Configuring QoS Policy Actions and Rules

The second step in creating a QoS service policy is to define how you want the router to handle the packets that match the classification rules you defined in Chapter 2, "Classifying Traffic." The Cisco 10000 series router supports a modular CLI element called a *policy map* to enable you to configure a QoS policy with the appropriate actions and rules.

This chapter describes how to create QoS policies that the Cisco 10000 series router applies to specific traffic classes. It includes the following topics:

QoS Policies

After the Cisco 10000 series router classifies traffic based on the classification rules applied on an inbound or outbound interface, the router needs to know how to handle the traffic that meets the matching criteria. A modular quality of service command-line interface (MQC) element called a *policy map* enables you to create QoS policies that tell the router the QoS actions and rules to apply to packets belonging to a particular traffic class.

The following sections describe policy maps and QoS actions:

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

Feature History for QoS Policies

Cisco IOS Release	Description	Required PRE
Release 12.0(17)SL	The policy map feature was introduced on the router.	PRE1
Release 12.2(15)BX	This feature was introduced on the PRE2.	PRE2
Release 12.2(28)SB	This feature was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.	PRE2

Defining QoS Actions Using a Policy Map

A policy map associates a traffic class with one or more QoS actions. When configuring a policy map, you specify the name of a class map and configure the actions you want the router to take on the matching traffic. Before you can create class policies in a policy map, the class must have classification criteria configured in a class map. The router supports QoS actions such as marking, policing, and bandwidth distribution.

A single policy map can be attached to multiple interfaces concurrently. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

System Limits for Policy Maps

Table 2 lists the system limits for policy maps supported on the Cisco 10000 series router.

Table 2 System Limits for Policy Maps

Processor	Cisco IOS Release	Policy Maps per System[1] (up to this amount)	No. Classes per Policy Map[2]
PRE1	All Releases prior to Release 12.0(17)SL	256	16
	Release 12.0(17)SL and later releases	256	256
	Release 12.0(25)SX and later releases	4096	32

Table 2 System Limits for Policy Maps

Processor	Cisco IOS Release	Policy Maps per System[1] (up to this amount)	No. Classes per Policy Map[2]
PRE2	Release 12.2(15)BX and later releases	256	64
	Release 12.3(7)XI and later releases	4096	127
	Release 12.2(27)SBB	4096	64
PRE3	Release 12.2(31)SB2 and later releases	4096	64

1. Depending on the complexity of your configuration
2. Including the class-default class

Each **policy-map** command counts as one policy map, which counts against the 4096 system limit. When a policy map includes percent-based policing, the router sometimes converts a single QoS policy to multiple policies and applies each one of the multiple policies to each interface to which percent-based policing is applied. In this case, each multiple policy counts against the 4096 limit. In complex configurations, however, the maximum number of policy maps can be as small as a few hundred.

policy-map Command

To create or modify a policy map, use the **policy-map** command in global configuration mode. Use the **no** form of the command to remove a policy map. This command has no default behavior or values.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name	Is the name of the policy map. The name can be a maximum of 40 alphanumeric characters.

policy-map Command History

Cisco IOS Release	Description
Release 12.0(17)SL	The **policy-map** command was introduced on the PRE1.
Release 12.2(15)BX	This command was introduced on the PRE2.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.

Usage Guidelines for the policy-map Command

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

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

Types of QoS Actions

The following sections describe the QoS actions supported on the Cisco 10000 series router. These are the actions that you configure in a policy map for specific traffic classes.

Input and Output Policy Actions

The Cisco 10000 series router does not impose any restrictions on the classification definitions you include in a class map. However, it does limit the input and output policy actions that you can define in a policy map. These limitations are based on the type of interface on which you apply the service policy. As indicated in Table 3 and Table 4, the interface types are:

- Normal interface, including variable bit rate (VBR) virtual circuits (VCs) on ports configured in **pxf queuing** mode
- Tag interface (MPLS VPN)
- Virtual access interface (VAI)
- ATM unspecified bit rate (UBR) VCs and VCs configured on ports in **no atm pxf queuing** mode

Table 3 lists the input policy actions that you can define in a policy map for specific interface types.

