

oam-bundle

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for all virtual circuit (VC) members of a bundle or a VC class that can be applied to a VC bundle, use the **oam-bundle** command in switched virtual circuit (SVC)-bundle configuration mode or VC-class configuration mode. To remove OAM management from the bundle or class configuration, use the **no** form of this command.

To enable end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, use the **oam-bundle** command in bundle configuration mode. To remove OAM management from the bundle, use the **no** form of this command.

oam-bundle [**manage**] [*frequency*]

no oam-bundle [**manage**] [*frequency*]

Syntax Description

manage	(Optional) Enables OAM management. If this keyword is omitted, loopback cells are sent, but the bundle is not managed.
<i>frequency</i>	(Optional) Number of seconds between transmitted OAM loopback cells. Values range from 0 to 600 seconds. The default value for the <i>frequency</i> argument is 10 seconds.

Defaults

End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back.

Command Modes

SVC-bundle configuration (for an SVC bundle)
 VC-class configuration (for a VC class)
 Bundle configuration (for an ATM VC bundle)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(4)T	This command was made available in SVC-bundle configuration mode.

Usage Guidelines

This command defines whether a VC bundle is OAM managed. If this command is configured for a bundle, every VC member of the bundle is OAM managed. If OAM management is enabled, further control of OAM management is configured using the **oam retry** 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. In this case, the attributes are ignored by the VC.

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

To use this command in bundle configuration mode, enter the **bundle** subinterface configuration command to create the bundle or to specify an existing bundle before you enter this command.

VCs in a VC bundle are subject to the following configuration inheritance rules (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)

Examples

The following example enables OAM management for a bundle called “chicago”:

```
bundle chicago
oam-bundle manage
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).

police

To configure traffic policing, use the **police** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

```
police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

```
no police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

Syntax Description

<i>bps</i>	Average rate in bits per second. Valid values are 8000 to 200000000.
<i>burst-normal</i>	(Optional) Normal burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes.
<i>burst-max</i>	(Optional) Excess burst size in bytes. Valid values are 1,000 to 51200000.
conform-action <i>action</i>	Action to take on packets that conform to the rate limit.
exceed-action <i>action</i>	Action to take on packets that exceed the rate limit.
violate-action <i>action</i>	(Optional) Action to take on packets that violate the normal and maximum burst sizes.
<i>action</i>	Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> • drop—Drops the packet. • set-clp-transmit <i>value</i>—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1. • set-discard-class-transmit—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. • set-dscp-transmit <i>value</i>—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • set-frde-transmit <i>value</i>—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the frame relay frame and transmits the packet with the DE bit set to 1. • set-mpls-experimental-imposition-transmit <i>value</i>—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. • set-mpls-experimental-topmost-transmit <i>value</i>—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. • set-prec-transmit <i>value</i>—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • set-qos-transmit <i>value</i>—Sets the qos-group value and transmits the packet with the new qos-group value setting. • transmit—Transmits the packet. The packet is not altered.

Defaults Disabled

Command Modes Policy-map class configuration (when specifying a single action to be applied to a marked packet)
Policy-map class police configuration (when specifying multiple actions to be applied to a marked packet)

Release	Modification
12.0(5)XE	This police command was introduced.
12.1(1)E	This command was integrated in Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T. The violate-action keyword was added.
12.2(2)T	The set-clp-transmit option for the <i>action</i> argument was added. The set-frde-transmit keyword for the <i>action</i> argument was added. The set-mpls-exp-transmit keyword for the <i>action</i> argument was added.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate.
12.2(13)T	In the <i>action</i> argument, the set-mpls-experimental-transmit keyword was renamed to set-mpls-experimental-imposition-transmit .

Usage Guidelines Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action** *transmit* and **conform-action** *drop*.

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in Release 12.0(5)XE, refer to the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the *New Features for 12.0(5)XE* feature documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

The following are explanations of how the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T work.

Token Bucket Algorithm with One Token Bucket

The one token bucket algorithm is used when the **violate-action** option is not specified in the **police** command command-line interface (CLI).

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:
$$(\text{time between packets} <\text{which is equal to } T - T1 > * \text{policer rate})/8 \text{ bytes}$$
- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in the conform bucket B (minus the packet size to be limited) is fewer than 0, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets

The two-token bucket algorithm is used when the **violate-action** option is specified in the **police** command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at t, the bucket is updated with T - T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.
The token arrival rate is calculated as follows:
$$(\text{time between packets} <\text{which is equal to } T - T1 > * \text{policer rate})/8 \text{ bytes}$$
- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Examples

Token Bucket Algorithm with One Token Bucket Example

The following example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0:

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets Example

In this particular example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets $((.40 * 8000)/8)$. Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because it only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket $((.20 * 8000)/8)$. Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Conforming to the MPLS EXP Value Example

The following example shows that if packets conform to the rate limit, the MPLS EXP field is set to 5. If packets exceed the rate limit, the MPLS EXP field is set to 3.

