



IP QoS Policy Parameters

This appendix describes the parameters, both required and optional, for IP QoS provisioning using the Cisco IP Solution Center (ISC) user interface.

This appendix contains the following sections and subsections:

- [Service Level IP QoS Parameters, page B-1](#)
 - [VoIP, Routing Protocol, and Management Service Classes, page B-2](#)
 - [Business Data and Best Effort Service Classes, page B-10](#)
 - [Adding a Data Service Class, page B-20](#)
 - [Deleting a Service Class, page B-20](#)
- [Link Level QoS Parameters, page B-21](#)
 - [Aggregated Traffic Shapers, page B-21](#)
 - [Link Efficiency Settings, page B-30](#)
 - [Interface-Based Aggregated Rate Limiters, page B-31](#)



Note

For information on service level Ethernet QoS parameters, see [Service Level Ethernet QoS Parameters, page C-1](#).

Service Level IP QoS Parameters

Service level IP QoS parameters see the entry fields on the service class windows and dialog boxes. These parameters include all entry fields in the VoIP, Management, Routing Protocol, Business-Data-1 and Best Effort service classes, and the traffic classification options for data service classes.

You must enter the bandwidth parameter for all service classes. Typically, a value of one percent is sufficient for Routing Protocol traffic. However, it is common for customers or providers to combine the Management and Routing Protocol into one service class policy. In this case, a larger percentage of bandwidth might be required.

Any class of service can be a *class-default* class of service. You can simply name the class of service as *class-default* and ISC will generate the same. Bandwidth is not mandatory for this class of service. Traffic classification is assumed to be *rest of traffic*.



Note

Class-default is a reserved class of service name in IOS and is created by IOS if ISC does not create one.

VoIP, Routing Protocol, and Management Service Classes

Each service class has a different set of entry fields. The VoIP, Routing Protocol, and Management service classes require similar parameters, and are combined in this section. [Figure B-1](#) displays these service classes.

For Business-Data-1 and Best Effort service class entry fields, see [Business Data and Best Effort Service Classes](#), [page B-10](#). The window you see depends on the service class being edited.

Figure B-1 Edit VoIP Service Class

The screenshot shows the 'Edit Service Class' window in the Cisco IP Solution Center. The window is titled 'Edit Service Class' and has a 'Service Attributes' section. The 'General' tab is selected, showing the following fields:

- Service Name:** VoIP
- Traffic Classification:**
 - Filter: match-any (selected), match-all
 - UDP Port Information: 16384, 16383
 - DSCP (0-63): (af41, af42, af43,...) or (34, 36, 38,...)
 - IP Precedence (0-7): (3, 4, 5,...)
- Marking:**
 - Enabled: ☒
 - DSCP: ef
 - IP Precedence: none
 - MPLS Experimental: none
- Rate Limiting:**
 - Enabled: ☒
 - Mean Rate (8000 - 10000000000 bps): 10000
 - Peak Information Rate (8000 - 10000000000 bps): 20000
 - Conformed Burst Size (1 - 14294967295 bytes): 5
 - Extended or Peak Burst Size (1 - 14294967295 bytes): 10000
 - Conform Action:
 - Type: transmit
 - Value: set-mpls-exp-transmit
 - Exceed Action:
 - Type: drop
 - Value: none
 - Violate Action:
 - Type: drop
 - Value: none
- Congestion Management:**
 - Bandwidth in Kbps: *
 - Bandwidth Percent (1 - 100%): ** 48 (relative selected, absolute unselected)
 - Queue Limit in Packets (1 - 262144 packets):
 - Queue Limit in Cells (1 - 262144 cells):

At the bottom of the window, there are 'OK' and 'Cancel' buttons. A note at the bottom states: "Note: * - Required Field. Note: ** - At least one bandwidth is required except for 'class-default' and VoIP class. 'Bandwidth in Kbps', 'Bandwidth Percent', and 'Bandwidth Remaining' are mutually exclusive."

[Table B-1](#) describes the entry fields for the VoIP, Routing Protocol, and Management service classes.

Table B-1 *Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management)*

Entry Field	Description
General	
Service Name	The name of the service class (VoIP, Routing Protocol, Management, or the name of your choice).
Traffic Classification (Routing Protocol service class only)	Traffic classification based on routing protocol. Choose from the list of routing protocols. Click Edit to activate one or more of the following routing protocols: RIP, BGP, OSPF, EIGRP. These options are further described in Editing the Routing Protocol Service Class , page B-7.
Traffic Classification	
Filters:	match-any: Traffic classification passes when any one of the following classifications is met. match-all: Traffic classification passes when all of the below classifications are met. This is restrictive; for example, combination of UDP Port and DSCP makes sense but not UDP Port and DSCP and IP_Precedence because an IP packet cannot have DSCP and IP_Precedence values at the same time.
UDP Port Information (VoIP service class only)	On routers supporting MQC these two fields see “lower bound UDP port” and “upper bound UDP port”. On non-MQC routers, the two fields see port range.
DSCP (VoIP and Management service classes only)	Traffic classification based on the packet’s DSCP marking.
IP Precedence (VoIP and Management service classes only)	Traffic classification based on the packet’s IP Precedence marking.
Management LAN Address (Management service class only)	Traffic classification based on management LAN address.
Marking (VoIP and Management service classes only)	
Enabled	Enable packet marking.
DSCP	Mark packets with a DSCP value. Note You can mark packets with either DSCP or IP Precedence, but not both.
IP Precedence	Mark packets with an IP Precedence value.
MPLS Experimental	Mark packets with an MPLS Experimental value. This field only appears if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.
Rate Limiting (VoIP service class only)	
Enabled	Enable rate-limiting
Mean Rate	The long-term average transmission rate.