Table 3 Input Policy Map Actions

Policy Map Actions	Interface Type			
	Normal	Tag (MPLS VPN)	Virtual Access	ATM UBR VCs
bandwidth	Not Applicable	Not Applicable	Not Applicable	Not Applicable
queue-limit	Not Applicable	Not Applicable	Not Applicable	Not Applicable
priority	Not Applicable	Not Applicable	Not Applicable	Not Applicable
shape	Not Available	Not Available	Not Available	Not Available
random-detect	Not Applicable	Not Applicable	Not Applicable	Not Applicable
set ip prec/dscp	Valid	Not Applicable	Valid	Valid
set qos-group	Valid	Valid	Valid	Valid
set atm-clp	Not Applicable	Not Applicable	Not Applicable	Not Applicable
set cos	Not Applicable	Not Applicable	Not Applicable	Not Applicable
police	Valid	Valid	Valid	Valid
set mpls experimental	Not Available	Not Available	Not Available	Not Available

Note In Table 3 and Table 4, "Not Applicable" indicates that you cannot perform the action on a Cisco product or that it has no meaning in the context indicated. "Not Available" means the action is not supported. When configuring an input policy map for a virtual access interface (VAI), be careful that you do not include the "Not Applicable" or "Not Available" policy actions indicated. If you do, an error message appears.

Table 4 lists the output policy actions that you can define in a policy map for specific interface types.

Table 4 Output Policy Map Actions

Policy Map Actions	Interface Type			
	Normal	Tag (MPLS VPN)	Virtual Access	ATM UBR VCs
bandwidth	Valid	Valid	Valid (Applied to the VC, not the VAI)	Not Applicable
queue-limit	Valid	Valid	Not Available	Not Available
priority	Valid	Valid	Valid (Applied to the VC, not the VAI)	Not Applicable
shape	Valid	Valid	Valid (Applied to the VC, not the VAI)	Not Applicable
random-detect	Valid	Valid	Not Available	Not Available

Table 4 Output Policy Map Actions

Policy Map Actions	Interface Type			
	Normal	**Tag (MPLS VPN)**	**Virtual Access**	**ATM UBR VCs**
set ip prec/dscp	Valid	Not Applicable	Valid	Valid
set qos-group	Not Applicable	Not Applicable	Not Applicable	Not Applicable
set atm-clp	Valid	Not Available	Not Available	Not Available
set cos	Valid[1]	Not Available	Valid[2]	Not Applicable
police	Valid	Valid	Valid	Valid
set mpls experimental	Not Applicable	Not Available	Not Applicable	Not Applicable

1. The interface must be an Ethernet interface that is configured for 802.1Q VLAN.
2. The virtual access interface must be using an 802.1Q VLAN interface.

Policy Map Actions—Releases Prior to Cisco IOS Release 12.0(17)SL

Table 5 lists the QoS action commands supported in all releases prior to Cisco IOS Release 12.0(17)SL. These actions are also available in later releases.

Table 5 Policy Map Actions—Releases Prior to Cisco IOS Release 12.0(17)SL

Action	Description
police *bps* [*burst-normal* | *burst-excess*] [**conform-action** *action* | **exceed-action** *action*]	Configures traffic policing in policy-map class configuration mode. *bps* is the average rate in bits per second. Valid values are from 8,000 to 200,000,000. (Optional) *burst-normal* is the normal burst size in bytes. Valid values are from 1,000 to 51,200,000. (Optional) *burst-excess* is the excess burst size in bytes. Valid values are from 1,000 to 51,200,000. **conform-action** *action* specifies the action to take on packets that conform to the rate limit. The default *action* is transmit. **exceed-action** *action* specifies the action to take on packets that exceed the rate limit. The default *action* is drop. **Note** You can specify only one action each for conform or exceed. Do not specify multiple actions. See Table 10 on page 11 for a list of available policing actions.
queue-limit *number-of-packets*	Specifies or modifies the maximum number of packets that the queue can hold for this class. For PRE1, *number-of-packets* is a number from 32 to 16,384; the number must be a power of 2. If the number you specify is not a power of 2, the router uses the nearest power of 2 to your number. For Cisco IOS Release 12.2(15)BX and Release 12.2(16)BX, *number-of-packets* is a number from 32 to 16,384. The number does not need to be a power of 2. For Cisco IOS Release 12.3(7)XI and later releases, if the interface speed is less than 500 MB, *number-of-packets* is a number from 8 to 4096; the number must be a power of 2. If the interface speed is greater than 500 MB, *number-of-packets* is a number from 128 to 64,000; the number must be a power of 2.