```
policy-map input-IP-dscp
  class dscp24
    police 8000 1500 1000
      conform-action set-mpls-experimental-imposition-transmit 5
      exceed-action set-mpls-experimental-imposition-transmit 3
      violate-action drop
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Specifies the name of the service policy to be attached to the 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.

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** (percent) command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir percent percent [**bc conform-burst-in-msec**] [**pir percent percent**]
 [**be peak-burst-in-msec**]

no police cir percent percent [**bc conform-burst-in-msec**] [**pir percent percent**]
 [**be peak-burst-in-msec**]

Syntax Description

cir	Committed information rate (CIR). Indicates that the CIR will be used for policing traffic.
percent	Specifies that percent of bandwidth will be used for calculating the CIR.
<i>percent</i>	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
<i>conform-burst-in-msec</i>	(Optional) Specifies the bc value in milliseconds (ms). Valid range is a number from 1 to 2000.
pir	(Optional) Peak information rate (PIR). Indicates that the PIR will be used for policing traffic.
percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
<i>percent</i>	(Optional) Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
be	(Optional) Peak burst (be) size used by the second token bucket for policing traffic.
<i>peak-burst-in-msec</i>	(Optional) Specifies the peak burst (be) size in ms. Valid range is a number from 1 to 2000.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)XE	This police command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	This command was modified for the Percentage-Based Policing and Shaping feature.

Usage Guidelines

This command calculates the CIR and PIR based on a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent CIR and PIR values in bits per second (bps) are calculated based on the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated CIR and PIR bps rates must be in the range of 8000 and 2000000000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the CIR and the PIR are recalculated based on the revised amount of bandwidth. If the CIR and PIR percentages are changed after the policy map is attached to the interface, the bps values of the CIR and PIR are recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Policy maps can be configured in two-level (nested) hierarchies; a primary (or “parent”) level and a secondary (or “child”) level. The **police** (percent) command can be configured for use in either a parent or child policy map.

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```

policy-map parent_policy
  class parent
    shape average 512000
    service-policy child_policy

policy-map child_policy
  class normal_type
    police cir percent 30

```

In this sample configuration, there are two hierarchical policies; one called “parent_policy” and one called “child_policy.” In the policy map called “child_policy,” the **police** (percent) command has been configured in the class called “normal_type.” In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command will use 512 kbps, the peak rate, as the bandwidth reference point for “class parent” in “parent policy.” The **police** (percent) command will use 512 kbps as the basis for calculating the CIR rate (512 kbps * 30 percent).

```

interface serial 4/0
  service-policy output parent_policy

Policy-map parent_policy
  class parent
    bandwidth 512
    service-policy child_policy

```

In the above example, there is one policy map called “parent_policy.” In this policy map, a peak rate has not been specified. The **bandwidth** (policy-map class) command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command will look to the next higher level (in this case Serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of the Series interface s4/0 is 1.5 Mbps, the **police** (percent) command will use 1.5 Mbps as the basis for calculating the CIR rate (1500000 * 30 percent).

How Bandwidth Is Calculated

The **police** (percent) command is often used in conjunction with the **bandwidth** (policy-map class) and **priority** commands. The **bandwidth** (policy-map class) and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** (policy-map class) and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
 - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
 - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, refer to the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example configures traffic policing using a CIR and a PIR based on a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```

Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms pir percent 40 be 400 ms
Router(config-pmap-c)# service-policy child-policy1
Router(config-pmap-c)# exit
Router(config-pmap-c)# interface serial 3/1
Router(config-if)# service-policy output policy1

```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	priority	Gives priority to a class of traffic belonging to a policy map.
	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.
	shape (percent)	Specifies average or peak rate traffic shaping based on a percentage of bandwidth available on an 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 packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

```
police {cir cir} [bc conform-burst] {pir pir} [be peak-burst] [conform-action action
[exceed-action action [violate-action action]]]
```

```
no police {cir cir} [bc conform-burst] {pir pir} [be peak-burst] [conform-action action
[exceed-action action [violate-action action]]]
```

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated.
<i>cir</i>	Specifies the CIR value in bits per second. The value is a number from 8000 to 200000,000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
<i>conform-burst</i>	(Optional) Specifies the bc value in bytes. The value is a number from 1000 to 51200,000.
pir	Peak information rate (PIR) at which the second token bucket is updated.
<i>pir</i>	Specifies the PIR value in bits per second. The value is a number from 8000 to 200000000.
be	(Optional) Peak burst (be) size used by the second token bucket for policing.
<i>peak-burst</i>	(Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use.
conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to take on packets exceed the PIR.
<i>action</i>	(Optional) Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> • drop—Drops the packet. • set-clp-transmit—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1. • set-dscp-transmit <i>new-dscp</i>—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • set-frde-transmit—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1. • set-mpls-exp-transmit—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting. • set-prec-transmit <i>new-prec</i>—Sets the IP precedence and sends the packet with the new IP precedence value setting. • set-qos-transmit <i>new-qos</i>—Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting. • transmit—Sends the packet with no alteration.