Table B-1 *Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

Entry Field	Description
Peak Information Rate	Allows support for sustained excess rate.
Conformed Burst Size	<p>How large traffic bursts can be before some traffic exceeds the rate limit.</p> <p>Note IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.</p>
Extended or Peak Burst Size	How large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the conformed burst size and the extended burst size exceeds the rate limit with a probability that increases as the burst size increases. Configure extended burst by setting the extended burst value greater than the conformed burst value.
Conform Action–Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sets MPLS exp value and sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Conform Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Conform Action-Type.

Table B-1 *Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

Entry Field	Description
Exceed Action-Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sets MPLS exp value and sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Exceed Action-Value	The DSCP or IP Precedence or MPLS Exp value for the Exceed Action-Type.

Table B-1 *Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

Entry Field	Description
Violate Action–Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Violate Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Violate Action-Type.
Congestion Management	Routing Protocol and Management CoS can be configured with Bandwidth Remaining.
Bandwidth in kbps	The bandwidth in kbps (absolute bandwidth) for this service class. This field translates to Priority x and Bandwidth x commands where x is in kbps.

Table B-1 *Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

Entry Field	Description
Bandwidth Percent	<p>Percentage of bandwidth to dedicate to congestion management parameters. The range is 1-100 percent. Bandwidth is relative or absolute.</p> <ul style="list-style-type: none"> • Relative: This field specifies the bandwidth in percentage that you need to allocate to this CoS. This corresponds to relative bandwidth commands <i>Priority Percent x</i> and <i>Bandwidth Percent x</i> where <i>x</i> is the percentage specified. • Absolute: The percentage specified is used in conjunction with the circuit (or link) bandwidth to compute the absolute bandwidth (in kbps) that needs to be allocated to this CoS. Although this field translates to the same command as that for <i>Bandwidth in kbps</i>, it differs as follows: the absolute bandwidth varies with the circuit (or link) bandwidth. For example, if the percentage specified is 10 and if the policy is applied to a 64 kbps link, then absolute bandwidth allocated for this CoS is 6.4 kbps. If the same policy is applied to a 128 kbps link, then the absolute bandwidth allocated for this CoS is 12.8 kbps. Thus, the policy can be used on disparate bandwidth links.
Queue Limit in Packets	Limit the queue depth of the congesting traffic. The range is 1 to 262144 packets.
Queue Limit in Cells	Limit the queue depth of the congesting traffic. The range is 1 to 262144 cells.

**Note**

The process for marking packets with DSCP and IP Precedence bits is described in detail in the following document on Cisco.com:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Editing the Routing Protocol Service Class

The Routing Protocol service class provides you with a method of classifying traffic based on the routing protocols. This is the default method for traffic classification in ISC.

Use the Edit Traffic Classification window (Policies > Edit RP > Edit Traffic Classification) to change the list of protocols to use for the Routing Protocol service class (Figure B-2).

Figure B-2 *Edit Traffic Classification—Routing Protocol Service Class*

Traffic Classification Editor	
Traffic Classification based on Routing Protocols:	
Activate	Protocol Name
<input checked="" type="checkbox"/>	rip
<input checked="" type="checkbox"/>	ospf
<input checked="" type="checkbox"/>	bgp
<input checked="" type="checkbox"/>	eigrp

Select the routing protocols to use and click **OK**.

Editing the Management Service Class

This section describes how to edit the Management service class.

[Figure B-3](#) shows the Edit Service Class window for the Management service class.

Figure B-3 Edit Management Service Class

Edit Service Class

Service Attributes	
General	
Service Name *	Mgmt
Traffic Classification	
Filter:	<input checked="" type="radio"/> match-any <input type="radio"/> match-all
Management Subnet Address Mask (a.b.c.d/e):	0.0.0.0/0
DSCP (0-63):	(af41, af42, af43,...) or (34, 36, 38,...)
IP Precedence (0-7):	(3, 4, 5,...)
Marking	
Enabled:	<input checked="" type="checkbox"/>
DSCP:	af41
IP Precedence:	none
MPLS Experimental:	none
Congestion Management	
Bandwidth in Kbps *	
Bandwidth Percent (1 - 100%) **:	1 <input checked="" type="radio"/> relative <input type="radio"/> absolute
Bandwidth Remaining Percent (1 - 100%) **:	
Queue Limit in Packets (1 - 262144 packets):	
Queue Limit in Cells (1 - 262144 cells):	
<div>OK Cancel</div>	

Note: * - Required Field

Note: ** - At least one bandwidth is required except for "class-default" and VoIP class. "Bandwidth in Kbps", "Bandwidth Percent", and "Bandwidth Remaining" are mutually exclusive.

