

policy-map

To create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** global configuration command. To delete a policy map, use the **no** form of this command.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description	<i>policy-map-name</i>	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
--------------------	------------------------	--

Defaults	This command has no default behavior or values.
----------	---

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you can configure policies for classes whose match criteria are defined in a class map. Entering the **policy-map** command enables QoS policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. You use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, no policy map can contain more than 64 class policies.

A single policy map can be attached to multiple interfaces concurrently. When you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies comprising the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, CBWFQ is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Examples

The following example creates a policy map called policy1 and configures two class policies included in that policy map. The class policy called class1 specifies policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-map class1 and defines its match criteria:
class-map class1
  match access-group 136
```

```
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
```

```
class class1
  bandwidth 2000
  queue-limit 40

class class-default
  fair-queue 16
  queue-limit 20
```

The following example creates a policy map called policy9 and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called **class-default** to which packets that do not satisfy configured match criteria are directed.

```
policy-map policy9

class acl136
  bandwidth 2000
  queue-limit 40

class ethernet101
  bandwidth 3000
  random-detect exponential-weighting-constant 10

class class-default
  fair-queue 10
  queue-limit 20
```

Related Commands

Related Commands

Command	Description
bandwidth (policy-map-class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.

precedence (VC bundle)

To configure precedence levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **precedence** vc-class configuration command. To remove the precedence levels from the VC class, use the **no** form of this command.

To configure the precedence levels for a VC member of a bundle, use the **precedence** bundle-vc configuration command. To remove the precedence levels from the VC, use the **no** form of this command.

precedence [**other** | *range*]

no precedence

Syntax Description

other	(Optional) Any precedence levels in the range from 0 to 7 that are not explicitly configured.
<i>range</i>	(Optional) A single precedence level specified as a number, or a range of precedence levels, specified as a hyphenated range.

Defaults

Defaults to **other**, that is, any precedence levels in the range from 0 to 7 that are not explicitly configured.

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T. This command was extended to configure precedence levels for a VC member of a bundle.

Usage Guidelines

Assignment of precedence levels to VC bundle members allows you to create differentiated service because you can distribute the IP Precedence levels over the different VC bundle members. You can map a single precedence level or a range of levels to each discrete VC in the bundle, thereby enabling VCs in the bundle to carry packets marked with different precedence levels. Alternatively, you can configure a VC with the **precedence other** command to indicate that it can carry traffic marked with precedence levels not specifically configured for it. Only one VC in the bundle can be configured with the **precedence other** command to carry all precedence levels not specified. This VC is considered the default one.

To use this command in vc-class configuration mode, enter the **vc-class atm** global configuration command before you enter this command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command to configure an individual bundle member in bundle-vc configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then, use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-vc configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures a class called control-class that includes a **precedence** command that, when applied to a bundle, configures all VC members of that bundle to carry IP Precedence level 7 traffic. Note, however, that VC members of that bundle can be individually configured with the **precedence** command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
  precedence 7
```

The following example configures permanent virtual circuit (PVC) 401 (with the name of control-class) to carry traffic with IP Precedence levels in the range of 4-2, overriding the precedence level mapping set for the VC through vc-class configuration:

```
pvc-bundle control-class 401
  precedence 4-2
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

precedence (WRED group)

To configure a Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) group for a particular IP Precedence, use the **precedence** random-detect-group configuration command. To return the values for each IP Precedence for the group to the default values, use the **no** form of this command.

precedence *precedence min-threshold max-threshold mark-probability-denominator*

no precedence *precedence min-threshold max-threshold mark-probability-denominator*

Syntax Description		
<i>precedence</i>		IP Precedence number. Values range from 0 to 7.
<i>min-threshold</i>		Minimum threshold in number of packets. Value range from 1 to 4096. When the average queue length reaches this number, WRED or DWRED begins to drop packets with the specified IP Precedence.
<i>max-threshold</i>		Maximum threshold in number of packets. The value range is <i>min-threshold</i> to 4096. When the average queue length exceeds this number, WRED or DWRED drops all packets with the specified IP Precedence.
<i>mark-probability-denominator</i>		Denominator for the fraction of packets dropped when the average queue depth is <i>max-threshold</i> . For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the <i>max-threshold</i> . The value is 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the <i>max-threshold</i> .

Defaults

For all IP Precedences, the *mark-probability-denominator* argument is 10, and the *max-threshold* argument is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* argument depends on the IP Precedence. The *min-threshold* argument for IP Precedence 0 corresponds to half of the *max-threshold* argument. The values for the remaining IP Precedences fall between half the *max-threshold* argument and the *max-threshold* argument at evenly spaced intervals. See [Table 9](#) in the “Usage Guidelines” section of this command for a list of the default minimum value for each IP Precedence.

Command Modes

Random-detect-group configuration

Command History

Release	Modification
11.1(22)CC	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP).

If used, this command is issued after the **random-detect-group** command.

When you configure the **random-detect group** command on an interface, packets are given preferential treatment based on the IP Precedence of the packet. Use the **precedence** command to adjust the treatment for different IP Precedences.

If you want WRED or DWRED to ignore the IP Precedence when determining which packets to drop, enter this command with the same parameters for each IP Precedence. Remember to use reasonable values for the minimum and maximum thresholds.

**Note**

The default WRED or DWRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

Table 9 lists the default minimum value for each IP Precedence.

Table 9 *Default WRED Minimum Threshold Values*

IP Precedence	Minimum Threshold Value (Fraction of Maximum Threshold Value)
0	8/16
1	9/16
2	10/16
3	11/16
4	12/16
5	13/16
6	14/16
7	15/16

Examples

The following example specifies parameters for the WRED parameter group called sanjose for the different IP Precedences:

```
random-detect-group sanjose
  precedence 0 32 256 100
  precedence 1 64 256 100
  precedence 2 96 256 100
  precedence 3 128 256 100
  precedence 4 160 256 100
  precedence 5 192 256 100
  precedence 6 224 256 100
  precedence 7 256 256 100
```

Related Commands	Command	Description
	exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
	random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
	random-detect-group	Defines the WRED or DWRED parameter group.
	random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
	show queueing	Lists all or selected configured queueing strategies.
	show queueing interface	Displays the queueing statistics of an interface or VC.

priority

To give priority to a class of traffic belonging to a policy map, use the **priority** policy-map class configuration command. To remove a previously specified priority specified for a class, use the **no** form of this command.

priority *bandwidth-kbps* [*burst*]

no priority *bandwidth-kbps* [*burst*]

Syntax Description

<i>bandwidth-kbps</i>	Guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved.
<i>burst</i>	(Optional) Specifies the burst size, in bytes. The range of the burst is 32 to 2,000,000 bytes.

Defaults

This command has no default behavior or values.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(5)XE5	This command was introduced for the Versatile Interface Processor (VIP) as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.
12.0(9)S	This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.
12.1(2)E	The <i>burst</i> argument was added.
12.1(3)T	The <i>burst</i> argument was added.
12.1(5)T	This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.

Usage Guidelines

This command configures low latency queueing (LLQ), providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The **priority** command allows you to set up classes based on a variety of criteria (not just User Datagram Ports (UDP) ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, **ip rtp priority**, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The *burst* argument is used to specify the burst size and, therefore, configure the network to accommodate temporary bursts of traffic. The default *burst* value, which is computed as 200 milliseconds of traffic at the configured *bandwidth* rate, is used when the *burst* argument is not specified.

The **bandwidth** and **priority** commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map, however.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

Remember the following guidelines when using the **priority** command:

- Layer 2 encapsulations are accounted for in the amount of bandwidth specified with the **priority** command. However, care must be taken to configure a bandwidth that has room for cell tax overhead and possible jitter introduced by the routers in the voice path.
- The **priority** command can be used for Voice over IP (VoIP) on serial links, Frame Relay links, and ATM PVCs.
- The **priority** command cannot be used in conjunction with other policy-map class configuration command, such as the **random-detect**, **queue-limit**, and **bandwidth** commands.
- The **priority** command can be configured in multiple classes, but it should only be used for voice-like, constant bit rate (CBR) traffic.
- Configuring the **priority** command in multiple classes provides the ability to police the priority classes individually. For an example, see the following configuration:

```
policy-map policy1
  class voice1
    priority 24
  class voice2
    priority 48
  class data
    bandwidth 20
```

In this example, voice1 and voice2 classes of traffic go into the high priority queue and get priority queueing over data traffic. However, voice1 traffic will be rate-limited to 24 kbps and voice2 traffic will be rate-limited to 48 kbps.

Examples

The following example configures PQ with a guaranteed bandwidth of 50 kbps and a one-time allowable burst size of 60 bytes for the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

In the following example, 10 percent of the available bandwidth is reserved for the class called voice on interfaces that have attached the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

Related Commands	Command	Description
	ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
	ip rtp reserve	Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.
	max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
	show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.

priority-group

To assign the specified priority list to an interface, use the **priority-group** interface configuration command. To remove the specified priority group assignment, use the **no** form of this command.

priority-group *list-number*

no priority-group *list-number*

Syntax Description	<i>list-number</i>	Priority list number assigned to the interface. Any number from 1 to 16.
---------------------------	--------------------	--

Defaults	This command is disabled by default.
-----------------	--------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Only one list can be assigned per interface. Priority output queueing provides a mechanism to prioritize packets sent on an interface.
	Use the show queueing and show interfaces commands to display the current status of the output queues.

Examples	The following example causes packets for transmission on serial interface 0 to be classified by priority list 1:
-----------------	--

```
interface serial 0
 priority-group 1
```

The following example shows how to establish queueing priorities based on the address of the serial link on a serial tunnel (STUN) connection. Note that you must use the **priority-group** interface configuration command to assign a priority group to an output interface.