Defaults Disabled

Command Modes Policy-map configuration

Release	Modification
12.0(5)XE	The police command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. The violate-action keyword was added.
12.2(2)T	The following keywords for the <i>action</i> argument were added: <ul style="list-style-type: none"> • set-clp-transmit • set-frde-transmit • set-mpls-exp-transmit
12.2(4)T	This command expanded for the Two-Rate policing feature. The cir and pir keywords were added to accommodate two-rate traffic policing.

Usage Guidelines

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the conform burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

$$Tc(t) = \min(CIR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR * (t-t1) + Tp(t1), Be)$$

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If $B > Tp(t)$, the packet is marked as violating the specified rate.
- If $B > Tc(t)$, the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as $Tp(t) = Tp(t) - B$.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

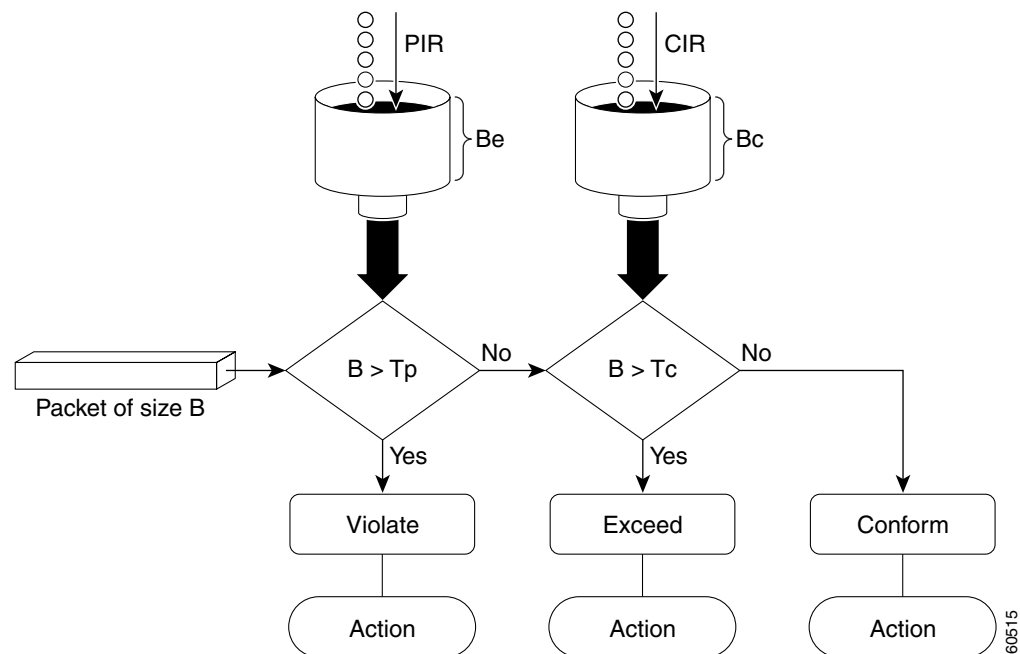
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate
- 100 kbps would be marked as exceeding the rate
- 50 kbps would be marked as violating the rate

Marking Packets and Assigning Actions Flowchart

The flowchart in [Figure 4](#) illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

Figure 4 *Marking Packets and Assigning Actions with the Two-Rate Policer*



Examples

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
```

```
Policy Map policy1
Class police
  police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

