 2009, OL-15510-10

### New Commands

Command	Cisco IOS Software Release
<code>cable clock dti</code>	12.3(23)BC
<code>cable clock dti clear-counters</code>	12.3(23)BC
<code>cable attribute-mask</code>	12.2(33)SCB
<code>cable cm-status enable</code>	12.2(33)SCB
<code>cable admission-control max-reserved-bandwidth</code>	12.2(33)SCC
<code>cable clock upgrade</code>	12.2(33)SCC

### Modified Commands

Command	Cisco IOS Software Release
<code>cable application-type include</code>	12.2(33)SCA
<code>cable clock clear-counters</code>	12.3(23)BC
<code>cable admission-control ds-bandwidth</code>	12.2(33)SCC
<code>cable admission-control us-bandwidth</code>	12.2(33)SCC

# cable admission-control

To configure the CPU and memory thresholds for a Cisco CMTS router supporting broadband processing engines (BPEs), use the **cable admission-control** command in global configuration mode. This command sets the CPU averaging method and memory thresholds. To remove thresholds from a Cisco CMTS router, use the **no** form of this command.

```
cable admission-control { cpu-5sec | cpu-avg } {[ io-mem] [proc-mem] [total-memory] } minor
  num1 major num2 critical num3
```

```
no cable admission control { cpu-5sec | cpu-avg } {[ io-mem] [proc-mem] [total-memory] }
  minor num1 major num2 critical num3
```

Syntax Description	
<b>cpu-5sec</b>	This keyword sets Admission Control thresholds on the Cisco CMTS based on a five-second average for the CPU. This setting must be combined with the additional <b>minor</b> , <b>major</b> and <b>critical</b> threshold percentage values.
<b>cpu-avg</b>	This keyword sets Admission Control thresholds on the Cisco CMTS based on a one-minute average for the CPU. This setting must be combined with the additional <b>minor</b> , <b>major</b> and <b>critical</b> threshold percentage values.
<b>io-mem</b>	This keyword sets Admission Control thresholds for input/output (IO) memory on the Cisco CMTS route processors and BPE processors.
<b>proc-mem</b>	This keyword sets Admission Control thresholds according to CPU processor memory on the Cisco CMTS.
<b>total-memory</b>	This keyword sets Admission Control thresholds on the Cisco CMTS according to total-memory allocation.
<b>minor</b> <i>num1</i>	Keyword sets the minor threshold level for the CPU or memory resource to be configured. <i>Num1</i> expresses a percentage and must be an integer between 1 and 100.
<b>major</b> <i>num2</i>	Keyword sets the major threshold level for the CPU or memory resource to be configured. <i>Num2</i> expresses a percentage and must be an integer between 1 and 100.
<b>critical</b> <i>num3</i>	Keyword sets the critical threshold level for the CPU or memory resource to be configured. <i>Num3</i> expresses a percentage and must be an integer between 1 and 100.

**Command Default** By default, admission control is disabled with no CPU or memory resource threshold settings on the Cisco CMTS router.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.3(13a)BC	This command was introduced on the Cisco uBR10012 router and the Cisco uBR7246VXR router, with supporting broadband processing engines (BPEs) or cable interface line cards on the respective routers.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

**Usage Guidelines**

The threshold counters are set to zero when the resource is reconfigured.

An important concept for system resources that are set with this command (CPU and memory) is the concept of *dampening*. Without dampening, and when admission control is configured for the first time, the system resource check is unsuccessful if the current value exceeds the critical threshold. When this happens, the system resource check subsequently succeeds only if the current value drops below the major threshold.

**Note**

When the **minor** threshold value set with *Num1* or a major threshold value set with *Num2* is crossed, the Cisco CMTS router sends an alarm (SNMP trap, when supported). When the **critical** threshold value set with *Num3* is crossed, the Cisco CMTS router drops the call request.

This dampening approach helps prevent significant fluctuations in the outcome of resource checks. For example, if the critical threshold were 80 percent and the current values fluctuated between 79 and 81 percent, this scenario would lead to an alternate success then failure event without dampening. The first check would succeed, the second check would fail, and so forth.

For additional Admission Control feature information, refer to the *Admission Control for the Cisco Cable Modem Termination System* document on Cisco.com.

**Examples**

The following example configures the Cisco CMTS router with a Quality of Service (QoS) policy that includes admission control dampening. This example illustrates the following conditions:

- When the **cpu-avg** exceeds 60%, a minor alarm (SNMP trap, when supported) is sent.
- When the **cpu-avg** exceeds 70%, a major alarm (SNMP trap, when supported) is sent.
- When the **cpu-avg** exceeds 80%, the incoming call request is rejected, and additional calls are not accepted until after the **cpu-avg** returns to below 60% (the minor alarm level).

```
Router(config)# cable admission-control cpu-avg minor 60 major 70 critical 80
```

**Related Commands**

Command	Description
<b>cable admission-control event</b>	Configures and enables admission control event types on the Cisco CMTS router.
<b>cable admission-control ds-bandwidth</b>	Configures admission control downstream bandwidth thresholds on the Cisco CMTS router.
<b>cable admission-control us-bandwidth</b>	Configures admission control upstream bandwidth thresholds on the Cisco CMTS router.
<b>clear cable admission control counters</b>	Clears all admission control resource counters on the Cisco CMTS router.
<b>debug cable admission-control</b>	Enables automatic admission control troubleshooting processes on the Cisco CMTS router.
<b>show cable admission-control</b>	Displays the current admission control configuration and status on the Cisco CMTS router, or on a specified interface.

## cable admission-control ds-bandwidth

To set the minor, major, and exclusive thresholds for downstream voice or data bandwidth for all interfaces on a Cisco CMTS router, use the **cable admission-control ds-bandwidth** command in global configuration mode or interface configuration mode. To remove this setting from a Cisco CMTS router or from a specified interface, use the **no** form of this command.

**cable admission-control ds-bandwidth** *traffic-type* **minor** *minor-threshold* **major** *major-threshold*  
**exclusive** *exclusive-percentage* **non-exclusive** *non-exclusive-percentage*

**no cable admission-control ds-bandwidth** *traffic-type* **minor** *minor-threshold* **major**  
*major-threshold* **exclusive** *exclusive-percentage* **non-exclusive** *non-exclusive-percentage*

Syntax Description		
<b>ds-bandwidth</b>		Sets downstream throughput thresholds.
<i>traffic-type</i>		Either of the following keywords sets the traffic type for which Admission Control applies. Both settings can be applied to the Cisco CMTS. <ul style="list-style-type: none"> <li><b>voice</b>—Applies thresholds to downstream voice traffic.</li> <li><b>data</b>—Applies thresholds to downstream data traffic.</li> </ul>
<b>minor</b> <i>minor-threshold</i>		Sets the minor alarm threshold. The <i>minor-threshold</i> value is a percentage value from 1 to 100.
<b>major</b> <i>major-threshold</i>		Sets the major alarm threshold. The <i>major-threshold</i> value is a percentage value from 1 to 100.
<b>exclusive</b> <i>exclusive-percentage</i>		Specifies the percentage of throughput reserved exclusively for this class (voice or data). The <i>exclusive-percentage</i> value is an integer between 1 and 100. No other class can use this throughput.
<b>non-exclusive</b> <i>non-exclusive-percentage</i>		Specifies the percentage of throughput, over and above the exclusive share, that can be used by this class. The <i>non-exclusive-percentage</i> value is an integer between 1 and 100. Because this throughput is non-exclusive, it can be used by other classes as specified.

**Command Default** Admission control is disabled by default on the Cisco CMTS router.

**Command Modes** Global configuration (config)  
Interface configuration (config-if)

**Command History**

Release	Modification
12.3(13a)BC	This command was introduced on the Cisco uBR10012 and the Cisco uBR7246VXR router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SCC	This command was modified to run on modular cable and integrated cable interfaces.

**Usage Guidelines**

Downstream bandwidth settings support all interfaces on the Cisco CMTS router through global configuration.

Downstream bandwidth settings can be further refined per-interface or per-upstream, the latter of which provides optimal downstream Admission Control granularity on the Cisco CMTS router.

When interface-level downstream configuration is used in combination with global configuration, then the interface configuration supersedes global configuration.

**Note**

The **critical** keyword is not present for the upstream throughput resource management with the Cisco Service Flow Admission Control feature.

**Note**

The **minor** threshold level cannot be greater than the **major** threshold level.