Table 5 Policy Map Actions—Releases Prior to Cisco IOS Release 12.0(17)SL (continued)

Action	Description
random-detect dscp *dscpvalue min-threshold max-threshold drop-rate*	Changes the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value. *dscpvalue* specifies the DSCP value, which is a number from 0 to 63, or one of the following keywords: EF, AF*xy*, or CS1 through CS7. For more information, see the "DSCP Per-Hop Behavior" section on page 7-6. *min-threshold* is the minimum threshold. Valid values are from 32 to 16,384 (PRE1) or 1 to 16,384 (PRE2). *max-threshold* is the maximum threshold. Valid values are from 32 to 16,384 (PRE1) or 1 to 16,384 (PRE2). *drop-rate* is the drop probability and is a number from 1 to 65,535. For example, if you set this value to 256, 1 out of 256 packets is dropped when the average queue is at the maximum threshold. **Note** Default values for random-detect vary from release to release. Use the **show policy interface** command to view default values.
random-detect exponential-weight-constant *value*	Allows you to modify the default method that random-detect uses to calculate average queue size. Random-detect determines the average queue size based on the current queue length and the last average queue length. *value* is a number from 1 to 16. The default value is typically 9. • The higher the value, the more dependent the average is on the historical average, making weighted random early detection (WRED) slow to react to changing traffic conditions that may be only temporary. • The lower the value, the less dependent the average is on the historical average, making WRED more sensitive to rapidly changing traffic conditions. **Note** In most cases, the benefits of WRED can be best realized if you enter the **random-detect** command without arguments.

Table 5 Policy Map Actions—Releases Prior to Cisco IOS Release 12.0(17)SL (continued)

Action	Description
random-detect precedence *precedence min-threshold max-threshold drop-rate*	Changes the minimum and maximum packet thresholds for the precedence level you specify. *precedence* is a number from 0 to 7, where 0 typically represents low priority traffic that can be aggressively managed (dropped) and 7 represents high priority traffic. For more information, see the **set ip precedence** command in this table. *min-threshold* is the minimum threshold. Valid values are from 32 to 16,384 (PRE1) or 1 to 16,384 (PRE2). *max-threshold* is the maximum threshold. Valid values are from 32 to 16,384 (PRE1) or 1 to 16,384 (PRE2). *drop-rate* is the drop probability and is a number from 1 to 65,535. For example, if you set this value to 256, 1 out of 256 packets is dropped when the average queue is at the maximum threshold. **Note** Default values for random-detect vary from release to release. Use the **show policy interface** command to view default values.
set atm-clp	Sets the cell loss priority (CLP) bit setting. Configure this command as an output action only.
set ip dscp *dscp-value*	Marks a packet by setting the IP differentiated services code point (DSCP) in the type of service (TOS) byte. *dscp-value* is a number from 0 to 63.
set ip precedence {*number* | *name*}	Sets the precedence value in the IP header. *number* and the corresponding *name* are listed below from least important to most important (for example, 0—routine is the least important and 7—network is the most important). 0—routine, 1—priority, 2—immediate, 3—flash, 4—flash-override, 5—critical 6—internet, 7—network
set qos-group *group-id*	Sets a group ID that can be used later to classify packets. Configure this command as an input action only. *group-id* is a number from 0 to 99.

Policy Map Actions—Cisco IOS Release 12.0(17)SL and Later Releases

Cisco IOS Release 12.0(17)SL adds support for the QoS action commands listed in Table 6. These commands are also available in later releases.

Table 6 Policy Map Actions—Cisco IOS Release 12.0(17)SL and Later Releases

Action	Description
bandwidth {*bandwidth-kbps* | **percent** *percent*}	Specifies or modifies the bandwidth allocated for a traffic class in a policy map. *bandwidth-kbps* is the guaranteed minimum bandwidth (in kilobits per second) that you want to allocate. Valid values are from 8 to 2,488,320. **percent** *percent* is the percentage of the available bandwidth that you want to allocate. Valid values are from 1 to 99.
priority {*bandwidth-kbps* | **percent** *percent*}[1]	Assigns a priority to a traffic class in a policy map. The priority class receives preference over other class queues. *bandwidth-kbps* is the guaranteed minimum bandwidth (in kilobits per second) that you want to allocate for the priority queue. Valid values are from 8 to 2,000,000. **percent** *percent* is the percentage of the available bandwidth that you want to allocate for the priority queue. Valid values are 1 to 99.
shape *rate*	Shapes traffic to the specified bit rate. *rate* is a number from 8 to 2,488,320.

1.In Cisco IOS Release 12.0(23)SX1, Release 12.0(25)S, and Release 12.3(7)XI, and later releases, the syntax of the **priority** command changed to **priority** (without any arguments). For these later releases, use the **priority** command with the **police** command so that the priority class does not starve other traffic on a link. For more information, see the "Avoiding Bandwidth Starvation Due to Priority Services" section on page 6-21 and the "Bandwidth Starvation" section on page 8-3.

Policy Map Actions—Cisco IOS Release 12.0(20)ST and Later Releases

Cisco IOS Release 12.0(20)ST adds support for the QoS action command listed in Table 7. This command is also available in later releases.

Table 7 Policy Map Actions—Cisco IOS Release 12.0(20)ST and Later Releases

Action	Description
bandwidth remaining percent *percent*	Specifies or modifies the bandwidth allocated for a traffic class in a policy map. **percent** *percent* is the percentage of the remaining bandwidth that you want to allocate. Valid values are 1 to 99.