Use this window to specify QoS parameters for the Management service class. The following are required fields:

- Name—This field is prepopulated with the name Management. However, you can enter a new name.
- Management LAN Address—Specifies the management LAN address for traffic classification.
- DSCP—Specifies the traffic classification based on the packet's DSCP marking.
- IP Precedence—Specifies the traffic classification based on the packet's IP Precedence marking.
- Bandwidth—Specifies the bandwidth to dedicate to congestion management parameters. See [Table B-1](#) for an explanation of the bandwidth fields.

**Note**

The bandwidth in kbps is an absolute bandwidth for this service class. Bandwidth specified as a percentage of link bandwidth can be an absolute value or a relative value. The percentage is converted to an absolute value (if the percent command is not supported) when the QoS configlet is generated during service request deployment.

To add another Management service class, use the **Add Data CoS** button on the Edit QoS Policy window. See [Adding a Data Service Class, page B-20](#) for more information.

Business Data and Best Effort Service Classes

For the two data service classes, Business Data (Busin) and Best Effort (BE), the parameters are nearly identical. The entry field descriptions are combined in this section. The only difference between the two data service classes is the Traffic Classification parameter:

- Business Data classifies traffic using selected protocols, packet markings, or network addresses.
- Best Effort uses the traffic classification “All Traffic.”

For VoIP, Routing Protocol, and Management service class entry fields, see [VoIP, Routing Protocol, and Management Service Classes, page B-2](#).

[Figure B-4](#) shows the general information, marking, and shaping fields for the Business Data service class (Busin).

Figure B-4 *Edit Business Data Service Class*

Edit Service Class	
Service Attributes	
General	
Service Name *	Busin
Traffic Classification *	http, ftp, telnet, smtp, tftp Edit
Marking	
Enabled:	<input checked="" type="checkbox"/>
DSCP:	af41
IP Precedence	none
MPLS Experimental:	none
Shaping	
Enabled:	<input checked="" type="checkbox"/>
Shape:	Average
Rate (8000 - 10000000000 bps) *	100000
Rate Limiting	
Enabled:	<input checked="" type="checkbox"/>
Mean Rate (8000 - 10000000000 bps) *	100000
Peak Information Rate (8000 - 10000000000 bps):	200000
Conformed Burst Size (1 - 14294967295 bytes) *	
Extended or Peak Burst Size (1 - 14294967295 bytes) *	
Conform Action	
Type:	transmit
Value:	none
Exceed Action	
Type:	drop
Value:	none
Violate Action	
Type:	drop
Value:	none
Congestion Management	
Bandwidth in Kbps ** *	
Bandwidth Percent (1 - 100%) ** *	<input type="checkbox"/> relative <input checked="" type="radio"/> absolute
Bandwidth Remaining Percent (1 - 100%) ** *	
Queue Limit in Packets (1 - 262144 packets):	
Queue Limit in Cells (1 - 262144 cells): *	
Congestion Avoidance	
Enabled:	<input checked="" type="checkbox"/>
Drop based on:	dscp
Exponential Weighting Constant (1 - 16):	
Advanced Avoidance Options:	Edit
OK Cancel	

Note: * - Required Field

Note: ** - At least one bandwidth is required except for "class-default" and VoIP class. "Bandwidth in Kbps", "Bandwidth Percent", and "Bandwidth Remaining" are mutually exclusive.

138777

[Table B-2](#) describes the entry fields for the data service classes. The entry fields you see depend on which service class is being edited.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort)

Entry Field	Description
General	
Service Class	The name of the service class (Busin, BE, or the name of your choice).
Traffic Classification	<p>Traffic classification based on protocols.</p> <p>Choose from the list of protocols, or add another protocol. Click Edit to activate one or more of the following protocols: HTTP, FTP, Telnet, SMTP, TFTP.</p> <p>These options are further described in Traffic Classification, page B-16.</p>
Marking	
Enabled	Enable packet marking.
DSCP	<p>Mark packets with a DSCP value.</p> <p>Note You can mark packets with either DSCP or IP Precedence, but not both.</p>
IP Precedence	Mark packets with an IP Precedence value.
MPLS Experimental	Mark packets with an MPLS Experimental value. This field only appears if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.
Shaping	
Enabled	<p>Enable class-based traffic shaping parameters.</p> <p>To specify interface-based traffic shaping parameters, see Aggregated Traffic Shapers, page B-21.</p>
Shape	<p>Specify average or peak rate shaping.</p> <ul style="list-style-type: none"> Average rate shaping limits the transmission rate to the committed information rate (CIR). Peak rate shaping configures the router to send more traffic than the CIR. <p>Note ISC does NOT provision ATM shapers and class-based shapers at the same time. If you configure an ATM shaper, ISC automatically turns off the class-based shaper. This shape is for class-based shaper support when the ATM shaper is not configured.</p>
Rate	Committed information rate.
Rate Limiting	
Enabled	Enable rate-limiting
Mean Rate	The long-term average transmission rate.
Peak Information Rate	Allows support for sustained excess rate.

Table B-2 *Edit Service Class Entry Fields (Business Data and Best Effort) (continued)*

Entry Field	Description
Conformed Burst Size	<p>How large traffic bursts can be before some traffic exceeds the rate limit.</p> <p>Note IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.</p>
Extended or Peak Burst Size	<p>How large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the conformed burst size and the extended burst size exceeds the rate limit with a probability that increases as the burst size increases. Configure extended burst by setting the extended burst value greater than the conformed burst value.</p>
Conform Action–Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Conform Action–Value	<p>The DSCP or IP Precedence or MPLS Exp value for the Conform Action-Type.</p>

Table B-2 **Edit Service Class Entry Fields (Business Data and Best Effort) (continued)**

Entry Field	Description
Exceed Action–Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Exceed Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Exceed Action-Type.