**Examples**

The following example configures downstream bandwidth in the global configuration mode, with 30% of downstream bandwidth reserved exclusively for voice traffic. Minor and major alarms for voice traffic are also set to be generated at 15% and 25% respectively.

```
Router(config)# cable admission-control ds-bandwidth voice minor 15 major 25 exclusive 30
```

**Related Commands**

Command	Description
<b>cable admission-control</b>	Configures the CPU and memory thresholds for the Cisco CMTS router and supporting broadband processing engines (BPEs).
<b>cable admission-control event</b>	Configures and enables admission control event types on the Cisco CMTS router.
<b>cable admission-control max-reserved-bandwidth</b>	Defines the maximum reserved bandwidth per bonding group for all service flows that are allowed by the Cisco CMTS.
<b>cable admission-control us-bandwidth</b>	Configures admission control upstream bandwidth thresholds on the Cisco CMTS router.
<b>clear cable admission control counters</b>	Clears all admission control resource counters on the Cisco CMTS router.

<b>Command</b>	<b>Description</b>
<b>debug cable admission-control</b>	Enables automatic admission control troubleshooting processes on the Cisco CMTS router.
<b>show cable admission-control</b>	Displays the current admission control configuration and status on the Cisco CMTS router or on a specified interface.

# cable admission-control event

To configure admission control event types on a Cisco CMTS router, and to enable admission control for all previously configured resources on a Cisco CMTS router, use the **cable admission-control event** command in global configuration mode. To disable admission control event types on a Cisco CMTS router, use the **no** form of this command.

**cable admission-control event** { **cm-registration** | **dynamic-service** }

**no cable admission-control event** *event\_type*

## Syntax Description

<b>cm-registration</b>	Performs admission control checks when a cable modem registers with the Cisco CMTS router headend. This setting can be combined with the <b>dynamic-service</b> setting, in which cable modems are allowed to register but remain subject to a Quality of Service (QoS) policy on the Cisco CMTS.
<b>dynamic-service</b>	Performs admission control checks each time a voice call is made, and rejects voice calls if they would impede QoS policies on the Cisco CMTS router. This setting can be combined with the <b>cm-registration</b> setting.

## Command Default

Admission control event types are not defined on the Cisco CMTS router.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(13a)BC	This command was introduced for the Cisco uBR10012 router and the Cisco uBR7246VXR router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

At least one event type must be configured in order to enable admission control on the Cisco CMTS router.

For additional Admission Control feature information, refer to the *Admission Control for the Cisco Cable Modem Termination System* document on Cisco.com.

## Examples

The following example configures each available option for the **cable admission-control event** command on the Cisco CMTS router.

```
Router(config)# cable admission-control event cm-registration
Router(config)# cable admission-control dynamic-service
```

Related Commands	Command	Description
	<b>cable admission-control</b>	Configures the CPU and memory thresholds for a Cisco CMTS router and supporting broadband processing engines (BPEs).
	<b>cable admission-control ds-bandwidth</b>	Configures admission control downstream bandwidth thresholds on a Cisco CMTS router.
	<b>cable admission-control us-bandwidth</b>	Configures admission control upstream bandwidth thresholds on a Cisco CMTS router.
	<b>clear cable admission control counters</b>	Clears all admission control resource counters on a Cisco CMTS router.
	<b>debug cable admission-control</b>	Enables automatic admission control troubleshooting processes on a Cisco CMTS router.
	<b>show cable admission-control</b>	Displays the current admission control configuration and status on a Cisco CMTS router, or on a specified interface.

# cable admission-control max-reserved-bandwidth

To define the maximum reserved bandwidth per bonding group for all service flows that are allowed by the Cisco CMTS, use the **cable admission-control max-reserved-bandwidth** command in the interface configuration mode. To reset or disable the maximum reserved bandwidth value, use the **no** form of this command.

**cable admission-control max-reserved-bandwidth** *bw-in-kbps*

**no cable admission-control max-reserved-bandwidth**

<b>Syntax Description</b>	<i>bw-in-kbps</i>	Maximum admission control reserved bandwidth. The value is in kbps and is based on the RF bandwidth percent defined for the bonding group. Valid range is from 0 to 14762.
---------------------------	-------------------	--

<b>Command Default</b>	The max-reserved-bandwidth value is 80 percent of the aggregate bandwidth of the RF channels configured in the US or DS bonding group.
------------------------	--

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SCC	This command was introduced.

<b>Usage Guidelines</b>	This command allows the user to define the maximum reserved bandwidth per bonding group. The default maximum reserved bandwidth value is 80 percent. However the user can choose to configure a higher (up to 96 percent) or lower reserved bandwidth so that there is bandwidth allocated for zero committed information rate (CIR) best effort traffic.
-------------------------	---

<b>Examples</b>	The following example shows a sample definition of the maximum reserved bandwidth value.
-----------------	--

```
Router> enable
Router# configure terminal
Router(config)# interface c5/0/1
Router(config-if)# cable admission-control max-reserved-bandwidth 6344
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cable admission-control</b>	Configures the CPU and memory thresholds for the Cisco CMTS router and supporting broadband processing engines (BPEs).
	<b>cable admission-control event</b>	Configures and enables admission control event types on the Cisco CMTS router.

<b>Command</b>	<b>Description</b>
<b>cable admission-control ds-bandwidth</b>	Configures admission control downstream bandwidth thresholds on the Cisco CMTS router.
<b>cable admission-control us-bandwidth</b>	Configures admission control upstream bandwidth thresholds on the Cisco CMTS router.
<b>debug cable admission-control</b>	Enables automatic admission control troubleshooting processes on the Cisco CMTS router.
<b>show cable admission-control</b>	Displays the current admission control configuration and status on the Cisco CMTS router or on a specified interface.

# cable admission-control preempt priority-voice

To change the default PacketCable emergency 911 call preemption functions on a Cisco CMTS router to support throughput and bandwidth requirements for emergency 911 calls above all other buckets on the Cisco CMTS router, use the **cable admission-control preempt priority-voice** command in global configuration mode. To disable preemption and return the bucket that supports PacketCable emergency 911 calls to its default configuration, use the **no** form of this command.

**cable admission-control preempt priority-voice**

**no cable admission-control preempt priority-voice**

## Defaults

Emergency 911 call preemption and service flow admission control is enabled on the Cisco CMTS router.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router and the Cisco uBR7246VXR router.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

By default, PacketCable Emergency 911 calls are given priority on the Cisco CMTS. This priority may be preempted or removed from the Cisco CMTS router with non-standard configuration of the Service Flow Admission Control feature.

For additional information for Service Flow Admission Control beginning in Cisco IOS Release 12.3(21)BC, refer to the *Service Flow Admission Control for the Cisco Cable Modem Termination System* document on Cisco.com.

## Examples

The following example disables and then restores emergency 911 call preemption on the Cisco CMTS router.