```
stun peer-name 131.108.254.6
stun protocol-group 1 sdlc
!
interface serial 0
! Disable the ip address for interface serial 0:
no ip address
! Enable the interface for STUN:
encapsulation stun
!
stun group 2
stun route address 10 tcp 131.108.254.8 local-ack priority
!
```

```

! Assign priority group 1 to the input side of interface serial 0:
priority-group 1
! Assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7:
priority-list 1 stun low address 2 A7

```

Related Commands

Command	Description
locaddr-priority-list	Maps LUs to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list protocol ip tcp	Establishes BSTUN or STUN queueing priorities based on the TCP port.
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

priority-list default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-list default** global configuration command. To return to the default or assign **normal** as the default, use the **no** form of this command.

priority-list *list-number* **default** { **high** | **medium** | **normal** | **low** }

no priority-list *list-number* **default**

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
high medium normal low	Priority queue level. The normal queue is used if you use the no form of this command.

Defaults

This command is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Examples

The following example sets the priority queue for those packets that do not match any other rule in the priority list to a low priority:

```
priority-list 1 default low
```

Related Commands	Command	Description
	priority-group	Assigns the specified priority list to an interface.
	priority-list interface	Establishes queueing priorities on packets entering from a given interface.
	priority-list protocol	Establishes queueing priorities based on the protocol type.
	priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

priority-list interface

To establish queueing priorities on packets entering from a given interface, use the **priority-list interface** global configuration command. To remove an entry from the list, use the **no** form of this command with the appropriate arguments.

priority-list *list-number* **interface** *interface-type* *interface-number* { **high** | **medium** | **normal** | **low** }

no priority-list *list-number* **interface** *interface-type* *interface-number* { **high** | **medium** | **normal** | **low** }

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>interface-type</i>	The type of the interface.
<i>interface-number</i>	The number of the interface.
high medium normal low	Priority queue level.

Defaults

No queueing priorities are established by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Examples

The following example assigns a list entering on serial interface 0 to a medium priority queue level:

```
priority-list 3 interface serial 0 medium
```



Note

This command defines a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group** command.

Related Commands	Command	Description
	priority-group	Assigns the specified priority list to an interface.
	priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
	priority-list protocol	Establishes queueing priorities based on the protocol type.
	priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

priority-list protocol

To establish queueing priorities based upon the protocol type, use the **priority-list protocol** global configuration command. To remove a priority list entry assigned by protocol type, use the **no** form of this command with the appropriate arguments.

priority-list *list-number* **protocol** *protocol-name* {**high** | **medium** | **normal** | **low**} *queue-keyword* *keyword-value*

no priority-list *list-number* **protocol** [*protocol-name* {**high** | **medium** | **normal** | **low**} *queue-keyword* *keyword-value*]

Syntax Description	<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
	<i>protocol-name</i>	Protocol type: aarp , apollo , appletalk , arp , bridge (transparent), clns , clns_es , clns_is , compressedtcp , cmns , decnet , decnet_node , decnet_router-l1 , decnet_router-l2 , dls , ip , ipx , pad , rsrb , stun , vines , xns , and x25 .
	high medium normal low	Priority queue level.
	<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are fragments , gt , list , lt , tcp , and udp . For more information about keywords and values, see Table 10 in the “Usage Guidelines” section of this command.

Defaults No queueing priorities are established.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines When you use multiple rules for a single protocol, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

The **decnet_router-l1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

The **dls**, **rsrb**, and **stun** keywords refer only to direct encapsulation.

Use [Table 10](#), [Table 11](#), and [Table 12](#) to configure the queueing priorities for your system.

Table 10 Protocol Priority Queue Keywords and Values




Option	Description
fragments	<p>Assigns the priority level defined to fragmented IP packets (for use with IP only). More specifically, this command matches IP packets whose fragment offset field is nonzero. The initial fragment of a fragmented IP packet has a fragment offset of zero, so such packets are not matched by this command.</p> <p> Note Packets with a nonzero fragment offset do not contain TCP or User Datagram Protocol (UDP) headers, so other instances of this command that use the tcp or udp keyword will always fail to match such packets.</p>
gt <i>byte-count</i>	<p>Specifies a greater-than count. The priority level assigned goes into effect when a packet size exceeds the value entered for the <i>byte-count</i> argument.</p> <p> Note The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.</p>
list <i>list-number</i>	<p>Assigns traffic priorities according to a specified list when used with AppleTalk, bridging, IP, IPX, VINES, or XNS. The <i>list-number</i> argument is the access list number as specified by the access-list global configuration command for the specified <i>protocol-name</i>. For example, if the protocol is AppleTalk, <i>list-number</i> should be a valid AppleTalk access list number.</p>
lt <i>byte-count</i>	<p>Specifies a less-than count. The priority level assigned goes into effect when a packet size is less than the value entered for the <i>byte-count</i> argument.</p> <p> Note The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.</p>
tcp <i>port</i>	<p>Assigns the priority level defined to TCP segments originating from or destined to a specified port (for use with IP only). Table 11 lists common TCP services and their port numbers.</p>
udp <i>port</i>	<p>Assigns the priority level defined to UDP packets originating from or destined to a specified port (for use with IP only). Table 12 lists common UDP services and their port numbers.</p>

Table 11 Common TCP Services and Their Port Numbers

Service	Port
FTP data	20
FTP	21

Table 11 Common TCP Services and Their Port Numbers (continued)

Service	Port
Simple Mail Transfer Protocol (SMTP)	25
Telnet	23

Table 12 Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111
SNMP	161
TFTP	69

**Note**

Table 11 and Table 12 include some of the more common TCP and UDP port numbers. However, you can specify any port number to be prioritized; you are not limited to those listed.

For some protocols, such as TFTP and FTP, only the initial request uses port 69. Subsequent packets use a randomly chosen port number. For these types of protocols, the use of port numbers fails to be an effective method to manage queued traffic.

Examples

The following example assigns 1 as the arbitrary priority list number, specifies DECnet as the protocol type, and assigns a high-priority level to the DECnet packets sent on this interface:

```
priority-list 1 protocol decnet high
```

The following example assigns a medium-priority level to every DECnet packet with a size greater than 200 bytes:

```
priority-list 2 protocol decnet medium gt 200
```

The following example assigns a medium-priority level to every DECnet packet with a size less than 200 bytes:

```
priority-list 4 protocol decnet medium lt 200
```

The following example assigns a high-priority level to traffic that matches IP access list 10:

```
priority-list 1 protocol ip high list 10
```

The following example assigns a medium-priority level to Telnet packets:

```
priority-list 4 protocol ip medium tcp 23
```

The following example assigns a medium-priority level to UDP DNS packets:

```
priority-list 4 protocol ip medium udp 53
```

The following example assigns a high-priority level to traffic that matches Ethernet type code access list 201:

```
priority-list 1 protocol bridge high list 201
```

The following example assigns a high-priority level to data-link switching plus (DLSw+) traffic with TCP encapsulation:

```
priority-list 1 protocol ip high tcp 2065
```

The following example assigns a high-priority level to DLSw+ traffic with direct encapsulation:

```
priority-list 1 protocol dls w high
```


Note

This command defines a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group** command.

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

priority-list queue-limit

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-list queue-limit** global configuration command. To select the normal queue, use the **no** form of this command.

priority-list *list-number* **queue-limit** [*high-limit* [*medium-limit* [*normal-limit* [*low-limit*]]]]

no priority-list *list-number* **queue-limit**

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>high-limit</i>	(Optional) Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue.
<i>medium-limit</i>	
<i>normal-limit</i>	For default values for these arguments, see Table 13.
<i>low-limit</i>	

Defaults

This command is not enabled by default.

See [Table 13](#) in the “Usage Guidelines” section of this command for a list of the default queue limit arguments.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If a priority queue overflows, excess packets are discarded and messages can be sent, if appropriate, for the protocol.

The default queue limit arguments are listed in [Table 13](#).

Table 13 Default Priority Queue Packet Limits

Priority Queue Argument	Packet Limits
<i>high-limit</i>	20
<i>medium-limit</i>	40
<i>normal-limit</i>	60
<i>low-limit</i>	80

**Note**

If priority queueing is enabled and there is an active ISDN (Integrated Services Digital Network) call in the queue, changing the configuration of the **priority-list queue-limit** command drops the call from the queue. For more information about priority queueing, refer to the *Quality of Service Configuration Guide*, Release 12.2.

Examples

The following example sets the maximum packets in the priority queue to 10:

```
priority-list 2 queue-limit 10 40 60 80
```

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

protect

To configure a virtual circuit (VC) class with protected group or protected VC status for application to a VC bundle member, use the **protect** command in vc-class configuration mode. To remove the protected status from the VC class, use the **no** form of this command.

To configure a specific VC as part of a protected group of the bundle or to configure it as an individually protected VC bundle member, use the **protect** command in bundle-vc configuration mode. To remove the protected status from the VC, use the **no** form of this command.

protect {group | vc}

no protect {group | vc}

Syntax Description

group	Configures the VC bundle member as part of the protected group of the bundle.
vc	Configures the VC member as individually protected.

Defaults

The VC neither belongs to the protected group nor is it an individually protected VC.

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use this command in vc-class configuration mode to configure a VC class to contain protected group or individual protected VC status. When the class is applied to the VC bundle member, that VC is characterized by the protected status. You can also apply this command directly to a VC in bundle-vc configuration mode.

When a protected VC goes down, it takes the bundle down. When all members of a protected group go down, the bundle goes down.

To use this command in vc-class configuration mode, first enter the **vc-class atm** global configuration command.

This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command in bundle-vc configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle containing the VC member to be configured. Then enter the **pvc-bundle** configuration command to add the VC to the bundle as a member of it.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures a class called control-class to include a **protect** command, which, when applied to a VC bundle member, configures the VC as an individually protected VC bundle member. When this protected VC goes down, it takes the bundle down.

```
vc-class atm control-class
protect vc
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
precedence (VC bundle)	Configures precedence levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle.
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class for an ATM VC or interface.

pvc-bundle

To add a virtual circuit (VC) to a bundle as a member of the bundle and enter bundle-vc configuration mode in order to configure that VC bundle member, use the **pvc-bundle** bundle configuration command. To remove the VC from the bundle, use the **no** form of this command.

pvc-bundle *pvc-name* [*vpi*] [*vci*]

no pvc-bundle *pvc-name* [*vpi*] [*vci*]

Syntax Description

<i>pvc-name</i>	The name of the permanent virtual circuit (PVC) bundle.
<i>vpi</i>	<p>(Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the “f” and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.</p> <p>On the Cisco 7200 and 7500 series routers, the value range is from 0 to 255; on the Cisco 4500 and 4700 routers, the value range is from 0 to 1 less than the quotient of 8192 divided by the value set by the atm vc-per-vp command.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<i>vci</i>	<p>(Optional) ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (ILMI), and so on) and should not be used.</p> <p>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>

Defaults

This command has no default behavior or values.

Command Modes

Bundle configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Each bundle can contain multiple VCs having different QoS attributes. This command associates a VC with a bundle, making it a member of that bundle. Before you can add a VC to a bundle, the bundle must exist. Use the **bundle** command to create a bundle. You can also use this command to configure a VC that already belongs to a bundle. You enter the command in the same way, giving the name of the VC bundle member.

The **pvc-bundle** command enters bundle-vc configuration mode, in which you can specify VC-specific and VC class attributes for the VC.

Examples

The following example specifies an existing bundle called `chicago` and enters bundle configuration mode. Then it adds two VCs to the bundle. For each added VC, bundle-vc mode is entered and a VC class is attached to the VC to configure it.

```
bundle chicago
pvc-bundle chicago-control 207
  class control-class
pvc-bundle chicago-premium 206
  class premium-class
```

The following example configures the PVC called `chicago-control`, an existing member of the bundle called `chicago`, to use class-based weighted fair queueing (CBWFQ). The example configuration attaches the policy map called `policy1` to the PVC. Once the policy map is attached, the classes comprising `policy1` determine the service policy for the PVC `chicago-control`.

```
bundle chicago
pvc-bundle chicago-control 207
  class control-class
  service-policy output policy1
```

Related Commands

Command	Description
atm vc-per-vp	Sets the maximum number of VCs to support per VPI.
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
precedence (VC bundle)	Configures precedence levels for a VC member of a bundle, or for a VC class that can be assigned to a VC bundle.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

qos pre-classify

To enable QoS preclassification, use the **qos pre-classify** interface configuration command. To disable the QoS preclassification feature, use the **no** form of this command.

qos pre-classify

no qos pre-classify

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)XE3	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The **qos pre-classify** command is unavailable on all other interface types.

The **qos pre-classify** command can be enabled for IP packets only.

Examples The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:

```
Router(config-if)# qos pre-classify
```

The following example enables the QoS for VPNs feature on crypto maps:

```
Router(config-crypto-map)# qos pre-classify
```

Related Commands	Command	Description
	show interfaces	Displays the statistical information specific to a serial interface.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.