Table B-2 *Edit Service Class Entry Fields (Business Data and Best Effort) (continued)*

Entry Field	Description
Violate Action–Type	<p>The action to take on packets that conform to the specified rate limit.</p> <p>Single Action</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. <p>Note If you select Set-dscp-transmit or Set-prec-transmit, you must specify the DSCP or IP Precedence in the Conform-Action Value field.</p> <p>Dual Action</p> <ul style="list-style-type: none"> • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. <p>Note The set-mpls fields only appear if you select the Mark MPLS Exp. check box under At Provider Ingress: on the first window of the policy creation.</p>
Violate Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Violate Action-Type.
Congestion Management	Routing Protocol and Management CoS can be configured with Bandwidth Remaining.
Bandwidth in kbps	The bandwidth in kbps (absolute bandwidth) for this service class. This field translates to Bandwidth x commands where x is in kbps.

Table B-2 *Edit Service Class Entry Fields (Business Data and Best Effort) (continued)*

Entry Field	Description
Bandwidth Percent	<p>Percentage of bandwidth to dedicate to congestion management parameters. The range is 1-100 percent. Bandwidth is relative or absolute.</p> <ul style="list-style-type: none"> Relative: This field specifies the bandwidth in percentage that you need to allocate to this CoS. This corresponds to relative bandwidth command Bandwidth Percent x where x is the percentage specified. Absolute: The percentage specified is used in conjunction with the circuit (or link) bandwidth to compute the absolute bandwidth (in kbps) that needs to be allocated to this CoS. Although this field translates to the same command as that for Bandwidth in kbps, it differs as follows: the absolute bandwidth varies with the circuit (or link) bandwidth. For example, if the percentage specified is 10 and if the policy is applied to a 64 kbps link, then absolute bandwidth allocated for this CoS is 6.4 kbps. If the same policy is applied to a 128 kbps link, then the absolute bandwidth allocated for this CoS is 12.8 kbps. Thus, the policy can be used on disparate bandwidth links.
Bandwidth Remaining Percent	The range is 1-100 percent.
Queue Limit in Packets	Limit the queue depth of the congesting traffic. The range is 1-262144 packets.
Queue Limit in Cells	Limit the queue depth of the congesting traffic. The range is 1-262144 cells.
Congestion Avoidance	
Enabled	Enable congestion avoidance.
Drop based on	Drops packets based on the IP Precedence or DSCP value.
Exponential Weighing Constant	The value used in the average queue size (weighted random early detection, or WRED) calculation. This value is used to determine the queue reserved for this service class.
Advanced Avoidance Options	Click Edit to add Advanced Avoidance Options. See Advanced Avoidance Options , page B-19.

Editing the Data Service Classes

This section describes how to change the traffic classification parameters for the data service classes and how to add advanced options for congestion avoidance.

Traffic Classification

Use the Traffic Classification window to set or change the traffic classification parameters. [Figure B-5](#) show the traffic classification settings for this service class. It includes some protocols that are enabled by default.

Figure B-5 Traffic Classification Editor—Business Data Service Class

Edit Traffic Classification

Traffic Classification Editor

Filter: ☒ match-any ☐ match-all

All Traffic ☐

Traffic Classification based on Protocols:

Enable	Protocol Name	Optional Port Information				Based on
		Type	Number	Range Begin	Range End	
<input checked="" type="checkbox"/>	http	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	Destination ▼
<input checked="" type="checkbox"/>	ftp	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	Destination ▼
<input checked="" type="checkbox"/>	telnet	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	Destination ▼
<input checked="" type="checkbox"/>	smtp	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	Destination ▼
<input checked="" type="checkbox"/>	tftp	UDP	<input type="text"/>	<input type="text"/>	<input type="text"/>	Destination ▼

Traffic Classification based on Packet Marking:

Marking	Value
DSCP (0-63):	<input type="text"/> (af41, af42, af43,...) or (34, 36, 38,...)
IP Precedence (0-7):	<input type="text"/> (3, 4, 5,...)

Traffic Classification based on Addresses:

Address Based On	Device Prefix Properties
Source:	<input type="text"/> (var1, var2,...)

138778

The entry fields are described in [Table B-3](#).

Table B-3 Traffic Classification Editor Entry Fields

Entry Field	Description
Filter:	<p>match-any: Traffic classification passes when any one of the following classifications is met.</p> <p>match-all: Traffic Classification passes when all of the conditions below are met. This is restrictive; for example, a combination of any one protocol and DSCP makes sense but not more than one protocol and DSCP and IP_PRECEDENCE since an IP packet cannot belong to more than one Protocol and cannot have DSCP and IP_PRECEDENCE values at the same time.</p>
All Traffic	Selects traffic classification based on all protocols.
Traffic Classification Based on Protocols	
Enable	Enables traffic classification for this protocol.