```
Router(config)# no cable admission-control preempt priority-voice
Router(config)# cable admission-control preempt priority-voice
```

## cable admission-control us-bandwidth

To configure upstream bandwidth thresholds for admission control on a Cisco CMTS router, use the **cable upstream admission-control us-bandwidth** command in global configuration or interface configuration mode. To disable or to remove this configuration from a Cisco CMTS router or the specified port, use the **no** form of this command.

**cable admission-control us-bandwidth** [*sched scheduling-type* | **service** *service-class-name*]  
**minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* **non-exclusive**  
*non-exclusive-percentage*

**no cable admission-control us bandwidth** [*sched scheduling-type* | **service** *service-class-name*]  
**minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* **non-exclusive**  
*non-exclusive-percentage*

### Syntax Description

<i>n</i>	Upstream on the router interface.
<b>us-bandwidth</b>	Configures the upstream throughput thresholds.
<b>sched</b> <i>scheduling-type</i>	(Optional) Specifies the scheduling type for a traffic class, where sched-type is one of the following values: <ul style="list-style-type: none"> <li>- <b>BE</b>—Selects best effort traffic.</li> <li>- <b>NRTPS</b>—Selects non-real-time polling service.</li> <li>- <b>RTPS</b>—Selects real time polling service.</li> <li>- <b>UGS-AD</b>—Selects UGS-AD service.</li> <li>- <b>UGS</b>—Selects UGS service.</li> </ul>
<b>service</b> <i>service-class-name</i>	(Optional) Displays a string representing a previously defined service class. Instead of specifying a class by a scheduling type, this keyword can be used to specify a class using the <i>service-class-name</i> .
<b>minor</b> <i>minor-threshold</i>	Sets the minor alarm threshold in a percentage value between 1 and 100.
<b>major</b> <i>major-threshold</i>	Sets the major alarm threshold in a percentage value between 1 and 100.
<b>exclusive</b> <i>exclusive-percentage</i>	Represents the critical threshold for the upstream throughput resource in a percentage value between 1 and 100. Specifies the percentage of throughput reserved exclusively for this class.
<b>non-exclusive</b> <i>non-exclusive-percentage</i>	Specifies the percentage of throughput, over and above the exclusive share, that can be used by this class. The <i>non-exclusive-percentage</i> value is an integer between 1 and 100. Because this throughput is non-exclusive, it can be used by other classes as specified.

### Command Default

Admission control is disabled by default on a Cisco CMTS router.

<b>Command Modes</b>	Global configuration (config)
	Interface configuration (config-if)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(13a)BC	This command was introduced on the Cisco uBR10012 and the Cisco uBR7246VXR routers.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
	12.2(33)SCC	This command was modified to run on modular cable and integrated cable interfaces.

<b>Usage Guidelines</b>	Upstream bandwidth settings support all interfaces on a Cisco CMTS router through global configuration.
	Upstream bandwidth settings can be further refined on a per-interface or per-upstream basis using interface configuration mode. Per-upstream settings provide the optimal upstream admission control granularity on the Cisco CMTS router.
	When interface or per-upstream configuration is used in combination with global configuration, then interface or per-upstream configuration supersedes global configuration. Per-upstream configuration also supersedes per-interface configuration.



**Note** The **critical** keyword is not present for the upstream throughput resource management with Cisco Admission Control.



**Note** The **minor** threshold level cannot be greater than the **major** threshold level.

<b>Examples</b>	For additional Admission Control feature information and examples, refer to the <i>Admission Control for the Cisco Cable Modem Termination System</i> document on Cisco.com.
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cable admission-control</b>	Configures the CPU and memory thresholds for the Cisco CMTS router and supporting broadband processing engines (BPEs).
	<b>cable admission-control event</b>	Configures and enables admission control event types on the Cisco CMTS router.
	<b>cable admission-control ds-bandwidth</b>	Configures admission control downstream bandwidth thresholds on the Cisco CMTS router.
	<b>cable admission-control max-reserved-bandwidth</b>	Defines the maximum reserved bandwidth per bonding group for all service flows that are allowed by the Cisco CMTS.
	<b>clear cable admission control counters</b>	Clears all admission control resource counters on the Cisco CMTS router.

<b>Command</b>	<b>Description</b>
<b>debug cable admission-control</b>	Enables automatic admission control troubleshooting processes on the Cisco CMTS router.
<b>show cable admission-control</b>	Displays the current admission control configuration and status on the Cisco CMTS router or on a specified interface.

# cable application-type include

To associate an application type with a specific and prioritized bucket on a Cisco CMTS router, use the **cable application-type include** command in global configuration mode. To remove the application type settings, use the **no** form of this command.

```
cable application-type bucket-number include { Best-effort | multicast application-id |
packetcable { normal | priority } | pcmm { app-id gate-app-id | priority gate-priority } |
sched-type type | service-class service-class-name }
```

```
no cable application-type bucket-number include { Best-effort | multicast application-id |
packetcable { normal | priority } | pcmm { app-id gate-app-id | priority gate-priority } |
sched-type type | service-class service-class-name }
```

Syntax Description	
<i>bucket-number</i>	Bucket number to which an application type is associated. Range is from 1 to 8, with 1 as the first in the sequence.
Best-effort	Applies best effort committed information rate (CIR) to the specified bucket.
multicast <i>application-id</i>	Specifies the application identification for the multicast service flow. The valid range is 1 to 65535.
<b>packetcable</b> { <b>normal</b>   <b>priority</b> }	Specifies PacketCable service flows for the designated bucket, with the following priorities: <ul style="list-style-type: none"> <li><b>normal</b>—Selects PacketCable calls with normal priority.</li> <li><b>priority</b>—Selects PacketCable calls with high priority.</li> </ul>
<b>pcmm</b> { <b>app-id</b> <i>gate-app-id</i>   <b>priority</b> <i>gate-priority</i> }	Specifies PacketCable Multimedia (PCMM) service flows for the designated bucket, with the following options: <ul style="list-style-type: none"> <li><b>app-id</b> <i>gate-app-id</i>—Selects the gate application identifier from 0 to 65535. For each bucket, up to ten application type rules may be defined.</li> <li><b>priority</b> <i>gate-priority</i>—Selects the priority level from 0 to 7.</li> </ul>
<b>sched-type</b> <i>type</i>	Specifies upstream scheduling types, with one of the following additional keywords used for the DOCSIS scheduling type: <ul style="list-style-type: none"> <li><b>be</b>—Best effort.</li> <li><b>nrtps</b>—Non-real-time polling service.</li> <li><b>rtps</b>—Real-time polling service.</li> <li><b>ugs</b>—Unsolicited Grant Service.</li> <li><b>ugs-ad</b>—UGS-AD (unsolicited grant service-activity detection) service.</li> </ul>
<b>service-class</b> <i>service-class-name</i>	Specifies the name of the service class being assigned to the designated bucket, where <i>service-class-name</i> is an alphanumeric string.

## Command Default

Service flow admission control is enabled without the application types.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.3(21)BC	This command was introduced for the Cisco uBR10012 router and the Cisco uBR7246VXR router.
	12.2(33)SCA	This command was introduced in Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added. The <b>multicast</b> keyword was added to this command.

### Usage Guidelines

The details of this command vary according to the bucket number and application type being mapped to a service flow on the Cisco CMTS router. This command overrides default service flow admission control settings on the Cisco CMTS.

#### Best Effort

The best effort CIR service flow rule may be applicable to both upstream and downstream. However, in the case of upstream service flows, in most cases, the same service flow may map both the rules.

For best effort, there is also the **sched-type** keyword option that applies to upstream service flows. This best effort scheduling type rule is applicable only for upstream service flows.

#### Service Classes

DOCSIS 1.1 introduced the concept of service classes. A service class is identified by a service class name. A service class name is a string the CMTS router associates with a QoS parameter set. One of the objectives of using a service class is to allow the high-level protocols to create the service flows with the desired QoS parameter set. Using a service class is a convenient way to bind the application with the service flows. The rules provide a mechanism to implement such binding.

Note the following factors when using the **service-class** keyword:

- Service classes are separately configured using the **cable match** command to provide the QoS for multicast traffic. This step maps a bucket using a rule to allocate bandwidth for multicast traffic.
- A named service class may be classified into any application type.
- Up to ten service class names may be configured per application type. Attempting to configure more than ten service classes results in an error message.

For additional information, refer to the Service Flow Admission Control feature documentation on Cisco.com.

### Examples

The following example maps high-priority PacketCable service flows into application bucket 5:

```
Router(config)# cable application-type 5 include packetcable priority
```

The following example maps normal PacketCable service flows into application bucket 1:

```
Router(config)# cable application-type 1 include packetcable normal
```

The following example maps the specified bucket number with PCMM service flow with a priority of 7, then maps an application identifier of 152 for the same bucket number:

```
Router(config)# cable application-type 2 include pcmm priority 7
Router(config)# cable application-type 2 include pcmm app-id 152
```

The following example maps both UGS and UGS-AD into bucket number 1:

```
Router(config)# cable application-type 1 include sched-type ugs
Router(config)# cable application-type 1 include sched-type ugs-ad
```

The following example maps the best effort CIR flows to bucket 3:

```
Router(config)# cable application-type 3 include Best-effort
```

The following example maps the service class name with a value of service-name1 into application bucket 3:

```
Router(config)# cable application-type 3 include service-class service-name1
```

The following example maps the multicast application type with a value of 18 into application bucket 3:

```
Router(config)# cable application-type 3 include multicast 18
```

### Related Commands

Command	Description
<b>cable admission-control ds-bandwidth</b>	Sets the minor, major, and exclusive thresholds for downstream voice or data bandwidth for all interfaces on the Cisco CMTS router.
<b>cable admission-control preempt priority-voice</b>	Changes the default PacketCable emergency 911 call preemption functions on the Cisco CMTS router to support throughput and bandwidth requirements for emergency 911 calls above all other buckets on the Cisco CMTS router.
<b>cable admission-control us-bandwidth</b>	Configures upstream bandwidth thresholds for admission control on the Cisco CMTS router.
<b>cable application-type name</b>	Assigns an alphanumeric name for the specified bucket.
<b>cable upstream admission-control</b>	Configures per-upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS router.
<b>debug cable admission-control flow-categorization</b>	Displays service flow categorization results, enabled when a service flow is classified.
<b>show application-buckets</b>	Displays rules for any or all buckets supporting service flow admission control on the Cisco CMTS router.
<b>show interface cable admission-control reservation</b>	Displays service flows, categorizations, and bandwidth consumption on the Cisco CMTS router, for the specified interface, and the specified service flow direction.

# cable application-type name

To assign an alphanumeric name for the specified bucket, use the **cable application-type name** command in global configuration mode. To remove this configuration, use the **no** form of this command.

**cable application-type** *bucket-number* **name** *bucket-name*

**no cable application-type** *bucket-number* **name** *bucket-name*

## Syntax Description

<i>bucket-number</i>	Bucket number to which the name is applied. The priority sequence of the buckets, according to their original numeration of 1 to 8, still applies, whether the default bucket numbers or customized alphanumeric names are used.
<i>bucket-name</i>	Alphanumeric bucket name.

## Command Default

Service flow admission control and the default configuration of this command is enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 router and the Cisco uBR7246VXR router.
12.2(33)SCA	This command was introduced in Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

This bucket name appears in supporting **show** and **debug** commands along with the default bucket number.

For additional information, refer to the Service Flow Admission Control feature documentation on Cisco.com.

## Examples

The following example illustrates the use of descriptive names for the associated buckets:

```
Router(config)# cable application-type 2 name video
Router(config)# cable application-type 3 name gaming
```

Related Commands	Command	Description
	<b>cable admission-control ds-bandwidth</b>	Sets minor, major and exclusive thresholds for downstream voice or data bandwidth for each or all interfaces on the Cisco CMTS
	<b>cable admission-control preempt priority-voice</b>	Changes the default PacketCable Emergency 911 call preemption functions on the Cisco CMTS, supporting throughput and bandwidth requirements for Emergency 911 calls above all other buckets on the Cisco CMTS.
	<b>cable admission-control us-bandwidth</b>	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS.
	<b>cable application-type include</b>	Associates an application type with a specific and prioritized bucket on the Cisco CMTS.
	<b>cable upstream admission-control</b>	Configures per-upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS.
	<b>debug cable admission-control flow-categorization</b>	Displays service flow categorization results, enabled when a service flow is classified.
	<b>show application-buckets</b>	Displays rules for any or all buckets supporting Service Flow Admission Control on the Cisco CMTS.
	<b>show interface cable admission-control reservation</b>	Displays service flows, categorizations, and bandwidth consumption on the Cisco CMTS, for the specified interface, and the specified service flow direction.

# cable arp

To activate cable Address Resolution Protocol (ARP), use the **cable arp** command in cable interface or subinterface configuration mode. To block ARP requests for cable modems (CMs), use the **no** form of this command.

**cable arp**

**no cable arp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** ARP is enabled.

**Command Modes** Cable interface and subinterface configuration

## Command History

Release	Modification
12.1T	This command was introduced.
12.0(6)SC	This command was supported.
12.1(2) EC1	This command was supported.
12.1(3a)EC	Subinterface support was added.
12.2(8)BC1	Interaction with the <b>clear arp-cache</b> command was changed. Previously, the <b>clear arp-cache</b> command sent an ARP request to a CM before clearing its ARP entry. Now, the <b>clear arp-cache</b> command clears the ARP entry without communicating with the CM. The CM (or its CPE devices) must send one or more IP packets to the CMTS before IP communications can be restored (assuming the CM or CPE devices are authorized to connect to the network).
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

ARP is an Internet protocol used to map IP addresses to MAC addresses on computers and other equipment installed in a network. You must activate ARP requests so that the Cisco CMTS router can perform IP address resolution on the downstream path.

Occasionally, you might want to use the **no cable arp** and **clear arp-cache** commands to block out new ARP requests and clear the existing ARP table. In this situation, the Cisco CMTS router will retain the ARP addresses of currently online CMs (CMs with a known IP address) and will continue to send ARP requests for those CMs when those ARP entries time out or are cleared, so that those CMs can continue to remain online. ARP requests for CMs that are currently offline and for any other unknown IP addresses, however, will remain blocked until ARP requests are reenabled on the downstream using the **cable arp** command.

**Note**

Using the **no cable arp** and **no cable proxy-arp** commands shifts all responsibility for the management of the IP addresses used by CMs and CPE devices to the DHCP server and provisioning system.

**Tip**

You can expect to see a temporary spike in CPU usage after initially giving the **no cable arp** command, because of the need to verify CPE IP addresses. CPU usage drops after the router has verified and learned all of the CPE IP addresses that are currently online. (This same situation occurs after initially enabling the **cable source-verify dhcp** command, because the router must send a DHCP LEASEQUERY request for every unknown CPE IP address.)

**Examples**

The following example shows how to activate cable ARP requests for port 0 on the cable interface line card installed in slot 6 of a Cisco CMTS router:

```
router(config)# interface cable 6/0
router(config-if)# cable arp
```

The following example shows how to activate cable ARP requests for port 0 on the cable interface line card installed in slot 6, subinterface 1, of a Cisco CMTS router:

```
router(config)# interface cable 6/0.1
router(config-subif)# cable arp
```

**Related Commands**

Command	Description
<b>clear arp-cache</b>	Clears the ARP table on the router.
<b>cable proxy-arp</b>	Activates cable proxy ARP on the cable interface.

# cable arp filter

To control the number of Address Resolution Protocol (ARP) packets that are allowable for each Service ID (SID) on a cable interface, use the **cable arp filter** command in cable interface configuration mode. To stop the filtering of ARP broadcasts for CMs, use the **no** form of this command.

**cable arp filter** { **reply-accept** | **request-send** } *number window-size*

**no cable arp filter** { **reply-accept** | **request-send** }

**default cable arp filter** { **reply-accept** | **request-send** }

## Syntax Description

<b>reply-accept</b>	Configures the cable interface to accept only the specified <i>number</i> of ARP reply packets every <i>window-size</i> seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number.
<b>request-send</b>	Configures the cable interface to send only the specified <i>number</i> of ARP request packets every <i>window-size</i> seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number.
<i>number</i>	Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface drops all ARP reply packets.
<i>window-size</i>	Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds.

## Command Default

ARP packets are not filtered, which means the Cisco CMTS router accepts all ARP reply packets and sends all ARP request packets.

## Command Modes

Cable interface configuration (config-if)

## Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
12.3(9a)BC	The values of <i>number</i> and <i>window-size</i> are optional for the the respective <b>reply-accept</b> and <b>request-send</b> settings. In this release and for earlier supporting releases, when ARP filtering is enabled, the default values for <i>number</i> and <i>window-size</i> are 4 and 2 respectively.
12.3(17a)BC	In this release and for later releases, when ARP filtering is enabled, the default values for <i>number</i> and <i>window-size</i> are 3 and 2 respectively.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

**Usage Guidelines**

Viruses, worms, and theft-of-service attacks can generate a large volume of ARP requests on a cable interface. In some situations, the volume of ARP traffic can become so large that it throttles all other traffic.

To control the number of ARP replies and ARP requests that are allowed for each SID on a cable interface, use the **cable arp filter** command. This command configures the interface so that it accepts only a certain number of ARP reply or request packets per a specified time period. If a SID generates more ARP packets than what is allowed, the cable interface drops the excessive traffic.

By default, no ARP filtering is done. ARP filtering is enabled on individual cable interfaces, and you can choose to filter ARP packets only on the specific cable interfaces that require it. You can further choose to filter only ARP request packets, only ARP reply packets, or both. You can configure different threshold values on each interface, allowing you to customize the feature for each interface's traffic patterns.

If using bundled cable interfaces, the Cable ARP Filtering feature is configured separately on the master and slave interfaces. This allows you to configure the feature only on the particular interfaces that require it.

**Note**

Cisco IOS Release 12.3(9a)BC introduces enhanced command option syntax for the **cable arp filter** command, where *number* and *window-size* values are optional for **reply-accept** and **request-send** settings.

**Note**

Disabling the cable ARP filtering feature, using the **no cable arp filter** command, does not reset the ARP packet counters. The ARP packet counters do not increment when cable ARP filtering is disabled, but the counters retain their current values until the interface counters are specifically cleared, using the **clear counters** command.

**Linksys Wireless-B BEFW11S4 Router**

The Linksys Wireless-B Broadband Router BEFW11S4 version 4 with 1.44.2 firmware incorrectly sends its own ARP reply packet for every ARP request packet it receives, instead of replying only to the ARP requests that are specifically for itself. Customers with these routers should upgrade the firmware to the latest revision to fix this bug. To upgrade the firmware, go to the download section on the Linksys web site.

The following example shows how to filter cable ARP reply packets, so that the cable interface accepts a maximum of 15 ARP replies every three seconds per SID:

```
Router(config)# interface cable 5/1/0
Router(config-if)# cable arp filter reply-accept 15 3
```

The following example shows how to filter cable ARP request packets, so that the cable interface sends a maximum of 10 requests per second per SID:

```
Router(config)# interface cable 6/0
Router(config-if)# cable arp filter request-send 10 1
```

The following example shows how to enable the filtering of cable ARP request and reply packets on a cable interface, using the default values of 4 packets per CPE per every 2 seconds:

```
Router(config)# interface cable 3/0
Router(config-if)# default cable arp filter reply-accept
Router(config-if)# default cable arp filter request-send
Router(config-if)# end
Router# show running-config | include filter
```

## ■ cable arp filter

```
cable arp filter reply-accept 4 2
cable arp filter request-send 4 2
```

The following example shows how to disable the filtering of cable ARP request and reply packets on a cable interface:

```
Router(config)# interface cable 1/0
Router(config-if)# no cable arp filter reply-accept
Router(config-if)# no cable arp filter request-send
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cable arp</b>	Activates cable ARP.
<b>cable proxy-arp</b>	Activates cable proxy ARP on the cable interface.
<b>clear arp-cache</b>	Refreshes dynamically created entries from the ARP cache.
<b>clear counters</b>	Clears the packet counters on all interfaces or on a specific interface.
<b>debug cable arp filter</b>	Displays debugging messages about the filtering of ARP broadcasts.
<b>show cable arp-filter</b>	Displays the total number of ARP replies and requests that have been sent and received, including the number of requests that have been filtered.

# cable attribute-mask

To configure an attribute for a modular cable interface, use the **cable attribute-mask** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

**cable attribute-mask** *mask*

**no cable attribute-mask** *mask*

## Syntax Description

<i>mask</i>	Specifies the mask value for the interface.
-------------	---

## Command Default

If this command is not used, the default attribute will be used for the modular cable interface. The default attribute for a modular cable interface is zero.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SCB	This command was introduced.

## Usage Guidelines

The attribute mask comprises 32 attributes and each attribute represents a single bit in the mask. You can configure a provisioned attribute mask for each channel and provisioned bonding group to assign values to the operator-defined binary attributes, or to override the default values of the specification-defined attributes. The operator may configure, in the CM configuration file, a required attribute mask and a forbidden attribute mask for a service flow. Additionally, in a CM-initiated dynamic service request, the CM can include a required attribute mask and a forbidden attribute mask for a service flow.

## Examples

The following example shows how to configure an attribute for a modular cable interface:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable attribute-mask 2000ff00
```

## Related Commands

Command	Description
<b>interface modular-cable</b>	Specifies a modular cable interface.
<b>cable downstream attribute-mask</b>	Specifies an attribute mask value for a wideband cable interface.
<b>interface wideband-cable</b>	Specifies a wideband cable interface.
<b>interface cable</b>	Specifies a cable interface.

# cable bonding-group-id

To specify a Bonding Group ID and indicate whether the bonding group is a primary or secondary bonded channel, use the **cable bonding-group-id** command in wideband-cable interface configuration mode. To remove a bonding group configuration and revert to the default bonding group (a primary bonding group), use the **no** form of this command.

**cable bonding-group-id** *id\_num* [**secondary**]

**no cable bonding-group-id** *id\_num* [**secondary**]

<b>Syntax Description</b>	<i>id_num</i>	A unique Bonding Group ID. Valid values are 1 to 255. The bonding group ID must be unique for each wideband channel on the CMTS.
	<b>secondary</b>	Specifies that the bonding group is a secondary bonding group. If the <b>secondary</b> keyword is not used, the bonding group is a primary bonding group.

**Command Default** If the **cable bonding-group-id** command is not issued, Cisco IOS software assigns a default ID to the bonding group and configures the wideband-channel cable interface as a primary bonding group.

**Command Modes** Interface configuration mode for a wideband-cable interface (config-if)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(21)BC	This command was introduced for the Cisco uBR10012 router.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

**Usage Guidelines** The **cable bonding-group-id** command is *not needed* for the wideband channels that will be received by the Scientific Atlanta DPC2505 or EPC2505 wideband cable modems.

The **cable bonding-group-id** command is used only for wideband channels that will be received by the Linksys WCM300-NA, WCM300-EURO, or WCM300-JP wideband cable modems.

### Linksys WCM300 Cable Modem

For wideband channels that will be received by the Linksys WCM300-NA, WCM300-EURO, and WCM300-JP cable modems, the **cable bonding-group-id** command assigns a Bonding Group ID to a wideband-channel cable interface and configures the bonding group as a primary bonding group if the **secondary** keyword is not specified, or as a secondary bonding group if the **secondary** keyword is specified.

- A primary bonding group is a primary bonded channel.
- A secondary bonding group is a secondary bonded channel.

The primary bonded channel is the wideband channel on which the Linksys WCM300 modem receives all of its unicast traffic and some of its multicast traffic. The cable modem may identify the primary bonded channel and any secondary bonded channels to the CMTS at cable modem registration time. The DOCSIS configuration file may define the primary bonded channel for the CMTS to assign to the cable modem.

In addition to joining one primary bonded channel, the Linksys WCM300 may join up to two secondary bonded channels simultaneously in order to receive additional data streams. The DOCSIS configuration file may define the secondary bonded channels for the modem to pass to the CMTS. Secondary bonded channels are intended to receive multicast traffic such as broadcast video that is not available on the primary bonded channel.

For information on the TLV encodings that can be used in the DOCSIS configuration file to identify primary and secondary bonded channels, see the *Cisco Cable Wideband Solution Design and Implementation Guide, Release 1.0*.

**Note**

If a wideband channel is specified as a primary or secondary bonded channel in the DOCSIS configuration file, it *must be identically defined* as a primary or secondary bonded channel in the CMTS active, running configuration file.

- If a wideband channel is configured with the **cable bonding-group-id** command or by default to be a primary bonded channel, the Linksys WCM300 modem will not register using it as one of its secondary bonded channels.
- If a wideband channel is configured with the **cable bonding-group-id** command to be a secondary bonded channel, the Linksys WCM300 modem will not register using it as its primary bonded channel.

**Note**

When a wideband channel is defined on a Wideband SPA, Cisco IOS software configures the wideband channel as a primary bonding group (primary bonded channel) and assigns a default ID to the bonding group. If a wideband channel is to be used as a secondary bonded channel, use the **cable bonding-group-id** command with the **secondary** keyword to specify that the channel is a secondary bonded channel.

If you specify a non-unique Bonding Group ID for the *id\_num* argument, **cable bonding-group-id** displays an error message and does not modify the ID.

**Scientific Atlanta DPC2505 Cable Modem**

The **cable bonding-group-id** command *is not needed* for the wideband channels that will be received by the Scientific Atlanta DPC2505 or EPC2505 cable modems.

**Examples**

The following examples show how to use the **cable bonding-group-id** command for a variety of purposes. The following **cable bonding-group-id** command specifies that wideband channel 10 on the Wideband SPA in slot/subslot/bay 1/0/1 will be a secondary bonding group (secondary bonded channel) having the bonding group ID 20.

```
Router# configure terminal
Router(config)# interface wideband-cable 1/0/1:10
Router(config-if)# cable bonding-group-id 20 secondary
```

The following example shows how to change a bonding group with an ID of 20 from a secondary to a primary bonding group by omitting the **secondary** keyword:

## ■ cable bonding-group-id

```
Router(config-if)# cable bonding-group-id 20
```

The **no** form of the **cable bonding-group-id** removes the configured bonding group and reverts the configuration to the default bonding group. For a secondary bonding group with the ID of 20, the following **no** forms of the command are equivalent:

```
Router(config-if)# no cable bonding-group-id 20
```

OR

```
Router(config-if)# no cable bonding-group-id 20 secondary
```

When either of the preceding commands are issued, the wideband-channel cable interface is configured to use a default bonding group, which has a default bonding group ID assigned by Cisco IOS software and is a primary bonding group.

### Related Commands

Command	Description
<b>interface</b>	Enters interface configuration mode.

# cable bundle

To configure a cable interface to belong to an interface bundle, use the **cable bundle** command in cable interface configuration mode. To delete a cable interface bundle definition, use the **no** form of this command.

**cable bundle** *n* [**master**]

**no cable bundle** *n* [**master**]

## Syntax Description

<i>n</i>	Specifies the bundle identifier. Valid range is from 1 to 255.
<b>master</b>	(Optional) Defines the specified interface as the master.

## Defaults

No default behavior or values

## Command Modes

Interface configuration—cable interface only (config-if)

## Command History

Release	Modification
12.1(1a)T1	This command was introduced.
12.0(8) SC	This command was supported.
12.1(2) EC1	This command was supported.
12.2(15)BC2	This command was enhanced, so that adding an interface as a slave interface automatically removes the following Layer 3 parameters, if they are configured on that interface: IP address, IP helper address, IP access group, PIM configuration, and IP policy-based routing.  Also, creating subinterfaces on slave interfaces has been specifically prohibited. Previously, subinterfaces could be created on slave interfaces, although a warning message appeared advising users to remove the subinterface.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

You can configure a maximum of four interface bundles. In each bundle, specify one interface as the master interface by using the optional **master** keyword. The cable interface that is designated as master is configured with Layer 3 configuration such as primary and secondary IP addresses and other Layer 3 specific configuration commands such as the **cable arp** command.

The following guidelines are required when using bundled cable interfaces:

- Configure an IP address only on the master interface. Any attempt to add an interface to a bundle is rejected, if an IP address is configured and the interface is not specified as master interface.

- You must specify all generic IP networking information (IP address, routing protocols, switching modes, and so on) on the bundle master interface. Do not specify generic IP networking information on bundle slave interfaces.
- If you attempt to add an interface to a bundle as slave interface and an IP address is assigned to this interface, the command fails. You must remove the IP address configuration before you can add the interface to a bundle.
- If you have configured an IP address on a bundled interface and the interface is not the master interface, a warning message appears.
- Do not create subinterfaces on a slave interface. In Cisco IOS Release 12.2(15)BC2 and later releases, this is specifically prohibited. In prior releases, a warning message appeared when trying to create a subinterface on a slave interface, but the subinterface was still created.

Specify generic (that is, not downstream or upstream) cable interface configurations, such as source-verify or Address Resolution Protocol (ARP) handling, on the master interface. Do not specify generic configuration on nonmaster interfaces.

If you configure an interface as part of a bundle and it is not the master interface, all generic cable configuration for this interface is removed. This includes the IP address, access groups, PIM configuration, and any other IP Layer 3 configurations. The master interface configuration then applies to all interfaces in the bundle.

**Tip**

We recommend configuring the **no ip address** command on all slave interfaces. This command is optional but recommended, because the **show ip interface brief** command reports an interface as being not OK if its configuration does not include some form of the **ip address** command. Specifying **no ip address** corrects this.

When creating subinterfaces over the bundle master, the bundle master is not assigned any IP address and only the subinterfaces are assigned IP addresses, helper addresses, and other Layer 3 configurations. The reason the bundle master is not assigned an IP address is because CMs are associated with subinterfaces rather than with a bundle master.

**Note**

Cable interface bundling is applicable only in two-way cable configurations. It is not supported in telco-return configurations.

If you shut down or remove the master interface in a bundle, no data packets is sent to any of the interfaces in this bundle. Packets are still physically received from nonmaster interfaces that have not been shut down, but those packets are discarded. This means that CMs connected to those interfaces are not disconnected immediately, but CMs coming online are not able to obtain an IP address, download their configuration file, or renew their IP address assignment if the DHCP lease expires.

If you shut down a slave interface, only this shutdown interface is affected.

**Note**

When using bundled interfaces, the **show interface cable** command divides the interface counters between the master and slave interfaces. The output for the master interface shows the upstream packets per second count, while the output for the slave interfaces shows the downstream packets per second count.

**Examples**

See the following example to configure interface 25 to be the master interface:

```
Router(config)# interface cable 3/0
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

The following example shows the error message you get if you try to configure an interface with an IP address that is not the master interface:

```
Router(config)# interface cable 3/0
Router(config-if)# cable bundle 5
Please remove ip address config first then reenter this command
Router(config-if)#
```

The following example shows how to remove a cable interface from a bundle:

```
Router(config)# interface cable 5/1/0
Router(config-if)# no cable bundle 5
Router(config-if)#
```

**Note**

When you remove a slave cable interface from a bundle (using the **no cable bundle** command), you must manually reconfigure all of the Layer 3 IP information on the interface, before cable modems can resume communicating on that interface.

**Related Commands**

Command	Description
<b>show cable bundle</b>	Displays the forwarding table for the specified interface bundle.

# cable clock clear-counters

To reset the counters that are displayed with the **show controllers clock-reference** command, use the **cable clock clear-counters** command in privileged EXEC mode.

## cable clock clear-counters

**Syntax Description** This command has no keywords or arguments.

**Command Default** No default behavior or values

**Command Modes** Privileged EXEC (#)

### Command History

Release	Modification
12.1(1a)T1	This command was introduced.
12.1(2)EC1	This command was supported on the EC train for the Cisco uBR7246VXR router.
12.2(2)XF	This command was supported for the TCC+ card on Cisco uBR10012 routers.
12.2(4)BC1	Support for this command was added to the Release 12.2 BC train for the Cisco uBR7246VXR and Cisco uBR10012 routers.
12.3(23)BC	This command is supported only for standalone (freerun) mode.

### Usage Guidelines

This command resets any counters that were displayed from the last time the **show controllers clock-reference** command was used.



#### Note

This command is not supported on the SC train.

This command supports the Cisco CMTS clock feature set, which provides a synchronized clock for improved Voice-over-IP (VoIP) operations. The clock feature set requires one of the following configurations:

- A Cisco uBR10012 router with one or two TCC+ cards that are connected to an external national clock source.



#### Note

Beginning in Cisco IOS Release 12.3(23)BC, TCC+ is replaced with the DOCSIS Timing and Control Card (DTCC) and does not require to be connected to an external national clock source.

- A Cisco uBR7246 VXR router using a Cisco uBR-MC16S, Cisco uBR-MC16E, Cisco uBR-MC28C, or Cisco uBR-MC28C-BNC cable interface line card. The router must also be equipped with a Cisco cable clock card and be running Cisco IOS Release 12.1(1a)T1, Cisco IOS Release 12.1(2)EC1, or a later release. The Cisco cable clock card should be connected to an external national clock source.

Only these cable interface cards support the external clock card reference from a clock card to distribute that signal to CMs or set-top boxes (STBs) attached to the specific network segments. You can use other cable interface cards, such as the Cisco uBR-MC16C, with the clock card, but these other cable interfaces will not synchronize their downstream SYNC messages with the external clock source.

Each CM or STB must also support VoIP applications and the clock feature set. For example, the Cisco uBR924, running Cisco IOS Release 12.0(7)T or later releases, supports the clock card feature automatically.

**Note**

The **show controllers clock-reference** command might display compare errors on the Cisco uBR10012 router because there could be a slight delay at system startup before the clock cards synchronize with each other. These initial compare errors can be ignored and cleared with the **cable clock clear-counters** command.

**Examples**

The following example shows how to reset all counters that are displayed for the clock card:

```
Router# cable clock clear-counters
```

**Related Commands**

Command	Description
<b>show controllers clock-reference</b>	Displays the cable clock card's hardware information.

# cable clock dti

To configure the DOCSIS Timing Interface (DTI) clock reference mode, use the **cable clock dti** command in global configuration mode. To terminate the DTI clock reference mode and restart the standalone mode, use the **no** form of the command.

**cable clock dti**

**no cable clock dti**

---

**Syntax Description** This command has no keywords or arguments.

---

**Command Default** Standalone mode

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.3(23)BC	This command was introduced for the Cisco uBR10012 router.

---



---

**Usage Guidelines** Use this command to configure DTI clocking mode. This command may be stored in NVRAM as part of the DOCSIS Timing and Control Card (DTCC) configuration.

---

**Examples**

```
Router# config terminal
Router(config)# cable clock dti
```

---

Related Commands	Command	Description
	<b>show cable clock dti</b>	Displays DTI information.

---

## cable clock dti clear-counters

To reset the counters that are displayed with the **show cable clock dti counters** command in DOCSIS Timing Interface (DTI) mode, use the **cable clock dti clear-counters** command in privileged EXEC mode.

**cable clock dti clear-counters** *slot/subslot*

<b>Syntax Description</b>	<i>slot/subslot</i>	Specifies the slot and subslot location of the DTCC ports. Valid values are 1/1 or 2/1.
---------------------------	---------------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(23)BC	This command was introduced on the Cisco uBR10012 router .

<b>Usage Guidelines</b>	<p>This command resets any counters that were displayed from the last time the <b>show cable clock dti client</b> command was used in DTI mode.</p> <p>This command supports the Cisco CMTS clock feature set, which provides a synchronized clock for improved Voice-over-IP (VoIP) operations.</p>
-------------------------	--

<b>Examples</b>	<p>The following example shows how to reset all counters that are displayed for the clock card:</p> <pre>Router# <b>cable clock dti clear-counters</b></pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show cable clock dti counters</b>	Displays the cable clock card's hardware information.

# cable clock force

To select the external timing source when the clock card is in holdover mode, use the **cable clock force** command in global configuration mode. To disable the selection and return to the default, use the **no** form of this command.