Policy Map Actions—Cisco IOS Release 12.0(22)S and Later Releases

Cisco IOS Release 12.0(22)S adds support for the QoS action command listed in Table 8. This command is also available in later releases.

Table 8 Policy Map Actions—Cisco IOS Release 12.0(22)S and Later Releases

Action	Description
set mpls experimental *value*	Copies the setting of the IP precedence or DSCP bits to the MPLS experimental bits of a packet. *value* is a number from 0 to 7. Multiple values must be space-delimited (for example, 3 4 7).

Policy Map Actions—Cisco IOS Release 12.2(31)SB2 and Later Releases

Cisco IOS Release 12.2(31)SB2 adds support for the QoS action command listed in Table 9. This command is also available in later 12.2 SB releases for the PRE3.

Table 9 Policy Map Actions—Cisco IOS Release 12.2(31)SB2 and Later Releases

Action	Description
priority level *level*	Copies the setting of the IP precedence or DSCP bits to the MPLS experimental bits of a packet. *value* is a number from 0 to 7. Multiple values must be space-delimited (for example, 3 4 7).

Policing Actions

The **police** command allows you to specify what you want the router to do when traffic meets, exceeds, or violates the policing parameters you specified. Table 10 describes the policing actions the router supports and the minimum Cisco IOS release required.

Table 10 Policing Actions

Action	Description	Introduced in Cisco IOS Release
drop	Drops the packet. This is the default action for traffic that exceeds the committed rate.	Release 12.0(9)SL
set-clp-transmit *value*	Sets the ATM cell loss priority (CLP) bit on the ATM cell. Valid values are from 0 to 1.	Release 12.3(7)XI
set-discard-class-transmit	Sets the discard class attribute of a packet and transmits the packet with the new discard class setting.	Release 12.3(7)XI

Table 10 Policing Actions (continued)

Action	Description	Introduced in Cisco IOS Release
set-dscp-transmit *value*	Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. Valid values are from 0 to 63.	Release 12.0(9)SL
set-mpls-exp-transmit *value*	Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits and transmits the packet with the new MPLS EXP bit value setting. Valid values are from 0 to 7.	Release 12.0(22)S
set-mpls-exp-imposition-transmit *value*	Modifies the **set-mpls-exp-transmit** command to set the MPLS experimental (EXP) bits in the imposed label headers and transmit the packet with the new MPLS EXP bit value setting. Valid values are from 0 to 7.	Release 12.3(7)XI
set-prec-transmit *value*	Sets the IP precedence and transmits the packet with the new IP precedence value setting. Valid values are from 0 to 7.	Release 12.0(9)SL
set-qos-transmit *value*	Sets the qos-group value and transmits the packet with the new qos-group value setting. Valid values are from 0 to 99.	Release 12.0(9)SL
transmit	Transmits the packet. The packet is not altered.	Release 12.0(9)SL

QoS Inheritance

The Cisco 10000 series router applies service policies using the following QoS inheritance rules:

- ATM port—A service policy configured on an ATM port applies to all unspecified bit rate (UBR) PVCs configured on the port without a service policy. Only unshaped UBR PVCs inherit the service policy of the port. Variable bit rate (VBR), constant bit rate (CBR), and shaped UBR PVCs configured on the port do not inherit the service policy of the port.

  For more information about the ATM service classes, see the "ATM Service Categories" section on page 13.

- Label-controlled ATM (LC-ATM) subinterface—A service policy configured on an LC-ATM subinterface applies to the traffic of all constituent labeled VCs (LVCs).
- Frame Relay physical interface—A service policy configured on a Frame Relay physical interface applies to the traffic of all PVCs configured on the port without a service policy.
- Ethernet port—A service policy configured on an Ethernet port applies to the traffic of all VLANs configured on the port without a service policy.
- Session—If a service policy is not configured, the session inherits the service policy applied to the virtual circuit (VC) or the inherited policy of the VC. If a session inherits a policy, the **show policy interface virtual access** command does not display the state of the inherited policy. You can display the state of the policy only on the interface where you configured the policy.

ATM Service Categories

The Cisco 10000 series router supports the following ATM service classes:

- Constant Bit Rate, page 13
- Unspecified Bit Rate, page 13
- Variable Bit Rate, page 14

When operating in no atm pxf queuing mode, the router supports unshaped UBR PVCs, which do not specify a peak cell rate (PCR). The router can support a high number of VCs when you configure the **no atm pxf queuing** command on each port of the router. Point-to-Point Protocol over ATM (PPPoA) supports one session per VC and requires that you enable no atm pxf queuing to support 32,000 PPPoA sessions. Layer 2 Tunnel Protocol (L2TP) does not require that you enable no atm pxf queuing and Point-to-Point Protocol over Ethernet (PPPoE) sessions do not require that you enable this queuing mode because you can have 32,000 sessions on a single VC.