Table B-3 Traffic Classification Editor Entry Fields (continued)

Entry Field	Description
Port Type	TCP or UDP port (optional).
Port Number	The TCP or UDP port number to use for this protocol. (optional)
Port Range Begin	Specifies the beginning port number in a range of ports. (optional)
Port Range End	Specifies the end port number in a range of ports. (optional)
Based On	Traffic classification is based on the source or destination port for this protocol. (optional)
Add Protocol	Add another protocol to use for traffic classification.
NBAR	<p>NBAR (Network Based Application Recognition)</p> <p>On platforms running IOS that support NBAR based traffic classification, you can provide NBAR support such as:</p> <ul style="list-style-type: none"> match protocol <i>protocol name</i> where <i>protocol name</i> is citrix, cuseeme, for example. match protocol http url <i>url name</i> <p>To make use of this feature, enter the <i>protocol</i> or <i>url name</i> in the protocol name field. Do not edit the remaining fields for the protocol.</p>
Extended ACL	<p>Extended ACL (Access Control List)</p> <p>To create named ACLs such as:</p> <ul style="list-style-type: none"> permit <i>port_type</i> any any eq <i>port_number</i>, permit <i>port_type</i> any range <i>port_range_begin</i> <i>port_range_end</i> any <p>where <i>port_type</i> is UDP or TCP. Port information can be source-based or destination-based.</p> <p>To make use of this feature, leave the protocol name field blank.</p>
Traffic Classification Based on Packet Marking	
DSCP (0-63):	Selects traffic classification based on DSCP value.
IP Precedence (0-7):	Selects traffic classification based on IP Precedence value.
Traffic Classification Based on Addresses	
Source	Selects traffic classification based on source IP addresses. This is accomplished using variables defined using the Network Objects Manager. For more information, see the Traffic Classification, page 1-5 .

Advanced Avoidance Options

This section describes the advanced congestion avoidance parameters for the data service classes.

To add advanced congestion avoidance options:

- Step 1** From the Edit Service Class window for a data service class, enable congestion avoidance.
- Step 2** Click **Edit** next to the Advanced Avoidance Options field on the Edit Service Class window. The Avoidance List window appears ([Figure B-6](#)).

Figure B-6 Avoidance List

This window lists any available congestion avoidance options that have been configured, including the DSCP or IP Precedence value, the minimum and maximum threshold, and the mark probability.

From this window you can also Add, Edit, or Delete any congestion avoidance option.

- Step 3** Click **Edit** to add a new option. The Avoidance Edit window appears as shown in [Figure B-7](#).

Figure B-7 Avoidance Edit

Step 4 Enter the congestion avoidance attributes.

- DSCP or IP Precedence value—This value corresponds to the “Drop based on” value for this service class.
- Minimum and Maximum Threshold—When a packet arrives at a router, the following happens:
 - The average queue size is calculated.
 - If the average is less than the minimum queue threshold, the arriving packet is queued.
 - If the average is between the minimum queue threshold for a particular type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for the traffic.
 - If the average queue size is greater than the maximum threshold, the packet is dropped.
- Mark Probability—The fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if this value is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold.

Step 5 Click **OK** (twice) to return to the Edit Service Class window.

Adding a Data Service Class

If your QoS policy requires additional service classes, use the data service class template provided with ISC to add another management or data service class.

To add another service class, click **Add Data CoS** from the Edit QoS Policy window. Enter a name and the service class attributes. See [Table B-2](#) for a description of each field.

Deleting a Service Class

To delete an unwanted service class from your QoS policy, select the service class on the Edit QoS Policy window. Click **Delete**, confirm ([Figure B-8](#)), and click **OK**.

Figure B-8 Delete Service Class

Confirm Delete		
#	Name	Service Class
1.	MyCoS	DATA

Showing 1 - 1 of 1 record

Rows per page: 10

Go to page: 1 of 1

OK Cancel

Link Level QoS Parameters

Link level QoS parameters see QoS settings that are based on the CE-PE link (called IP link QoS settings). These interface-based parameters include aggregated traffic shaping, link efficiency settings, and interface-based rate limiting.

This section describes the link level QoS parameters for IP link QoS settings. Link level QoS parameters include all entry fields for the link QoS settings.

Aggregated Traffic Shapers

Aggregated traffic shaping allows you to control the traffic leaving an interface. In ISC, you can select an aggregated traffic shaper for each IP link.

To apply class-based traffic shaping parameters, see the [Editing the Data Service Classes, page B-16](#).

Aggregated traffic shapers are optional. ISC supports the following aggregated traffic shapers:

- Frame Relay (FR) Traffic Shaper
- FR Traffic Shaper (Non-MQC)
- Parent-level Class-based Shaper
- ATM Traffic Shaper (VBR-rt)
- ATM Traffic Shaper (VBR-nrt)
- ATM Traffic Shaper (CBR)
- ATM Traffic Shaper (ABR)

You set aggregated traffic shaping parameters from the IP Link QoS Settings Editor window by clicking the Aggregated Traffic Shaper link. This opens the Aggregated Traffic Shaper window ([Figure B-9](#)).

Figure B-9 Select Aggregated Traffic Shaper Type

The screenshot shows the IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The user is logged in as 'admin'. The main menu has tabs for Service Inventory, Service Design (selected), Monitoring, Diagnostics, and Administration. Under Service Design, there are sub-tabs for Policies, Templates, Protocols, Link QoS (selected), and Network Objects. The breadcrumb trail shows 'You Are Here: Service Design > Link QoS'. The page title is 'IP Link QoS Settings Editor'. The main content area is titled 'Aggregated Traffic Shaper' and contains two sections: 'CE Aggregated Traffic Shaper Type' and 'PE Aggregated Traffic Shaper Type'. Each section has a dropdown menu currently set to 'None' and a table with columns 'Attribute' and 'Value'. At the bottom of the form are 'OK' and 'Cancel' buttons. A note at the bottom states: 'Note: * - Required Field'. The Cisco Systems logo is in the top left corner.