**cable clock force** { **primary** | **secondary** }

**no cable clock force**

## Syntax Description

**primary** Forces the primary source to act as the clock reference.

**secondary** Forces the secondary source to act as the clock reference.

## Command Default

The clock card automatically uses the primary external source, if available. If the primary source fails, the clock card enters holdover mode and, after a few seconds, switches to the secondary external source. The clock card switches back to the primary source when it becomes available.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.1(1a)T1	This command was introduced.
12.1(2)EC1	This command was integrated into Cisco IOS Release 12.1(2)EC1.

## Usage Guidelines

This command overrides the default behavior of the clock card when the clock card is in holdover mode. If the clock card is not in holdover mode, this command is ignored. You cannot force the reference to a port if the clock card is in free-running mode.



### Note

This command is not applicable on the SC train.



### Note

The clock card enters holdover mode if the forced reference is lost, even if the other external reference is available.

To support the clock feature set in VoIP configurations, a Cisco uBR7246 VXR chassis, equipped with a clock card; and a Cisco uBR-MC16S, a Cisco uBR-MC16E, or a Cisco uBR-MC28C cable interface line card must be used running Cisco IOS Release 12.1(1a)T1 or later releases. Only these cable interface line cards support the external clock card reference from a clock card to distribute that signal to CMs or set-top boxes (STBs) attached to the specific network segments. You can use other cable interface cards, such as the Cisco uBR-MC16C, with the clock card, but these other cable interfaces will not synchronize their downstream SYNC messages with the external clock source.

Each CM or STB must also support VoIP applications and the clock feature set. For example, the Cisco uBR924, running Cisco IOS Release 12.0(7)T or later releases, supports the clock card feature automatically.

---

**Examples**

The following example shows how to force the timing reference for the cable clock card to come from the secondary external source, when the clock card is in holdover mode:

```
Router(config)# cable clock force secondary
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show cable clock</b>	Displays status information for the cable clock card.
<b>show controllers clock-reference</b>	Displays hardware information, register values, and current counters for the cable clock card.

# cable clock source-midplane

To make the midplane time-division multiplexing (TDM) clock the primary timing reference for the clock card, use the **cable clock source-midplane** command in global configuration mode. To disable the selection and return to the default, use the **no** form of this command.

**cable clock source-midplane**

**no cable clock source-midplane**

**Syntax Description** This command has no keywords or arguments.

**Command Default** The clock card does not get its timing reference from the midplane TDM clock.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.1(1a)T1	This command was introduced.
	12.1(2)EC1	This command was integrated into Cisco IOS Release 12.1(2)EC1.
	12.3BC	This command was integrated into Cisco OS Release 12.3BC.

**Usage Guidelines** Because the clock card automatically provides the timing reference to the midplane TDM clock, the midplane cannot in turn act as the reference for the clock card. This means that the **cable clock source-midplane** command does not take effect unless a port adapter is configured as the primary clock reference source for the midplane.



**Note** This command is not applicable on the SC train.

To support the clock feature set in VoIP configurations, a Cisco uBR7246 VXR chassis, equipped with a clock card; and a Cisco uBR-MC16S, a Cisco uBR-MC16E, or a Cisco uBR-MC28C cable interface line card must be used running Cisco IOS Release 12.1(1a)T1 or higher releases. Only these cable interface line cards support the external clock card reference from a clock card to distribute that signal to CMs or set-top boxes (STBs) attached to the specific network segments. You can use other cable interface cards, such as the Cisco uBR-MC16C, with the clock card, but these other cable interfaces will not synchronize their downstream SYNC messages with the external clock source.

Each CM or STB must also support VoIP applications and the clock feature set. The Cisco uBR924, running Cisco IOS Release 12.0(7)T or later releases, supports the clock card feature automatically.

**Examples** The following example shows how to set the primary clock reference to the midplane TDM clock:

```
Router(config)# cable clock source-midplane
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show cable clock</b>	Displays status information for the cable clock card.

# cable clock upgrade

To upgrade the Field-Programmable Gate Array (FPGA) image manually on the DOCSIS Timing & Control Card (DTCC), use the **cable clock upgrade** command in privileged EXEC mode.

**cable clock upgrade** *slot/subslot*

Syntax Description	slot	Chassis slot number of the DTCC card. The valid slot is 1.
	<i>subslot</i>	Secondary slot number of the DTCC card. Valid subslots are 1 or 2.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SCC	This command was introduced.

**Usage Guidelines** In Cisco IOS Release 12.2(33) SCC and later, you can manually upgrade the FPGA image only if a single DTCC card is installed on the Cisco uBR 10012 router. If the manual upgrade fails or is interrupted, the DTCC card may become unusable. Do not reset or unplug the DTCC card during the manual upgrade. We recommend that you take precaution against extended downtime if the FPGA upgrade fails unexpectedly by having a standby DTCC card installed on the Cisco uBR10012 router.



**Note** You will have to enter **y (yes)** when the system prompts you to continue the manual upgrade.

**Examples** The following example shows how to start the manual FPGA upgrade process on the DTCC card:

```
Router# cable clock upgrade 1/1
```

Related Commands	Command	Description
	<b>cable clock dti</b>	Configures the DOCSIS Timing Interface (DTI) clock reference mode.

# cable cmcpe-list valid-time

To set the length of time that a CMTS router will consider the current list of CM and CPE devices to be valid, use the **cable cmcpe-list valid-time** command in global configuration mode. To reset the time period to its default value of 3 minutes, use the **no** form of this command.

**cable cmcpe-list valid-time** *time*

**no cable cmcpe-list valid-time**

## Syntax Description

*time* Specifies the time period, in seconds, that the Cisco CMTS router should consider the current CM/CPE list to be valid. In Cisco IOS Release 12.2(15)BC1 and earlier releases, the valid range is 0 to 3600 seconds, with a default value of 180 seconds (3 minutes). In Cisco IOS Release 12.2(15)BC2 and later releases, the valid range is 0 to 86400 seconds, with a default value of 900 seconds (15 minutes).

## Command Default

180 seconds (3 minutes)—Cisco IOS Release 12.2(15)BC1 and earlier releases  
900 seconds (15 minutes)—Cisco IOS Release 12.2(15)BC2 and later releases

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(15)SC1, 12.1(8)EC1,	This command was introduced for the Cisco uBR7100 series and Cisco uBR7200 series routers.
12.2(4)BC1	This command was supported on the 12.2 BC train for the Cisco uBR10012 router.
12.2(15)BC2	The maximum range for time was expanded from 3600 to 86400 seconds, and the default was changed from 180 to 900 seconds.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

## Usage Guidelines

The Cisco CMTS router maintains an internal list of CMs and CPE devices that are currently connected on its cable interfaces. The CMTS router uses this list to provide the data for various **show** commands and to respond to SNMP requests that query the entries in the `cdxCmCpeTable` table in the CISCO-DOCS-EXT-MIB MIB.

By default, the Cisco CMTS router uses the current list if it is less than 3 minutes old. If the current list is older than 3 minutes, the Cisco CMTS router considers it invalid and rebuilds a new list. This prevents the CMTS router from having to build a new list for every query, which could impact system performance.

You can use the **cable cmcpe-list valid-time** command to change the length of time that the CMTS router considers the current CM and CPE device list to be valid. This allows you to find the optimum time value that provides the most current information without affecting the number of CPU cycles that are available for network processing.

A smaller time period ensures that the CM and CPE device list is more current but it requires more processing time to maintain the list. A longer time period reduces the load on the processor but the CM/CPE list might not be current.

If CPU usage dramatically increases when performing SNMP queries of the cdxCmCpeTable table, use this command to increase the valid list time so that the Cisco CMTS router does not have to rebuild the CM/CPE list more often than needed to respond to the queries.

**Note**

To find the current valid list time, use the **show running-config** command and look for the **cable cmcpe-list valid-time** command in the output. If the command does not appear, the valid list time is set for its default value.

**Examples**

The following example shows how to set the valid list time to 60 seconds (1 minute):

```
Router(config)# cable cmcpe-list valid-time 60
```

The following example shows how to find the current valid list time setting:

```
Router# show running-config | include cmcpe-list
cable cmcpe-list valid-time 60
```

**Related Commands**

Command	Description
<b>show cable modem</b>	Displays information for the registered and unregistered CMs.

# cable cm-status enable

To enable a CM status event or a group of CM status events on a primary cable interface, use the **cable cm-status enable** command in interface configuration mode. To disable a particular event on a primary cable interface, use the **no** form of this command.