When operating in atm pxf queuing mode, the router supports the following ATM service classes:

- UBR (Unshaped)—No peak cell rate (PCR) specified
- Shaped UBR—PCR specified
- VBR-nrt—Non-real-time VBR
- CBR—Constant bit rate with PCR specified

If you specify a PCR value for UBR+, the router accepts the value, but does not use it, and it does not notify you when this occurs.

For information about how the ATM service classes inherit QoS service policies, see the "QoS Inheritance" section on page 12.

Constant Bit Rate

The constant bit rate (CBR) service class is a fixed bandwidth class, designed for ATM virtual circuits (VCs) requiring a specific amount of bandwidth to be continuously available throughout the duration of an active connection. CBR traffic is more time-dependent, less tolerant of delay, and generally more deterministic in bandwidth requirements. Voice, circuit emulation, and high-resolution video are typical examples of traffic utilizing this type of connection.

You define the required bandwidth in kbps by specifying a PCR. For example, the **cbr 64** command creates a CBR PVC with a PCR of 64 kbps.

An ATM VC configured as CBR can transmit cells at peak cell rate (PCR) at any time and for any duration. It can also transmit cells at a rate less than the PCR or even emit no cells. CBR is characterized by PCR.

Unspecified Bit Rate

The unspecified bit rate (UBR) service class is intended for non-real-time applications that do not require any maximum boundary on the transfer delay or on the cell loss ratio. The router delivers UBR traffic only when there is spare bandwidth in the network. This behavior is enforced by setting the cell loss priority (CLP) bit on UBR traffic when it enters a port.

The router delivers UBR traffic out to the network only when no other traffic is waiting to be served first. The UBR traffic does not affect the trunk loading calculations performed by the switch software.

UBR is the default class of service running at the maximum line rate of the physical interface.

The router supports both unshaped (no PCR specified) and shaped UBRs.

Shaped UBR

Traffic shaping allows you to control the traffic going out an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Traffic that adheres to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

The Cisco 10000 series router supports traffic shaping for unspecified bit rate (UBR) traffic. Traffic shaping is performed on a per-port basis and involves passing UBR traffic streams through VC queues for scheduled rate shaping. When traffic shaping is enabled, all traffic exiting the port out to the network is subject to VC scheduling based on the parameters you configure for the connection.

Configuring UBRs

To configure a UBR, enter the following commands in ATM VC configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *type slot/module/port.subinterface*	Specifies an interface or subinterface and enters interface configuration mode.

Step 2	`Router(config-if)# atm pxf queuing`
	or
	`Router(config-if)# no atm pxf queuing`
		Specifies one of two ATM PXF queuing modes for an interface or ATM port.
		Note Do not change this queuing mode while VCs are configured on the interface. If you need to change the mode, delete the VCs first and then change the mode. Changing the mode while VCs are configured can produce undesired results, and the change does not take effect until the router reloads.

Step 3	`Router(config-subif)# pvc` *vci/vpi*	Configures a PVC on the subinterface and enters ATM VC configuration mode. *vci* is the virtual channel identifier. *vpi* is the virtual path identifier.
Step 4	`Router(config-atm-vc)# ubr` *output-pcr*	Creates a UBR. *output-pcr* is the output peak cell rate. The router configures a shaped UBR when you specify the output PCR. Otherwise, the router configures unshaped UBR.

Variable Bit Rate

Variable bit rate (VBR) connections are classified as one of the following:

- Real time (VBR-rt)—Used for connections that transmit at a rate varying with time and that can be described as bursty, often requiring large amounts of bandwidth when active. The VBR-rt class is intended for applications that require tightly constrained delay and delay variation such as compressed voice video conferencing—for example, video conferencing requires real-time data transfer with bandwidth requirements that can vary in proportion to the dynamics of the video image at any given time. The VBR-rt category is characterized in terms of peak cell rate (PCR), sustained cell rate (SCR), and maximum burst size (MBS).

- Nonreal time (VBR-nrt)—Used for connections that are bursty but are not constrained by delay and delay variation boundaries. For those cells in compliance with the traffic contract, a low cell loss is expected. Non-time critical data file transfers are an example of a VBR-nrt connection. A VBR-nrt connection is characterized by PCR, SCR, and MBS.

Configuring VBRs

To configure VBR-nrt, enter the following commands in ATM VC configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *type slot/module/port.subinterface*	Specifies an interface or subinterface and enters interface configuration mode.