Select one aggregated traffic shaper for the CE and one for the PE. [Table B-4](#) describes the aggregated traffic shaper types.

Table B-4 Aggregated Traffic Shaper Types

Shaper Type	Description
FR Traffic Shaper	Frame Relay Traffic Shaper—A version of a class-based parent level shaper that operates only in distributed mode on versatile interface processor-based routers, such as the Cisco 7500 series platforms.
FR Traffic Shaper (Non-MQC)	Frame Relay Traffic Shaper—This shaper operates on the Cisco 7200 series and low-end routers.
Parent-level Class-based Shaper	Used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces or subinterfaces.
ATM Traffic Shaper (VBR-rt)	Variable bit rate-real time—Intended for real-time applications, such as compressed voice over IP and video-conferencing, that require tightly constrained delays (cell transfer delay or cell delay variation).
ATM Traffic Shaper (VBR-nrt)	Variable bit rate-non real time—Follows a leaky bucket or token bucket algorithm.

Table B-4 Aggregated Traffic Shaper Types (continued)

Shaper Type	Description
ATM Traffic Shaper (CBR)	Constant bit rate—Designed for ATM virtual circuits (VCs) that need a static amount of bandwidth that is continuously available for the duration of the active connection.
ATM Traffic Shaper (ABR)	Available bit rate—Configures a router to transmit at a rate that varies with the amount of bandwidth available in the network or along the end-to-end transmission path.

The following sections describe the windows and entry fields for the aggregated shaper types. You see a different dialog box depending on which of the following you choose.

FR Traffic Shaper

The FR Traffic Shaper (Figure B-10) is a version of a class-based parent level shaper that operates only in distributed mode on versatile interface processor-based routers, such as the Cisco 7500 series platforms.

Figure B-10 FR Traffic Shaper

Aggregated Traffic Shaper

CE Aggregated traffic shaper type: FR Traffic Shaper

Attribute	Value
Class-based Shaper *	AVERAGE
Rate in bps *: (8000-154400000)	1000000
Queue limit in packets/cells: (1-65535)	

PE Aggregated traffic shaper type: FR Traffic Shaper

Attribute	Value
Class-based Shaper *	AVERAGE
Rate in bps *: (8000-154400000)	1000000
Queue limit in packets/cells: (1-65535)	

OK Cancel

104201

The entry fields are described in Table B-5.

Table B-5 *Frame Relay Traffic Shaper Entry Fields*

Attribute	Description
Class-based Shaper	Choose average or peak. Peak rate shaping allows you to make better use of available bandwidth because it allows you to send more data than the CIR, if the bandwidth is available.
Rate in bps	This field might be prepopulated with the bandwidth value from the IP Link QoS Settings Editor window. The range is 8000 to 1554400000.
Queue limit in packets/cells	The maximum number of packets or cells allowed in the priority queue. The range is 1 to 65535.

FR Traffic Shaper (Non-MQC)

The Non-MQC Frame Relay traffic shaper (FRTS) uses queues on a Frame Relay network to limit surges that can cause congestion. Data is buffered and then sent into the network in regulated amounts to ensure that the traffic will fit within the promised traffic envelope for the particular connection.

Use FRTS Non-MQC (Figure B-11) on all ISC-supported low-end router platforms (Cisco 7200 series and below).

Figure B-11 *FRTS Non-MQC*

Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: FR Traffic Shaper (Non-MQC)

Attribute	Value
CIR in bps: (1-45000000)	1000000
Min. CIR in bps: (1000-45000000)	
Committed Burst Size in bits: (300-16000000)	
Excess Burst Size in bits: (0-16000000)	

PE Aggregated traffic shaper type*: FR Traffic Shaper (Non-MQC)

Attribute	Value
CIR in bps: (1-45000000)	1000000
Min. CIR in bps: (1000-45000000)	
Committed Burst Size in bits: (300-16000000)	
Excess Burst Size in bits: (0-16000000)	

OK Cancel

104202

The entry fields are described in Table B-6.

Table B-6 *Frame Relay Traffic Shaper (Non-MQC) Entry Fields*

Attribute	Description
CIR in bps	This field might be prepopulated with the bandwidth value from the IP Link QoS Settings Editor window. The range is 1 to 45000000.
Min. CIR in bps	The range is 1000 to 45000000.
Committed Burst Size in bits	The range is 300 to 16000000.
Excess Burst Size in bits	The range is 0 to 16000000.

**Note**

The CIR value is a required field even though it is not listed on the GUI as required.

Parent-level Class-Based Traffic Shaper

Parent-level class-based traffic shapers are used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces or subinterfaces.

The parent-level class-based shaper dialog box and entry fields are the same as the FR Traffic Shaper. See [FR Traffic Shaper, page B-23](#).