In the following example, 1.25 Mbps of traffic is sent (“offered”) to a policer class:

```
Router# show policy-map interface serial3/0
```

```
Serial3/0

Service-policy output: policy1

Class-map: police (match all)
 148803 packets, 36605538 bytes
 30 second offered rate 1249000 bps, drop rate 249000 bps
Match: access-group 101
police:
  cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
  conformed 59538 packets, 14646348 bytes; action: transmit
  exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
  violated 29731 packets, 7313826 bytes; action: drop
  conformed 499000 bps, exceed 500000 bps violate 249000 bps

Class-map: class-default (match-any)
 19 packets, 1990 bytes
 30 seconds offered rate 0 bps, drop rate 0 bps
Match: any
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

Related Commands	Command	Description
	police	Configures traffic policing.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	service-policy	Attaches a policy map to an input interface or an output interface to be used as the service policy for that 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 packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

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** command in 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	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

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** command in `vc-class` configuration mode. To remove the precedence levels from the VC class, use the **no** form of this command.

To configure the precedence levels for a VC or permanent virtual circuit (PVC) member of a bundle, use the **precedence** command in `bundle-vc` configuration mode for ATM VC bundle members, or in `switched virtual circuit (SVC)-bundle-member` configuration mode for an ATM SVC. To remove the precedence levels from the VC or PVC, 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 either as a number from 0 to 7 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)
 SVC-bundle-member configuration (for an ATM SVC)

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.
12.2(4)T	This command was made available in <code>SVC-bundle-member</code> configuration mode.
12.0(23)S	This command was made available in <code>vc-class</code> and <code>bundle-vc</code> configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.

Usage Guidelines

Assignment of precedence levels to VC or PVC bundle members allows you to create differentiated service because you can distribute the IP precedence levels over the various VC/PVC bundle members. You can map a single precedence level or a range of levels to each discrete VC/PVC in the bundle, thereby enabling VCs/PVCs in the bundle to carry packets marked with different precedence levels. Alternatively, you can use the **precedence other** command to indicate that a VC/PVC can carry traffic

marked with precedence levels not specifically configured for other VCs/PVCs. Only one VC/PVC in the bundle can be configured using the **precedence other** command. This VC/PVC is considered the default one.

To use this command in **vc-class** configuration mode, first enter the **vc-class atm** command in global configuration mode. The **precedence** 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 the **precedence** 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 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.
	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.
	dscp (frame-relay vc-bundle-member)	Specifies the DSCP value or values for a specific Frame Relay PVC bundle member.
	match precedence	Identifies IP precedence values as match criteria.
	mpls experimental	Configures the MPLS experimental bit values for a VC class that can be mapped to a VC bundle and thus applied to all VC members of that bundle.
	protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
	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.
	pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
	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.

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** command in random-detect-group configuration mode. 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 8](#) 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 8 lists the default minimum value for each IP Precedence.

Table 8 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** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority {*bandwidth-kbps* | **percent** *percentage*} [*burst*]

no priority {*bandwidth-kbps* | **percent** *percentage*} [*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.
percent	Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth.
<i>percentage</i>	Used in conjunction with the percent keyword, specifies the percentage of the total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.
<i>burst</i>	(Optional) Specifies the burst size in bytes. The burst size configures 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 range of the burst is from 32 to 2000000 bytes.

Defaults

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 integrated in Release 12.1(3)T.
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.
12.2(2)T	The percent keyword and the <i>percentage</i> argument were added.

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, the **ip rtp priority** command, 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 **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.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

For more information on bandwidth allocation, refer to the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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 to which the policy map called policy1 has been attached:

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	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 packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on 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** command in interface configuration mode. 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	Disabled
-----------------	----------

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** command in global configuration mode. 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 queuing priorities on packets entering from a given interface, use the **priority-list interface** command in global configuration mode. 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 queuing 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** command in global configuration mode. 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 , appletalk , arp , bridge (transparent), clns , clns_es , clns_is , compressedtcp , cmns , decnet , decnet_node , decnet_router-l1 , decnet_router-l2 , dls w, ip , ipx , pad , rsrb , stun 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 9 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.
12.2(13)T	This command was modified to remove apollo , vines , and xns from the list of protocol types. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T.

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

Use [Table 9](#), [Table 10](#), and [Table 11](#) to configure the queueing priorities for your system.

Table 9 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 10 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 11 lists common UDP services and their port numbers.</p>

Table 10 Common TCP Services and Their Port Numbers

Service	Port
FTP data	20
FTP	21
Simple Mail Transfer Protocol (SMTP)	25
Telnet	23

Table 11 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 10 and Table 11 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 dlsw 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** command in global configuration mode. 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 12 .
<i>low-limit</i>	

Defaults

This command is not enabled by default.

See [Table 12](#) 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 12](#).

Table 12 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*.

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

```
protect {group | vc}
```

```
no protect {group | vc}
```

Syntax Description

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

Defaults

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

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.
12.0(23)S	This command was made available in <code>vc-class</code> and <code>bundle-vc</code> configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.

Usage Guidelines

Use the **protect** 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 the **protect** command in `vc-class` configuration mode, first enter the **vc-class atm** global configuration command.

The **protect** 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 the **protect** 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	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; configures precedence levels for an individual VC or PVC bundle member.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
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** command in bundle configuration mode. 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>	(Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the “/” and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. 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. The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
<i>vci</i>	(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. 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. The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.

Defaults

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	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.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
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.