**cable cm-status enable** *range*

**no cable cm-status**

## Syntax Description

*range*

Specifies the CM status events you want to enable on a primary cable interface. The valid range is 1 to 10. You can enable a single event by specifying the event number or a group of events by specifying a range (for example, 1-9).

The following events respectively are enabled by default on cable and modular cable interfaces:

- Secondary channel MDD time-out
- QAM/FEC lock failure
- MDD recovery
- QAM/FEC lock recovery



### Note

The default events are not displayed in the output of the **show running-config interface cable** command.

## Command Default

The downstream related events such as secondary channel MDD time-out, QAM/FEC lock failure, MDD recovery, and QAM/FEC lock recovery are enabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SCB	This command was introduced.

## Usage Guidelines

This command applies to all non-primary RF channels on a CMTS.

The ten CM status events per interface are:

1. Secondary channel MDD time-out
2. QAM/FEC lock failure
3. Sequence out of range
4. MDD recovery
5. QAM/FEC lock recovery

6. T4 time-out
7. T3 re-tries exceeded
8. Successful ranging after T3 re-tries exceeded
9. CM operating on battery backup
10. CM returned to A/C power

**Note**

If the no version of the command is executed on the interface for specific events, then the **show running-config interface** command lists the events only that are enabled. If no events are enabled then, the show running interface cable command displays **no cable cm-stauts enable** with the events.

**Examples**

The following example shows how to enable all CM status events on a primary cable interface:

```
Router# configure terminal
Router(config)# interface cable 8/0/0
Router(config-if)# cable cm-status enable 1-10
```

The following example shows the **no cable cm-status enable** command being configured and the corresponding example shows **show running-config interface** command output:

```
Router(config)# interface cable 8/0/0
Router(config-if)# cable cm-status enable 1-10
Router(config-if)# no cable cm-status enable 1-2 4-5
Router(config-if) exit
```

```
Router# show running-config interface cable 8/0/0
Building configuration...
```

```
Current configuration : 1557 bytes
!
interface Cable8/0/0
 shutdown
 cable cm-status enable 3 6-10
 no cable packet-cache
 cable default-phy-burst 0
 cable map-advance dynamic 300 500
 cable bundle 1
 cable downstream channel-id 145
```

The following example shows the **show running-config interface cable** command output when no events are enabled on the CMTS:

```
Router#show running-config interface cable 8/0/0
Building configuration...
```

```
Current configuration : 1558 bytes
!
interface Cable8/0/0
 shutdown
 no cable cm-status enable 1-10
 no cable packet-cache
 cable default-phy-burst 0
 cable map-advance dynamic 300 500
 cable bundle 1
 cable downstream channel-id 145
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
```

```
cable downstream frequency 55500000
cable downstream rf-shutdown
cable upstream max-ports 4
no cable upstream 0 connector
cable upstream 0 frequency 40000000
cable upstream 0 channel-width 3200000 3200000
cable upstream 0 power-level 26
cable upstream 0 docsis-mode tdma-atdma
cable upstream 0 minislots-size 4
--More--
```

**Related Commands**

Command	Description
<b>show cable modem</b>	Displays information for the registered and unregistered CMs.

# cable config-file

To create a configuration filename for a Cisco CMTS router internal CM configuration file, use the **cable config-file** command in global configuration mode. To delete the configuration filename, use the **no** form of this command.

**cable config-file** *filename*

**no cable config-file** *filename*

---

**Syntax Description**     *filename* Specifies the configuration filename to create and edit.

---



---

**Command Default**     No default behaviors or values

---

**Command Modes**     Global configuration (config)

---

Command History	Release	Modification
	12.1(2)EC1	This command was introduced.
	12.2(4)BC1	This command was integrated into Cisco IOS Release 12.2(4)BC1.
	12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

---



---

## Usage Guidelines

A DOCSIS CMTS router automatically downloads a DOCSIS configuration file to a CM during its initial registration procedure. The DOCSIS configuration file configures the CM for its network operations and includes information such as the maximum number of CPE devices that are supported, the quality of service (QoS) options provided for the CM, and whether the CM should upgrade to a new software image.

The DOCSIS specification defines the format of the DOCSIS configuration files, which can be created by any number of tools. In addition to the other tools that Cisco provides for this purpose, the **cable config-file** command can be used to create the DOCSIS configuration files needed for your network. These configuration files are stored in the Flash memory on the Cisco CMTS router and can be automatically downloaded to the CM as needed.

The **cable config-file** command creates the DOCSIS configuration file if it does not already exist and then enters config-file configuration mode. You can then give one of the following subcommands to create the configuration file:

- **access-denied**
- **channel-id**
- **cpe max**
- **download**
- **frequency**

- **option**
- **privacy**
- **service-class**
- **snmp manager**
- **timestamp**

**Note**

When a DOCSIS shared secret is configured on the downstream interface (see the **cable shared-secret** command), the **cable config-file** command automatically inserts the appropriate MD5 Message Integrity Check (MIC) value at the end of the dynamically generated DOCSIS configuration file. You do not need to specify the DOCSIS shared secret string with the **cable config-file** command.

After using the **cable config-file** subcommands, enter the **exit** command to leave config-file mode and to save the configuration file in the Flash memory. After a configuration file is created, it also appears in the running-configuration file. To delete a configuration file and remove it from Flash memory, use the **no cable config-file** command.

To allow CMs to download the configuration files, you must also enable the router's onboard TFTP server, using the **tftp-server** configuration command. Unless you are running on a small lab network, you should also remove the default limit of 10 TFTP sessions by using the **service udp-small-serves max-servers no limit** command.

In addition, the following commands are also recommended:

- **cable time-server**—Enables the Cisco CMTS router to function as a time-of-day (ToD) server.
- **ip dhcp pool**—Configures the Cisco CMTS router as a DHCP server. Otherwise, you need an external DHCP server.
- **ip dhcp ping packets 0**—Improves the scalability of the Cisco CMTS router DHCP server.

**Note**

For complete information on DOCSIS configuration files, see Appendix C in the DOCSIS 1.1 Radio Frequency (RF) Interface Specification, available on the DOCSIS Cable Labs official web site at <http://www.cablemodem.com>

**Examples**

The following example shows two DOCSIS configuration files being configured. The first configuration file allows each CM to have up to four CPE devices and configures the QoS parameters for its traffic. The second configuration file denies network access to the CM and its CPE devices.

```
Router# configure terminal
Router(config)# cable config-file test.cm
Router(config-file)# cpe max 4
Router(config-file)# service-class 1 priority 2
Router(config-file)# service-class 1 max-upstream 128
Router(config-file)# service-class 1 max-downstream 1000
Router(config-file)# timestamp
Router(config-file)# exit
Router(config)# cable config-file denied.cm
Router(config-file)# access-denied
Router(config-file)# exit
Router(config)#
```

The following is a portion of a typical Cisco IOS configuration file that shows the above two DOCSIS configuration files, as well as a typical DHCP server configuration:

```

Router# show running-config
...
service udp-small-servers max-servers no-limit
!
cable time-server
!
cable config-file test.cm
  cpe max 4
  service-class 1 priority 2
  service-class 1 max-upstream 128
  service-class 1 max-downstream 1000
  timestamp
cable config-file disable.cm
  access-denied
!
ip dhcp pool modems-c3
  network 10.30.128.0 255.255.240.0
  bootfile test.cm
  next-server 10.30.128.1
  default-router 10.30.128.1
  option 7 ip 10.30.128.1
  option 4 ip 10.30.128.1
  option 2 hex 0000.0000
!
...

```

**Related Commands**

Command	Description
<b>cable config-file</b>	Creates a DOCSIS configuration file and enters configuration file mode.
<b>access-denied</b>	Disables access to the network.
<b>channel-id</b>	Specifies upstream channel ID.
<b>cpe max</b>	Specifies the maximum number of CPE devices allowed access.
<b>debug cable config-file</b>	Displays information about the DOCSIS configuration files that are generated by the internal DOCSIS configuration file editor.
<b>download</b>	Specifies the filename and server IP address for downloading a new software image.
<b>frequency</b>	Specifies the downstream frequency.
<b>option</b>	Specifies options for the configuration file that are not provided for by the other commands.
<b>privacy</b>	Specifies privacy options for baseline privacy images.
<b>service-class</b>	Specifies service class definitions for the configuration file.
<b>snmp manager</b>	Specifies Simple Network Management Protocol (SNMP) options.
<b>timestamp</b>	Enables time-stamp generation.
<b>show running-config</b>	Displays the current run-time configuration, which includes any configuration files that have been defined.
<b>show startup-config</b>	Displays the current saved configuration, which includes any configuration files that have been defined and saved.