ATM Traffic Shaper (VBR-rt)

VBR-rt is intended for real-time applications, (for example, those requiring tightly constrained delay and delay variation, like voice and video applications). VBR-rt connections are characterized in terms of a peak cell Rate (PCR), sustainable cell rate (SCR), and maximum burst size (MBS). See [Figure B-12](#).

Figure B-12 ATM Traffic Shaper VBR-rt

Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-rt)

Attribute	Value
Peak Cell Rate in kbps:	128
Average Cell Rate in kbps*:	
Maximum Burst Size in cells:	

PE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-rt)

Attribute	Value
Peak Cell Rate in kbps:	128
Average Cell Rate in kbps*:	
Maximum Burst Size in cells:	

OK Cancel

97058

The entry fields are described in [Table B-7](#).

Table B-7 Frame Relay Traffic Shaper VBR-rt Entry Fields

Attribute	Description
Peak Cell Rate in kbps	The maximum rate at which you expect to transmit data, voice and video.
Average Cell Rate in kbps	The sustained rate at which you expect to transmit data, voice and video. SCR is the true bandwidth of a VC and not the long-term average traffic rate
Maximum Burst Size in cells	The amount of time or the duration at which the router sends at PCR.

**Tip**

Configure PCR and MBS parameters for reducing latency, not increasing bandwidth.

ATM Traffic Shaper (VBR-nrt)

This section describes ATM traffic shaping using variable bit rate non real-time.

VBR-nrt implementations follow a leaky bucket or token bucket algorithm. An ATM VC requires a token in the bucket to transmit a cell. The algorithm replenishes tokens in the bucket at the rate of the sustained cell rate (SCR). If a source is idle and does not transmit for a period of time, tokens accumulate in the bucket. An ATM VC can use the accumulated tokens to burst at the rate of peak cell rate (PCR) until the bucket is empty, at which point tokens are replenished at the rate of SCR. See [Figure B-13](#).

Figure B-13 *ATM Traffic Shaper VBR-nrt*

Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-nrt)

Attribute	Value
Peak Cell Rate in kbps:	128
Sustained Cell Rate in kbps*:	
Maximum Burst Size in cells:	

PE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-nrt)

Attribute	Value
Peak Cell Rate in kbps:	128
Sustained Cell Rate in kbps*:	
Maximum Burst Size in cells:	

OK Cancel

97067

The entry fields are described in [Table B-8](#).

Table B-8 *ATM Traffic Shaper VBR-nrt Entry Fields*

Attribute	Description
Peak Cell Rate in kbps	The maximum rate at which you expect to transmit data, voice and video.
Sustained Cell Rate in kbps	The sustained rate at which you expect to transmit data, voice and video. SCR is the true bandwidth of a VC and not the long-term average traffic rate.
Maximum Burst Size in cells	The amount of time or the duration at which the router sends at PCR.

**Tip**

Configure PCR and MBS parameters for reducing latency, not increasing bandwidth.

The values for this dialog box can be calculated using the following formulas:

- $(2 \times \text{maximum number of calls}) \times 16 \text{ Kbps} = \text{peak cell rate (PCR)}$
- $(1 \times \text{maximum number of calls}) \times 16 \text{ Kbps} = \text{sustained cell rate (SCR)}$
- $(4 \times \text{maximum number of calls}) = \text{burst size in cells (MBS)}$



Tip

Both real-time and non-real-time VBR services are characterized by PCR, SCR and MBS or burst tolerance (BT). VBR-rt makes better use of bandwidth if the traffic tends to burst, since the ATM interface reserves bandwidth equal to the SCR only.

ATM Traffic Shaper (CBR)

The CBR traffic shaper is used by connections that require static amount of bandwidth that is continuously available during the connection lifetime. This amount of bandwidth is characterized by a Peak Cell Rate (PCR) value. Use CBR traffic shapers for real-time traffic. See [Figure B-14](#).

Figure B-14 ATM Traffic Shaper CBR

Aggregated Traffic Shaper	
CE Aggregated traffic shaper type *: ATM Traffic Shaper(CBR)	
Attribute	Value
Peak Cell Rate in kbps:	128
PE Aggregated traffic shaper type *: ATM Traffic Shaper(CBR)	
Attribute	Value
Peak Cell Rate in kbps:	128
<div>OK Cancel</div>	

The Peak Cell Rate is the maximum rate at which you expect to transmit data, voice and video.

ATM Traffic Shaper (ABR)

ABR traffic shaping configures a router to transmit at a rate that varies with the amount of bandwidth available in the network or along the end-to-end transmission path. When the network is congested and other source devices are transmitting, there is little available or leftover bandwidth. However, when the network is not congested, bandwidth is available for use by other active devices. ABR allows end-system devices like routers to take advantage of this extra bandwidth and increase their transmission rates. See [Figure B-15](#).

Figure B-15 ATM Traffic Shaper ABR

Aggregated Traffic Shaper

CE Aggregated traffic shaper type : ATM Traffic Shaper(ABR)

Attribute	Value
Peak Cell Rate in kbps:	128
Minimum Cell Rate in kbps :	
Enable Rate Factors:	<input type="checkbox"/>
Rate Factor 1 :	
Rate Factor 2 :	

PE Aggregated traffic shaper type : ATM Traffic Shaper(ABR)

Attribute	Value
Peak Cell Rate in kbps:	128
Minimum Cell Rate in kbps :	
Enable Rate Factors:	<input type="checkbox"/>
Rate Factor 1 :	
Rate Factor 2 :	

OK Cancel

97056

The entry fields are described in [Table B-9](#).