Step 2	`Router(config-if)# atm pxf queuing`
	or
	`Router(config-if)# no atm pxf queuing`
		Specifies one of two ATM PXF queuing modes for an interface or ATM port.
		Note Do not change this queuing mode while VCs are configured on the interface. If you need to change the mode, remove the VCs first and then change the mode. Changing the mode while VCs are configured can produce undesired results, and the change does not take effect until the router reloads.

Step 3	`Router(config-subif)# pvc` *vci/vpi*	Configures a PVC on the subinterface and enters ATM VC configuration mode. *vci* is the virtual channel identifier. *vpi* is the virtual path identifier.
Step 4	`Router(config-atm-vc)# vbr-nrt` *output-pcr output-scr output-mbs*	Creates a VBR-nrt. *output-pcr* is the output peak cell rate (PCR). *output-scr* is the output sustained cell rate (SCR). *output-mbs* is the output maximum burst cell size (MBS). **Note** If the PCR and SCR values are equal, the MBS value is 1.

Traffic Subject to QoS Policies

Table 11 lists the types of traffic on the Cisco 10000 series router that are subject to QoS policies.

Table 11 QoS Applicability

Traffic Types	Subject to QoS
In-transit IP packets	Yes
Locally Destined Traffic	
Layer 2 signaling packets such as PPP or Frame Relay negotiation packets, status packets, and keepalive messages	No
Packets with IP precedence 6 or 7, which IP-based routing protocols typically use	No
All other locally destined traffic	Yes
Locally Originated Traffic	
Packets marked by Cisco IOS software as PAK_Priority	No
Packets marked as IP precedence 6 or 7	No[1]
All other locally originated traffic	Yes

1. IP precedence 6 and 7 are not subject to QoS in all releases prior to Cisco IOS Release 12.0(22)S and in Cisco IOS Release 12.3(7)XI2.

ATM Virtual Circuits Without QoS Policies

For all ATM virtual circuits (VCs) that do not have a class-default class configured with a shape service policy (the **shape** command is configured), the Cisco 10000 series router limits the transmission rate of the VC to the interface bandwidth minus the sum of the shape rates of other VCs on the interface that do have service policies.

For example, if you have two VCs on a 150-Mbps interface and VC1 has a shaped service policy of 90 Mbps and VC2 does not have a service policy, the router polices VC2 to 60 Mbps (150 minus 90).

You can change this default behavior by using a shaped service policy on either the VC or the interface:

- If you apply the shaped service policy to a single VC that is not an unshaped UBR VC, the router applies the specified bandwidth to only that specific VC.

  By default, the router first allocates bandwidth to the VBR VCs and then allocates any bandwidth leftover to unshaped UBR VCs. To override this default behavior, apply a service policy to the unshaped UBR VC using an hierarchical shaping policy. For more information, see Chapter 12, "Defining QoS for Multiple Policy Levels."
- If you apply the policy to an interface, the router applies the specified bandwidth to all of the VCs on the interface that do not have their own service policies.

QoS Performance

The parallel express forwarding (PXF) engine processes QoS traffic. Sometimes the PXF engine cannot finish processing a packet before the packet completes a single pass through the PXF; the packet requires additional processing. As a result, the packet is fed back through the PXF and processing continues. This is referred to as a *feedback* operation.

Packets that are subject to both inbound and outbound QoS policies require additional PXF processing, resulting in a feedback. However, packets subject to only one QoS policy (either inbound or outbound) require only one pass through the PXF; a feedback is not needed.

Extra PXF passes reduce the system forwarding capacity. For example, if *x* packets per second require *y* extra passes, the system forwarding capacity diminishes by *xy*—the system has *xy* fewer packets per second forwarding capacity than before. Although the forwarding capacity diminishes, system performance is not affected. Packet classification processing affects only the forwarding capacity of the system, not the speed. Packet delay due to additional PXF passes is negligible. Therefore, system performance degradation occurs only at high system utilization.

The following describes PXF requirements:

- All releases prior to Cisco IOS Release 12.0(17)SL—For each packet, the PXF requires one pass per class-map match statement.
- Cisco IOS Release 12.0(17)SL—For each packet, the PXF requires one pass for every four non-access control list (ACL) class-map match statements. For each packet, the PXF requires one pass for one ACL class-map match statement.
- Cisco IOS Release 12.0(19)SL and later releases—For each packet, the PXF requires one pass per policy, regardless of the sum of the match statements in each class of the policy.

Configuring QoS Policies

To create a QoS policy, perform the following required tasks:

- Creating a Policy Map, page 17
- Defining QoS Actions in a Policy Map, page 18
- Attaching Service Policies, page 18 (See Chapter 4, “Attaching Service Policies.”)