Table B-9 ATM Traffic Shaper ABR Entry Fields

Attribute	Description
Peak Cell Rate in kbps	Maximum cell rate at which the source can transmit.
Minimum Cell Rate in kbps	Rate at which a source router can always send.
Enable Rate Factors	Enable rate factors.
Rate Factor 1	Rate Factor 1 is the inverse of RIF. The rate increase factor (RIF). The amount by which the transmission rate increases after the source interface receives a resource management (RM) cell with no increase (NI) and congestion indication (CI) set to zero. The value is specified as a (negative) power of two (2x). The range is between 1/32768 and 1.
Rate Factor 2	Rate Factor 2 is the inverse of RDF. The rate decrease factor (RDF). The amount by which the transmission rate decreases after the source interface receives an RM cell with the CI bit set to one. The value is specified as a power of two (2x). The range is between 1 and 1/32768.

Link Efficiency Settings

Link efficiency settings are based on the CE-PE link itself and are used to minimize serialization delay on the link. ISC uses methods of fragmentation and compression to minimize this delay.

ISC supports the following link efficiency settings:

- LFI on Frame Relay (FRF.12)—Supports the transport of real-time voice and data traffic on Frame Relay virtual circuits (VCs) without causing excessive delay to the real-time traffic.
- LFI on MLPPP—Multilink PPP (MLPPP) provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.

Figure B-16 shows the IP Link QoS Settings Editor window.

Figure B-16 Link Efficiency Settings

Table B-10 describes the entry fields for the Link Efficiency Settings window.

Table B-10 Link Efficiency Settings Entry Fields

Entry fields	Description
LFI on Frame Relay (FRF.12)	Enables LFI settings on Frame Relay interfaces.
FRF.12 fragmentation size in bytes.	The range is 16 to 1600 bytes. If you enable this LFI setting, the Cisco IOS default setting can be used, or you can enter a value manually.
LFI on MLPPP	Enables LFI settings for Multi link Point-to-Point interfaces. You must enter the PPP multilink fragment delay.
PPP multilink fragment delay in ms	The amount of delay between packet fragments. The range is 1 to 1000 ms.

Interface-Based Aggregated Rate Limiters

Interface-based aggregated rate limiters allow you to control the maximum rate of traffic sent or received on an interface for the CE-PE link. You can also specify traffic handling policies for when the traffic conforms or exceeds the specified rate limit.

Aggregate rate limits match all packets or a specified subset of packets on an interface or subinterface. To specify class-based rate limiting parameters, see the [Creating the Service Level IP QoS Policy, page 3-9](#).

ISC supports the following interface-based rate limiter parameters:

- Traffic classification
- Direction
- Mean rate
- Burst sizes (conformed and extended)
- Conform and exceed actions

Figure B-17 shows the Interface-based Aggregated Rate Limiter window.

Figure B-17 **Interface Based Aggregated Limiter**

IP Link QoS Settings Editor

Interface-based Aggregated Rate Limiter

Traffic Classification *: none Edit

Direction *: OUTPUT

Mean Rate in bps *: 1000000000 (16000 - 100000000000 bps)

Conformed Burst Size *: (1500 - 512000000 Bytes)

Extended Burst Size *: (2000 - 1024000000 Bytes)

Conform-Action *: transmit

Exceed-Action *: drop

OK Cancel

Note: * - Required Field

138784

Table B-11 describes the entry fields for the Interface-based Aggregated Rate Limiter window. All fields in this window are required.

Table B-11 **Interface-based Aggregated Rate Limiter Entry Fields**

Entry field	Description
Traffic Classification	Specifies the method for classifying traffic. Click Edit to access the Traffic Classification Editor. For more information, see Traffic Classification, page B-16 .
Direction	The direction of traffic to apply rate limiting parameters to. Choose from Input or Output.

Table B-11 *Interface-based Aggregated Rate Limiter Entry Fields (continued)*

Entry field	Description
Mean rate in bps	The range is 8000 to 2000000000 bps.
Conformed burst size in bytes	<p>The range is 1000 to 512000000 bytes.</p> <p>Note IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.</p>
Extended burst size in bytes	The range is 2000 to 1024000000 bytes.
Conform-Action	<p>Specifies how to handle packets that conform to the configured rate limit.</p> <ul style="list-style-type: none"> • Transmit—Sends the packet. • Drop—Drops the packet. <p>Note If you select any of the following, you must specify the DSCP, IP, or MPLS Precedence value in the adjacent drop-down menus.</p> <ul style="list-style-type: none"> • Set-dscp-transmit—Sets the DSCP value (0-63) and transmits the packet. • Set-prec-transmit—Sets the IP precedence value (0 to 7) and sends the packet. • Set-mpls-exp-transmit—Sets the MPLS value (0 to 7) and transmits the packet. • Set-dscp-continue—Sets the DSCP value (0 to 63) and transmits the packet. • Set-prec-continue—Sets the IP precedence (0 to 7) value and sends the packet. • Set-mpls-exp-continue—Sets the MPLS value (0-7) and sends the packet.
Exceed-Action	Specifies how to handle packets that exceed the configured rate limit. The options are the same as Conform-Action.