Creating a Policy Map

To create a policy map, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map policy-map-name`	Creates or modifies a policy map template with the name you specify and enters policy-map configuration mode. *policy-map-name* is the name of the policy map. The name can be a maximum of 40 alphanumeric characters.
Step 2	`Router(config-pmap)# class class-map-name`	Specifies the class to which the policy map applies. **Note** On a given interface, the router uses the class-default class to assign QoS policies to any packets that do not belong to the classes defined in a policy map. *class-map-name* is the name of the class map. The name can be a maximum of 40 alphanumeric characters.

Configuration Examples for Creating a Policy Map

Example 4 shows how to create two policy maps named bronze and gold. The bronze policy includes a class map named class1, which is configured with a bandwidth of 100 kbps. The gold policy includes two class maps named voice and vlan. The voice class is the priority class and is policed at 50 kbps. The vlan class has a bandwidth configuration of 20 percent of the link bandwidth.

Example 4 Assigning a Class to a Policy Map

```
Router(config)# policy-map bronze
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 100
Router(config-pmap-c)# exit
Router(config-pmap-c)# exit
Router(config)# policy-map gold
Router(config-pmap)# class voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 50
Router(config-pmap)# class vlan
Router(config-pmap-c)# bandwidth percent 20
```

Example 5 shows how to configure the class-default class in the policy map named mypolicy. In this example, class-default has a bandwidth configuration of 128 kbps:

Example 5 Assigning the Default Class to a Policy Map

```
Router(config)# policy-map mypolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 128
```

Note For more information about defining QoS actions in a policy map, see the "Input and Output Policy Actions" section on page 4.

Defining QoS Actions in a Policy Map

To define QoS actions in a policy map, see the appropriate chapter in this guide.

Attaching Service Policies

Before the router can apply QoS service policies to packets, it needs to know which service policy to apply. By attaching a service policy to the appropriate interface or virtual circuit, the router can then apply the classification rules and QoS actions of the policy to the packets arriving at or leaving the router.

You can apply QoS service policies to:

- Physical interfaces
- Multilink PPP (MLPPP) and Multilink Frame Relay (MFR) interfaces
- ATM unspecified bit rate (UBR) PVCs and point-to-point subinterfaces
- ATM shaped UBR PVCs and point-to-point subinterfaces
- ATM constant bit rate (CBR) and variable bit rate (VBR) PVCs and point-to-point subinterfaces
- Label-controlled ATM (LC-ATM) subinterfaces

- Frame Relay PVCs, point-to-point subinterfaces, and map classes
- Ethernet VLANs
- IP tunnel interfaces
- Virtual access interfaces

For more information, see Chapter 4, "Attaching Service Policies."

Verifying QoS Policy Configurations

To verify a policy map configuration, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router# show policy map policy-map-name`	Displays the configuration of all classes contained in the policy map you specify. *policy-map-name* is the name of the policy map whose configuration information you want to display. The name can be a maximum of 40 characters. If you do not specify a *policy-map-name*, the command displays the configuration of all policy maps configured on the router.
`Router# show policy-map policy-map-name class class-name`	Displays the configuration of the class you specify. The policy map you specify includes this class. *policy-map-name* is the name of the policy map that contains the class configuration you want to display. *class-name* is the name of the class whose configuration you want to display. If you do not specify *class-name*, the router displays class configuration for all classes in the policy map.
`Router# show policy-map interface`	Displays the configuration of all classes configured for all policy maps attached to all interfaces.
`Router# show policy-map interface interface-name [input | output]`	Displays the configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. *interface-name* is the name of the interface or subinterface whose policy configuration you want to display. **input** indicates to display the statistics for the attached inbound policy. **output** indicates to display the statistics for the attached outbound policy. **Note** If you do not specify **input** or **output**, the router displays information about all classes that are configured for all inbound and outbound policies on all interfaces.

Command	Purpose
`Router# show policy-map interface [type number] [input | output]`	Displays the configuration of all classes configured for all inbound or outbound service policies on all interfaces. *type* is the interface type such as ATM. *number* is the port number on the selected interface. **Note** If you do not specify **input** or **output**, the router displays information about all classes that are configured for both inbound and outbound policies on all interfaces.
`Router# show policy-map interface [type number] {input | output} class class-name`	Displays the configuration of the class you specify for the inbound or outbound policy map you specify for all interfaces. *type* is the interface type such as ATM. *number* is the port number on the selected interface. *class-name* is the name of the class configuration you want to display.
`Router# show queue interface-type interface-number`	Displays queuing configuration information and statistics for the specified interface.

Verification Example for Service Policies

Example 6 shows the information displayed when you enter the **show policy-map interface** command. In the example output, random early detection (RED) drop statistics display for each IP precedence.

Example 6 show policy-map interface Command

```
Router# show policy-map interface atm 7/0/0.1
ATM7/0/0.1

Service-policy output: wred_1 (21036)

Class-map: prec_0_0 (match-all) (21037/2)
1445 packets, 1502800 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 100 (21038)
Output queue: 0/64; 1445/1502800 packets/bytes output, 0 drops
Bandwidth: 75 kbps (Weight 50)
Random-detect (precedence-based):
Exponential weight: 3 (1/8)
Current average queue length: 0 packets
----------------------------------------
    Min Max ProbRand-DropsTail-Drops
0   16  32  1/1 0   0
1   18  32  1/100   0
2   20  32  1/100   0
3   22  32  1/100   0
4   24  32  1/100   0
5   26  32  1/100   0
6   28  32  1/100   0
7   30  32  1/100   0
Class-map: prec_0_1 (match-all) (21041/3)
1417 packets, 1473680 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 101 (21042)
Output queue: 0/64; 1417/1473680 packets/bytes output, 0 drops
```

```
Bandwidth: 73 kbps (Weight 49)
Random-detect (precedence-based):
Exponential weight: 3 (1/8)
Current average queue length: 0 packets
----------------------------------------
    Min Max ProbRand-DropsTail-Drops
0   16  32  1/1 0   0
1   18  32  1/100   0
2   20  32  1/100   0
3   22  32  1/100   0
4   24  32  1/100   0
5   26  32  1/100   0
6   28  32  1/100   0
7   30  32  1/100   0
Class-map: class-default (match-any) (21045/0)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any (21046)
0 packets, 0 bytes
5 minute rate 0 bps
Output queue: 0/32; 0/0 packets/bytes output, 0 drops
```

Related Documentation

This section provides hyperlinks to additional Cisco documentation for the features discussed in this chapter. To display the documentation, click the document title or a section of the document highlighted in blue. When appropriate, paths to applicable sections are listed below the documentation title.

Feature	Related Documentation
Class maps	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 8: Modular Quality of Service Command-Line Interface > Configuring the Modular Quality of Service Command-Line Interface > Modular QoS CLI Configuration Task List > Creating a Traffic Class *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.2 access-list rate-limit -- fair-queue (WFQ) > class-map command
Constant Bit Rate (CBR) ATM service class	ATM Traffic Management, Understanding the CBR Service Category for ATM VCs ATM Traffic Management, Understanding Router Support for ATM Real-Time Service Categories

Feature	Related Documentation
Policy maps	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 8: Modular Quality of Service Command-Line Interface > Configuring the Modular Quality of Service Command-Line Interface > Modular QoS CLI Configuration Task List > Creating a Traffic Policy *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.2 policy map - qos preclassify > policy-map command
Policy map scaling	Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.0(25)SX New Features in Cisco IOS Release 12.0(25)SX > Policy Map Scaling
QoS service policies	*QoS Configuration and Monitoring, Creating Time-of-Day QoS Service Policies* tech note *QoS Configuration and Monitoring, Monitoring Voice over IP Quality of Service* tech note *Site-to-Site MPLS VPN Solution for Service Providers, Service Provider Quality-of-Service Overview* tech note

Feature	Related Documentation
Unspecified bit rate (UBR) ATM service class	ATM Traffic Management, Understanding the UBR Service Category for ATM Virtual Circuits ATM Traffic Management, Understanding Router Support for ATM Real-Time Service Categories Cisco 10000 Series Router Line Card Configuration Guide ATM Line Cards > 1-Port OC-12 ATM Line Card Configuration > Commands > Interface and Subinterface Commands > Creating a PVC ATM Line Cards > 4-Port OC-3/STM-1 ATM Line Card Configuration > ATM Commands > Interface and Subinterface Commands > Creating a PVC Cisco BPX 8600 Series Installation and Configuration, Release 9.3.00 Configuring ATM Connections > ATM Connection Flow > Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR Configuring ATM Connections > ATM Connection Configuration > Unspecified Bit Rate Connections
Variable bit rate (VBR) ATM service class	ATM Traffic Management, Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs ATM Traffic Management, Understanding Router Support for ATM Real-Time Service Categories Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs tech note Cisco 10000 Series Router Line Card Configuration Guide ATM Line Cards > 4-Port OC-3/STM-1 ATM Line Card Configuration > ATM Commands > ATM PVC Commands > Configuring VBR-nrt Cisco BPX 8600 Series Installation and Configuration, Release 9.3.00 Configuring ATM Connections > ATM Connection Flow > Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR Configuring ATM Connections > ATM Connection Configuration > Variable Bit Rate Connections